پژوهشکده نوآوری حقوقی

فصلنامه نوآوری حقوقی

بهار ۱۴۰۵ | دوره ۲ | شماره ۳

فهرست مقالات

➢ **بزه‌انگاری تهدیدات نوظهور ناشی از هوش مصنوعی: تحلیل چالش‌ها و راهکارهای تقنینی**

سعید قماشی، محمدرضا کاملی، مجتبی نیکوکلام ندیم ۱

➢ **قتل نامرئی؛ امکان‌سنجی انتساب قتل در مرگ‌های ناشی از فشار روانی، تحقیر مستمر و سوق دادن قربانی به خودکشی**

زینب باقری‌نژاد، میلاد چکاو، مرجان محرم ۵۵

➢ **تحلیل تطبیقی حق حفظ حریم خصوصی کودکان در عصر هوش مصنوعی و فضای دیجیتال در نظام‌های حقوقی ایران و کانادا**

منصوره حسینی، مجتبی فرهمند ۸۳

➢ **هوش مصنوعی و فرایندهای عدالت کیفری: جلوه‌ها و کاربردها**

مجید قورچی بیگی، غلامعلی اندیشور ۱۰۷

➢ **سیاست جنایی ایران در قبال خشونت دیجیتالی علیه سلامت روانی زنان با نگاهی بر رویکرد سازمان بهداشت جهانی**

جمال بیگی، زهرا اقبالی ۱۳۵

➢ **بررسی فقهی پیشگیری از جرم و مجازات با تأکید بر بند ۵ اصل ۱۵۶ قانون اساسی جمهوری اسلامی ایران**

طهورا نوروزی، سید محمد مهدی احمدی، علیرضا عسگری ۱۶۱

Journal Website

Legal Innovation Quarterly

Spring 2026

Volume 2, Issue 3

E-ISSN: 3115-8498

Criminalization of Emerging Threats Arising from Artificial Intelligence: An Analysis of the Challenges and Legislative Solutions

Saeed Ghomashi[1], Mohammad Reza Kameli*[2], Mojtaba Nikokalam Nadim[3]

1. Associate Professor, Department of Criminal Law and Criminology, Faculty of Law and Humanities, Kashan University, Kashan, Iran.
2. M.A. in Criminal Law and Criminology, Faculty of Law and Humanities, Kashan University, Kashan, Iran (Corresponding Author)*
3. M.A. in Criminal Law and Criminology, Faculty of Law and Humanities, Kashan University, Kashan, Iran.

***Corresponding author email address:** mrkameli1524@gmail.com

Extended Abstract

1. Introduction

The expansion of artificial intelligence has given rise to emerging threats and challenged fundamental concepts of criminal law, including mens rea (guilty mind), criminal intent, and the attribution of liability, because intelligent systems, in addition to facilitating the commission of offenses by humans, sometimes become sources of harmful conduct by virtue of their autonomous operation.

Deepfakes and intelligent phishing in the field of threats against persons threaten reputation and privacy, respectively, and facilitate access to information through behavioral data analysis. Errors in self-driving vehicles may lead to murder or bodily harm, and autonomous weapons increase the risk of violations of international humanitarian law. Artificial intelligence-based cyberattacks threaten critical infrastructure and national security; ransomware and the illicit mining of cryptocurrencies through botnets also damage property and trust in the digital economy.

Received: October 15, 2025 - **Accepted:** March 11, 2026 - **Published:** March 21, 2026

Ghomashi, Saeid; Kameli, Mohammadreza; & Nikookalam Nadim, Mojtaba. (2026). "Criminalization of Emerging Threats Arising from Artificial Intelligence: An Analysis of Challenges and Legislative Solutions." *Legal Innovation Quarterly*, 2(3), pp 1–53.
Doi: https://doi.org/10.22034/lir.2026.2074805.1026

© 2026 The Authors. Published by Legal Innovation Research Institute, Tehran, Iran. This is an open access article distributed under the terms of the Creative Commons Attribution 4.0 International (CC BY 4.0) License.

Domestic studies, unlike some international research, have focused more on prevention; these include studies on the preventive capacity of artificial intelligence and Martha Stroppa's (2023) study on maintaining human control over autonomous cyber capabilities. The principal question is the adequacy of Iranian criminal law in addressing these threats. The hypothesis is that the laws are fragmented and inadequate, and the objective is to analyze the gaps and propose solutions in four areas: threats against persons, autonomous technologies, cybersecurity, and property.

2. Research Methodology

The research methodology is based on a theoretical-analytical approach and relies on documentary research and content analysis of domestic laws, international instruments, scholarly articles, specialized reports, and comparative studies. The findings are used to identify gaps and propose legislative solutions.

3. Research Findings

The findings of this study indicate that the existing criminal law provisions in Iran are fragmented and inadequate to address emerging threats arising from artificial intelligence. In the field of threats against persons, existing provisions, such as Articles 6 and 16 of the Computer Crimes Law, may be applicable to some instances of deepfakes and phishing, but these provisions do not provide for a distinct offense or a specific framework for such conduct.

In the field of autonomous systems and autonomous weapons, the Iranian criminal law system lacks a clear mechanism for determining criminal liability in cases where decision-making is independently performed by an algorithm. Artificial intelligence-based cyberattacks against critical infrastructure, despite their increasing speed and complexity, lack a distinct offense of “cyberattack” or a definition of “artificial intelligence-enhanced cybercrime.” In the field of property, automated ransomware and the illicit mining of cryptocurrencies through botnets call into question the adequacy of traditional classifications of financial crimes. Overall, the findings confirm the research hypothesis and demonstrate the need to reconsider the legal elements, criminal intent, and rules governing the attribution of liability.

4. Recommendations

To address legislative gaps, the article proposes draft statutory provisions for the criminalization of emerging technological conduct and the determination of criminal liability in autonomous systems:

1. Criminalization of Deepfakes in the Iranian Criminal Law System

Altering digital content to create a false and deceptive representation, with the intent to harm the personality, reputation, or pecuniary or non-pecuniary rights

of natural or legal persons, shall constitute an offense. Where serious harm is caused, the maximum punishment shall apply; use for educational, research, artistic, or journalistic purposes, in the absence of any intent to deceive or cause harm, shall be excluded.

2. Criminalization of Phishing Attacks in Iranian Criminal Law

The use of fraudulent webpages, misleading emails, or text messages with the intent to commit fraud or unlawfully obtain information shall constitute an offense. The proposed punishments include taʿzir imprisonment of the sixth degree, confiscation of proceeds derived from the offense, and deprivation of the right to use computer and Internet services for a period of two to five years. Where serious harm occurs, the most severe punishment prescribed shall apply, and an unsuccessful attempt accompanied by criminal intent shall be deemed an attempt to commit an offense.

3. Criminalization of the Use of Artificial Intelligence-Based Autonomous Weapons

The use of autonomous weapons that violate international humanitarian law or the rules governing armed conflicts shall be prohibited and shall constitute an offense; participation in the production, design, distribution, sale, import, export, possession, or use of such weapons shall be subject to taʿzir imprisonment of the fifth degree, and in cases of murder or bodily harm, the corresponding punishments shall also apply. Where preventive measures are established and the offense occurs as a result of an unforeseeable defect, criminal liability shall be attributed to the system under the proposed provision. Government oversight, approval of high-risk modification, and the establishment of a compensation fund or insurance for compensation of losses is also proposed.

4. Criminalization of Conduct Arising from Artificial Intelligence in Self-Driving Vehicles

Where an error in the system is not attributable to any prior programming or planning by engineers or users and results in murder or bodily harm, the draft provides for the attribution of liability to the system and compensation for the damage caused; where it is not possible to directly enforce a punishment, liability shall, on a combined basis, rest with the owner, operator, or entity responsible for the system. Where there is a defect in design or manufacture, the manufacturing company or the owner shall be liable, and a special insurance fund is proposed.

5. Criminalization of Artificial Intelligence-Based Cyberattacks

Intelligent cyberattacks involving manipulation, destruction, unauthorized access to, or disruption of systems, critical infrastructure, or personal data shall

be punishable by imprisonment and a pecuniary penalty of the fifth degree; serious harm to persons, national security, or the economy shall result in the maximum punishment. In an automated offense, the designer, programmer, owner, or operator shall be responsible, unless it is established that the commission of the offense resulted from factors beyond their control and foreseeability; lawful use is excluded.

6. Criminalization of Artificial Intelligence-Based Ransomware

The design, development, dissemination, distribution, or control of ransomware with the assistance of artificial intelligence, or the use of ransomware to threaten and extort natural or legal persons, shall constitute an offense. Serious damage to critical systems, national infrastructure, or public security shall result in the most severe punishment.

7. Criminalization of Cryptocurrency Mining Using Botnets and Artificial Intelligence

Cryptocurrency mining using artificial intelligence or botnets, without legal authorization from the competent authorities, shall be criminalized as unauthorized cryptocurrency mining.

At the legislative level, conduct that can be subsumed under existing offenses may be addressed through the amendment or addition of statutory provisions, including Articles 6 and 16 of the Computer Crimes Law concerning deepfakes; however, with regard to autonomous weapons and self-driving vehicles, an independent and comprehensive law is necessary because of the uncertainty surrounding the attribution of liability. The drafts should be completed through expert review and in accordance with international standards.

5. Conclusion

The existing criminal law frameworks in Iran lack the necessary coherence and adequacy to address emerging crimes based on artificial intelligence, particularly with regard to automated conduct and the attribution of liability. Traditional frameworks based on human reason, will, and intent have demonstrated their inadequacy in addressing autonomous technologies, and gaps are evident in defining offenses, identifying offenders, and establishing the mens rea (guilty mind).

The main innovation of this study lies in presenting a roadmap for four key areas, namely offenses against persons, security, property, and autonomous technologies: the independent criminalization of deepfakes and intelligent phishing, the definition of artificial intelligence-enhanced cybercrime, the establishment of specific regulations for ransomware and the illicit mining of cryptocurrencies, and the design of a combined liability regime for human actors and intelligent systems. The possibility of recognizing a special form of

legal personality for artificial intelligence, based on financial autonomy, capacity to litigate, and layered liability, is also raised.
Effective counteraction requires clear legal definitions, criteria for establishing mens rea (guilty mind) in automated decisions, accuracy and safety standards, specialized evidentiary procedures, oversight, and international cooperation. An interdisciplinary approach should safeguard individual and collective rights while preserving the responsible development of artificial intelligence.

Keywords: Artificial intelligence ; criminalization ; deepfakes ; intelligent phishing ; legislative gaps in Iranian criminal law.

Funding
This article has no financial support or funding.

Authors' Contributions
Saeid Ghomashi: Conceptualization, data curation, validation, project administration, and resources.
Mohammadreza Kameli & Mojtaba Nikookalam Nadim: Methodology, formal analysis, writing – review & editing, investigation, writing – original draft.

Conflict of Interest
According to the authors' declaration, there is no conflict of interest regarding this article.

Ethical Considerations
This study was conducted based on the analysis of legal documents, statutes, judicial decisions, and library-based sources. It did not involve human participants, animals, or personal data; therefore, ethical approval from an institutional ethics committee was not required. Nevertheless, the authors adhered to the principles of academic integrity, research honesty, proper citation practices, and respect for intellectual property rights throughout all stages of the research.Generative artificial intelligence (AI) tools were used solely to assist with language editing, improving the structure of the manuscript, and enhancing the readability of the text. These tools did not contribute to the study design, scientific analysis, interpretation of findings, drawing of conclusions, or any research-related decision-making. The author(s) assume full responsibility for the accuracy, originality, and final content of the manuscript.

Authors' Approval
All authors have read and approved the final version of the manuscript and consent to its publication.

بهار ۱۴۰۵
دوره ۲، شماره ۳
شاپای الکترونیکی:
۳۱۱۵-۸۴۹۸

فصلنامه نوآوری حقوقی

وبسایت مجله

بزه‌انگاری تهدیدات نوظهور ناشی از هوش مصنوعی: تحلیل چالش‌ها و راهکارهای تقنینی

سعید قماشی[۱]، محمدرضا کاملی[*۲]، مجتبی نیکوکلام ندیم[۳]

۱. دانشیار گروه حقوق کیفری و جرم‌شناسی، دانشکدهٔ حقوق و علوم انسانی، دانشگاه کاشان، کاشان، ایران.
۲. کارشناس ارشد حقوق کیفری و جرم‌شناسی، دانشکدهٔ حقوق و علوم انسانی، دانشگاه کاشان، کاشان، ایران (نویسندهٔ مسئول)
۳. کارشناسی ارشد حقوق کیفری و جرم‌شناسی، دانشکدهٔ حقوق و علوم انسانی، دانشگاه کاشان، کاشان، ایران

[*] **ایمیل نویسندهٔ مسئول:** mrkameli1524@gmail.com

چکیده

گسترش سریع فناوری‌های مبتنی بر هوش مصنوعی، چالش‌های تازه‌ای را در حوزه‌های اجتماعی، امنیتی و اقتصادی پدید آورده است. این تحولات، پرسش‌هایی را دربارهٔ میزان کارآمدی چارچوب‌های موجود حقوق کیفری ایران در مواجهه با این پدیده‌ها مطرح می‌کند. مسئلهٔ اصلی این پژوهش، بررسی چالش‌های بزه‌انگاری تهدیدات ناشی از هوش مصنوعی و تحلیل خلأهای تقنینی موجود در نظام حقوقی ایران است. این مطالعه با رویکردی نظری ـ تحلیلی و بر پایهٔ منابع معتبر داخلی و بین‌المللی، به واکاوی تهدیدات علیه اشخاص (مانند جعل عمیق و فیشینگ)، تهدیدات ناشی از فناوری‌های خودران و خودمختار (مانند خودروهای خودران و سلاح‌های خودمختار مرگبار)، تهدیدات علیه امنیت (حملات سایبری به زیرساخت‌های حیاتی) و تهدیدات علیه اموال (باج‌افزار و استخراج غیرقانونی ارزهای دیجیتال) می‌پردازد. یافته‌ها نشان می‌دهد قوانین موجود در زمینهٔ جرم‌انگاری رفتارهای فناورانهٔ ناشی از هوش مصنوعی، پراکنده و ناکافی بوده و توان پاسخ‌گویی به پیچیدگی‌های تهدیدات نوظهور را ندارند. نوآوری پژوهش در تحلیل و ارائهٔ راهکارهای تقنینی برای مواجهه با تهدیدات مذکور است. نتیجه‌گیری مقاله، بازنگری و توسعهٔ مقررات کیفری ایران با تأکید بر بزه‌انگاری‌های نو است تا ضمن تضمین عدالت کیفری و صیانت از امنیت ملی، امکان مدیریت تهدیدات نوظهور ناشی از هوش مصنوعی فراهم شود.

واژگان کلیدی: هوش مصنوعی، بزه‌انگاری، جعل عمیق، فیشینگ هوشمند، خلأهای تقنینی در حقوق کیفری ایران.

دریافت‌شده در تاریخ: ۲۳ مهر ۱۴۰۴ - **پذیرش‌شده در تاریخ:** ۲۰ اسفند ۱۴۰۴- **منتشرشده در تاریخ:** ۱ فروردین ۱۴۰۵

قماشی، سعید؛ کاملی، محمدرضا؛ نیکولام ندیم، مجتبی. (۱۴۰۵). «بزه‌انگاری تهدیدات نوظهور ناشی از هوش مصنوعی: تحلیل چالش‌ها و راهکارهای تقنینی». فصلنامه نوآوری حقوقی، دوره ۲، شماره ۳، صص۱-۵۳.

Doi: https://doi.org/10.22034/lir.2026.2074805.1026

© 2026 The Authors. Published by Legal Innovation Research Institute, Tehran, Iran. This is an open access article distributed under the terms of the Creative Commons Attribution 4.0 International (CC BY 4.0) License.

مقدمه

تحولات فناورانه در دهه‌های اخیر، به‌ویژه در حوزهٔ هوش مصنوعی، موجب شکل‌گیری گونه‌های نوینی از تهدیدات شده است که نظام‌های سنتی حقوق کیفری را با چالش‌های بنیادین مواجه ساخته‌اند. هوش مصنوعی به‌عنوان ابزاری پیچیده و خودکار، نه‌تنها در ارتکاب جرائم توسط انسان‌ها نقش‌آفرینی می‌کند، بلکه در مواردی به‌واسطهٔ عملکرد مستقل خود، منشأ رفتارهای مجرمانه نیز تلقی می‌شود. این وضعیت، مفاهیم کلیدی حقوق کیفری نظیر «عنصر معنوی»، «قصد مجرمانه» و «انتساب مسئولیت» را در معرض چالش قرار داده و ضرورت بازنگری و بازتعریف مبانی بزه‌انگاری را ایجاب می‌کند.

در حوزهٔ تهدید تمامیت اشخاص، فناوری‌هایی همچون جعل عمیق (دیپ‌فیک) و حملات فیشینگ هوشمند با بهره‌گیری از الگوریتم‌های یادگیری ماشین، مصادیق بارز تهدیدات علیه حیثیت، حریم خصوصی و اعتماد عمومی محسوب می‌شوند. دیپ‌فیک می‌تواند با تولید تصاویر و ویدئوهای جعلی واقع‌گرایانه، شخصیت معنوی افراد را مخدوش کند و زمینه‌ساز افترا، هتک حیثیت و حتی اخاذی شود. فیشینگ هوشمند نیز با استفاده از پردازش زبان طبیعی و داده‌کاوی رفتاری، پیام‌های فریبنده‌ای تولید می‌کند که قربانیان را به افشای اطلاعات شخصی یا مالی سوق می‌دهد و بدین ترتیب اعتماد عمومی به محیط‌های دیجیتال را تضعیف می‌کند.

در حوزهٔ فناوری‌های خودران و خودمختار، خودروهای خودران و سلاح‌های خودمختار مرگبار نمونه‌هایی از تهدیدات نوین هستند که می‌توانند خطاهای جنایی یا خسارات گسترده‌ای ایجاد کنند. خودروهای خودران در صورت نقص فنی یا تصمیم‌گیری الگوریتمی نادرست، ممکن است به حوادث مرگبار منجر شوند که مسئولیت کیفری آن‌ها هنوز با ابهام مواجه است. سلاح‌های خودمختار نیز با قابلیت تصمیم‌گیری مستقل در میدان نبرد، خطر نقض قواعد حقوق بشردوستانه و ارتکاب جرائم جنگی را به همراه دارند و جرم‌انگاری آن‌ها نیازمند بازنگری جدی در مقررات بین‌المللی و داخلی است.

در حوزهٔ امنیت، حملات سایبری به زیرساخت‌های حیاتی کشورها ازجمله شبکه‌های انرژی، حمل‌ونقل، ارتباطات و خدمات مالی، تهدیدی جدی برای امنیت ملی و نظم عمومی محسوب می‌شوند. این حملات می‌توانند موجب فلج شدن سیستم‌های حیاتی، ایجاد بحران‌های اجتماعی و اقتصادی، و تضعیف اعتماد عمومی به نهادهای دولتی شوند. در چنین شرایطی، جرم‌انگاری دقیق

و صریح این رفتارها و تدوین مقررات بازدارنده برای مقابله با حملات سایبری مبتنی بر هوش مصنوعی، ضرورتی انکارناپذیر است.

در حوزهٔ اموال نیز جرائم اقتصادی نوین همچون باج‌افزار و استخراج غیرقانونی ارزهای دیجیتال از طریق بات‌نت‌ها، چالش‌های جدی برای نظام کیفری سنتی ایجاد کرده‌اند. باج‌افزار با رمزگذاری داده‌های کاربران و مطالبهٔ وجه در قبال آزادسازی آن‌ها، مصداق بارز اخاذی دیجیتال است. استخراج غیرقانونی ارزهای دیجیتال نیز با سوءاستفاده از منابع پردازشی قربانیان، موجب تحصیل منفعت نامشروع و آسیب به دارایی‌های دیجیتال می‌شود. این جرائم نه‌تنها خسارات مالی گسترده‌ای به افراد و سازمان‌ها وارد می‌کنند، بلکه اعتماد به نظام اقتصادی دیجیتال را نیز تضعیف می‌سازند.

با وجود گسترش پژوهش‌های بین‌المللی در زمینهٔ جرائم سایبری و تهدیدات فناورانه، مطالعات داخلی در ایران محدود بوده و بیشتر بر پیشگیری متمرکز شده‌اند تا بزه‌انگاری. برای نمونه، در مقالهٔ «هوش مصنوعی به‌عنوان پیش‌بینی‌کنندهٔ جرائم سایبری: فرصت‌ها و چالش‌ها» اثر فاطمه فلاح تفتی (۱۴۰۳)، ظرفیت‌های الگوریتم‌های یادگیری ماشین در پیش‌بینی و پیشگیری از جرائم سایبری بررسی شده و در کنار آن به چالش‌های حریم خصوصی و تعصب الگوریتمی اشاره گردیده است. همچنین در پژوهش «هوش مصنوعی در خدمت پیشگیری از جرائم سایبری: رویکردی فقهی ـ حقوقی» اثر فاطمه فلاح تفتی (۱۴۰۳)، تلاش شده است تا با تکیه بر مبانی فقه امامیه و اصول حقوقی، چارچوبی برای استفادهٔ مشروع و اخلاقی از هوش مصنوعی در پیشگیری از جرائم ارائه شود. در سطح بین‌المللی نیز در مقاله‌ای با عنوان پیامدهای قانونی و اخلاقی قابلیت‌های سایبری خودمختار: فراخوانی برای حفظ کنترل انسانی در فضای مجازی که توسط مارتا استروپا در سال ۲۰۲۳ منتشر شده است (Marta Stroppa, 2023)، بر ضرورت حفظ کنترل انسانی در عملیات سایبری تأکید کرده و چالش‌های حقوقی و اخلاقی ناشی از توانمندی‌های خودکار هوش مصنوعی در فضای مجازی را واکاوی نموده است. این پژوهش درپی آن است که با تمرکز بر جرم‌انگاری تهدیدات نوظهور ناشی از هوش مصنوعی، به پرسش اصلی پاسخ دهد که آیا نظام حقوق کیفری ایران ظرفیت لازم برای مواجهه با این تهدیدات را دارد یا نیازمند اصلاح و توسعهٔ مقررات است. فرضیهٔ پژوهش بر آن است که قوانین موجود پراکنده و ناکافی بوده و توان پاسخ‌گویی به پیچیدگی‌های جرائم فناورانه را ندارند.

اهداف اصلی مقاله عبارت‌اند از: تحلیل چالش‌های حقوقی ناشی از تهدیدات نوظهور هوش مصنوعی، بررسی خلأهای قانونی در نظام کیفری ایران، و ارائهٔ راهکارهای تقنینی برای جرم‌انگاری رفتارهای فناورانه. نوآوری پژوهش در ارائهٔ پیش‌نویس‌های قانونی برای جرم‌انگاری دیپ‌فیک و فیشینگ، تقویت مقررات مقابله با حملات سایبری مبتنی بر هوش مصنوعی، پیشنهاد رژیم تقنینی ترکیبی درخصوص فناوری‌های خودران و خودمختار، و همچنین تبیین چارچوب‌های حقوقی برای مقابله با جرائم اقتصادی نوین ازجمله باج‌افزار و استخراج غیرقانونی ارزهای دیجیتال از طریق بات‌نت‌ها نهفته است.

ساختار مقاله در چهار بخش سامان یافته است: نخست، تهدیدات علیه اشخاص ازجمله جعل عمیق و حملات فیشینگ هوشمند بررسی می‌شود؛ سپس تهدیدات ناشی از فناوری‌های خودران و خودمختار مانند خطاهای جنایی خودروهای خودران و به‌کارگیری سلاح‌های خودمختار مرگبار تحلیل می‌شود؛ در ادامه تهدیدات علیه امنیت ازجمله حملات سایبری به زیرساخت‌های حیاتی مورد مطالعه قرار می‌گیرد و درنهایت تهدیدات علیه حقوق مالی همچون باج‌افزار و استخراج غیرقانونی ارزهای دیجیتال از طریق بات‌نت‌ها تبیین می‌شود.

این تقسیم‌بندی به‌گونه‌ای طراحی شده است که هم با نمونه‌های واقعی تهدیدات نوظهور منطبق باشد و هم امکان تحلیل حقوقی و تقنینی آن‌ها را در چارچوبی منسجم فراهم سازد. بدین ترتیب، مقالهٔ حاضر می‌کوشد سهمی در ارتقای ادبیات حقوق کیفری ایران ایفا کند و زمینه‌ای برای اصلاح و توسعهٔ مقررات کیفری در مواجهه با تهدیدات نوظهور ناشی از هوش مصنوعی فراهم آورد.

۱. تهدیدات علیه اشخاص

هوش مصنوعی با توانایی‌های گسترده در پردازش داده‌ها، یادگیری الگوها و تولید محتوا، عرصه‌ای نوین از تهدیدات علیه اشخاص را پدید آورده است. این تهدیدات بیش از هر حوزه‌ای، مستقیماً بر حقوق بنیادین افراد ازجمله حیثیت، حریم خصوصی، آزادی‌های فردی و اعتماد اجتماعی اثرگذارند. درواقع، فناوری‌های مبتنی بر هوش مصنوعی می‌توانند با تولید محتوای جعلی، دستکاری اطلاعات شخصی یا بهره‌برداری از داده‌های رفتاری، زمینهٔ ارتکاب جرائمی را فراهم کنند که در نظام‌های حقوقی سنتی پیش‌بینی نشده‌اند.

از منظر حقوق کیفری، این تهدیدات پرسش‌های جدی دربارهٔ حدود حمایت قانونی از شخصیت و کرامت انسانی مطرح می‌سازند. آیا تولید و انتشار تصاویر و ویدئوهای جعلی واقع‌گرایانه (دیپ‌فیک) صرفاً نقض اخلاقی است یا باید به‌عنوان جرم مستقل مورد شناسایی قرار گیرد؟ آیا حملات فیشینگ هوشمند که با تقلید از سبک گفتاری و رفتاری قربانیان طراحی می‌شوند، مصداقی از کلاهبرداری رایانه‌ای محسوب می‌شوند یا نیازمند جرم‌انگاری خاص هستند؟ این پرسش‌ها نشان می‌دهند که تهدیدات علیه اشخاص، نقطهٔ آغازین و حساس در بحث بزه‌انگاری تهدیدات نوظهور ناشی از هوش مصنوعی به‌شمار می‌روند. بنابراین، در این بخش ابتدا به جعل عمیق (دیپ‌فیک) به‌عنوان تهدیدی علیه حیثیت و اعتبار اشخاص پرداخته می‌شود، سپس حملات فیشینگ هوشمند به‌عنوان تهدیدی علیه اعتماد عمومی و امنیت داده‌های شخصی بررسی خواهد شد.

۱ـ۱. ماهیت و پیامدهای کیفری جعل عمیق (دیپ‌فیک) مبتنی بر هوش مصنوعی

جعل عمیق ترکیبی از دو مفهوم «جعل» و «یادگیری عمیق» است. این فناوری نوین با بهره‌گیری از شبکه‌های عصبی و تحلیل حجم گسترده‌ای از داده‌ها، توانایی بازسازی و تقلید حالات چهره و حرکات افراد را دارد. در این فرایند، تصاویر یا فیلم‌های مربوط به دو شخص در الگوریتمی ویژه قرار داده می‌شود تا چهرهٔ یکی جایگزین دیگری شود. به بیان ساده‌تر، جعل عمیق با استفاده از فناوری نگاشت صورت و هوش مصنوعی، امکان تغییر چهرهٔ فردی در یک فیلم و جایگزینی آن با چهرهٔ فرد دیگر را فراهم می‌کند. دشواری تشخیص این نوع محتوا ناشی از آن است که بر پایهٔ فیلم‌های واقعی ساخته می‌شود؛ بنابراین صدا و تصویر آن طبیعی جلوه کرده و قابلیت انتشار سریع در شبکه‌های اجتماعی را دارد. همین امر سبب می‌شود بسیاری از مخاطبان، ویدئوی تولیدشده را واقعی تصور کنند (احسان‌پور و امی، ۱۴۰۱: ۳).

جعل عمیق یا دیپ‌فیک روشی است که از هوش مصنوعی برای ایجاد ویدیوهای جعلی واقع‌گرایانه با ترکیب تصاویر و ویدیوهای موجود با فیلم منبع بهره می‌گیرد. این فرایند، موسوم به جعل عمیق، با استفاده از شبکه‌های مولد متخاصم[1] در یادگیری ماشینی، تصاویر و ویدیوها را بر

۱. شبکه‌های مولد متخاصم نوعی الگوریتم هوش مصنوعی هستند که از دو بخش تشکیل می‌شوند: یکی «تولیدکننده» که تلاش می‌کند تصاویر یا ویدیوهای جعلی بسازد، و دیگری «تشخیص‌دهنده» که سعی دارد واقعی یا جعلی بودن آن‌ها را تشخیص دهد. این دو بخش با هم رقابت می‌کنند تا درنهایت، محتوای تولیدشده آن‌قدر واقعی به‌نظر برسد که تشخیص جعلی بودنش بسیار سخت شود.

روی یکدیگر هم‌پوشانی می‌کند (Ben Aissa et al., 2023: 32343). نتیجهٔ نهایی ویدیویی است که به‌نظر می‌رسد افراد را درگیر فعالیت‌ها یا سناریوهایی نشان می‌دهد که هرگز رخ نداده‌اند. برای نمونه، فناوری دیپ‌فیک می‌تواند ویدیوهای ساختگی تولید کند و نشان دهد اشخاص در اعمال جنسی مشارکت داشته‌اند، در حالی‌که چنین چیزی واقعیت ندارد؛ یا سخنان و حرکات یک سیاستمدار را تغییر دهد تا به‌نظر برسد مطلبی را بیان کرده است که هرگز جزو نطق او نبوده است. با توجه به این قابلیت‌ها، از ویدیوهای دیپ‌فیک می‌توان برای ساخت هرزه‌نگاری غیرواقعی با حضور افراد مشهور، انتشار اخبار جعلی و انجام کلاهبرداری‌های مخرب استفاده کرد (Chesney & Citron, 2019: 1772).

دستکاری عکس پیشینه‌ای طولانی دارد و به قرن نوزدهم بازمی‌گردد؛ سپس به‌سرعت در تصاویر متحرک به‌کار گرفته شد. در قرن بیستم، پیشرفت‌های فناورانه به‌طور پیوسته روش‌های دستکاری عکس را بهبود بخشید و با ورود ویدیوهای دیجیتال سرعت بیشتری یافت. توسعهٔ فناوری دیپ‌فیک در دههٔ ۱۹۹۰ توسط پژوهشگران دانشگاهی آغاز شد و بعدها در میان افراد غیرحرفه‌ای در جوامع برخط رواج پیدا کرد. در سال‌های اخیر، این روش‌ها در صنعت نیز مقبولیت گسترده‌ای یافته‌اند. با این حال، امروزه این فناوری‌ها به‌طور نادرست برای تولید محتوای صریح، وادارسازی افراد و انتشار اطلاعات نادرست به‌کار گرفته می‌شوند و پیامدهای اجتماعی منفی و فرساینده‌ای به همراه دارند[1] (Khan & Rehman, 2024: 49). افزون بر این، دیپ‌فیک‌ها به‌طور گسترده به‌عنوان منبع مخرب اطلاعات نادرست در دادگاه‌ها مورد استفاده قرار می‌گیرند و می‌توانند تصمیم قضات را تحت تأثیر قرار دهند (Taeb & Chi, 2022: 89).[2]

۲-۱-۱. کارکردهای هوش مصنوعی در تولید و گسترش محتوای دیپ‌فیک

فناوری جعل عمیق (دیپ‌فیک) با بهره‌گیری از الگوریتم‌های هوش مصنوعی ـ به‌ویژه شبکه‌های مولد متخاصم ـ توانایی تولید و دستکاری محتوای صوتی و تصویری را به سطحی بی‌سابقه رسانده است. این فناوری نه‌تنها امکان بازآفرینی چهره‌ها و صداهای واقعی را فراهم می‌کند، بلکه قادر است تصاویر و ویدئوهای کاملاً جدید و باورپذیر از افراد غیرواقعی بسازد. در کنار این قابلیت‌ها

1. “These technologies are now being misapplied for the creation of explicit content, coercing individuals and disseminating false information, resulting in an erosion of and potentially negative societal consequences”.
2. “Deepfakes are being widely used as a malicious source of misinformation in court that seek to sway a court’s decision”.

پژوهشگران از همان ابزارهای هوش مصنوعی برای تشخیص و پیشگیری از جعل‌های عمیق نیز استفاده می‌کنند. بنابراین کارکردهای هوش مصنوعی در حوزهٔ دیپ‌فیک را می‌توان در سه محور اصلی بررسی کرد: سنتز چهره و صدا، مدل‌سازی عمیق و تشخیص و پیشگیری. این تقسیم‌بندی چارچوبی علمی برای تحلیل ابعاد مختلف فناوری جعل عمیق و پیامدهای کیفری آن فراهم می‌سازد.

ـ سنتز چهره و صدا: الگوریتم‌های هوش مصنوعی قادرند چهره‌ها و صداها را تولید یا دستکاری کنند و به این وسیله چنین وانمود سازند که فردی خاص در حال سخن گفتن یا انجام عملی است (Dehghani & Saberi, 2025: 1).

ـ مدل‌سازی عمیق: این فناوری امکان ایجاد تصاویر یا ویدیوهای جدید و واقعی از افرادی که وجود ندارند یا تغییراتی در تصاویر موجود ایجاد می‌کند.

ـ تشخیص و پیشگیری: جالب است هوش مصنوعی تنها برای تولید جعل عمیق به‌کار نمی‌رود، بلکه در شناسایی و جلوگیری از آن نیز نقش دارد. پژوهشگران در حال توسعهٔ روش‌های مبتنی بر هوش مصنوعی هستند تا ناسازگاری‌ها و نشانه‌های مصنوعی باقی‌مانده در جعل‌های عمیق را شناسایی کنند.

هوش مصنوعی در حوزهٔ فناوری جعل عمیق، به‌عنوان ابزاری بالقوه برای ارتکاب جرائم نوظهور شناخته می‌شود. این فناوری با بهره‌گیری از الگوریتم‌های یادگیری ماشین، به‌ویژه شبکه‌های مولد متخاصم، قادر است محتوای صوتی و تصویری جعلی تولید کند که از نمونه‌های واقعی به‌سختی قابل تشخیص است. به‌دلیل توانایی این ابزار در جعل هویت، انتشار اطلاعات نادرست، و تولید محتوای صریح و اغواگرانه، جعل عمیق به‌عنوان تهدیدی جدی در حوزه‌های امنیتی، اجتماعی و حقوقی مطرح شده است. کاربردهای آن در زمینه‌هایی مانند تروریسم سایبری، باج‌گیری دیجیتال، و فریب نهادهای قضایی، ضرورت تدوین مقررات قانونی و توسعهٔ سامانه‌های تشخیص را دوچندان کرده است.

۳-۱-۱. ابعاد کیفری و جرائم ناشی از بهره‌گیری از دیپ‌فیک مبتنی بر هوش مصنوعی

برای تحلیل ابعاد کیفری جعل عمیق، می‌توان مراحل اصلی ارتکاب این جرم را به دو بخش اساسی تقسیم کرد: ایجاد محتوای جعلی و انتشار یا پخش آن. این تقسیم‌بندی هم در ادبیات علمی

بین‌المللی مطرح شده و هم با منطق حقوق کیفری سازگار است، زیرا هر یک از این مراحل می‌تواند به‌طور مستقل واجد آثار مجرمانه باشد. در مرحلهٔ ایجاد، فناوری هوش مصنوعی برای تولید محتوای جعلی و تقلید صدا یا چهره‌ها به‌کار می‌رود. در مرحلهٔ انتشار یا پخش شدن، همین محتوای جعلی در پلتفرم‌های مختلف منتشر می‌شود و می‌تواند به جرائمی چون باج‌گیری، انتشار اخبار جعلی، افترا و نقض حریم خصوصی منجر شود.

ـ ایجاد: هوش مصنوعی برای تولید محتوای جعل عمیق، تقلید صداها یا چهره‌ها با دقت بالا استفاده می‌شود(Sandoval et al., 2024: 1) .

ـ انتشار یا پخش شدن: هوش مصنوعی می‌تواند به انتشار محتوای جعل عمیق در پلتفرم‌های مختلف کمک کند و به‌طور بالقوه به اطلاعات نادرست یا افترا منجر شود. درواقع جرائم مربوط به دیپ‌فیک می‌تواند شامل باج‌گیری، انتشار اخبار جعلی، افترا و نقض حریم خصوصی باشد[1](Sembiring & Firdaus, 2025: 1).

نظام حقوقی ایران تاکنون جرم مستقلی با عنوان «جعل عمیق» پیش‌بینی نکرده است؛ با این حال، اقداماتی همچون ایجاد یا انتشار دیپ‌فیک می‌تواند ذیل مقررات جرائم سایبری موجود قرار گیرد. برای نمونه، مادهٔ ۶ قانون جرائم رایانه‌ای، جعل رایانه‌ای را جرم‌انگاری کرده و برای آن مجازات حبس از یک تا پنج سال مقرر داشته است. همچنین، مادهٔ ۶۸ قانون تجارت الکترونیک موارد مشابه را در زمرهٔ جعل دانسته و حداکثر سه سال حبس تعزیری برای مرتکبان پیش‌بینی کرده است.

علاوه بر مقررات کلی، در نظام حقوقی ایران می‌توان مواد قانونی متعددی را مرتبط با جرائم ناشی از جعل عمیق شناسایی کرد. برای نمونه، تبصرهٔ ۴ مادهٔ ۱۴ قانون جرائم رایانه‌ای تولید، توزیع و انتشار آثار مستهجن غیرواقعی را جرم‌انگاری کرده است؛ امری که به‌طور مستقیم می‌تواند مصداق استفادهٔ مجرمانه از فناوری دیپ‌فیک باشد. همچنین، مادهٔ ۱۶ همان قانون هتک حیثیت افراد از طریق تغییر یا تحریف داده‌های رایانه‌ای را جرم دانسته و در صورتی که این تغییرات ماهیت مستهجن داشته و منتشر شوند، مرتکب به حداکثر مجازات قانونی محکوم خواهد شد. افزون بر این، مادهٔ ۱۳۱ قانون جرائم نیروهای مسلح به تغییرات غیرمجاز در داده‌ها یا تصاویر توسط نظامیان اشاره دارد و در صورت سوءاستفاده، آن را قابل تعقیب کیفری می‌داند.

1. “Crimes involving deepfakes can include blackmail, spreading fake news, defamation, and privacy violations”.

این مقررات نشان می‌دهد که اگرچه عنوان مستقل «جعل عمیق» در قوانین ایران پیش‌بینی نشده است، اما رفتارهای مرتبط با دیپ‌فیک را می‌توان تحت شمول مواد موجود قرار داد. با این حال، پراکندگی و عدم انسجام این مقررات، ضرورت تدوین قواعد اختصاصی و صریح برای مواجهه با چالش‌های پیچیده و نوظهور ناشی از فناوری جعل عمیق را آشکار می‌سازد.

نقش هوش مصنوعی در ایجاد جعل عمیق یک موضوع پیچیده است. هوش مصنوعی به خودی خود یک ابزار است و مانند هر ابزاری می‌توان از آن برای اهداف مفید و مضر استفاده کرد. در زمینهٔ جعل‌های عمیق، الگوریتم‌های هوش مصنوعی قادر به تولید محتوای صوتی یا تصویری جعلی بسیار واقعی و متقاعدکننده هستند. هوش مصنوعی در این زمینه صرفاً به‌عنوان ابزاری برای ارتکاب جرم عمل می‌کند؛ بنابراین مسئولیت کیفری بر عهدهٔ افرادی است که از این فناوری برای ایجاد و انتشار جعل‌های عمیق با هدف فریب، آسیب‌رسانی یا ارتکاب کلاهبرداری بهره‌برداری می‌کنند. جعل‌های عمیق به‌عنوان تهدیدی جدی شناخته شده‌اند که می‌توانند برای بی‌اعتبار کردن شخصیت‌های عمومی، دستکاری افکار عمومی یا حتی اخاذی مورد استفاده قرار گیرند. آسیب‌های اجتماعی ناشی از این فناوری فراتر از موارد فردی است و می‌تواند اعتماد عمومی به شواهد صوتی و تصویری را تضعیف کند (Romero Moreno, 2024: 297). قوانین در حوزه‌های قضائی مختلف برای مقابله با استفادهٔ مخرب از جعل‌های عمیق تدوین شده‌اند و تمرکز آن‌ها بر زمینه‌هایی چون هرزه‌نگاری، کلاهبرداری و افتراست. هوش مصنوعی به‌عنوان یک فناوری، خود مسئول ارتکاب جرم محسوب نمی‌شود؛ ازاین‌رو همکاری سیاست‌گذاران، مجریان قانون و توسعه‌دهندگان هوش مصنوعی برای کاهش خطرات ناشی از سوءاستفاده و پاسخ‌گو نگه‌داشتن عاملان ضروری است. به‌طور خلاصه، مسئولیت کیفری جعل عمیق متوجه نیت و اقدامات سوء افراد در بهره‌برداری از هوش مصنوعی است. تلاش‌ها برای تنظیم و مدیریت ظرفیت‌های این فناوری در مسیرهای زیان‌بار، ازجمله تولید جعل‌های عمیق، همچنان ادامه دارد.

۲-۱. ماهیت و پیامدهای کیفری حملات فیشینگ هوشمند مبتنی بر یادگیری ماشین

فیشینگ روشی فریبنده برای دسترسی به اطلاعات حساس مانند نام کاربری، گذرواژه، جزئیات حساب بانکی، نشانی اینترنتی (IP) و سایر داده‌هاست. این کار معمولاً از طریق جعل هویت پایگاه‌های اینترنتی معتبر یا نشانی‌های رایانامه انجام می‌گیرد. در اصل، فیشینگ شامل تلاش فردی

برای فریب دادن شخص دیگری به افشای اطلاعات شخصی است. این عمل غیرقانونی باعث ایجاد یک بازار زیرزمینی پرسود به ارزش میلیاردها دلار شده است. در اصل، فیشینگ یک شکل رایج از حملهٔ سایبری است که برای به‌دست آوردن غیرقانونی داده‌های کاربر، ازجمله اعتبار ورود و جزئیات کارت اعتباری استفاده می‌شود (Ramzan, 2010: 439). اصطلاح «فیشینگ» نخستین‌بار در سال ۱۳۷۴ در جعبه‌ابزار نفوذگر «ای او هل»[1] ثبت شد، اما ممکن است قبلاً در مجلهٔ هکر «۲۶۰۰»[2] استفاده شده باشد (Wright et al., 2016: 1115). اقدامات برای جلوگیری یا کاهش تأثیر حملات فیشینگ شامل قوانین، آموزش کاربر، آگاهی عمومی و اقدامات امنیتی فنی است. اهمیت آگاهی از فیشینگ در محیط‌های شخصی و حرفه‌ای افزایش یافته است، به‌طوری که حملات فیشینگ در بین مشاغل از ۷۲ درصد به ۸۶ درصد از سال ۲۰۱۷ تا ۲۰۲۰ افزایش یافته است ("Phishing attacks have increased …", 2020: 37).

در سطح اتحادیهٔ اروپا، پارلمان و شورای اروپا درخصوص حملات علیه سیستم‌های اطلاعاتی، کشورهای عضو را موظف ساخته است که دسترسی غیرمجاز به سامانه‌های اطلاعاتی با قصد تحصیل داده‌ها را به‌عنوان جرم مستقل در قوانین داخلی خود پیش‌بینی کنند. این دستورالعمل با تأکید بر ضرورت جرم‌انگاری رفتارهایی نظیر فیشینگ، بر این نکته تصریح دارد که هرگونه ورود به سیستم‌های اطلاعاتی از طریق نقض تدابیر امنیتی و با هدف دستیابی به اطلاعات، باید مشمول ضمانت اجراهای کیفری شود[3] (European Union, 2013, Art. 3).

۱-۲-۱. نقش هوش مصنوعی در ارتکاب و توسعهٔ حملات فیشینگ

هوش مصنوعی نقش مهمی در حملات فیشینگ، به‌ویژه برای مهاجمان دارد. در اینجا نحوهٔ استفادهٔ مهاجمان از هوش مصنوعی در حملات فیشینگ آمده است:

ـ خودکارسازی حملات فیشینگ: هوش مصنوعی می‌تواند ایجاد و توزیع پیام‌های فیشینگ را خودکار کند و به مهاجمان اجازه می‌دهد حملات در مقیاس بزرگ را به‌طور مؤثر انجام دهند.

1. AOHell
2. 2600: The Hacker Quarterly
3. Member States shall take the necessary measures to ensure that, when committed intentionally, the access without right, to the whole or to any part of an information system, is punishable as a criminal offence where committed by infringing a security measure, at least for cases which are not minor.

حملات فیشینگ مبتنی بر هوش مصنوعی از روش‌های پیشرفته‌ای برای افزایش کارایی عملیات فیشینگ استفاده می‌کنند (Khan & Alam, 2025: 32).

ـ ایجاد پیام‌های قانع‌کننده: هوش مصنوعی قادر است ایمیل‌های فیشینگ را به‌گونه‌ای طراحی کند که با بهره‌گیری از جزئیات اختصاصی هر مخاطب، احتمال پاسخ‌گویی افزایش یابد. استفاده از پردازش زبان طبیعی این امکان را فراهم می‌کند تا متن ایمیل‌ها دقیقاً متناسب با علایق و رفتار برخط قربانی شکل گیرد و درنتیجه نرخ موفقیت حملات بیشتر شود[1](Khan & Alam, 2025: 33).

ـ درس گرفتن از موفقیت‌ها و شکست‌ها: سیستم‌های هوش مصنوعی می‌توانند از حملات گذشته درس بگیرند تا تلاش‌های فیشینگ آینده را بهبود بخشند و مشخص کنند کدام استراتژی‌ها مؤثرترند. درواقع فناوری‌های هوش مصنوعی اثربخشی حملات را بهبود می‌بخشند و در چشم‌انداز جرائم سایبری، تغییردهندهٔ بازی هستند (Jabbar & Al-Janabi, 2025: 1.)

ـ فیشینگ نیزه‌ای:[2] هوش مصنوعی می‌تواند به مهاجمان کمک کند تا با جمع‌آوری و استفاده از اطلاعات شخصی برای ایجاد پیام‌های بسیار سفارشی‌شده، فیشینگ نیزه‌ای، شکلی هدفمند از فیشینگ را انجام دهند. به بیان دیگر در حملات هدفمند، هوش مصنوعی با جمع‌آوری اطلاعات شخصی قربانی، پیام‌هایی بسیار دقیق و متناسب تولید می‌کند که تشخیص آن‌ها برای قربانی دشوار است. از تکنیک‌های پردازش زبان طبیعی برای تولید محتوای فیشینگ متناسب با متن و از نظر دستوری صحیح استفاده می‌شود[3] (Jabir et al., 2025:19). برای مثال، نشان داده شده است که ایمیل‌های فیشینگ تولیدشده توسط هوش مصنوعی نرخ کلیک بالاتری نسبت به ایمیل‌های نوشته‌شده توسط انسان دارند، که نشان‌دهندهٔ اثربخشی هوش مصنوعی در ایجاد محتوای فیشینگ قانع‌کننده است.

1. “Models such as GPT and BERT can generate convincing email messages tailored to the interests and online behavior of the target”.
2. spear phishing
3. “when targeting organisations, attackers may gather information about the implemented systems and infras-tructure, which can be used in attacks to customise phishing messages that, for example, require employees to deploy urgent software patches or log in to a company website link after an upgrade or maintenance, which is then used in subsequent attack”.

۲-۲-۱. زیرساخت قانونی و مقررات کیفری ایران در مواجهه با حملات فیشینگ

در نظام حقوق کیفری ایران، حملات فیشینگ به‌طور مستقیم جرم‌انگاری نشده‌اند؛ با این حال، برخی مواد قانونی در حوزهٔ جرائم رایانه‌ای قابلیت انطباق با این نوع رفتارها را دارند. برای نمونه، مادهٔ ۷۴۰ قانون مجازات اسلامی (تعزیرات، اصلاحی ۱۳۹۹) به ربایش غیرمجاز داده‌ها پرداخته و مادهٔ ۷۴۱ نیز تحصیل مال یا منفعت از طریق دسترسی غیرمجاز به سیستم‌های رایانه‌ای یا مخابراتی را جرم‌انگاری کرده است. هرچند این مواد می‌توانند بر حملات فیشینگ قابل اعمال باشند، اما اصطلاح فیشینگ به‌طور صریح در قانون ذکر نشده است. از همین رو، کارشناسان بر ضرورت تقویت و روزآمدسازی مقررات کیفری تأکید دارند تا بتوان با پیچیدگی‌ها و تحول مداوم تهدیدات سایبری مقابله کرد. این امر شامل شناسایی دقیق‌تر انواع حملات فیشینگ، توسعهٔ همکاری‌های بین‌المللی، ارتقای زیرساخت‌های فناوری اطلاعات و آموزش عمومی برای افزایش آگاهی و پیشگیری از این جرائم است. چنین دیدگاهی بیانگر نیاز به رویکردی جامع‌تر در مواجهه با جرائم سایبری است.

۲. تهدیدات ناشی از فناوری‌های خودران و خودمختار

فناوری‌های خودران و خودمختار، به‌ویژه خودروهای بدون راننده و سامانه‌های تسلیحاتی خودکار، یکی از مهم‌ترین جلوه‌های تحول هوش مصنوعی در عرصه‌های مدنی و نظامی به‌شمار می‌روند. این فناوری‌ها با اتکا به الگوریتم‌های یادگیری ماشین و پردازش داده‌های پیچیده، توانایی تصمیم‌گیری مستقل در شرایط واقعی را پیدا کرده‌اند. هرچند این قابلیت‌ها می‌توانند کارایی و ایمنی را در بسیاری از حوزه‌ها افزایش دهند، اما در عین حال تهدیدات نوظهور و پیچیده‌ای را برای نظام حقوق کیفری ایجاد می‌کنند.

در حوزهٔ مدنی، خودروهای خودران در صورت نقص فنی یا تصمیم‌گیری الگوریتمی نادرست، ممکن است به حوادث مرگبار یا خسارات گسترده منجر شوند. پرسش اساسی این است که در چنین مواردی مسئولیت کیفری بر عهدهٔ چه کسی قرار می‌گیرد: تولیدکننده، برنامه‌نویس، مالک خودرو یا خود سامانهٔ هوش مصنوعی؟ در حوزهٔ نظامی نیز سلاح‌های خودمختار مرگبار با قابلیت انتخاب و هدف‌گیری مستقل، خطر نقض قواعد حقوق بشردوستانه و ارتکاب جرائم جنگی را به همراه دارند. این وضعیت، ضرورت بازنگری در مقررات بین‌المللی و داخلی را آشکار می‌سازد.

۱-۲. ماهیت و چالش‌های کیفری سلاح‌های خودمختار مرگبار مبتنی بر هوش مصنوعی

سلاح‌های خودمختار مرگبار (سامانه‌های تسلیحاتی خودکار مرگبار) نوعی سیستم نظامی مستقل هستند که می‌توانند به‌طور مستقل اهداف را براساس محدودیت‌ها و توصیفات برنامه‌ریزی‌شده جست‌وجو کنند و درگیر شوند. این سلاح‌ها همچنین با نام‌های سیستم‌های اسلحه‌های خودران مرگبار، سیستم‌های سلاح‌های خودمختار (سامانه‌های تسلیحاتی خودکار)، سلاح‌های روباتیک یا روبات‌های قاتل نیز شناخته می‌شوند. این سلاح‌ها ممکن است در هوا، روی زمین، روی آب، زیر آب یا در فضا عمل کنند. استقلال سیستم‌های کنونی از سال ۱۳۹۷ به این معنا محدود شده بود که یک انسان فرمان نهایی حمله را می‌دهد، اگرچه استثناهایی درمورد سیستم‌های «دفاعی» خاصی وجود دارد. مفهوم خودمختاری در رشته‌های مختلف علمی و فناوری معانی متفاوتی دارد. در حوزه‌هایی مانند رباتیک غیرنظامی یا خودروهای خودران، معیارهای شناسایی خودمختاری نسبتاً روشن و استانداردهای مشخصی وجود دارد. اما در زمینهٔ توسعهٔ تسلیحات نظامی، تعریف و شناسایی یک سلاح به‌عنوان خودمختار همچنان با ابهام و اختلاف نظر همراه است (Crootof, 2015:1837). پژوهش‌های حقوقی نشان داده‌اند که استانداردهای مربوط به مفهوم خودمختاری می‌تواند میان دانشمندان، دولت‌ها و سازمان‌های بین‌المللی بسیار متفاوت باشد و همین امر موجب می‌شود شناسایی سلاح‌های خودمختار در عرصهٔ نظامی به وضوح سایر حوزه‌ها نباشد.

ارتش بریتانیا وسایل نقلیهٔ بدون سرنشین و روبات‌های نظامی جدید را در سال ۲۰۱۹ مستقر کرد. (Army Recognition, 2019). نیروی دریایی ایالات متحده در حال توسعهٔ ناوگان «شبح» کشتی‌های بدون سرنشین است (Army Recognition, 2019).

۱-۱-۲. کاربرد هوش مصنوعی در طراحی و عملکرد سلاح‌های خودمختار

هوش مصنوعی نقش مهمی در توسعه و بهره‌برداری از سیستم‌های تسلیحاتی خودمختار ایفا می‌کند. این سیستم‌ها که می‌توانند شامل هواپیماهای بدون سرنشین، موشک‌ها و وسایل نقلیهٔ زمینی باشند، از هوش مصنوعی برای افزایش قابلیت‌های خود به طرق مختلف استفاده می‌کنند:

ـ تصمیم‌گیری: هوش مصنوعی می‌تواند حجم وسیعی از داده‌ها را برای تصمیم‌گیری در زمان واقعی درمورد هدف‌گیری و تعامل بدون دخالت انسان پردازش کند. طی بیش از سه دههٔ گذشته، بهره‌گیری از فناوری هوش مصنوعی در طراحی و توسعهٔ سامانه‌های تسلیحاتی توسط تولیدکنندگان

این حوزه به‌طور مستمر دنبال شده است. مطالعات حقوقی و فنی متعدد، مدل‌های مبتنی بر یادگیری نظارت‌شده را به‌عنوان زیرساختی مؤثر در ارتقای قابلیت تصمیم‌گیری خودکار این سامانه‌ها شناسایی و تحلیل کرده‌اند (Abaimov & Martellini, 2020: 141).

ـ دقت و درستی: الگوریتم‌های هوش مصنوعی می‌توانند دقت سلاح‌ها را بهبود بخشند، آسیب‌های جانبی را کاهش و احتمال اصابت به اهداف مورد نظر را افزایش دهند. درواقع مدل‌های عصبی پیشرفته می‌توانند محل دقیق اصابت موشک یا گلوله را پیش‌بینی کنند، که باعث افزایش دقت و کاهش آسیب‌های جانبی می‌شود (Altmann & Sauer, 2017: 118).

ـ خودمختاری: با هوش مصنوعی، سامانه‌های تسلیحاتی خودکار می‌توانند وظایف پیچیده‌ای مانند هدایت، پایش و شناسایی هدف را به‌طور مستقل انجام دهند. سیستم‌های هدف‌گیری مبتنی بر هوش مصنوعی به پهپادها اجازه می‌دهند تا اهداف را با حداقل دخالت انسان، حتی در محیط‌های بسیار شلوغ، شناسایی و مورد اصابت قرار دهند (Ibid: 118).

– بهره‌وری: سیستم‌های پشتیبانی تصمیم‌گیری مبتنی بر هوش مصنوعی، عملیات را ساده می‌کنند و زمان پاسخ‌گویی را کاهش می‌دهند و امکان کنترل هم‌زمان چندین دارایی را فراهم می‌کنند (Ibid: 119).

– تطبیق‌پذیری: سلاح‌های مجهز به هوش مصنوعی می‌توانند از درگیری‌های گذشته درس بگیرند و با موقعیت‌های جدید تطبیق داده شوند، و به‌طور بالقوه بر سیستم‌های عملیاتی انسانی غلبه کنند.

۲-۱-۲. چالش‌های مسئولیت کیفری ناشی از تصمیم‌گیری هوش مصنوعی در سلاح‌های خودمختار

در بررسی مسئولیت کیفری هوش مصنوعی در سلاح‌های خودمختار، نخست باید میان وضعیت‌های مختلف تفکیک قائل شد. حالت نخست زمانی است که سلاح خودمختار براساس برنامه‌ریزی و طراحی قبلی کاربر یا مهندس اقدام به شلیک می‌کند. در چنین وضعیتی، مسئولیت کیفری متوجه سازنده، برنامه‌ریز یا مالک سلاح خواهد بود، زیرا تصمیم و نقشهٔ قبلی آنان مبنای عملکرد سامانه بوده و نقش تعیین‌کننده در وقوع نتیجهٔ زیان‌بار داشته است. این مسئولیت درواقع ناشی از طراحی و هدایت اولیه‌ای است که مهندسان و عوامل پشت صحنه بر فرایند عملکرد سلاح

اعمال کرده‌اند (Gaeta, 2023: 1033). حالت دوم زمانی مطرح می‌شود که مهندسان و عوامل انسانی پشت صحنه، برنامه یا طرح مشخصی را از پیش در اختیار سامانه قرار نداده باشند و سلاح خودمختار صرفاً براساس خطا یا تصمیم‌گیری مستقل هوش مصنوعی اقدام به شلیک کند. در چنین وضعیتی، پرسش اساسی آن است که آیا باید مسئولیت کیفری را مستقیماً متوجه خود هوش مصنوعی دانست، یا آن‌که باید به سوی الگوی مسئولیت کیفری ترکیبی حرکت کرد؛ الگویی که ضمن پذیرش نقش سامانهٔ هوشمند در وقوع نتیجه، همچنان جایگاه عوامل انسانی و ساختاری را در تعیین مسئولیت نادیده نمی‌گیرد[1](Acquaviva, 2022: 89).

مطالعات به مسئله‌ای به نام «شکاف در مسئولیت» اشاره دارند که ناشی از ذات منحصربه‌فرد هوش مصنوعی است و بر این باورند که مقررات کنونی درخصوص هوش مصنوعی نارسایی دارد[2](Smith, 2022: 2). بنابراین، توصیه شده است که جامعهٔ بین‌المللی باید برای تطبیق با شرایط جدید، سازندگان را ملزم به ارائهٔ شفافیت حداکثری کند و برخی از انواع هوش مصنوعی را ممنوع سازد. برخی پژوهشگران بر این باورند که برای جلوگیری از بی‌کیفرمانی ناشی از استفاده از سلاح‌های هوش مصنوعی، باید اساسنامهٔ دیوان کیفری بین‌المللی نیز مورد بازنگری و اصلاح قرار گیرد (Bátori, 2025: 2).

مسئلهٔ جرم‌انگاری سلاح‌های خودمختار مبتنی بر هوش مصنوعی در حقوق کیفری ایران موضوع بسیار مهم و پیچیده‌ای است. براساس تحقیقات و مقالات علمی، بحث‌هایی در این زمینه وجود دارد که به بررسی مسئولیت کیفری هوش مصنوعی و نحوهٔ برخورد با جرائم ناشی از استفاده از این فناوری‌ها می‌پردازند. از یک طرف، هوش مصنوعی به‌دلیل فقدان شعور و اراده، نمی‌تواند به‌عنوان مباشر جرم شناخته شود و بنابراین، نمی‌توان برای آن مسئولیت کیفری قائل شد. از طرف دیگر، پیشنهاد شده است که باید قوانین موجود را برای پاسخ‌گویی به چالش‌های ناشی از استفاده از هوش مصنوعی در سلاح‌های خودمختار به‌روزرسانی کرد و به‌نظر می‌رسد که پذیرش فرض قانونی

1. “three main theoretical possibilities are explored: that humans remain the only subject capable of being considered criminally respon-sible for harm to interests protected by ICL; that AWS come to be considered ‘persons’ subject to (a form of) individual criminal responsibility; or, a hybrid new system combining aspects of the two”.
2. “As a consequence of this chaotic and unpredictable autonomy and the corresponding likelihood of just war violations, LAWS will almost certainly be involved in responsibility gaps”.

اشخاص الکترونیکی، به‌عنوان سازوکاری برای هویت‌بخشی به سامانه‌های هوش مصنوعی، می‌تواند نقش مؤثری در تحقق مسئولیت کیفری این سامانه‌ها ایفا کند[1] (Swart, 2023: 589). همان‌گونه که در نظام حقوقی، مسئولیت کیفری اشخاص حقوقی پذیرفته شده است، به‌منظور ایجاد مسئولیت کیفری برای اشخاص الکترونیکی نیز، نخست باید شناسایی و تعریف دقیق این شخصیت حقوقی نوظهور صورت گیرد. با وجود پیامدهای زیان‌بار و مخاطرات امنیتی ناشی از توسعه و به‌کارگیری سلاح‌های مبتنی بر هوش مصنوعی، در قانون مجازات قاچاق اسلحه و مهمات و دارندگان سلاح و مهمات غیرمجاز مصوب ۱۳۹۰، هیچ‌گونه تصریحی نسبت به سلاح‌های خودمختار مبتنی بر هوش مصنوعی صورت نگرفته است. این فقدان قانون‌گذاری را می‌توان به‌عنوان یکی از خلأهای حقوقی اساسی در نظام قانون‌گذاری کیفری تلقی کرد، که ضرورت بازنگری و به‌روزرسانی قوانین موجود را در مواجهه با تحولات فناورانه ایجاب می‌کند. با توجه به اینکه هوش مصنوعی می‌تواند خطراتی را برای جان و زندگی انسان‌ها ایجاد کند، ممکن است جرم‌انگاری برخی استفاده‌های خاص از سلاح‌های خودمختار مبتنی بر هوش مصنوعی به‌منظور حفاظت از حقوق بشر و جلوگیری از سوءاستفاده‌ها مصلحت باشد. هرچند برخی ممکن است استدلال کنند که این نوع سلاح‌ها در عموم و اطلاق قواعد سنتی مربوط به سلاح‌ها می‌گنجند، اما واقعیت آن است که ویژگی تصمیم‌گیری کاملاً مستقل، آن‌ها را از چارچوب‌های سنتی خارج می‌کند و نیازمند قواعد خاص و مستقل می‌سازد. بنابراین، تصمیم‌گیری درمورد جرم‌انگاری یا عدم جرم‌انگاری این سلاح‌ها باید با درنظر گرفتن تمام جوانب اخلاقی، حقوقی، امنیتی و فناوری انجام شود و نیازمند گفت‌وگو و همکاری بین متخصصان حقوقی، نظامی، فناوری و سیاست‌مداران است. همچنین، باید به نظرات جامعه بین‌المللی و توافق‌های بین‌المللی در این زمینه توجه شود.

۲-۲. ماهیت و چالش‌های کیفری خودروهای خودران مبتنی بر هوش مصنوعی

خودروی خودران، که گاه با اصطلاحاتی چون ماشین بدون راننده، روبوتاکسی[2] یا خودرو روباتیک نیز شناخته می‌شود؛ وسیله‌ای است که قادر است با حداقل یا بدون دخالت انسانی عمل کند

1. "This article aims to construct 'electronic liability' for such international crimes. It will argue that it is not sufficient to hold the persons or programmers behind the autonomous agents liable, but that it should be possible to hold the autonomous agents that commit international crimes liable".
2. Robotaxi

(Gherardini & Cabri, 2023: 1). اتومبیل‌های خودران مسئول تمام فعالیت‌های رانندگی مانند درک محیط، نظارت بر سیستم‌های مهم و کنترل وسیلهٔ نقلیه هستند که شامل حرکت از مبدأ تا مقصد است (Pendleton et al., 2017: 1). خودروهای خودران پتانسیل تأثیرگذاری بر صنعت خودرو، هزینه‌های حمل و نقل، سلامت، رفاه، برنامه‌ریزی شهری، ترافیک، بیمه، بازار کار و سایر حوزه‌ها را دارند. مقررات مناسب برای ادغام خودروهای خودران در محیط رانندگی موجود ضروری است. سازمان‌هایی مانند انجمن مهندسان خودرو استانداردهای اصطلاحات را پیشنهاد کرده‌اند. با این حال، بیشتر اصطلاحات هیچ تعریف استانداردی ندارند و توسط فروشندگان و سایرین به‌طور متفاوتی به‌کار می‌روند.

۱-۲-۲. هوش مصنوعی و تحولات فنی در عملکرد خودروهای خودران

کارکردهای هوش مصنوعی در خودروهای خودران را می‌توان در چند محور اصلی دسته‌بندی کرد. این محورها شامل تفسیر اطلاعات، تصمیم‌گیری در زمان واقعی، ناوبری در محیط‌های پیچیده و تست ایمنی هستند. هر یک از این کارکردها نقشی اساسی در ارتقای عملکرد خودروهای خودران ایفا می‌کنند و به‌طور مستقل می‌توانند زمینه‌ساز چالش‌های حقوقی و کیفری شوند.

ـ تفسیر اطلاعات: سیستم‌های هوش مصنوعی مقادیر زیادی داده از حسگرهای خودرو مانند دوربین‌ها، رادار و لیدار[1] را پردازش می‌کنند تا محیط اطراف خودرو را تفسیر کنند (Garikapati & Shetiya, 2024: 19). این مدل‌سازی محیطی پایه‌گذار تصمیم‌گیری‌های بعدی خودرو است و به آن امکان می‌دهد تا اشیا، موانع و کاربران جاده را شناسایی کند.

ـ تصمیم‌گیری در زمان واقعی: براساس داده‌های تفسیرشده، هوش مصنوعی تصمیماتی را در زمان واقعی برای پیمایش ایمن اتخاذ می‌کند، مانند شناسایی موانع، پیش‌بینی اقدامات سایر کاربران جاده، و برنامه‌ریزی مسیر وسیلهٔ نقلیه بر این اساس (Schwarting et al., 2018: 190).

ـ ناوبری در محیط‌های پیچیده: هوش مصنوعی خودروهای خودران را قادر می‌سازد تا در محیط‌های پیچیده و پویا حرکت کنند، با تغییر شرایط جاده، الگوهای ترافیکی و موقعیت‌های غیرمنتظره بدون دخالت انسان سازگار شوند(Ibid: 191).

1. Lidar

– تست ایمنی: هوش مصنوعی برای شبیه‌سازی شرایط دنیای واقعی برای تست ایمنی وسایل نقلیهٔ خودران استفاده می شود و به مهندسان کمک می‌کند تا سیستم‌ها را بهبود بخشند و از قابلیت امنیت آن‌ها قبل از استقرار، اطمینان حاصل کنند (Yeong et al., 2025: 12).

۲-۲-۲. ابعاد کیفری ارتکاب جرائم توسط خودروهای خودران مبتنی بر هوش مصنوعی

هوش مصنوعی در خودروهای خودران به‌خودی‌خود واجد وصف مجرمانه نیست، زیرا صرف وجود یا استفاده از این فناوری جرم محسوب نمی‌شود. با این حال، این فناوری می‌تواند به‌عنوان ابزار یا وسیله‌ای مورد سوءاستفاده قرار گیرد و زمینهٔ ارتکاب جرائم مختلف را فراهم سازد. بنابراین، باید میان ماهیت بی‌طرفانهٔ فناوری و کارکردهای مجرمانه ناشی از سوءاستفاده از آن تفکیک قائل شد. این فناوری قابلیت آن را دارد که در بسترهای گوناگون مورد سواستفاده قرار گیرد:

ـ تهدیدات امنیت سایبری: سیستم‌های هوش مصنوعی در خودروهای خودران در برابر هک و حملات سایبری آسیب‌پذیر هستند که می‌تواند به کنترل غیرمجاز خودرو منجر شود.[1] (Brown et al., 2025: 1)

ـ بهره‌برداری: مجرمان به‌طور بالقوه می‌توانند از فرایندهای تصمیم‌گیری هوش مصنوعی برای ایجاد تصادفات عمدی یا استفاده از وسایل نقلیهٔ خودران برای فعالیت‌های غیرقانونی سوءاستفاده کنند[2] (Ibid: 17).

ـ عدم پیش‌بینی: مدل‌های فعلی هوش مصنوعی برای اتومبیل‌های خودران ممکن است به‌طور کامل امکان سوء استفاده از آن‌ها برای اهداف مجرمانه را درنظر نگیرند.

توجه به این نکته مهم است که مسئولیت چنین جرائمی معمولاً بر عهدهٔ افرادی است که هوش مصنوعی را دستکاری یا سوءاستفاده می‌کنند، نه خود هوش مصنوعی. با پیشرفت فناوری هوش

1. “Connected and Autonomous Vehicles (CAVs) integrate advanced communication and autonomous driving tech-
nologies, enabling them to operate independently or with minimal human intervention. Despite the anticipated
benefits for transportation, CAVs could be vulnerable to a wide variety of crimes unless security and crime preven-
tion measures are proactively integrated into the technologies enabling their operation”.
2. “The absence of human drivers in CAVs may facilitate illegal transportation, similar to how drone technology is currently misused to smuggle illicit goods including nar- cotics (Daly, 2024) and human trafficking using vehicles”.

مصنوعی، نیاز فزاینده‌ای به اقدامات امنیتی قوی و دستورالعمل‌های اخلاقی برای جلوگیری و رسیدگی به این خطرات وجود دارد. چارچوب‌های قانونی و نظارتی نیز برای مدیریت پیامدهای هوش مصنوعی در وسایل نقلیهٔ خودران و تضمین ایمنی و مسئولیت‌پذیری در حال تکامل هستند. در مواردی که ماشینی که با هوش مصنوعی کار می‌کند و مرتکب جرم می‌شود یا تصادف می‌کند، ممکن است طرف‌های زیر برای مسئولیت درنظر گرفته شوند:

ـ طراحان و توسعه‌دهندگان: اگر اقدامات هوش مصنوعی ناشی از نقص طراحی یا برنامه‌نویسی باشد، کسانی که هوش مصنوعی را ایجاد کرده‌اند می‌توانند مسئول باشند.

ـ تولیدکنندگان: اگر حادثه به‌دلیل نقص ساخت باشد، ممکن است سازنده مسئول باشد.

ـ کاربران: اگر کاربران از هوش مصنوعی سوءاستفاده کردند یا پروتکل‌های ایمنی را رعایت نکردند، می‌توانند پاسخ‌گو باشند.

– تنظیم‌کننده: اگر نقصی در چارچوب نظارتی وجود داشته باشد که باید از وقوع چنین حوادثی جلوگیری می‌کرد، ممکن است نهادهای نظارتی مورد بررسی دقیق قرار گیرند.

۳. تهدید علیه امنیت

هوش مصنوعی با قابلیت‌های گسترده در تحلیل داده‌ها، یادگیری الگوها و تصمیم‌گیری مستقل، علاوه بر فرصت‌های بی‌سابقه، تهدیدات جدی علیه امنیت در ابعاد مختلف ایجاد کرده است. این تهدیدات می‌توانند امنیت ملی، امنیت سایبری، امنیت اقتصادی و حتی امنیت اجتماعی را تحت تأثیر قرار دهند. درواقع، هرچه فناوری‌های هوشمند بیشتر در زیرساخت‌های حیاتی ادغام شوند، آسیب‌پذیری این زیرساخت‌ها در برابر حملات پیچیده و خودکار افزایش می‌یابد.

از منظر حقوق کیفری، تهدید علیه امنیت ناشی از هوش مصنوعی پرسش‌های بنیادینی را دربارهٔ کفایت قوانین موجود و ضرورت جرم‌انگاری نوین مطرح می‌سازد. آیا حملات سایبری مبتنی بر هوش مصنوعی باید به‌عنوان جرائم مستقل شناخته شوند؟ آیا استفاده از الگوریتم‌های خودکار در تخریب یا اختلال زیرساخت‌های حیاتی نیازمند تدوین مقررات ویژه است؟ این پرسش‌ها نشان می‌دهند که تهدید علیه امنیت، یکی از مهم‌ترین عرصه‌های بزه‌انگاری تهدیدات نوظهور ناشی از هوش مصنوعی محسوب می‌شود.

۱-۳. ماهیت و ابعاد حقوقی حملات سایبری علیه زیرساخت‌ها و سامانه‌های اطلاعاتی

حملهٔ سایبری، هر گونه مانور تهاجمی است که سیستم‌های اطلاعاتی رایانه‌ای، شبکه‌های رایانه‌ای، زیرساخت‌ها، دستگاه‌های رایانهٔ شخصی یا گوشی‌های هوشمند را هدف قرار می‌دهد. مهاجم به شخص یا فرایندی گفته می‌شود که سعی می‌کند بدون مجوز به داده‌ها، عملکردها یا سایر مناطق محدودشدهٔ سیستم دسترسی پیدا کند، که احتمالاً با قصد مخرب است (Agrafiotis et al., 2018: 2). حسب زمینه، حملات سایبری می‌تواند بخشی از جنگ سایبری یا تروریسم سایبری باشد. یک حملهٔ سایبری می‌تواند توسط دولت‌ها، افراد، گروه‌ها، جوامع یا سازمان‌های مستقل به کار گرفته شود و ممکن است از یک منبع ناشناس سرچشمه بگیرد. محصولی که حملهٔ سایبری را تسهیل می‌کند، گاهی اوقات سلاح سایبری نامیده می‌شود. حملات سایبری در چند سال گذشته افزایش یافته است. یک حملهٔ سایبری ممکن است با هک کردن یک شبکهٔ خصوصی یا سیستم حساس، یک هدف مشخص را بدزدد، تغییر دهد یا ازبین ببرد. حملات سایبری می‌تواند از نصب نرم‌افزارهای جاسوسی بر روی رایانهٔ شخصی تا تلاش برای تخریب زیرساخت‌های کل کشورها را شامل شود. کارشناسان حقوقی به دنبال محدود کردن استفاده از این اصطلاح به حوادثی هستند که باعث آسیب فیزیکی می‌شوند و آن را از نقض‌های معمول داده‌ها و فعالیت‌های هک گسترده‌تر متمایز می‌کنند.

۱-۱-۳. زیرساخت‌های حیاتی به‌عنوان اهداف بالقوهٔ حملات سایبری مبتنی بر هوش مصنوعی

با آغاز هر حملهٔ سایبری، مجموعه‌ای از اهداف راهبردی وجود دارد که هدف قرار گرفتن آن‌ها می‌تواند به فلج شدن کامل حریف منجر شود. در این میان، زیرساخت‌های حیاتی در زمان درگیری بیش از سایر بخش‌ها برجسته می‌شوند، زیرا آسیب به آن‌ها توان یک ملت را به‌طور جدی مختل می‌سازد. از جملهٔ این زیرساخت‌ها می‌توان به سامانه‌های کنترل صنعتی، منابع انرژی، شبکه‌های مالی، مخابرات، حمل‌ونقل و تأسیسات آب اشاره کرد که در ادبیات امنیت سایبری به‌عنوان اهداف اصلی شناخته می‌شوند.

براساس گزارشی از مؤسسهٔ فناوری بریتیش کلمبیا، که با بهره‌گیری از داده‌های تاریخی تهیه شده است، تعداد حملات موفق علیه زیرساخت‌ها طی چند دههٔ اخیر رشدی چشمگیر داشته و در مقایسه با سال ۱۹۸۱ حدود ده برابر افزایش یافته است. به‌ویژه از ابتدای دههٔ ۲۰۰۰، حملاتی که به آثار

فیزیکی نامطلوب بر سامانه‌های کنترل و نظارت منجر شده‌اند، در ادبیات تخصصی با عنوان «حملات سایبری ـ فیزیکی» مورد شناسایی قرار گرفته‌اند (Sin & Washburn, 2022: 133).

۲-۱-۳. نقش هوش مصنوعی در طراحی و اجرای حملات سایبری پیشرفته

برای مهاجمان، هوش مصنوعی می‌تواند اثربخشی و کارایی حملات سایبری را به میزان قابل توجهی افزایش دهد. در اینجا نحوهٔ استفاده از هوش مصنوعی در انجام حملات سایبری آمده است:

ـ یادگیری و تکامل: سیستم‌های هوش مصنوعی می‌توانند از محیط بیاموزند و استراتژی‌های خود را برای دور زدن اقدامات امنیتی توسعه دهند. آن‌ها می‌توانند پاسخ‌های ابزارهای امنیت سایبری را تجزیه و تحلیل کنند و الگوهای حملهٔ خود را برای جلوگیری از شناسایی تطبیق دهند (Rigaki & García, 2018: 70).

ـ کشف آسیب‌پذیری خودکار: هوش مصنوعی می‌تواند فرایند اسکن آسیب‌پذیری‌های سیستم را خودکار کند و به مهاجمان این امکان را می‌دهد تا به سرعت نقاط ضعف را شناسایی و از آن‌ها سوءاستفاده کنند (Salem et al., 2024: 1).

ـ فیشینگ پیچیده:[1] با تجزیه و تحلیل داده‌های شخصی، هوش مصنوعی می‌تواند کمپین‌های فیشینگ بسیار شخصی‌سازی‌شده ایجاد کند که احتمال فریب دادن اهداف را افزایش می‌دهد.

ـ بدافزار خود ـ اصلاح‌شونده[2]: هوش مصنوعی می‌تواند بدافزار را قادر سازد تا کد خود را در زمان واقعی تغییر دهد و تشخیص و خنثی کردن این تهدیدات را برای نرم‌افزارهای آنتی‌ویروس سنتی سخت‌تر کند.

ـ سرعت و مقیاس: هوش مصنوعی می‌تواند حملات را با سرعتی بسیار بیشتر و در مقیاسی بزرگ‌تر از مهاجمان انسانی انجام دهد و تأثیر بالقوهٔ تهدیدات سایبری را افزایش دهد.

هوش مصنوعی تهاجمی[3] (Girhepuje et al., 2024: 1)[4]، این اصطلاح به سیستم‌های هوش مصنوعی اطلاق می‌شود که می‌توانند به‌طور مستقل حملات را انجام دهند، عملیات خود را پنهان

1. advanced phishing
2. self-modifying malware
3. Offensive Artificial Intelligence (Offensive AI)
4. "The paper will explore adversarial machine learning, attacks against AI models, infrastructure, and interfaces, along with offensive techniques like information gathering, social engineering, and weaponized AI".

کنند و با فعالیت‌های منظم ترکیب شوند و تشخیص آن‌ها را دشوار کند. استفاده از هوش مصنوعی در حملات سایبری نشان‌دهندهٔ تغییر قابل توجهی در چشم‌انداز تهدید است، زیرا امکان تهدیدات سایبری پیچیده‌تر، سازگارتر و بالقوه مستقل را فراهم می‌کند. این امر بر نیاز به مکانیسم‌های دفاعی پیشرفته مبتنی بر هوش مصنوعی برای محافظت در برابر چنین حملات سایبری تقویت‌شده با هوش مصنوعی تأکید می‌کند. این یک مسابقهٔ تسلیحاتی مداوم بین مهاجمان و مدافعان سایبری است که از فناوری‌های هوش مصنوعی در هر دو طرف استفاده می‌شود.

۳-۱-۳. بررسی مواد قانونی موجود در حقوق کیفری ایران مرتبط با حملات سایبری

در حقوق کیفری ایران، مواد قانونی مرتبط با حملات سایبری عمدتاً در قانون جرائم رایانه‌ای و قانون مجازات اسلامی تعریف شده‌اند. برخی از مواد کلیدی عبارت‌اند از مادهٔ ۷۳۷ قانون مجازات اسلامی به جرائمی مانند تخریب یا اخلال در تأسیسات رایانه‌ای و مخابراتی می‌پردازد. همچنین مادهٔ ۷۳۹ همین قانون نیز در رابطه با جرائم سایبری و تأسیسات زیرساختی است، لکن قانون جرائم رایانه‌ای ایران فاقد اصطلاح و جرم‌انگاری مستقل حملهٔ سایبری است. این در حالی است که حملات سایبری ماهیتی فراملی و سازمان‌یافته دارند و امنیت ملی کشور را هدف قرار می‌دهند. ازاین‌رو، ضرورت دارد در نظام حقوقی ایران، حملات سایبری به‌طور مستقل جرم‌انگاری شوند و ضمانت اجراهای متناسب با شدت و خسارت آن‌ها پیش‌بینی شود (بهره‌مند و مرسی، ۱۴۰۱: ۳۲۰).

۴. تهدیدات علیه اموال(حقوق مالی)

هوش مصنوعی علاوه بر فرصت‌های گسترده در حوزه‌های اقتصادی و صنعتی، تهدیدات نوظهوری را علیه اموال اشخاص و سازمان‌ها ایجاد کرده است. این تهدیدات می‌توانند هم در حوزهٔ اموال مادی مانند تجهیزات و زیرساخت‌های فیزیکی و هم در حوزهٔ اموال مالی و دیجیتال مانند داده‌های شخصی، حساب‌های بانکی، ارزهای دیجیتال و دارایی‌های مجازی بروز یابند.

یکی از مهم‌ترین جلوه‌های این تهدیدات، ظهور باج‌افزارهای هوشمند است که با بهره‌گیری از الگوریتم‌های یادگیری ماشین می‌توانند حملات پیچیده‌تر و هدفمندتری علیه دارایی‌های دیجیتال انجام دهند. این باج‌افزارها قادرند داده‌های حساس را رمزگذاری و قربانی را به پرداخت مبالغ هنگفت برای بازیابی اطلاعات وادار کنند. در کنار آن، استخراج غیرقانونی ارزهای دیجیتال با

استفاده از بات‌نت‌ها و سامانه‌های هوشمند، شکل دیگری از تهدید علیه اموال است که نه‌تنها خسارات اقتصادی مستقیم به همراه دارد، بلکه اعتماد عمومی به نظام‌های مالی و فناوری‌های نوین را نیز تضعیف می‌کند.

از منظر حقوق کیفری، این تهدیدات پرسش‌های بنیادین دربارهٔ کفایت قوانین موجود و ضرورت جرم‌انگاری نوین مطرح می‌سازند. آیا باج‌افزارهای مبتنی بر هوش مصنوعی باید به‌عنوان جرائم مستقل شناخته شوند؟ آیا استخراج غیرقانونی ارزهای دیجیتال با بهره‌گیری از سامانه‌های هوشمند نیازمند مقررات ویژه است؟ این پرسش‌ها نشان می‌دهند که تهدیدات علیه اموال در بستر هوش مصنوعی، یکی از مهم‌ترین عرصه‌های بزه‌انگاری تهدیدات نوظهور محسوب می‌شوند.

۱-۴. ماهیت و پیامدهای کیفری باج‌افزارهای مبتنی بر هوش مصنوعی

باج‌افزار نوعی بدافزار رمزنگاری شده است که دسترسی به داده‌های شخصی قربانی را برای همیشه مسدود می‌کند مگر اینکه باج پرداخت شود. در حالی که برخی از باج افزارهای ساده ممکن است سیستم را بدون آسیب رساندن به هیچ فایلی قفل کنند، بدافزارهای پیشرفته‌تر از تکنیکی به نام اخاذی ویروسی استفاده می‌کنند. فایل‌های قربانی را رمزگذاری می‌کند، آن‌ها را غیرقابل دسترسی می‌کند و برای رمزگشایی آن‌ها باج می‌خواهد (Kharraz et al., 2015: 1). در یک حملهٔ اخاذی ویروسی رمزنگاری‌شده که به‌درستی اجرا می‌شود، بازیابی فایل‌ها بدون کلید رمزگشایی یک مشکل حل‌نشدنی است و از ارزهای دیجیتالی با ردیابی دشوار مانند یا بیت‌کوین[1] و سایر ارزهای رمزنگاری‌شده برای باج‌گیری استفاده می‌شود که ردیابی و تعقیب مجرمان را دشوار می‌کند. حملات باج‌افزار معمولاً با استفاده از یک تروجان[2] مبدل به‌عنوان یک فایل قانونی انجام می‌شوند که کاربر فریب داده می‌شود تا آن را دانلود یا باز کند.

۱-۱-۴. کاربرد هوش مصنوعی در توسعه و اجرای حملات باج‌افزاری

هوش مصنوعی نقشی اساسی در ارتقای توانایی مهاجمان برای اجرای حملات باج‌افزاری ایفا می‌کند. در این بخش، به شیوه‌هایی پرداخته می‌شود که بهره‌گیری از الگوریتم‌های هوشمند می‌تواند

1. Bitcoin
2. Trojan

اثربخشی این حملات را افزایش دهد و زمینه‌های پیچیده‌تر و هدفمندتری را برای ارتکاب چنین جرائمی فراهم سازد.

ـ برنامه‌ریزی و اجرا: مجرمان می‌توانند از هوش مصنوعی برای برنامه‌ریزی و اجرای حملات باج‌افزار پیچیده استفاده کنند. حتی کسانی که دانش فناوری اطلاعات محدودی دارند ممکن است توسط چت‌ربات‌های مبتنی بر هوش مصنوعی قادر به انجام حملات پیچیده باشند (Teichmann, 2023: 399).

ـ فیشینگ هدفمند:[1] مهاجمان با تخصص فناوری اطلاعات می‌توانند از هوش مصنوعی برای تهیهٔ ایمیل‌های فیشینگ قانع‌کننده‌تر استفاده کنند، که اغلب اولین گام در حملهٔ باج‌افزار است. هوش مصنوعی می‌تواند به تنظیم این ایمیل‌ها برای افراد یا سازمان‌های خاص کمک کند و ایمیل‌هایی تولید کند که برای هر قربانی متفاوت و شخصی‌سازی‌شده هستند، و همین موضوع شناسایی آن‌ها را دشوارتر می‌سازد (Ibid: 403).

ـ سرعت و مقیاس: هوش مصنوعی می‌تواند مجرمان سایبری را قادر سازد تا حملات را با سرعت و مقیاس بی‌سابقه‌ای انجام دهند و از اقدامات تشخیص سنتی و مبتنی بر امضا دوری کنند. این امر، دفاع در برابر چنین حملاتی را برای سازمان‌ها چالش‌برانگیزتر می‌کند[2] (Salem et al., 2024: 1).

ـ بدافزار تطبیقی: از هوش مصنوعی می‌توان برای ایجاد بدافزاری استفاده کرد که با محیطی که در آن قرار دارد منطبق می‌شود و تشخیص و حذف آن را دشوارتر می‌کند. این ماهیت تطبیقی بدافزار مبتنی بر هوش مصنوعی می‌تواند به حملات باج‌افزاری مداوم و آسیب‌رسان منجر شود (Teichmann, 2023: 404).

ـ اتوماسیون: هوش مصنوعی می‌تواند بسیاری از جنبه‌های حملات باج‌افزار، از شناسایی آسیب‌پذیری‌ها تا بهره‌برداری از آن‌ها را خودکار کند. این اتوماسیون به مهاجمان اجازه می‌دهد تا با تلاش کمتر به اهداف بیشتری ضربه بزنند و تأثیر کلی آن‌ها را افزایش دهند[3] (Ferdous et al., 2024: 2).

---

1. spear-phishing
2. "Traditional security methods, with their reliance on fixed security controls like firewalls and intrusion detection and prevention systems, have struggled to keep pace with the sophisticated nature of contemporary cyber threats".
3. The REvil ransomware group uses AI to automate the attacks

در حوزهٔ حملات باج‌افزاری، هوش مصنوعی می‌تواند به‌عنوان ابزاری برای برنامه‌ریزی و اجرای این حملات مورد استفاده قرار گیرد. این امر از یک سو امکان ارتکاب حملات پیچیده‌تر را برای افراد فاقد دانش تخصصی در فناوری اطلاعات تسهیل می‌کند و از سوی دیگر به متخصصان این حوزه توانایی تولید ایمیل‌های فیشینگ با سطح بالاتری از اقناع و واقع‌نمایی را می‌دهد. دسترسی گسترده به هوش مصنوعی مولد، بالقوه موجب افزایش کمّی و کیفی حملات باج‌افزاری خواهد شد. با این حال، چارچوب‌های قانونی موجود هنوز با چالش‌های ناشی از این فناوری در حال سازگاری‌اند. باید توجه داشت که هرچند هوش مصنوعی می‌تواند به‌عنوان بردار یا سطح حمله عمل کند، مسئولیت کیفری عمدتاً متوجه عوامل انسانی است که این فناوری را طراحی، هدایت یا بهره‌برداری می‌کنند و از قابلیت‌های آن برای مقاصد غیرقانونی استفاده می‌کنند. این مسئولیت می‌تواند شامل برنامه‌نویسان، گردانندگان سامانه و حتی اشخاصی باشد که در اتخاذ تدابیر امنیتی لازم برای جلوگیری از سوءاستفاده از هوش مصنوعی قصور می‌ورزند (Ibid: 1).

۲-۴. استخراج غیرقانونی ارزهای دیجیتال با بهره‌گیری از بات‌نت‌ها و سامانه‌های هوشمند

اصطلاح «ماینینگ»[1] در زمینهٔ ارزهای رمزپایه به فرایند ایجاد و اعتبارسنجی تراکنش‌های ارزهای دیجیتال با حل مشکلات پیچیدهٔ محاسباتی اشاره دارد (Gandotra et al., 2020: 51). از آنجایی که ارزهای رمزنگاری‌شده مانند بیت‌کوین در یک شبکهٔ غیرمتمرکز کار می‌کنند، افراد در سراسر جهان به عملکرد شبکه کمک می‌کنند و خدمات ضروری را ارائه می‌دهند. در ازای مشارکت آن‌ها، جوایزی در قالب ارزهای دیجیتال به آن‌ها تعلق می‌گیرد. این پاداش‌ها به ایجاد ارزهای دیجیتالی مانند بیت‌کوین، اتریوم[2] و ... منجر می‌شود. این فرایند شبیه به استخراج سنتی است که در آن افراد منابع ارزشمندی مانند طلا یا سنگ‌های قیمتی را استخراج می‌کنند. در دنیای ارزهای دیجیتال، ماینرها[3] خدمات ضروری را به شبکه ارائه می‌کنند و برای تلاش‌های خود با ارزهای دیجیتال پاداش می‌گیرند. این پاداش‌ها اساساً تولید ارزهای دیجیتال از طریق این فرایند استخراج است. این صنعت به‌دلیل شباهت آن به مفهوم استخراج منابع ارزشمند از زمین، اصطلاح «معدن» را پذیرفت.

---

1. mining
2. Ethereum
3. Miners

باتنت گروهی از دستگاه‌های متصل به اینترنت است که هر کدام یک یا چند ربات را اجرا می‌کنند. از باتنت‌ها می‌توان برای انجام حملات انکار سرویس توزیع‌شده، سرقت داده‌ها، ارسال هرزنامه، و اجازهٔ دسترسی مهاجم به دستگاه و اتصال آن استفاده کرد (Haner & Knake, 2021: 1).[1] مالک می‌تواند باتنت را با استفاده از نرم‌افزار فرمان و کنترل، کنترل کند. کلمهٔ «باتنت» ترکیبی از دو کلمهٔ «ربات» و «شبکه» است. این اصطلاح معمولاً با مفهوم منفی یا مخرب استفاده می‌شود. باتنت مجموعه‌ای منطقی از دستگاه‌های متصل به اینترنت، مانند رایانه‌ها، تلفن‌های هوشمند یا دستگاه‌های اینترنت اشیاست که امنیت آن‌ها نقض شده و کنترل آن به شخص ثالث واگذار شده است. هر دستگاه در معرض خطر، که به‌عنوان «ربات» شناخته می‌شود، زمانی ایجاد می‌شود که یک دستگاه توسط نرم‌افزاری از یک توزیع بدافزار (نرم‌افزار مخرب) نفوذ کند. کنترل‌کنندهٔ یک باتنت قادر است فعالیت‌های این رایانه‌های در معرض خطر را از طریق کانال‌های ارتباطی تشکیل‌شده توسط پروتکل‌های شبکهٔ مبتنی بر استاندارد، مانند گفت‌وگوی اینترنتی و پروتکل انتقال ابرمتن هدایت کند (Bailey et al., 2009: 1) . باتنت‌ها به‌طور فزاینده‌ای توسط مجرمان سایبری به‌عنوان کالا برای مقاصد مختلف، ازجمله به‌عنوان خدمات راه‌انداز و استرس‌زا، اجاره داده می‌شوند[2] (Haner & Knake, 2021: 2). به بیان ساده‌تر، یک باتنت را به‌عنوان گروهی از ربات‌ها تصور کنید که تحت کنترل یک رئیس واحد با هم کار می‌کنند. هر ربات درواقع کامپیوتر یا دستگاهی است که بدون اطلاع مالک به نرم‌افزارهای مخرب آلوده شده است[3] (Ibid: 1). این رئیس که یک هکر یا مجرم سایبری است، می‌تواند به همهٔ این دستگاه‌های آلوده دستور دهد تا وظایف را به‌طور هم‌زمان انجام دهند. مانند داشتن یک کنترل از راه دور برای هر دستگاه فکر کنید، اما هکر به جای روشن کردن تلویزیون، از این دستگاه‌ها برای ارسال ایمیل‌های اسپم[4]، حمله به وب‌سایت‌ها یا

1. “Both states and nonstate actors use botnets to surreptitiously control the combined computing power of infected devices to engage in espionage, hacking, and to carry out distributed denial of service attacks to disable internet connected targets from businesses and banks to power grids and electronic voting systems”.
2. “Botmasters have a strong economic incentive to create and spread these networks because they can be used for identity theft, mining cryptocurrency, credit card fraud, ransomware extortion, DDoS extortion, or sold or rented to the highest bidder”.
3. “Malicious networks of botnets continue to grow in strength as millions of new users and devices connect to the internet each day, many becoming unsuspectingly complicit in cyber-attacks or unwitting accomplices to cybercrimes”.
4. spam

سرقت داده‌ها استفاده می‌کند. قسمت ترسناک این است که صاحبان این دستگاه‌ها نمی‌دانند که ماشین‌هایشان به این شکل استفاده می‌شود. مثل این است که یک مأمور خواب در خانهٔ خود داشته باشید که از خواب بیدار می‌شود و دستورات هکر را اجرا می‌کند. در اصل، بات‌نت شبکه‌ای از رایانه‌های ربوده‌شده است که تحت فرمان یک مقام مرکزی، می‌توانند برای انجام کارهایی معمولاً مضر یا غیرقانونی در اینترنت با یکدیگر همکاری کنند. مهم است که از دستگاه‌های خود با اقدامات امنیتی خوب محافظت کنید تا از تبدیل شدن آن‌ها به یک بات‌نت جلوگیری کنید.

۱-۲-۴. نقش هوش مصنوعی در استخراج غیرمجاز ارزهای دیجیتال از طریق بات‌نت‌ها

هوش مصنوعی می‌تواند نقش چندوجهی در استخراج ارزهای دیجیتال با بات‌نت‌ها برای مهاجمان داشته باشد و توانایی آن‌ها را برای انجام فعالیت‌های استخراج غیرقانونی افزایش دهد:

ـ بهینه‌سازی کارایی و هدف‌گذاری استراتژیک: هوش مصنوعی می‌تواند با افزایش کارایی فرایند استخراج، امکان استفادهٔ مؤثرتر از دستگاه‌های کم‌قدرت را فراهم آورد؛ به‌ویژه زمانی که این دستگاه‌ها در قالب یک بات‌نت به‌کار گرفته می‌شوند. همچنین الگوریتم‌های هوش مصنوعی قادرند حجم گسترده‌ای از داده‌ها را تحلیل و آسیب‌پذیرترین سیستم‌ها را شناسایی کنند تا آن‌ها را برای مقاصد استخراج به شبکهٔ بات‌نت اضافه نمایند (Kurtović et al., 2025: 27).

ـ اتوماسیون حملات: هوش مصنوعی می‌تواند فرایند انتشار بدافزار و مدیریت بات‌نت را خودکار کند و نیاز به مداخلهٔ دستی مهاجمان را کاهش دهد[1] (Fritsch et al., 2023: 41).

– تکنیک‌های فرار: هوش مصنوعی می‌تواند به بات‌نت‌ها کمک کند تا با تغییر پویا رفتارشان یا تقلید از فعالیت‌های عادی کاربر، از شناسایی فرار کنند[2] (Ibid: 43).

– سازگاری در زمان واقعی: هوش مصنوعی می‌تواند توانایی سازگاری بات‌نت‌ها را در زمان واقعی افزایش دهد؛ به این معنا که شبکه قادر خواهد بود همگام با تغییرات بازار ارزهای دیجیتال و

1. “AI’s potential for automation of complex tasks serves as a challenge in the face of defensive deployment of anti-malware AI techniques”.
2. “In particular, the evasion of detection of malware and the exfiltration of information through covert channels have been recently used in AI-powered malware”.

نوسانات سطح دشواری استخراج، عملکرد خود را تنظیم کرده و درنتیجه سودآوری پایدار را حفظ کند (Anandakumar et al., 2023: 46).

در حالی که هوش مصنوعی می‌تواند به‌طور قابل توجهی اثربخشی بات‌نت‌ها را برای استخراج ارزهای دیجیتال افزایش دهد، مهم است که تأکید شود استفاده از بات‌نت برای چنین فعالیت‌هایی غیرقانونی است و جرم سایبری محسوب می‌شود.

۵. ضرورت شناسایی و اعطای شخصیت مستقل به هوش مصنوعی در نظام حقوقی

پیش از تبیین دلایل ضرورت جعل شخصیت برای هوش مصنوعی، لازم است به تعاریف گوناگون این مفهوم و پیامدهای حقوقی ناشی از آن توجه شود. در ادبیات عمومی، هوش مصنوعی در برابر «هوش طبیعی» که ویژهٔ انسان و حیوانات است قرار می‌گیرد؛ با این حال، در حوزه‌های تخصصی هنوز تعریف واحد و مورد اجماعی برای آن ارائه نشده است (Banteka, 2021: 537-596). برای نمونه، مؤسسهٔ مهندسان برق و الکترونیک[1] طی سال‌های اخیر چندین بار اصطلاحات و تعاریف خود دربارهٔ هوش مصنوعی را تغییر داده است. همچنین، گروه کارشناسان ارشد هوش مصنوعی کمیسیون اروپا در سال ۲۰۲۰ با اصلاح تعاریف پیشین، سامانه‌های هوش مصنوعی را سیستم‌های نرم‌افزاری (و گاه سخت‌افزاری) معرفی کرد که توسط انسان طراحی شده و با اهداف پیچیده در بُعد فیزیکی یا دیجیتال عمل می‌کنند و از طریق تفسیر داده‌های جمع‌آوری‌شده، استدلال می‌کنند یا اطلاعات را پردازش می‌نمایند (European Commission, 2021, Art. 3) . اتحادیهٔ اروپا نیز در «قانون هوش مصنوعی» مصوب ۲۰۲۱، با تبعیت ضمنی از این تعریف، هوش مصنوعی را نرم‌افزاری دانست که به‌وسیلهٔ تکنیک‌های یادگیری ماشین، منطق و دانش و تحلیل‌های آماری توسعه یافته و قادر است برای اهداف مشخص‌شده توسط انسان خروجی تولید کند و از طریق توصیه‌ها یا تصمیم‌های خود بر محیط تعامل اثر بگذارد (Artificial Intelligence Act, 2021, Art. 3) .

فارغ از این تعاریف فنی، پرسش اصلی در حوزهٔ حقوقی آن است که جایگاه حقوقی هوش مصنوعی چگونه باید تعیین شود. برخی حقوقدانان آن را همانند بردگان روم باستان تلقی کرده و صرفاً ابزاری در خدمت انسان دانسته‌اند (Bryson, 2010; Sharifi & Birmi, 2018: 27-54) . در مقابل، گروهی دیگر بر این باورند که برخی گونه‌های هوش مصنوعی باید در قالب شخص حقوقی

1. IEEE

طبقه‌بندی شوند (Solum, 1992: 4) . افزون بر این، برخی پژوهشگران با تفکیک میان هوش مصنوعی ضعیف و قوی، تنها نوع قوی را واجد شرایط شناسایی شخصیت حقوقی دانسته‌اند (Schirmbacher & Rechtsanwälte, 2020: 71-78). از یک سو، هوش مصنوعی به‌دلیل برخورداری از نوعی ارادهٔ مستقل به اشخاص حقیقی شباهت می‌یابد و از سوی دیگر، به‌سبب فقدان ماهیت انسانی، باید در زمرهٔ اشخاص حقوقی قرار گیرد، زیرا کرامت انسانی بر پایهٔ ویژگی‌های شخص حقیقی استوار است و نمی‌توان آن را به سامانه‌های غیرانسانی تسری داد(Karimi & Karimi, 2014: 17) .

بر این مبنا، مناسب‌ترین قالب قانونی برای هوش مصنوعی، شناسایی شخصیت حقوقی با مختصات ویژه و از نوع «هوشمند» است. تحقق این رویکرد مستلزم بررسی شرایط لازم برای جعل شخصیت، ازجمله وجود مقتضی و فقدان مانع خواهد بود (Kurki, 2019: 180). تقسیم اشخاص به حقیقی و حقوقی نشان می‌دهد که می‌توان با ایجاد قالبی جدید، هوش مصنوعی را در زمرهٔ اشخاص حقوقی خاص ـ یا همان «اشخاص الکترونیکی» ـ قرار داد و بدین ترتیب زمینهٔ لازم برای بار کردن تکالیف کیفری بر آن فراهم ساخت.

۱-۵. مبانی و مقتضیات جعل شخصیت حقوقی برای هوش مصنوعی

بند حاضر در راستای بررسی مقتضیات لازم برای جعل شخصیت حقوقی هوش مصنوعی، ابتدا به مطالعهٔ روند توسعهٔ این فناوری و پیامدهای آن بر قابلیت تصمیم‌گیری مستقل می‌پردازد، زیرا نخستین پرسش در این زمینه، امکان برخورداری هوش مصنوعی از شخصیت است و پرسش بعدی، نوع و ماهیت چنین شخصیتی خواهد بود. بر همین اساس، در بخش دوم به تحلیل شرایط و الزامات لازم برای تحقق این شخصیت پرداخته می‌شود.

۱-۱-۵. خودمختاری عملی سامانه‌های الکترونیک در پرتو توسعهٔ هوش مصنوعی

هوش مصنوعی با گذر زمان و توسعهٔ شاخه‌هایی همچون یادگیری عمیق و یادگیری ماشین، به سطح بالاتری از استقلال عملی دست یافته است؛ به‌گونه‌ای که امروزه بسیاری از گونه‌های آن واجد حدی از خودمختاری هستند و می‌توانند بدون دخالت مستقیم انسان تصمیم‌گیری و اقدام کنند. نمونه‌هایی نظیر خودروهای هوشمند خودران، بات‌های معامله‌گر مستقل که در بازارهای مالی اقدام به خرید و فروش سهام و رمزارز می‌کنند، ربات‌های نظامی که در برخی مأموریت‌ها به‌طور مستقل عمل

می‌نمایند، پهپادهای خودران مورد استفاده در عملیات اطفای حریق یا کشاورزی و نیز بات‌های تولیدکنندهٔ آثار هنری، همگی بیانگر میزان بالای خودمختاری این فناوری در تصمیم‌گیری‌های کلیدی‌اند. برای نمونه، کاربرد بات‌های معامله‌گر در بازارهای مالی نظیر بورس، فارکس و رمزارز به‌طور گسترده مشاهده می‌شود؛ به‌گونه‌ای که کمیسیون بورس و اوراق بهادار ایالات متحده در سال ۲۰۲۰ گزارش داد حدود ۷۸ درصد معاملات توسط بات‌های هوشمند انجام شده است (U.S. Securities & Exchange Commission, 2020: 1). با پیشرفت فناوری، گونه‌های نوینی از بات‌های مبتنی بر هوش مصنوعی قوی پدیدار شده‌اند که با دریافت سرمایه از کاربر، به‌طور مستقل به تحلیل بازار می‌پردازند و صرفاً اهداف کلی همچون کسب سود بیشتر برای آن‌ها تعیین می‌شود؛ در حالی که نقش کاربر عمدتاً به نظارت بر معاملات و دریافت سود احتمالی محدود می‌گردد (Nakhjavani, 2022: 5).

برخی صاحب‌نظران بر این باورند که تا زمان تدوین معیارهای دقیق برای شناسایی شخصیت هوش مصنوعی، مسئولیت آن باید در چارچوب مسئولیت مطلق تولیدکنندگان و مصرف‌کنندگان مورد بررسی قرار گیرد (Rahbar & Dehghanpour Farashah, 2021: 525). بر همین اساس، از آنجا که هوش مصنوعی بر پایهٔ برنامه‌ریزی مشخص عمل می‌کند، مسئولیت باید متوجه طراحان آن باشد (Mele, 2001: 10). با این حال، توسعهٔ روزافزون فناوری موجب افزایش سطح خودمختاری سامانه‌های هوش مصنوعی شده است؛ به‌گونه‌ای که در بسیاری موارد میان ارادهٔ کاربر یا سازنده و فعل ارتکابی توسط سامانه فاصله ایجاد می‌شود. حتی تولید آثار مبتنی بر جعل عمیق، مقالات جعلی و اطلاعات گمراه‌کننده توسط هوش مصنوعی مسبوق به سابقه است (Nelson, 2023: 1). افزون بر این، سوءاستفادهٔ کاربران با سوءنیت از این فناوری در حوزه‌های مجرمانه نیز رایج شده و ضرورت دارد قانون‌گذاری به نحوی صورت گیرد که افراد نتوانند با استناد به حقوق شخصی خود زمینهٔ سوءاستفاده از این ابزار را فراهم سازند (Karimi & Karimi, 2022: 126).

برخی صاحب‌نظران بر این باورند که می‌توان با تدوین استانداردها و قواعدی مشابه قوانین سه‌گانهٔ آسیموف[1]، تبعیت هوش مصنوعی از اصول رفتاری را تضمین کرد. با این حال، چنین رویکردی نیز نمی‌تواند به‌طور کامل ایمنی این فناوری را تضمین کند، زیرا امکان دارد سازندگان از این قواعد پیروی نکنند یا با ارائهٔ تفاسیر متفاوت از آن‌ها، نتایج متعارضی پدید آید. برای نمونه، بنا

1. Asimov’s Law of Robotics

بر گزارش رئیس بخش آزمایش نیروی هوایی ایالات متحده، در جریان آزمایش یک پهپاد نظامی مبتنی بر هوش مصنوعی، که مأموریت اصلی آن انهدام اهداف تعیین‌شده بود و اختیار لغو یا ادامهٔ عملیات درنهایت به اپراتور انسانی واگذار شده بود، پهپاد به‌دلیل برنامه‌ریزی اولیه برای تخریب اهداف، دستور اپراتور انسانی را مانعی در اجرای مأموریت تلقی کرد و به سمت او حمله‌ور شد (Tuhin Das Mahapatra, 2023: 1). از این رو، بحث مسئولیت‌پذیری در قبال عملکردهای متنوع هوش مصنوعی ازجمله پهپادهای نظامی خودران، بات‌های تجاری و خودروهای هوشمند به‌طور جدی مطرح می‌شود (Chopra & White, 2007: 1-17). با این حال، انتساب مسئولیت صرفاً به طراحان و مالکان این فناوری به‌دلیل نقش آنان در تعیین الگوهای رفتاری، همواره موجه به‌نظر نمی‌رسد، زیرا بسیاری از سامانه‌های هوش مصنوعی پیشرفته قادرند الگوهای رفتاری جدید را به‌طور مستقل فراگیرند و از چارچوب‌های اولیه طراحی فراتر روند.

۲-۱-۵. شرایط لازم برای جعل شخصیت حقوقی هوش مصنوعی

بند حاضر به بررسی امکان برخورداری هوش مصنوعی از دارایی مستقل و همچنین قابلیت رسیدگی قضائی به دعاوی مطرح‌شده علیه آن می‌پردازد؛ امری که می‌تواند به‌عنوان یکی از شرایط اساسی در جعل شخصیت حقوقی برای این فناوری تلقی شود.

۱-۲-۱-۵. استقلال مالی و امکان دارایی مثبت و منفی برای شخصیت هوش مصنوعی

دارایی به مجموعه‌ای از اموال، مطالبات و دیون اطلاق می‌شود که می‌تواند به صورت مثبت (اموال و مطالبات) یا منفی (دیون) جلوه‌گر شود (Jafari Langroudi, 2022: 90) . با پیشرفت‌های فناورانه، امکان فرض دارایی مستقل برای هوش مصنوعی مطرح شده است، برای مثال بات‌های معامله‌گر خودمختار قادرند با دریافت سرمایهٔ اولیه از کاربر، به انعقاد معاملات بپردازند و سودآوری کنند. در صورت پذیرش دارایی و اموال برای هوش مصنوعی و اعطای مالکیت به آن، می‌توان مالیات بر این دارایی‌ها وضع کرد و حتی با کاهش مالیات در مواردی که به‌جای ربات‌ها نیروی انسانی استخدام می‌شود، ابزاری برای مدیریت رقابت شغلی میان انسان و ربات فراهم آورد (King et al., 2017: 56) . برخی از چهره‌های برجستهٔ اقتصادی، ازجمله بیل گیتس، نیز از ایدهٔ افزایش مالیات بر ربات‌هایی که جایگزین نیروی انسانی می‌شوند حمایت کرده‌اند (Delaney, 2017: 1) . در مقابل، گروهی دیگر

بر این باورند که چنین سیاستی می‌تواند آثار منفی بر رقابتی بودن بازار داشته باشد و درنهایت به کاهش بهره‌وری فناوری منجر شود (Prodhan, 2017: 1).

۲-۲-۱-۵. قابلیت دادرسی و اجرای احکام علیه شخصیت حقوقی هوش مصنوعی

یکی از اساسی‌ترین جنبه‌های اعطای شخصیت به هوش مصنوعی، امکان طرح دعوا به نفع یا علیه آن است. این قابلیت در مقررات مدنی رباتیک اتحادیهٔ اروپا[1] نیز مورد تأکید قرار گرفته است (EU Resolution, 2018: 12). پرسش اصلی آن است که آیا بهره‌برداران یا سازندگان این فناوری می‌توانند مستقیماً مسئول شناخته شوند و دعاوی حقوقی علیه آنان اقامه شود (Joizil et al., 2022: 2) . برخی حقوقدانان و حتی نظام‌های حقوقی، فرض مسئولیت را متوجه سازندگان دانسته‌اند؛ برای نمونه، اتحادیهٔ اروپا مسئولیت مطلق را برای اپراتورهای هوش مصنوعی پرخطر پیش‌بینی کرده است. براساس این رویکرد، اپراتورها مکلف به جبران خسارات ناشی از عملکرد سامانه‌های مبتنی بر هوش مصنوعی خواهند بود، حتی در شرایطی که اقدامات لازم برای تضمین ایمنی آن‌ها صورت گرفته باشد (European Parliament, 2020/2014(INL). با این حال، چالش‌هایی همچون عدم امکان درک کامل فرایند تفسیر دستورها، تصمیم‌گیری و اجرای آن‌ها توسط سامانه‌های خودمختار هوش مصنوعی از سوی سازندگان، می‌تواند تحقق عدالت حقوقی را با مشکل مواجه سازد، زیرا در بسیاری از موارد حتی سازندگان نیز از نحوهٔ تحلیل داده‌ها و نتیجه‌گیری این سامانه‌ها آگاهی دقیق ندارند. برای نمونه، بررسی سامانهٔ «کامپَس»[2] که به‌عنوان یک سیستم مبتنی بر هوش مصنوعی در دادگاه‌های ایالات متحده برای ارزیابی احتمال تکرار جرم مورد استفاده قرار می‌گیرد، نشان داد که سیاه‌پوستان در مقایسه با سفیدپوستان کمتر مشمول آزادی موقت می‌شوند؛ هرچند رنگ پوست به‌طور رسمی در معیارهای تصمیم‌گیری این سامانه لحاظ نشده بود (University of Helsinki, 2019: 2).

علاوه بر این، روند طرح دعاوی علیه شرکت‌های توسعه‌دهنده به‌دلیل عملکردهای ناشی از هوش مصنوعی رو به افزایش است؛ موضوعی که ضرورت اعطای شخصیت مستقل به برنامه‌های هوش مصنوعی و جداسازی آن‌ها از مسئولیت مستقیم سازندگان را برجسته‌تر می‌سازد. برای نمونه، دو نویسندهٔ رمان‌های پرفروش در سال ۲۰۲۳ با این ادعا که دسترسی رایگان کاربران به خلاصهٔ آثارشان

1. Civil Law Rules on Robotics
2.Correctional Offender Management Profiling for Alternative Sanction (COMPAS)

در چت‌جی‌پی‌تی[1] موجب کاهش قابل توجه فروش کتاب‌ها شده است، شکایتی را علیه شرکت توسعه‌دهندهٔ این فناوری در دادگاه‌های ایالات متحده مطرح کردند (Mona Awad & Paul Tremblay VS Open AI co, 2023). همچنین در جریان شکایتی گسترده علیه شرکت اوپن‌ای‌آی،[2] درخواست توقف توسعهٔ چت‌جی‌پی‌تی تا زمان روشن شدن مخاطرات احتمالی هوش مصنوعی ارائه شد (Winshel, 2023: 1).

نتیجه‌گیری

تحولات سریع در حوزهٔ هوش مصنوعی و گسترش کاربردهای آن در عرصه‌های اجتماعی، امنیتی و اقتصادی، ضرورت بازنگری در مبانی بزه‌انگاری و سازوکارهای تقنینی را بیش‌ازپیش آشکار کرده است. در چنین شرایطی، این پژوهش درپی پاسخ به این پرسش بود که آیا نظام حقوق کیفری ایران توانایی لازم برای مواجهه با جرائم نوظهور مبتنی بر هوش مصنوعی را دارد یا خیر. بررسی‌های انجام‌شده نشان داد که چارچوب‌های موجود حقوق کیفری، به‌ویژه در حوزهٔ جرم‌انگاری رفتارهای فناورانه و تعیین حدود مسئولیت، از انسجام و کفایت لازم برخوردار نیستند. قوانین فعلی عمدتاً بر مبنای رفتارهای انسانی تدوین شده‌اند و توانایی تطبیق با شرایطی را که در آن سامانه‌های هوشمند به‌طور مستقل تصمیم‌گیری و اقدام می‌کنند، ندارند.

یافته‌های تحقیق فرضیهٔ اصلی را تأیید کردند؛ بدین معنا که مقررات کنونی در برابر تصمیمات خودکار و خودمختار سامانه‌های هوش مصنوعی با خلأ جدی مواجه‌اند. این خلأ نه‌تنها در سطح تعریف جرم بلکه در سطح انتساب مسئولیت کیفری نیز آشکار است، برای مثال در مواردی که یک سامانهٔ هوشمند اقدام به تولید محتوای جعلی یا اجرای حملهٔ سایبری می‌کند، قوانین موجود قادر به تعیین دقیق مسئولیت و شناسایی عنصر معنوی جرم نیستند. از این رو، نظام حقوق کیفری ایران نیازمند بازنگری اساسی در مفاهیم بنیادین خود است تا بتواند با واقعیت‌های جدید فناوری هماهنگ شود. این نتیجه بیانگر آن است که نظام حقوق کیفری ایران در برابر تحولات فناورانه، به‌ویژه در حوزهٔ هوش مصنوعی، فاقد ابزارهای تقنینی کارآمد برای جرم‌انگاری و پاسخ‌گویی مؤثر است. به عبارت دیگر، چارچوب‌های سنتی که بر عقل، اراده و قصد انسانی بنا شده‌اند، در مواجهه با فناوری‌های

1. ChatGPT
2. OpenAI

خودمختار ناکارآمدی خود را نشان داده‌اند. بنابراین، ضرورت دارد که قانون‌گذار با تدوین مقررات نوین، هم امکان جرم‌انگاری مستقل تهدیدات ناشی از هوش مصنوعی را فراهم سازد و هم سازوکارهای جدیدی برای انتساب مسئولیت کیفری در شرایطی که تصمیمات توسط سامانه‌های هوشمند اتخاذ می‌شود، پیش‌بینی کند. تنها در این صورت است که می‌توان از یک سو امنیت دیجیتال شهروندان را تضمین کرد و از سوی دیگر مسیر توسعهٔ مسئولانهٔ فناوری‌های هوش مصنوعی را هموار ساخت.

نوآوری اصلی این پژوهش در ارائهٔ یک نقشه‌راه برای بزه‌انگاری تهدیدات نوظهور ناشی از هوش مصنوعی است؛ بدین معنا که برای نخستین‌بار مجموعه‌ای از مصادیق در چهار حوزهٔ کلیدی؛ جرائم علیه اشخاص، امنیت، اموال (حقوق مالی) و فناوری‌های خودران با رویکردی نظام‌مند و هم‌زمان نظری و کاربردی تحلیل شده‌اند. در حوزهٔ جرائم علیه تمامیت اشخاص، تمرکز بر جعل عمیق، دستکاری چهره، صوت و فیشینگ هوشمند نشان داد که آسیب به حریم خصوصی، حیثیت و خودمختاری فردی در مقیاسی بی‌سابقه ممکن است و جرم‌انگاری مستقل با تعریف عناصر مادی و معنوی خاص این رفتارها ضرورت پیدا می‌کند. در حوزهٔ تهدید امنیت، حملات تقویت‌شده با یادگیری ماشین علیه زیرساخت‌های حیاتی، از حملات تطبیقی تا اکتشاف خودکار رخنه‌ها، نشان دادند که صرف اتکا به دسته‌بندی‌های سنتی جرائم رایانه‌ای پاسخ‌گو نیست و نیاز به تعریف حقوقی «جرم سایبری تقویت‌شده با هوش مصنوعی» و سازوکارهای شناسایی و بازدارندگی متناسب وجود دارد. در حوزهٔ اموال، باج‌افزارهای هوشمند، استخراج غیرقانونی ارز دیجیتال مبتنی بر بات‌نت و تقلب‌های الگوریتمی در تراکنش‌ها، شکاف‌های کیفرگذاری و بی‌اثری نسبی سازوکارهای سنتی بازدارندگی را آشکار کردند. نهایتاً در حوزهٔ فناوری‌های خودران و سلاح‌های خودمختار، مسئلهٔ تصمیم‌گیری مستقل سامانه و توزیع مسئولیت بین طراح، بهره‌بردار و سیستم هوشمند، ضرورت رژیم‌های مسئولیت ترکیبی و قواعد خاص منع و کنترل را برجسته ساخت.

بررسی‌ها نشان داد که یکی از چالش‌های اساسی در مواجهه با تهدیدات نوظهور هوش مصنوعی، ناکارآمدی قواعد سنتی مسئولیت کیفری در برابر سطح بالای خودمختاری سامانه‌های هوشمند است. فاصلهٔ روزافزون میان ارادهٔ انسان و رفتار نهایی این سامانه‌ها، ضرورت بازاندیشی در مبانی انتساب مسئولیت و حتی امکان شناسایی نوعی شخصیت حقوقی ویژه برای هوش مصنوعی را برجسته می‌کند؛ رویکردی که با تکیه بر مفاهیمی چون استقلال مالی، قابلیت دادرسی و مسئولیت

لایه‌ای، می‌تواند چارچوبی واقع‌بینانه‌تر برای تنظیم‌گری و پاسخ کیفری فراهم سازد. این چارچوب، به‌جای برخورد موردی یا صرفاً فنی، با تلفیق تحلیل مفهومی (بازتعریف عنصر معنوی، قصد و تقصیر در بستر تصمیم‌گیری خودکار) و اقتراح تقنینی (طراحی عناوین مجرمانه مستقل، عناصر قانونی و حدود مسئولیت)، نشان می‌دهد که قواعد سنتی مبتنی بر انسانِ دارای عقل و اراده، برای مواجهه با کنش‌های غیرانسانیِ خودمختار کافی نیستند. افزون بر این، پژوهش با مقایسهٔ تطبیقی رویکردهای خارجی و اقتباس سنجیدهٔ مؤلفه‌هایی که با بستر حقوقی ایران سازگارند، یک چارچوب نظری برای طراحی مقررات آینده ارائه کرده است: تعریف‌های قانونی شفاف برای جرائم تقویت‌شده با هوش مصنوعی، معیارهای احراز عنصر معنوی در تصمیمات خودکار، رژیم مسئولیت ترکیبی و استانداردهای دقت و ایمنی برای توسعه و استقرار سامانه‌های هوشمند. این چارچوب به‌منزلهٔ نقشهٔ عمل تقنینی، مسیر تازه‌ای برای مطالعات حقوقی در پیوند با هوش مصنوعی می‌گشاید: از تدوین مواد مستقل و آیین‌های اثبات تخصصی، تا سازوکارهای نظارتی و همکاری‌های بین‌المللی. به این ترتیب، نوآوری پژوهش صرفاً در شناسایی خلأها خلاصه نمی‌شود، بلکه با ارائهٔ مدل مفهومی و تقنینی قابل‌اجرا، گذار از پارادایم سنتی به نظم کیفری سازگار با فناوری‌های خودمختار را امکان‌پذیر می‌کند.

بررسی مصادیق نشان داد که در حوزهٔ جرائم علیه اشخاص، نمونه‌هایی همچون جعل عمیق (دیپ‌فیک) و فیشینگ هوشمند، به‌طور جدی بنیان‌های سنتی حمایت کیفری از حیثیت، آبرو و امنیت فردی را به چالش کشیده‌اند. جعل عمیق با بهره‌گیری از الگوریتم‌های یادگیری عمیق قادر است تصاویر و ویدئوهای کاملاً مشابه واقعیت تولید کند و از این طریق، امکان تخریب شخصیت، انتشار اکاذیب یا سوءاستفاده‌های اخلاقی را فراهم سازد. فیشینگ هوشمند نیز با استفاده از تحلیل داده‌های رفتاری قربانیان، حملات هدفمند و شخصی‌سازی‌شده‌ای را طراحی می‌کند که احتمال فریب را به‌طور چشمگیری افزایش می‌دهد. قوانین موجود تنها به‌طور پراکنده و غیرمستقیم قابلیت انطباق با این جرائم را دارند و نمی‌توانند به‌طور کامل از حقوق فردی حمایت کنند؛ از این رو، جرم‌انگاری مستقل و صریح این رفتارها ضرورت دارد. در حوزهٔ جرائم علیه امنیت، نبود تعریف قانونی روشن از «جرم سایبری تقویت‌شده با هوش مصنوعی» تهدیدی جدی برای زیرساخت‌های حیاتی کشور محسوب می‌شود. حملات سایبری مبتنی بر هوش مصنوعی می‌توانند با سرعت و دقتی فراتر از توان انسان، آسیب‌های گسترده‌ای به شبکه‌های انرژی، حمل‌ونقل، ارتباطات و سامانه‌های

دفاعی وارد کنند. فقدان چارچوب قانونی مشخص برای شناسایی و مقابله با این نوع جرائم، نه‌تنها موجب سردرگمی در فرایند دادرسی می‌شود بلکه امنیت ملی را به‌طور مستقیم تحت تأثیر قرار می‌دهد. بنابراین، ضرورت دارد قانون‌گذار با تعریف دقیق این دسته از جرائم و تعیین عناصر قانونی آن‌ها، امکان واکنش سریع و مؤثر نظام کیفری را فراهم سازد. در حوزهٔ جرائم علیه اموال (حقوق مالی)، مصادیقی همچون باج‌افزارهای هوشمند و استخراج غیرقانونی ارز دیجیتال با استفاده از بات‌نت‌ها نشان دادند که چارچوب‌های سنتی بازدارندگی و مجازات پاسخ‌گوی پیچیدگی‌های ناشی از هوش مصنوعی نیستند. باج‌افزارهای مبتنی بر هوش مصنوعی قادرند به‌طور پویا روش‌های رمزگذاری و اخاذی خود را تغییر دهند و شناسایی آن‌ها را دشوار سازند. استخراج غیرقانونی ارز دیجیتال نیز با بهره‌گیری از شبکه‌های گستردهٔ بات‌نت، خسارت‌های مالی هنگفتی به کاربران و شرکت‌ها وارد می‌کند. قوانین موجود که عمدتاً بر سرقت سنتی یا کلاهبرداری کلاسیک تمرکز دارند، توانایی مقابله با این جرائم پیچیده و فناورانه را ندارند و نیازمند قواعد نوین و اختصاصی هستند. همچنین، در حوزهٔ فناوری‌های خودران و سلاح‌های خودمختار، فقدان رژیم مسئولیت ترکیبی میان عامل انسانی و سامانهٔ هوشمند خلأ تقنینی آشکاری ایجاد کرده است. خودروهای خودران یا سلاح‌های خودمختار می‌توانند بدون دخالت مستقیم انسان تصمیماتی اتخاذ کنند که پیامدهای کیفری گسترده‌ای داشته باشد؛ از تصادفات مرگبار گرفته تا حملات نظامی خارج از کنترل انسانی. در چنین شرایطی، پرسش اساسی آن است که مسئولیت کیفری بر عهدهٔ چه کسی قرار می‌گیرد؟ نبود پاسخ روشن به این پرسش، نظام کیفری را در وضعیت بلاتکلیفی قرار داده و ضرورت تدوین مقررات ویژه و مستقل را دوچندان ساخته است. این مقررات باید بتوانند مسئولیت را میان عامل انسانی و فناوری به‌صورت ترکیبی تقسیم کنند و از بروز خلأهای حقوقی در مواجهه با جرائم ناشی از فناوری‌های خودمختار جلوگیری نمایند.

درنهایت، پژوهش حاضر تأکید می‌کند که ثبات حقوقی در برابر پویایی فناوری تنها با رویکردی میان‌رشته‌ای و آینده‌نگر محقق می‌شود؛ رویکردی که بر پایهٔ پژوهش‌های دانشگاهی، مشارکت فعال نهادهای اجرایی و تعامل مستمر با جامعهٔ فناوران بنا شود. بدین ترتیب، نظام حقوق کیفری ایران باید در توازن میان حفظ نوآوری و صیانت از حقوق فردی و جمعی بازطراحی شود تا هم امنیت دیجیتال شهروندان تضمین شود و هم مسیر توسعهٔ فناوری‌های هوش مصنوعی مسدود نشود. این نتیجه‌گیری نشان می‌دهد که آیندهٔ حقوق کیفری ایران در گرو پذیرش واقعیت‌های فناورانه و ایجاد چارچوب‌های

تقنینی نوین است؛ چارچوب‌هایی که نه‌تنها پاسخ‌گوی تهدیدات نوظهور باشند، بلکه زمینه‌ساز توسعهٔ پایدار و مسئولانه فناوری‌های هوش مصنوعی نیز شوند.

پیشنهادها

یافته‌های پژوهش حاضر نشان داد که چارچوب‌های موجود حقوق کیفری ایران در مواجهه با جرائم نوظهور مبتنی بر هوش مصنوعی، به‌ویژه در حوزه‌های انتساب مسئولیت، عنصر معنوی و قصد مجرمانه، با خلأهای جدی روبه‌روست. این خلأها نه‌تنها موجب پراکندگی و عدم انسجام در مقررات موجود می‌شوند، بلکه امکان بهره‌برداری مجرمانه از ظرفیت‌های خودکار و مقیاس‌پذیر فناوری‌های هوش مصنوعی را نیز تسهیل می‌کنند. ازاین‌رو، ارائهٔ پیشنهادهای تقنینی مشخص و تدوین مواد قانونی مستقل، ضرورتی انکارناپذیر برای تضمین عدالت کیفری، صیانت از امنیت ملی و حمایت از حقوق فردی و جمعی است. پیشنهادهای زیر بر پایهٔ تحلیل‌های نظری و تطبیقی، و با الهام از تجربه‌های تقنینی بین‌المللی، به‌عنوان پیش‌نویس مواد قانونی ارائه می‌شوند. هدف آن‌ها ایجاد چارچوبی منسجم و آینده‌نگر برای جرم‌انگاری رفتارهای فناورانهٔ نوظهور، تعیین مسئولیت کیفری در حوزهٔ سامانه‌های خودمختار و تقویت کارآمدی نظام حقوق کیفری ایران در برابر تهدیدات ناشی از هوش مصنوعی است.

با توجه به خلأهای شناسایی‌شده در نظام حقوق کیفری ایران در مواجهه با جرائم نوظهور مبتنی بر هوش مصنوعی، این پژوهش مجموعه‌ای از پیش‌نویس مواد قانونی پیشنهادی را ارائه می‌کند که می‌تواند مبنای اصلاح و توسعهٔ تقنینی در آینده قرار گیرد.

۱. جرم‌انگاری دیپ‌فیک در نظام حقوق کیفری ایران

مادهٔ قانونی پیشنهادی: هر شخصی که با استفاده از فناوری‌های هوش مصنوعی یا هر وسیلهٔ دیگری، تصاویر، صداها، ویدئوها یا هر نوع محتوای دیجیتال دیگری را به نحوی تغییر دهد که به ایجاد یک نمایش غیرواقعی و فریبنده منجر شود و این عمل به قصد آسیب رساندن به شخصیت، حیثیت، حقوق مالی یا معنوی اشخاص حقیقی یا حقوقی انجام گیرد، به‌عنوان مرتکب جرم دیپ‌فیک شناخته شده و به مجازات مقرر در این قانون محکوم خواهد شد.

تبصرهٔ ۱: در صورتی که این عمل منجر به آسیب جدی به شخصیت، حیثیت، حقوق مالی یا معنوی اشخاص شود، مرتکب به حداکثر مجازات مقرر در این قانون محکوم خواهد شد.

تبصرهٔ ۲: استفاده از فناوری دیپ‌فیک برای اهداف آموزشی، تحقیقاتی، هنری و خبری که به‌منظور فریب و آسیب رساندن به اشخاص نباشد، از شمول این قانون خارج است.

۲. جرم‌انگاری حملات فیشینگ در حقوق کیفری ایران

مادهٔ قانونی پیشنهادی: هرگاه شخصی با استفاده از روش‌های فریبنده ازقبیل ایجاد صفحات وب جعلی، ارسال ایمیل‌های گمراه‌کننده، پیام‌های متنی یا هر وسیلهٔ ارتباطی دیگر، با قصد کلاهبرداری یا تحصیل غیرقانونی اطلاعات شخصی، مالی یا امنیتی افراد اقدام به حملهٔ فیشینگ کند، مرتکب جرم محسوب شده و به مجازات‌های زیر محکوم می‌شود:

الف) حبس تعزیری درجهٔ ۶ (بیش از شش ماه تا دو سال)؛

ب) مصادرهٔ اموال و منافع ناشی از جرم به‌عنوان مجازات تکمیلی؛

ج) محرومیت از استفاده از خدمات رایانه‌ای و اینترنتی به مدت دو تا پنج سال (در قالب محرومیت از حقوق اجتماعی درجهٔ ۶).

تبصرهٔ ۱: در صورتی که حملهٔ فیشینگ به آسیب جدی به امنیت ملی، اقتصاد کشور یا سلامت روانی اشخاص منجر شود، مرتکب به اشد مجازات مقرر در این ماده محکوم خواهد شد.

تبصرهٔ ۲: هرگونه اقدام به حملهٔ فیشینگ که به تحصیل اطلاعات منجر نشود، لیکن قصد کلاهبرداری یا فریب آشکار باشد، به‌عنوان شروع به جرم تلقی شده و مرتکب به مجازات‌های متناسب با آن محکوم می‌شود.

۳. جرم‌انگاری استفاده از سلاح‌های خودمختار مبتنی بر هوش مصنوعی

مواد قانونی پیشنهادی:

مادهٔ ۱ ـ استفاده از سلاح‌های خودمختار مبتنی بر هوش مصنوعی که قابلیت تصمیم‌گیری و اجرای عملیات نظامی به‌صورت مستقل دارند و به نقض حقوق بشردوستانهٔ بین‌المللی یا مقررات ناظر بر مخاصمات مسلحانه منجر شوند، ممنوع بوده و جرم محسوب می‌شود.

مادهٔ ۲ ـ هر شخص حقیقی یا حقوقی که در تولید، طراحی، توزیع، فروش، واردات، صادرات، نگهداری یا بهره‌برداری از سلاح‌های موضوع مادهٔ ۱ مشارکت یا مباشرت ورزد، به مجازات تعزیری درجهٔ ۵ محکوم خواهد شد.

مادهٔ ۳ ـ در صورتی که استفاده از سلاح‌های خودمختار به ایراد صدمهٔ جسمی یا قتل اشخاص منجر شود، مرتکب علاوه بر مجازات‌های مقرر در مادهٔ ۲، به مجازات‌های مقرر در قانون مجازات اسلامی برای قتل یا جرح عمدی محکوم خواهد شد.

مادهٔ ۴ ـ چنانچه سازندگان یا برنامه‌ریزان اثبات کنند که تمامی اقدامات لازم برای پیشگیری از ارتکاب جرم توسط سامانهٔ هوش مصنوعی را انجام داده‌اند و وقوع جرم ناشی از نقص غیرقابل پیش‌بینی در سیستم بوده است، مسئولیت کیفری به سامانهٔ هوش مصنوعی منتسب خواهد شد.

تبصره: به‌منظور پوشش خسارت‌های ناشی از خطاهای غیرقابل پیش‌بینی سامانه‌های هوش مصنوعی، صندوق‌های بیمه‌ای ویژهٔ خودروهای خودران ایجاد می‌شود و جبران خسارت از طریق این صندوق‌ها یا بیمه‌های اختصاصی انجام خواهد شد.

مادهٔ ۵ ـ دولت مکلف است نظارت مستمر و دقیق بر توسعه، تولید و استفاده از فناوری‌های هوش مصنوعی در حوزهٔ نظامی اعمال و تضمین کند که هرگونه بهره‌برداری از این فناوری‌ها با اصول حقوق بشر و قواعد حقوق بین‌الملل بشردوستانه مطابقت دارد.

مادهٔ ۶ ـ هرگونه تغییر، اصلاح یا ارتقا در سلاح‌های خودمختار مبتنی بر هوش مصنوعی که احتمالاً به نقض مقررات این قانون منجر شود، باید پیش از اجرا به تأیید مراجع قانونی ذی‌صلاح برسد.

۴. جرم‌انگاری رفتارهای ناشی از هوش مصنوعی در خودروهای خودران

مادهٔ قانونی پیشنهادی: هرگاه در نتیجهٔ خطا یا اختلال ناشی از سامانهٔ هوش مصنوعی به‌کاررفته در خودروهای خودران، قتل یا صدمهٔ بدنی واقع شود و این خطا ناشی از برنامه‌ریزی یا طرح‌ریزی قبلی مهندسان یا کاربران نباشد، مسئولیت کیفری به سامانهٔ هوش مصنوعی منتسب خواهد شد. در این موارد، علاوه بر الزام به جبران خسارت وارده، ضمانت اجراهای کیفری متناسب با شدت جرم بر سامانهٔ مذکور اعمال می‌شود. در صورتی که امکان اجرای مستقیم مجازات نسبت به سامانه وجود

نداشته باشد، مسئولیت کیفری به‌صورت ترکیبی بر عهدهٔ مالک، بهره‌بردار یا نهاد متولی سامانه قرار خواهد گرفت.

تبصرهٔ ۱: در صورتی که خطا ناشی از نقص طراحی یا تولید باشد، مسئولیت کیفری و مدنی بر عهدهٔ شرکت سازنده یا مالک خودرو قرار خواهد گرفت.

تبصرهٔ ۲: به‌منظور پوشش خسارت‌های ناشی از خطاهای غیرقابل پیش‌بینی سامانه‌های هوش مصنوعی، صندوق‌های بیمه‌ای ویژه خودروهای خودران ایجاد می‌شود و جبران خسارت از طریق این صندوق‌ها یا بیمه‌های اختصاصی انجام خواهد شد.

۵. جرم‌انگاری حملات سایبری مبتنی بر هوش مصنوعی

مادهٔ قانونی پیشنهادی: هرگاه شخصی با بهره‌گیری از هوش مصنوعی یا سامانه‌های خودکار، مرتکب دستکاری، تخریب، دسترسی غیرمجاز، اختلال یا ایجاد وقفه در سامانه‌های رایانه‌ای، شبکه‌های اطلاع‌رسانی، زیرساخت‌های حیاتی یا داده‌های شخصی شود، به مجازات حبس و جزای نقدی درجهٔ ۵ محکوم خواهد شد. در صورتی که این اقدامات به آسیب جدی به اشخاص، امنیت ملی یا اقتصاد کشور منجر شود، مرتکب به حداکثر مجازات مقرر محکوم می‌شود.

تبصرهٔ ۱: در مواردی که سامانهٔ هوش مصنوعی بدون دخالت مستقیم انسان و به‌صورت خودکار مرتکب جرم شود، مسئولیت کیفری بر عهدهٔ طراح، برنامه‌نویس، مالک یا بهره‌بردار سامانه خواهد بود؛ مگر آنکه ثابت شود وقوع جرم ناشی از عوامل خارج از اراده و پیش‌بینی آنان بوده است.

تبصرهٔ ۲: استفاده از هوش مصنوعی برای مقاصد دفاعی، امنیتی یا انجام وظایف قانونی توسط دولت و نهادهای ذی‌صلاح، مشروط به رعایت قوانین و مقررات مربوط، از شمول این ماده خارج است.

۶. جرم‌انگاری باج‌افزارهای مبتنی بر هوش مصنوعی

مادهٔ قانونی پیشنهادی: هرگاه شخصی با بهره‌گیری از هوش مصنوعی یا سایر فناوری‌های مرتبط، اقدام به طراحی، توسعه، انتشار، توزیع یا کنترل نرم‌افزارهای باج‌افزاری کند، یا به هر نحو از این نرم‌افزارها برای تهدید، اعمال فشار یا اخاذی از اشخاص حقیقی یا حقوقی استفاده کند، مرتکب جرم باج‌افزار محسوب می‌شود.

تبصره: در صورتی که اقدامات مذکور به آسیب یا اختلال جدی در سامانه‌های حیاتی، زیرساخت‌های ملی یا امنیت عمومی منجر شود، مرتکب به اشد مجازات مقرر محکوم خواهد شد.

۷. جرم‌انگاری استخراج ارز دیجیتال با استفاده از بات‌نت‌ها و هوش مصنوعی

مادۀ قانونی پیشنهادی: هرگاه شخصی با استفاده از هوش مصنوعی یا بات‌نت‌ها، بدون اخذ مجوز قانونی از مراجع ذی‌صلاح، اقدام به استخراج ارز دیجیتال کند، مرتکب جرم استخراج غیرمجاز ارز دیجیتال محسوب می‌شود.

پیشنهادهای قانونی مطرح‌شده در این پژوهش، با توجه به ماهیت تهدیدات نوظهور ناشی از هوش مصنوعی، در دو سطح قابل پیگیری است. نخست، در مواردی که رفتارهای جدید را می‌توان ذیل جرائم رایانه‌ای یا جرائم سنتی موجود قرار داد، اصلاح یا الحاق مواد قانونی کفایت می‌کند. برای نمونه، جعل عمیق (دیپ‌فیک) را می‌توان با افزودن تبصره‌ای به مادۀ ۶ قانون جرائم رایانه‌ای یا مادۀ ۱۶ همان قانون، به‌طور صریح و شفاف جرم‌انگاری کرد. این رویکرد ضمن حفظ انسجام نظام تقنینی موجود، امکان پاسخ‌گویی به بخشی از تهدیدات فناورانه را فراهم می‌سازد. در مقابل، در حوزه‌هایی که تهدیدات ماهیت کاملاً جدید دارند و چارچوب‌های موجود توانایی پاسخ‌گویی به آن‌ها را ندارند، تدوین قانون مستقل ضرورت می‌یابد. نمونۀ بارز این وضعیت را می‌توان در زمینۀ سلاح‌های خودمختار مرگبار و خودروهای خودران مشاهده کرد؛ فناوری‌هایی که تصمیمات الگوریتمی آن‌ها مسئولیت کیفری را با ابهام جدی مواجه ساخته است. در چنین مواردی، ایجاد یک رژیم تقنینی مستقل و جامع، نه‌تنها برای تعیین حدود مسئولیت کیفری بلکه برای تضمین انطباق با اصول حقوق بشردوستانه و عدالت کیفری، اجتناب‌ناپذیر است.

مواد قانونی پیشنهادی این پژوهش، با تمرکز بر جرائم نوظهور مبتنی بر هوش مصنوعی، تلاشی است برای پر کردن شکاف‌های تقنینی موجود در نظام حقوق کیفری ایران. این پیشنهادها نه‌تنها به جرم‌انگاری صریح رفتارهایی چون دیپ‌فیک، فیشینگ پیشرفته، باج‌افزار و استخراج غیرقانونی ارز دیجیتال می‌پردازند، بلکه ابعاد جدیدی از مسئولیت کیفری در حوزۀ فناوری‌های خودران و خودمختار، ازجمله خودروهای خودران و سلاح‌های هوشمند، را نیز روشن می‌سازند. پیش‌بینی مقررات ویژه برای حملات سایبری تقویت‌شده با هوش مصنوعی و تعیین مسئولیت ترکیبی میان عامل انسانی و سامانه‌های هوشمند، نشان‌دهندۀ ضرورت بازتعریف مفاهیم بنیادین حقوق کیفری

همچون «عنصر معنوی» و «قصد» در مواجهه با تصمیمات خودکار است. این مواد پیشنهادی، علاوه بر ایجاد انسجام تقنینی، می‌توانند عدالت کیفری را تضمین کنند، امنیت ملی و اجتماعی را تقویت سازند و از سوءاستفاده‌های فناورانه جلوگیری کنند. درنهایت، باید تأکید کرد که این پیش‌نویس‌ها نقطهٔ آغاز برای گفت‌وگوی علمی و تقنینی میان دانشگاهیان، قانون‌گذاران و نهادهای اجرایی هستند. تصویب و اجرای چنین مقرراتی نیازمند بررسی دقیق، اجماع کارشناسی و هماهنگی با استانداردهای بین‌المللی است تا نظام حقوق کیفری ایران بتواند همگام با تحولات فناورانه، کارآمدی خود را در مدیریت ریسک‌های نوظهور حفظ کند.

حامی مالی:

این مقاله هیچ حامی مالی ندارد.

مشارکت نویسندگان:

سعید قماشی: م فهوم‌سازی، نظارت بر داده‌ها، اعتبارسنجی، مدیریت پروژه، منابع.

محمدرضا کاملی و مجتبی نیکوکلام ندیم: روش‌شناسی، تحلیل، نوشتن بررسی و ویرایش، تحقیق و بررسی، پیش‌نویس اصلی.

تعارض منافع:

بنا بر اظهار نویسندگان این مقاله تعارض منافع ندارد.

ملاحظات اخلاقی:

این پژوهش بر پایهٔ مطالعهٔ اسناد، قوانین، رویه‌های قضائی و منابع کتابخانه‌ای انجام شده و در آن هیچ‌گونه مطالعه‌ای بر روی انسان، حیوان یا داده‌های شخصی صورت نگرفته است؛ بنابراین، اخذ تأییدیه کمیتهٔ اخلاق برای این پژوهش ضروری نبوده است. با این حال، نویسنده اصول امانت‌داری علمی، صداقت پژوهشی، استناددهی صحیح و رعایت حقوق مالکیت فکری را در تمامی مراحل پژوهش رعایت کرده است.

در تهیهٔ این مقاله از ابزارهای هوش مصنوعی مولد صرفاً برای کمک به ویرایش زبانی، بهبود ساختار نگارش و ارتقای خوانایی متن استفاده شده است. این ابزارها در طراحی پژوهش، تحلیل علمی، تفسیر یافته‌ها، استنتاج نتایج یا تصمیم‌گیری‌های پژوهشی نقشی نداشته‌اند و مسئولیت کامل صحت، اصالت و محتوای نهایی مقاله بر عهده نویسنده/نویسندگان است.

موافقت نویسندگان:

تمامی نویسندگان نسخه نهایی مقاله را مطالعه و تأیید کرده‌اند و با انتشار آن موافقت دارند.

منابع

آقاشاهی، حسین (۱۳۹۷)، امکان‌سنجی مسئولیت کیفری ناشی از سیستم‌های هوش مصنوعی در فقه و حقوق، پایان‌نامهٔ کارشناسی ارشد، دانشگاه شهید مطهری، گروه فقه و اصول.

ابوذری، مهدی (۱۴۰۱)، حقوق و هوش مصنوعی، چاپ دوم، تهران: میزان.

احسان‌پور، سیدرضا و امی، امیر (۱۴۰۱)، «جرائم فناوری جعل عمیق از منظر فقه و حقوق کیفری»، فقه جزای تطبیقی، ۲(۴)، ۱-۹.

ادیب‌نیا، محمد (۱۳۹۵)، هوش مصنوعی در پرتو حقوق کیفری، پایان‌نامهٔ کارشناسی ارشد، دانشگاه آزاد اسلامی واحد شاهرود، دانشکدهٔ علوم انسانی.

اشلی، کوین (۱۴۰۱)، هوش مصنوعی و تحلیل حقوقی، ترجمهٔ امیر اسلامی‌تبار و همکاران، تهران: مجد.

بهره‌مند، حسین و مرسی، هادی (۱۴۰۱)، «راهبرد جرم‌انگاری مستقل حملات سایبری در حقوق کیفری ایران»، مجلس و راهبرد، ۲۹(۱۱۱)، ۲۸۵-۳۲۴.

جعفری لنگرودی، م. ج. (۱۴۰۱). دانشنامه حقوقی (چاپ چهارم، جلدهای ۱-۵). گنج دانش.

دوگال، پریت (۱۳۹۸)، اینترنت اشیا، هوش مصنوعی و چالش‌های حقوقی پیش‌رو، ترجمهٔ علی غلامعلی‌پور و مهدی غلامعلی‌پور، تهران: مجد.

رهبر، نرگس و دهقان‌پور فراشاه، سمیه (۱۴۰۰)، «بررسی تطبیقی مبنای مسئولیت مدنی در تصادفات وسایل نقلیهٔ خودران»، مطالعات حقوق تطبیقی، ۱۲(۲)، ۵۲۳-۵۴۳.

عطازاده، سعید و انصاری، جواد (۱۳۹۸)، «بازپژوهی مفهوم مسئولیت کیفری هوش مصنوعی (مطالعهٔ موردی خودروهای خودران) در حقوق اسلام، ایران، آمریکا و آلمان»، پژوهش تطبیقی حقوق اسلام و غرب، ۶(۴)، ۵۵-۸۶.

قیاسی، جواد (۱۳۷۵)، تسبیب در قوانین کیفری، قم: مدین.

کریمی، علی و کریمی، سارا (۱۳۹۳)، «تعارض بین مالیت بالفعل و شخصیت بالقوهٔ جنین آزمایشگاهی»، فصلنامهٔ حقوق پزشکی، ۸(۳۰)، ۱۱-۳۶.

گلدوزیان، ایرج (۱۳۸۵)، بایسته‌های حقوق جزای عمومی، تهران: میزان.

محسنی، فاطمه (۱۴۰۱)، جرم‌شناسی، تهران: دانشگاه امام صادق.

میرهادی، سید و علوی‌امین، سید محمدطه (۱۴۰۲)، هوش مصنوعی، تحولی عظیم در حوزهٔ حقوق، تهران: مهراندیشان سپهر.

نجفی ابرندآبادی، علی‌حسین و هاشم‌بیکی، حسن (۱۳۹۰)، دانشنامهٔ جرم‌شناسی، تهران: گنج دانش.

نخجوانی، علی و یاقوتی، الهام (۱۴۰۱)، «وضعیت حقوقی معاملات انجام‌شده توسط هوش مصنوعی: نظریهٔ وکیل مجازی»، پژوهش‌های حقوق اقتصادی و تجاری، ۱(۱)، ۴۱ـ۶۸.

References

Abaimov, S., & Martellini, M. (2020), "Artificial intelligence in autonomous weapon systems", *In 21st Century Prometheus* (pp. 141–177), Springer.

Acquaviva, G. (2022), "Autonomous weapons systems controlled by artificial intelligence: A conceptual roadmap for international criminal responsibility", *Military Law and Law of War Review, 60*(1), 89–121.

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018), "A taxonomy of cyber-harms", *Journal of Cybersecurity, 4*(1), tyy006.

Altmann, J., & Sauer, F. (2017), "Autonomous weapon systems and strategic stability", *Survival, 59*(5), 117–142.

Anderljung, M., et al. (2023), Frontier AI regulation. arXiv:2307.03718.

Bailey, M., Cooke, E., Jahanian, F., Xu, Y., & Karir, M. (2009), "Botnet technology", In *Cybersecurity Applications & Technology Conference* (pp. 299–304), IEEE.

Banteka, N. (2021), "Artificially intelligent persons", *Houston Law Review, 58*(3), 537–596.

Bátori, A. (2025), "International criminal law issues of autonomous weapons: The Kargu-2 drone in Libya", *Gradus, 12*(1), 1–15.

Ben Aissa, F., Hamdi, M., Zaied, M., & Mejdoub, M. (2023), "An overview of GAN-DeepFakes detection", *Multimedia Tools and Applications, 83*, 32343–32365.

Blanchard, A., & Bruun, L. (2025), Autonomous weapon systems and AI-enabled decision support, SIPRI.

Brown, A., Johnson, S. D., & Tuptuk, N. (2025), "Crime and connected and autonomous vehicles", *Crime Science, 14*, Article 2.

Chesney, R., & Citron, D. K. (2019), "Deep fakes: A looming challenge", *California Law Review*, *107*(6), 1753–1819.
Chopra, S., & White, L. F. (2011), *A legal theory for autonomous artificial agents*, Ann Arbor: University of Michigan Press.
Crootof, R. (2015), "The killer robots are here", *Cardozo Law Review*, *36*, 1837–1914.
Damiani, E. (2025), *Autonomy and accuracy in weapon systems*. ISPI.
Delaney, K. J. (2017), *Robot tax debate*. Quartz.
European Union (2013), Directive 2013/40/EU on attacks against information systems.
Ferdous, J. (2024), "AI-based ransomware detection", *IEEE Access*, *12*, 136666–136695.
Fernández Llorca, D., et al. (2025), "Testing autonomous vehicles and AI", *European Transport Research Review*, *17*, Article 38.
Fritsch, L., Jaber, A., & Yazidi, A. (2023), "AI used in malware", In *NAIS 2022*. Springer.
Gaeta (2023), "Who acts when autonomous weapons strike?", *Journal of International Criminal Justice*, *21*(5), 1033–1055.
Gandotra, V., Racicot, F.-É., & Rahimzadeh, A. (2020), "Cryptocurrency mining", In *Cryptofinance and mechanisms of exchange* (pp. 51–67), Springer.
Garikapati, D., & Shetiya, S. S. (2024), "Autonomous vehicles", *Big Data and Cognitive Computing*, *8*(4), 42.
Gherardini, L., & Cabri, G. (2023), "Impact of autonomous vehicles", *World Electric Vehicle Journal*, *15*(12), 579.
Haner, J. K., & Knake, R. K. (2021), "Breaking botnets", *Journal of Cybersecurity*, *7*(1), tyab003.
Jabbar, H., & Al-Janabi, S. (2025), "AI-driven phishing detection", *Journal of Cybersecurity and Privacy*, *5*(2), 26.
Jabir, R., Le, J., & Nguyen, C. (2025), "Phishing in the age of AI", *AI*, *6*(8), 174.
Joizil, K., Goldenberg, A., & Ghaly, S. (2022). *AI litigation risk*. TechLex Blog.
Khan, A., & Alam, T. (2025), "Integration of AI in phishing attacks", *IJNRD*, *10*(3), 1–6.
Khan, M., & Rehman, A. (2024), E*xploring deepfake technology: Creation, consequences and countermeasures*, Springer.
Kharraz, A., et al. (2015), "Ransomware attacks", In *DIMVA 2015* (pp. 3–24), Springer.
King, B., Hammond, T., & Harrington, J. (2017), "Economic consequences of AI", *Journal of Strategic Innovation and Sustainability*, *12*(2), 53–67.
Kirichenko, D. (2025), AI's role in modern warfare. War Room – U.S. Army War College.

Kurki, V. (2019), *A theory of legal personhood*, Oxford: Oxford University Press.
Loukas, G. (2015), *Cyber-physical attacks: A growing invisible threat* (1st ed.), Oxford: Butterworth-Heinemann.
Mele, A. R. (2001), *Autonomous agents: From self-control to autonomy*, Oxford: Oxford University Press.
Nelson, J. (2023). *ChatGPT false accusation*. Decrypt.
Pendleton, S. D., et al. (2017), "Autonomous vehicles", *Machines*, *5*(1), 6.
Prodhan, G. (2017), *Robot law debate*. Reuters.
Ramzan, Z. (2010), "Phishing attacks", In Handbook of Information and Communication Security. Springer.
Rigaki, M., & García, S. (2018), "GAN malware communication", In *IEEE Security and Privacy Workshops* (pp. 70–75),
Romero Moreno, F. (2024), "Generative AI and deepfakes", *International Review of Law, Computers & Technology*, *38*(3), 297–326.
Sandoval, M.-P., et al. (2024), "Threat of deepfakes", *Crime Science*, *13*(1), Article 2.
Schwarting, W., Alonso-Mora, J., & Rus, D. (2018), "Planning for autonomous vehicles. Annual Review of Control", *Robotics, and Autonomous Systems*, *1*(1), 187–210.
Solum, L. B. (1992), "Legal personhood for artificial intelligences", *North Carolina Law Review*, *70*(4), 1231–1287.
Teichmann, F. (2023), "Ransomware and generative AI", *International Cybersecurity Law Review*, *4*(3), 399–414.
University of Helsinki (2019). AI responsibility.
Winshel, A. (2023). Complaint against OpenAI. Harvard JSEL.
Taeb, M., & Chi, H. (2022). Comparison of Deepfake Detection Techniques through Deep Learning. Journal of Cybersecurity and Privacy, *2*(1), 89–106. https://doi.org/10.3390/jcp2010007
Dehghani, A., & Saberi, H. (2025). Generating and detecting various types of fake image and audio content: A review of modern deep learning technologies and tools. arXiv. https://arxiv.org/abs/2501.06227
Sandoval, M.-P., de Almeida Vau, M., Solaas, J., & Rodrigues, L. (2024). Threat of deepfakes to the criminal justice system: a systematic review. Crime Science, *13*, Article 41. https://doi.org/10.1186/s40163-024-00239-1
Sembiring, J., & Firdaus, S. U. (2025). Criminal liability for misuse of artificial intelligence (AI) in deepfake crimes. International Journal of Multiscience, *6*(1), 78–95.
https://multisciencejournal.com/index.php/ijm/article/view/432

Wright, M., Sohrawardi, S. J., & Bhattacharjee, S. (2016). Towards a framework for detecting deepfake videos [Conference paper]. Rochester Institute of Technology

Ferdous, N., et al. (2024). Deepfake video detection: challenges and opportunities. Artificial Intelligence Review, *57*, Article 10810. https://doi.org/10.1007/s10462-024-10810-6

Girhepuje, S., Verma, A., & Raina, G. (2024). A survey on offensive AI within cybersecurity. arXiv. https://doi.org/10.48550/arXiv.2410.03566

Pendleton, S., et al. (2017). Perception, planning, control, and coordination for autonomous vehicles. Machines, *5*(1), Article 6. https://doi.org/10.3390/machines5010006

Salem, A. H., Azzam, S. M., Emam, O. E., & Abohany, A. A. (2024). Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. Journal of Big Data, *11*, Article 38. https://doi.org/10.1186/s40537-024-00969-8

Khanjani, Z., Watson, G., & Janeja, V. P. (2022). Audio deepfakes: A survey. Frontiers in Big Data, *5*, Article 1001063. https://doi.org/10.3389/fdata.2022.1001063

Koh, Y. K. (2025). Enhancing deepfake detection generalization through component-based development in a web platform [Final Year Project]. Universiti Tunku Abdul Rahman (UTAR). http://eprints.utar.edu.my/7295/

Sandoval, M.-P., de Almeida Vau, M., Solaas, J., & Rodrigues, L. (2024). Threat of deepfakes to the criminal justice system: a systematic review. Crime Science, *13*, Article 41. https://doi.org/10.1186/s40163-024-00239-1

Schwarting, W., Alonso-Mora, J., & Rus, D. (2018). Planning and decision-making for autonomous vehicles. Annual Review of Control, Robotics, and Autonomous Systems, *1*, 187–210. https://doi.org/10.1146/annurev-control-060117-105157

Sembiring, J., & Firdaus, S. U. (2025). Criminal liability for misuse of artificial intelligence (AI) in deepfake crimes. International Journal of Multiscience, *6*(1). https://multisciencejournal.com/index.php/ijm/article/view/432

Wright, M., Sohrawardi, S. J., & Bhattacharjee, S. (2016). Towards a framework for detecting deepfake videos [Conference paper]. Rochester Institute of Technology.

Smith, S. (2022). Audio deepfakes: A survey [Review article]. Frontiers in Big Data.

Anandakumar, H., et al. (2023). Artificial intelligence for sustainable internet research.

European Commission. (2021). Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union

legislative acts (COM/2021/206 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

Kurtović, S., Hasanbegović, A., & Krivić, S. (2025). Conditional variational auto encoder based dynamic motion for multitask imitation learning. In 2025 XXX International Conference on Information, Communication and Automation Technologies (ICAT).

U.S. Securities and Exchange Commission. (2020). Artificial intelligence in the securities industry (FINRA Report)

Schirmbacher, M. (2020). Germany. In International Bar Association, Guidelines and regulations to provide insights on public policies to ensure artificial intelligence's beneficial use as a professional tool (pp. 71–78). International Bar Association.

European Commission. (2021). Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM/2021/206 final).

European Parliament. (2019). European Parliament resolution of 12 February 2019 on a comprehensive European industrial policy on artificial intelligence and robotics (2018/2088(INI)). Official Journal of the European Union.

Joizil, K., Morgan, C., Glover, D., & Thérien, D. (2022). Canada. In J. Buyers (Ed.), Artificial intelligence: Law over borders comparative guide 2022. The Global Legal Post.

King, I., et al. (2017). Aspect-level sentiment classification with HEAT (HiErarchical ATtention) network. In Proceedings of the 2017 ACM on Conference on Information and Knowledge Management (pp. 97–106). Association for Computing Machinery. https://doi.org/10.1145/3132847.3132877

Mahapatra, T. D. (2023, April 7). For which device Sony files patent application will blow your mind. Hindustan Times. https://www.hindustantimes.com/technology/for-which-device-sony-files-patent-application-will-blow-your-mind-101680827599538-amp.html

Tremblay v. OpenAI, Inc., No. 3:23-cv-03223 (N.D. Cal. filed June 28, 2023).

Journal Website

Legal Innovation Quarterly

Spring 2026

Volume 2, Issue 3

E-ISSN: 3115-8498

Invisible Murder: Assessing the Possibility of Attributing Murder in Deaths Resulting from Psychological Pressure, Sustained Humiliation, and Driving a Victim to Suicide

Zeynab Bagherinejad[1], Milad Chakav[2]*, Marjan Mahram[3]

1. Assistant Professor, Department of Law and Political Science, Science and Research Branch, Islamic Azad University, Tehran, Iran.
2. M.A. Student in Criminal Law and Criminology, Science and Research Branch, Islamic Azad University, Tehran, Iran (Corresponding Author)*
3. M.A. Student in Criminal Law and Criminology, Science and Research Branch, Islamic Azad University, Tehran, Iran.

***Corresponding author email address:** miladchakav@gmail.com

Extended Abstract

1. Introduction

The right to life, as the most fundamental value protected across legal systems and, particularly, within the framework of Iranian criminal law, has long been a central concern of legislators and legal doctrine. Nevertheless, recent developments in the modes of offending and the growing complexities of human interactions demonstrate that the deprivation of life is not necessarily confined to direct and tangible acts of physical violence, such as assault and battery, strangulation, shooting, or poisoning. Within emerging forms of criminal conduct, particularly in familial, intimate, and occupational settings and in cyberspace, a form of offending has emerged that may be described as "invisible murder." In such cases, the victim's death may appear, on the surface, to result from a voluntary act, namely suicide. Nevertheless, in substance, that act may constitute the ultimate outcome of a gradual and systematic process involving severe psychological pressures, persistent and destructive humiliations, ongoing threats, emotional domination, comprehensive behavioral control, and the progressive erosion of the victim's free will.

Received: December 22, 2025 - **Accepted:** February 20, 2026 - **Published:** March 21, 2026

Bagherinejad, Zeinab; Chakav, Milad; **&** Moharram, Marjan. (2026). "Invisible Homicide: Assessing the Possibility of Attributing Homicide in Deaths Resulting from Psychological Pressure, Persistent Humiliation, and Driving the Victim to Suicide."*Legal Innovation Quarterly*, 2(3), pp 55–82.
Doi: https://doi.org/10.22034/lir.2026.2093909.1043

© 2026 The Authors. Published by Legal Innovation Research Institute, Tehran, Iran. This is an open access article distributed under the terms of the Creative Commons Attribution 4.0 International (CC BY 4.0) License.

The principal concern and central issue of this study is the feasibility of attributing criminal liability for murder to an external actor in cases of death resulting from psychological pressure, sustained humiliation, and conduct that drives the victim to suicide within the framework of Iranian criminal law. The central research question is whether, where an offender, without directly inflicting any physical harm, creates the objective and psychological conditions for the deprivation of the victim's life through systematic psychological violence and sustained humiliation and thereby drives the victim toward suicide, the resulting death may be characterized as a criminal act. If so, the further question is whether the conduct may be characterized as murder or quasi-intentional homicide, or as indirect causation, under the relevant legal and jurisprudential principles. The underlying hypothesis of this study is that, where the complete erosion of the victim's free will and the offender's pervasive psychological domination over the victim are established, causation may be recognized under both ordinary and legal criteria between the offender's psychological conduct and the victim's death. On this basis, the act of suicide ceases to operate as an independent act capable of breaking the causal chain and may instead be analyzed as a direct continuation of the offender's conduct. Accordingly, the attribution of criminal liability for the death to the offender, whether on the basis of murder or indirect causation, has substantial legal and jurisprudential grounds.

2. Research Methodology

The present study is developmental-applied in terms of its nature and orientation and adopts a descriptive-analytical method in terms of its research design. The data collection process in this study is based on library and documentary research, drawing on primary sources of Imami jurisprudence, enacted criminal legislation, particularly the Islamic Penal Code of 2013, relevant judicial decisions, advisory opinions issued by the Legal Department of the Judiciary, and authoritative legal doctrine and comparative law, through which the relevant concepts are examined and analyzed. In analyzing the data, a qualitative method with a reasoning-based and inferential approach is employed. The research population comprises all relevant statutory propositions, jurisprudential propositions, and legal theories concerning causation, indirect causation, the victim's free will, aiding and abetting suicide, and psychological violence resulting in death within Iranian law and comparative legal systems. The analysis of these concepts focuses on re-examining factual and legal causation and the criteria governing the attribution of the criminal result in non-physical cases.

3. Research Findings

The findings of this study may be summarized along the following lines.

First, with regard to the actus reus (guilty act) involved in conduct leading to invisible murder, legal and jurisprudential doctrines do not necessarily regard the material or physical nature of the offender's conduct as a prerequisite for the commission of an offense. Any conduct, including psychological conduct such as severe threats, persistent terrorization, or sustained humiliation resulting in psychological breakdown, may, where it is sufficiently continuous, reasonably severe, and has a direct effect on depriving the victim of the capacity for discernment, be recognized as the initial conduct in the process of attributing the criminal result.

Second, with regard to causation, the findings of the study indicate that the victim's suicide does not invariably preclude the attribution of death to the antecedent actor. Where, as a result of the offender's sustained conduct, the victim's free will, autonomous decision-making, and capacity for rational choice have been substantially undermined and effectively extinguished, suicide can no longer be regarded as an independent act capable of breaking the causal chain; rather, it may be construed as an instrument through which the offender brings about the fatal result. In such circumstances, a direct causal link may be established between the offender's psychologically destructive conduct and the resulting death, since the victim's act, as part of the causal chain, lacks independent volition and is, according to ordinary criteria of attribution, attributable to the offender's conduct.

Third, with regard to the mens rea (guilty mind), the findings indicate that the attribution of criminal liability requires establishing the offender's intent, whether general or specific, or the offender's full awareness of the victim's vulnerable and fragile condition, together with the reasonable foreseeability of the occurrence of the result, namely death. Where the offender continues his conduct with the intent to deprive the victim of life, or with full knowledge that his humiliating conduct and severe psychological pressure are ordinarily likely to result in the breakdown of the victim's will and lead the victim to commit suicide, the requisite mens rea of the offense is established.

Fourth, the research hypothesis was supported. This means that, within the framework of Iranian criminal law, where the foregoing conditions concur, the offender's liability may extend beyond the mere offense of aiding and abetting suicide, as provided in Article 743 of the Islamic Penal Code, Book of Taʿzirat. His or her conduct may instead be analyzed and attributed to him as that of the principal causal agent of the death through indirect causation and, where complete loss of the victim's free will is established, may be characterized as murder or quasi-intentional homicide.

4. Conclusion and Recommendations

Conclusion

Analysis and examination of cases involving deaths resulting from psychological pressure and sustained humiliation demonstrate that a traditional criminal law system focused solely on physical and material conduct is not sufficiently equipped to respond to concealed and emerging forms of offending. Deaths resulting from driving a victim to suicide through severe psychological violence cannot simply be treated as voluntary suicide or reduced merely to aiding and abetting suicide as a taʿ zir offense. The findings of this study establish that, by reconsidering the foundations of Islamic jurisprudence and the general principles of criminal liability within Iranian law, including the doctrine of indirect causation and the rules governing attribution of an offense according to ordinary criteria, where the offender's non-physical conduct is such as to deprive the victim of free will and the capacity for discernment, or to seriously impair them, the victim's act of suicide constitutes the natural extension and direct consequence of the offender's conduct, and criminal liability for the deprivation of life will accordingly attach to the offender. This analysis challenges the traditional theory that the causal chain is broken by the act of the direct perpetrator, namely the victim, in such specific scenarios and instead adopts attribution according to ordinary criteria as the applicable basis of legal attribution.

Recommendations

Legislative Recommendation: It is proposed that, in future amendments to the Islamic Penal Code, the Iranian criminal legislator expressly provide specific provisions criminalizing non-physical conduct that progressively erodes free will, such as systematic familial or cyber-based psychological abuse resulting in suicide, in order to prevent uncertainty in the attribution of criminal liability.

Judicial Recommendation (Application in Judicial Practice): Criminal courts are advised, when dealing with suspicious suicide cases or cases involving a history of severe psychological violence, not to confine their inquiry to the suicide itself, but to refer the matter to experts in forensic psychiatry and criminal psychology and to rely on digital evidence, including messages, emails, and cyberspace interactions between the victim and the offender, in order to assess the extent of the victim's loss of free will and the offender's psychological domination.

Research Recommendation: Ongoing interdisciplinary research involving criminal law, psychological criminology, and forensic medicine is necessary for the development of clinical guidelines and assessment criteria for measuring the 'erosion of free will' in cases of invisible murder.

Keywords: Invisible murder; psychological violence; induced suicide; causation; indirect causation; loss of free will.

Funding
This article has no financial support or funding.

Authors' Contributions
Zeinab Bagherinejad: Conceptualization, data curation, validation, project administration, and resources.
Milad Chakav **&** Marjan Moharram: Methodology, formal analysis, writing – review & editing, investigation, writing – original draft.

Conflict of Interest
According to the authors' declaration, there is no conflict of interest regarding this article.

Ethical Considerations
This study was conducted based on the analysis of legal documents, statutes, judicial decisions, and library-based sources. It did not involve human participants, animals, or personal data; therefore, ethical approval from an institutional ethics committee was not required. Nevertheless, the authors adhered to the principles of academic integrity, research honesty, proper citation practices, and respect for intellectual property rights throughout all stages of the research.Generative artificial intelligence (AI) tools were used solely to assist with language editing, improving the structure of the manuscript, and enhancing the readability of the text. These tools did not contribute to the study design, scientific analysis, interpretation of findings, drawing of conclusions, or any research-related decision-making. The author(s) assume full responsibility for the accuracy, originality, and final content of the manuscript.

Authors' Approval
All authors have read and approved the final version of the manuscript and consent to its publication.

بهار ۱۴۰۵
دوره ۲، شماره ۳
شاپای الکترونیکی:
۳۱۱۵-۸۴۹۸

فصلنامه نوآوری حقوقی

وبسایت مجله

قتل نامرئی؛ امکان‌سنجی انتساب قتل در مرگ‌های ناشی از فشار روانی، تحقیر مستمر و سوق دادن قربانی به خودکشی

زینب باقری‌نژاد[۱]، میلاد چکاو[۲*]، مرجان محرم[۳]

۱. استادیار گروه حقوق و علوم سیاسی، واحد علوم و تحقیقات تهران، دانشگاه آزاد اسلامی، تهران، ایران

۲. دانشجوی کارشناسی ارشد حقوق کیفری و جرم‌شناسی، واحد علوم و تحقیقات تهران، دانشگاه آزاد اسلامی، تهران، ایران

(نویسندهٔ مسئول)

۳. دانشجوی کارشناسی ارشد حقوق کیفری و جرم‌شناسی، واحد علوم و تحقیقات تهران، دانشگاه آزاد اسلامی، تهران، ایران.

*ایمیل نویسندهٔ مسئول: miladchakav@gmail.com

چکیده

مقالهٔ حاضر با هدف تحلیل امکان‌سنجی انتساب عنوان قتل در مرگ‌های ناشی از فشار روانی شدید، تحقیر مستمر و سوق دادن قربانی به خودکشی، به یکی از چالش‌های نوپدید و مناقشه‌برانگیز مسئولیت کیفری می‌پردازد. مسئلهٔ اصلی آن است که در مواردی که مرتکب بدون ایراد صدمهٔ فیزیکی مستقیم، از طریق اعمال خشونت روانی، سلطهٔ عاطفی، تهدید و فرسایش تدریجی ارادهٔ بزه‌دیده، زمینهٔ وقوع خودکشی را فراهم می‌سازد، آیا می‌توان با وجود اصول حاکم بر حقوق کیفری نظیر اصل قانونی بودن و تفسیر مضیق، نتیجهٔ مرگ را از منظر کیفری به وی منتسب و رفتار او را در قالب قتل یا تسبیب در جنایت تحلیل کرد یا خیر. این تحقیق با روش تحلیلی ـ انتقادی و با اتکا به منابع کتابخانه‌ای، مبانی فقهی و حقوقی، دکترین کیفری و برخی رویکردهای تطبیقی، به بررسی معیارهای احراز رابطهٔ سببیت، عنصر معنوی و مرز میان معاونت در خودکشی، تسبیب در جنایت و قتل می‌پردازد. یافته‌های پژوهش نشان می‌دهد که نص صریحی برای تسری مستقیم مقررات قتل عمدی به خشونت روانی وجود ندارد؛ با این حال، در فروض استثنایی و مشروط که رفتارهای روانی مستمر به زوال ارادهٔ آزاد بزه‌دیده منجر شود، انتساب رابطهٔ سببیت براساس نظریهٔ تسبیب در جنایت و به استناد موادی چون ۴۹۲ و ۵۰۶ قانون مجازات اسلامی قابل تبیین است. این امر مستلزم احراز معیارهای سنجش‌پذیری چون شدت و تکرار رفتار، آگاهی مرتکب از وضعیت خاص قربانی، و تأیید کارشناسی روان‌پزشکی قانونی مبنی بر سلب اختیار بزه‌دیده است. بنابراین، مقاله با پرهیز از ادعای قطعی انتساب قتل، بر امکان نظری مشروط در چارچوب موانع اثباتی و قانونی دادرسی کیفری تأکید می‌کند.

واژگان کلیدی: قتل نامرئی، خشونت روانی، خودکشی برانگیخته، رابطهٔ سببیت، تسبیب در جنایت، زوال اراده.

دریافت‌شده در تاریخ: ۱ دی ۱۴۰۴ - **پذیرش‌شده در تاریخ:** ۱ اسفند ۱۴۰۴- **منتشرشده در تاریخ:** ۱ فروردین ۱۴۰۵

باقری‌نژاد، زینب؛ چکاو، میلاد؛ محرم، مرجان. (۱۴۰۵). «قتل نامرئی؛ امکان‌سنجی انتساب قتل در مرگ‌های ناشی از فشار روانی، تحقیر مستمر و سوق دادن قربانی به خودکشی». فصلنامه نوآوری حقوقی، دوره ۲، شماره ۳، صص ۵۵- ۸۲.

Doi: https://doi.org/10.22034/lir.2026.2093909.1043

© 2026 The Authors. Published by Legal Innovation Research Institute, Tehran, Iran. This is an open access article distributed under the terms of the Creative Commons Attribution 4.0 International (CC BY 4.0) License.

مقدمه

حق حیات، به‌عنوان یکی از بنیادی‌ترین موضوعات حمایت کیفری، همواره در کانون توجه نظام‌های حقوقی قرار داشته است. با این حال، تحولات نوین بزهکاری نشان داده است که مرگ انسان صرفاً در قالب رفتارهای فیزیکی مستقیم، مانند ایراد ضرب و جرح یا به‌کارگیری ابزارهای کشنده، تحقق نمی‌یابد، بلکه در برخی موارد، مرگ قربانی می‌تواند نتیجهٔ فرایندی تدریجی از فشار روانی شدید، تحقیر مستمر، تهدیدهای آشکار یا پنهان، سلطهٔ عاطفی، کنترل رفتاری و فرسایش مستمر ارادهٔ آزاد او باشد. در این وضعیت، هرچند مرگ در ظاهر به صورت خودکشی نمود می‌یابد، انتساب کیفری آن به عامل خارجی، خودبه‌خود از عنوان خودکشی فراتر نمی‌رود و نیازمند احراز شرایط دقیق قانونی، روان‌پزشکی و سبب‌شناختی است. ازاین‌رو، پرسش اساسی آن است که آیا چنین مرگی را باید صرفاً خودکشی تلقی کرد یا آنکه در فرض وجود رفتار خارجی مؤثر، آگاهی یا قصد مرتکب و رابطهٔ سببیت قابل احراز، می‌توان آن را در پرتو قواعد مسئولیت کیفری به عامل خارجی منتسب و حتی در فروض استثنایی در قلمرو قتل تحلیل کرد. طرح این مسئله، به‌ویژه در پرتو اشکال جدید خشونت روانی در روابط خانوادگی، عاطفی و دیجیتال، اهمیت دوچندان یافته و ضرورت بازاندیشی محتاطانه و منطبق با اصل قانونی بودن جرائم و مجازات‌ها در مفاهیم کلاسیک حقوق کیفری را آشکار ساخته است.

در حقوق کیفری ایران، تحلیل جنایت علیه تمامیت جسمانی به‌طور سنتی بر رفتار مادی محسوس، مباشرت فیزیکی و رابطهٔ سببیت آشکار استوار بوده است. با وجود این، در پرونده‌هایی که مرگ بزه‌دیده در نتیجهٔ فشارهای روانی سازمان‌یافته، تحقیر مداوم، تهدید، آزار عاطفی یا سوق دادن تدریجی او به خودکشی رخ می‌دهد، کاربرد مفاهیم سنتی با ابهام‌های جدی مواجه می‌شود. مسئلهٔ اصلی آن است که آیا رفتارهای غیرفیزیکی مستمر می‌توانند از حیث حقوقی واجد وصف رفتار مؤثر در تحقق جنایت علیه نفس باشند و آیا می‌توان میان این رفتارها و نتیجهٔ مرگ، رابطهٔ استناد قابل قبول حقوقی و عرفی برقرار کرد. پاسخ به این پرسش، منوط به تعیین معیارهایی برای تفکیک فشار روانی متعارف از خشونت روانی شدید و نیز تشخیص زوال یا اختلال جدی در ارادهٔ بزه‌دیده است. ازجمله معیارهای قابل بررسی در این زمینه می‌توان به شدت و استمرار رفتار، تکرار و سازمان‌یافتگی آن، هدف‌مندی در تحقیر یا سلطه بر بزه‌دیده، وضعیت روانی و میزان آسیب‌پذیری وی، آثار قابل احراز رفتار بر کارکردهای شناختی و تصمیم‌گیری، فاصلهٔ زمانی میان رفتارهای آزاردهنده و مرگ، و فقدان عامل مستقل و مؤثر دیگری اشاره کرد. از همین رهگذر، پرسش‌هایی

دربارهٔ معیارهای مادی و معنوی احراز سببیت، نحوهٔ اثبات زوال یا اختلال جدی در اراده، مرز میان معاونت در خودکشی، تسبیب در جنایت و قتل در فرض‌های محدود و استثنایی، و نیز چالش‌های اثباتی مربوط به سوءنیت و ادلهٔ اثبات دعوا مطرح می‌شود.

بنابراین، پژوهش حاضر درپی آن است که با رعایت اصل قانونی بودن جرائم و مجازات‌ها و اصل تفسیر مضیق مقررات کیفری، امکان‌سنجی انتساب عنوان قتل به مرگ‌های ناشی از فشار روانی شدید، تحقیر مستمر و سوق دادن قربانی به خودکشی را در بستر حقوق کیفری ایران و با توجه به رهیافت‌های تطبیقی مورد بررسی قرار دهد. در این راستا، پژوهش حاضر ضمن تفکیک میان امکان نظری انتساب نتیجه و قابلیت تحقق آن در نظام حقوقی موجود، عناصر لازم برای احراز رفتار مؤثر، رابطهٔ سببیت و وضعیت ارادی بزه‌دیده را تحلیل می‌کند و می‌کوشد معیارهایی عملی برای تشخیص مرز میان فشار روانی متعارف، خشونت روانی شدید و زوال اراده ارائه دهد. همچنین، با توجه به فقدان نص صریح دربارهٔ عنوان «قتل نامرئی»، بررسی خواهد شد که آیا ظرفیت تفسیری مقررات موجود می‌تواند در فروض خاص، انتساب نتیجهٔ مرگ را توجیه کند یا آنکه چنین رفتاری، حسب مورد، باید در عناوین کیفری محدودتری همچون معاونت یا تسبیب تحلیل شود.

پیشینهٔ پژوهش نشان می‌دهد که اگرچه مسئلهٔ مرگ‌های ناشی از فشار روانی و خودکشی برانگیخته در ادبیات حقوقی و جرم‌شناختی بی‌سابقه نیست، اما بررسی آن در قالب «قتل نامرئی» و با تمرکز بر امکان انتساب قتل، همچنان با خلأ نظری و تحلیلی روبه‌روست. در حوزهٔ مبانی نظری و کیفری، بایندر و کیزا[1] (2019: 65-133) در سال ۲۰۱۹ در مقالهٔ «معمای تحریک به خودکشی» به دشواری‌های مفهومی و حقوقی انتساب مسئولیت کیفری در خودکشی دیگری پرداخته و نشان داده‌اند که تحریک به خودکشی در مرز میان خودآیینی قربانی و مداخلهٔ مجرمانهٔ مرتکب قرار دارد. در حوزهٔ مطالعات تجربی و روان‌پزشکی کیفری، فلین[2] و همکاران (2016: 877-884) در پژوهش خود دربارهٔ قتل ـ خودکشی و نقش اختلال روانی، پیوند میان وضعیت روانی، زمینه‌های رابطه‌ای و مرگ‌های ترکیبی را بررسی کرده‌اند. همچنین فلین و همکاران (2009: 306-321) در مطالعه‌ای مقطعی دربارهٔ قتل پس از خودکشی، بر پیچیدگی مرز میان قتل و خودکشی از منظر جرم‌شناختی و

1. Binder & Chiesa
2. Flynn

روان‌پزشکی تأکید کرده‌اند. در بستر خشونت خانگی، اورام[1] و همکاران (2013: 1006-1011) در مطالعه‌ای مبتنی بر جمعیت دربارهٔ بیماری روانی و قتل خانگی، اهمیت روابط نزدیک، سلطهٔ روانی و زمینه‌های خشونت‌آمیز را در شکل‌گیری مرگ‌های شدید روشن ساخته‌اند. افزون بر این، لوگان[2] و همکاران (2019: 1693-1706) در پژوهشی دربارهٔ هم‌بسته‌های قتل شریک صمیمی در میان مردان متوفی بر اثر خودکشی، به پیوند میان تعارضات رابطه‌ای، خشونت صمیمی و مرگ‌های خودخواسته پرداخته‌اند. با وجود اهمیت این آثار، هیچ‌یک به‌طور متمرکز امکان انتساب عنوان قتل به مرگ‌های ناشی از فشار روانی مستمر و تحقیر نظام‌مند را در چارچوب حقوق کیفری ایران بررسی نکرده‌اند.

بر این اساس، نوآوری پژوهش حاضر در آن است که نخست، با صورت‌بندی **تحلیلی** مفهوم «قتل نامرئی»، می‌کوشد ظرفیت‌ها و حدود انتساب مرگ‌های ناشی از خشونت روانی شدید و سوق دادن قربانی به خودکشی را از منظر مسئولیت کیفری و جنایت علیه نفس در حقوق ایران بازخوانی کند؛ دوم، معیارهای مادی و معنوی احراز رابطهٔ سببیت میان رفتارهای غیرفیزیکی مستمر و نتیجهٔ مرگ را با تکیه بر شاخص‌های عملی و روان‌پزشکی قانونی تحلیل نماید؛ سوم، **براساس** ارزیابی درجهٔ استقلال یا زوال ارادهٔ بزه‌دیده، مرز دقیق میان رفتارهایی مانند معاونت در خودکشی، تسبیب در جنایت و فروض نادر و استثنایی انتساب مستقیم قتل را روشن سازد؛ و چهارم، با تمرکز بر حقوق کیفری ایران و بهره‌گیری از ادبیات تطبیقی، ضمن تفکیک میان امکان نظری و محدودیت‌های ناشی از اصل تفسیر مضیق مقررات کیفری، ظرفیت‌ها و محدودیت‌های نظام حقوقی موجود را در پاسخ به این‌گونه مرگ‌ها ارزیابی کند. از این حیث، پژوهش حاضر نه‌تنها واجد اهمیت نظری در بازخوانی مفاهیم بنیادینی چون رفتار مادی، سببیت و سوءنیت است، بلکه از منظر عملی نیز می‌تواند با ارائهٔ معیارهای سنجش‌پذیر برای احراز اختلال یا زوال اراده، در تبیین ضوابط استناد کیفری، هدایت رویهٔ قضائی، تفسیر مضیق و ضابطه‌مند قوانین، تقویت کارآمدی ادلهٔ روان‌شناختی و دیجیتال، و حمایت مؤثرتر از بزه‌دیدگان آسیب‌پذیر نقش‌آفرین باشد.

---

1. Oram
2. Logan

۱. مبانی مفهومی و چارچوب نظری قتل نامرئی

۱ـ۱. مفهوم‌شناسی قتل نامرئی، خودکشی برانگیخته و خشونت روانی

قتل نامرئی به وضعیتی اطلاق می‌شود که مرگ انسان نه از رهگذر ضرب و جرح آشکار یا مداخلهٔ فیزیکی مستقیم بلکه در نتیجهٔ روندی تدریجی از فشار روانی، تحقیر مستمر، تهدید پنهان، سلطهٔ عاطفی، کنترل رفتاری و فرسایش ارادهٔ بزه‌دیده تحقق می‌یابد. در چنین فرضی ظاهر واقعه ممکن است خودکشی باشد، اما نمی‌توان صرفاً به شکلِ نهایی مرگ بسنده کرد (Paw□owska-Muc et al., 2023: 1-10)، زیرا آنچه اهمیت دارد نقش رفتار دیگری در ایجاد وضعیت روانی خطرناک و کاهش توان تصمیم‌گیری آزادانهٔ قربانی است (Greenfield et al., 2025: 8-19). از این منظر خودکشی برانگیخته مفهومی میان خودکشی مستقل و قتل مستقیم است؛ یعنی بزه‌دیده اقدام نهایی را انجام می‌دهد، اما این اقدام در فضایی شکل گرفته که مرتکب با رفتارهای مستمر و هدفمند امکان انتخاب متعارف را از او سلب یا به شدت محدود کرده است (Hannah et al., 1998: 275-283). در بسیاری از مرگ‌های ظاهراً خودخواسته زمینه‌های رابطه‌ای سلطهٔ روانی و تعارض شدید پیش از وقوع مرگ نقش تعیین‌کننده دارند و همین امر ضرورت تحلیل دقیق‌تر پیوند میان فشار روانی و نتیجهٔ مرگ را آشکار می‌سازد (Flynn, 2009: 306-321).

خشونت روانی در این چارچوب صرفاً به معنای ناراحتی روحی یا اختلاف عاطفی معمول نیست، بلکه ناظر به مجموعه رفتارهایی است که به صورت مکرر جهت‌دار و قابل انتساب علیه بزه‌دیده اعمال می‌شود و شأن انسانی امنیت روانی و قدرت ارادهٔ او را هدف قرار می‌دهد. این خشونت ممکن است در قالب تحقیر روزانهٔ تهدید به افشا، طرد اجتماعی، محروم‌سازی عاطفی، کنترل ارتباطات، القای بی‌ارزشی یا ایجاد احساس بن‌بست جلوه کند و در صورت شدت و استمرار می‌تواند از حیث کیفری در زمرهٔ رفتارهای خطرآفرین برای نفس قرار گیرد (Henrion, 2014: 893-903). اهمیت این مفهوم در آن است که حقوق کیفری نباید تنها نسبت به صدمهٔ بدنی قابل مشاهده حساس باشد، بلکه در مواردی که فشار روانی به صورت نظام‌مند به مرگ منتهی می‌شود باید ظرفیت انتساب نتیجه را بررسی کند (Marzukb et al., 1992: 3179-3190). سلطهٔ روانی و کنترل مستمر در روابط نزدیک می‌تواند زمینه‌ساز مرگ‌های شدید باشد و از این جهت خشونت روانی واجد ارزش اثباتی و تحلیلی در ارزیابی رابطهٔ سببیت است (Oram et al., 2013: 1006-1011).

قتل نامرئی زمانی می‌تواند وارد قلمرو مسئولیت کیفری سنگین شود که رفتار مرتکب از حد تحریک ساده یا رفتار اخلاقاً مذموم فراتر رود و در عرف سبب مؤثر غالب و قابل پیش‌بینی برای مرگ شناخته شود. در حقوق کیفری ایران با توجه به قواعد تسبیب در جنایت و معیار انتساب نتیجه در قانون مجازات اسلامی مصوب ۱۳۹۲[۱] امکان طرح چنین تحلیلی وجود دارد، اما این امکان مطلق نیست؛ دادگاه باید احراز کند که رفتار روانی مرتکب مستمر شدید و هدفمند است، ارادهٔ بزه‌دیده را به نحو جدی مخدوش می‌کند و اقدام به خودکشی حلقهٔ مستقل و قاطع رابطهٔ سببیت محسوب نمی‌شود. در این وضعیت اگر مرگ پیامد قابل پیش‌بینی فشار تحقیر و سلطهٔ روانی باشد تحلیل آن در سطحی فراتر از معاونت در خودکشی قابل دفاع است، اما در صورت فقدان دلیل کافی بر زوال یا اختلال جدی ارادهٔ بزه‌دیده اصل قانونی بودن جرم و مجازات و تفسیر مضیق قوانین کیفری مانع توسعهٔ عنوان قتل خواهد بود.

۱ـ۲. ارکان مسئولیت کیفری در مرگ‌های ناشی از فشار روانی

در مرگ‌های ناشی از فشار روانی بررسی مسئولیت کیفری بدون بازتعریف دقیق ارکان سه‌گانهٔ جرم امکان‌پذیر نیست، زیرا در این دسته از وقایع رفتار مرتکب غالباً در قالب فعل مادی محسوس و آنی ظهور نمی‌یابد، بلکه به صورت مجموعه‌ای از رفتارهای مستمر هدفمند و فرساینده تحقق پیدا می‌کند. رکن قانونی در این حوزه اقتضا دارد که هرگونه انتساب نتیجهٔ مرگ بر مبنای عناوین مصرح در قانون و در چهارچوب قواعد عام جنایات صورت گیرد. از این رو تحلیل باید بر پایهٔ مقررات قانون مجازات اسلامی دربارهٔ جنایت عمدی شبه‌عمدی خطای محض و نیز قواعد تسبیب در جنایت استوار شود (Pottinger et al., 2019: 1-8). در بُعد مادی نیز آنچه اهمیت دارد صرف نبود تماس فیزیکی نیست، بلکه احراز رفتاری است که در عرف واجد اثرگذاری واقعی بر وضع روانی بزه‌دیده و ایجادکنندهٔ خطر متعارف برای جان او باشد بنابراین فشار روانی زمانی می‌تواند در قلمرو حقوق کیفری مورد اعتنا قرار گیرد که صورت‌های رفتاری آن مانند تهدید، تحقیر مستمر، ارعاب، سلطهٔ عاطفی، حبس ارتباطی یا القای مداوم بی‌ارزشی به نحو روشن و مستند قابل اثبات باشد (Bourget et al., 2000: 179-182).

---

۱. قانون مجازات اسلامی مصوب ۱۳۹۲ مواد ۴۹۲ و ۵۰۶

رکن مادی در این گونه مرگ‌ها از سه مؤلفه تشکیل می‌شود: نخست رفتار مرتکب که ممکن است از افعال گفتاری نوشتاری دیجیتال یا رفتاری مرکب پدید آید؛ دوم وضعیت زیان‌بار روانی که در بزه‌دیده ایجاد یا تشدید می‌شود؛ و سوم نتیجهٔ نهایی که همان مرگ است. اهمیت این ساختار در آن است که دادگاه باید میان رنج روانی عادی و فشار روانی جرم‌زا تمایز بگذارد و تنها در صورتی به انتساب نتیجه حکم دهد که رفتار مرتکب از حیث شدت استمرار و جهت‌گیری چنان باشد که عرفاً برای ایجاد فروپاشی اراده یا استیصال شدید کفایت کند. در این میان رابطهٔ سببیت جایگاهی مرکزی دارد، زیرا هرگاه اقدام نهایی بزه‌دیده به خودکشی به صورت یک تصمیم مستقل آگاهانه و خارج از دایرهٔ سلطهٔ روانی مرتکب ارزیابی شود انتساب نتیجه با دشواری جدی روبه‌رو خواهد شد، اما اگر ثابت شود که رفتار مرتکب در زنجیرهٔ علل نقش غالب و تعیین‌کننده داشته و ارادهٔ متعارف بزه‌دیده را مختل کرده است، زمینه برای تحلیل کیفری در قالب تسبیب یا در فروض خاص در سطحی نزدیک به مباشرت فراهم می‌شود (Pereira et al., 2013: 1099-1107). رکن معنوی نیز در این حوزه از پیچیدگی خاصی برخوردار است، زیرا در اغلب موارد مرتکب صریحاً قصد اعلام‌شده برای قتل ندارد، با این حال فقدان اقرار یا تصریح به قصد سلب حیات مانع احراز سوء نیت نیست. هرگاه از مجموعه قرائن معلوم شود که مرتکب با علم به وضعیت آسیب‌پذیر بزه‌دیده و با آگاهی از آثار فرسایندهٔ رفتار خویش عمداً به اعمال فشار ادامه داده است عنصر روانی می‌تواند احراز شود. در حقوق کیفری ایران بر پایهٔ مادهٔ ۲۹۰ قانون مجازات اسلامی، جنایت در صورتی عمدی است که مرتکب قصد ایراد نتیجه را داشته باشد یا رفتاری را انجام دهد که نوعاً موجب جنایت می‌شود یا نسبت به شخص معین به‌سبب وضعیت خاص او نوعاً موجب جنایت باشد و مرتکب به آن وضعیت آگاه باشد. از این رو در فرضی که مرتکب از شکنندگی روانی بزه‌دیده آگاه است و با وجود این آگاهی به تهدید تحقیر یا کنترل مخرب ادامه می‌دهد. امکان استناد به بند پ مادهٔ ۲۹۰ در تحلیل برخی فروض دور از ذهن نیست. هر چند تفسیر این حکم باید محتاطانه و منطبق با اصل تفسیر مضیق باشد (کوشا و علی‌نژاد، ۱۳۹۲: ۱۶۱) افزون بر این مسئولیت کیفری در این مرگ‌ها منوط به آن است که رفتار مرتکب واجد وصف قابل سرزنش کیفری باشد و دخالت عوامل رافع مسئولیت یا عوامل مداخله‌گر مستقل نتیجه را مخدوش نکند، برای نمونه اگر بیماری روانی شدید بزه‌دیده یا مداخلهٔ عامل ثالث به نحوی باشد که زنجیرهٔ انتساب عرفی را قطع کند نمی‌توان بدون استدلال دقیق نتیجهٔ مرگ را به مرتکب منسوب کرد. با این حال مطالعات روان‌پزشکی و جرم‌شناختی دربارهٔ خشونت

خانگی و مرگ‌های رابطه‌ای نشان داده‌اند که در بسیاری از موارد فشار روانی مستمر نه یک عامل فرعی بلکه عامل مسلط در فرایند منتهی به مرگ است و همین یافته‌ها ضرورت توجه به ادلهٔ کارشناسی و ارزیابی چندرشته‌ای را تقویت می‌کند. بنابراین ارکان مسئولیت کیفری در این حوزه تنها با جمع میان مبانی حقوقی نظریهٔ سببیت و داده‌های کارشناسی قابل احراز است و هر تحلیل ساده‌انگارانه یا صرفاً اخلاقی از ماجرا با منطق دادرسی کیفری سازگار نخواهد بود (کیخا، ۱۳۹۵: ۹۰).

مهم‌ترین مبنا برای ارزیابی مسئولیت کیفری در مرگ‌های ناشی از فشار روانی آن است که حقوق کیفری نباید در اسارت برداشت سنتی از رفتار مادی باقی بماند، بلکه باید به این پرسش پاسخ دهد که آیا رفتار غیرفیزیکی نیز می‌تواند همان کارکرد سلب‌کنندهٔ حیات را ایفا کند یا خیر، پاسخ در چهارچوب قانون موجود مثبت اما مشروط است؛ بدین معنا که تنها در صورت احراز هم‌زمان رفتار فرسایندهٔ شدید رابطهٔ سببیت عرفی آگاهی مرتکب از وضعیت خاص بزه‌دیده و قابل پیش‌بینی بودن مرگ می‌توان از مسئولیت کیفری سنگین سخن گفت. در غیر این صورت توسعهٔ عنوان قتل فاقد پشتوانهٔ قانونی خواهد بود و با اصول بنیادین حقوق جزا تعارض پیدا می‌کند. از این حیث رویکرد درست نه انکار مطلق امکان انتساب است و نه تسری شتاب‌زدهٔ عنوان قتل، بلکه اتخاذ تفسیری منضبط از قواعد تسبیب و عمد در پرتو واقعیت‌های نوین خشونت روانی است.

۱ـ۳. جایگاه رابطهٔ سببیت و ارادهٔ بزه‌دیده در انتساب نتیجه

در مرگ‌های ناشی از فشار روانی مهم‌ترین گره حقوقی در احراز رابطهٔ سببیت آن است که نتیجهٔ مرگ با وجود دخالت فعل نهایی بزه‌دیده تا چه اندازه قابل انتساب به رفتار مرتکب باقی می‌ماند. در تحلیل کیفری صرف تقدم زمانی رفتار مرتکب بر خودکشی کافی نیست، بلکه باید احراز شود که فشار روانی تحقیر مستمر تهدید یا سلطهٔ عاطفی به گونه‌ای در فرایند وقوع مرگ دخالت داشته است که عرف آن را سبب مؤثر و غالب بشناسد. رابطهٔ سببیت در این حوزه ماهیتی صرفاً مادی ندارد، بلکه مستلزم ارزیابی هنجاری از نقش رفتار مرتکب در ایجاد وضعیت خطرناک برای نفس است. از همین رو هرگاه رفتار مرتکب زمینه‌ای فراهم سازد که بزه‌دیده در اثر فرسایش روانی و زوال توان مقاومت به نقطهٔ اقدام کشیده شود خودکشی دیگر لزوماً فعلی مستقل و قاطع زنجیرهٔ علیت محسوب نخواهد شد (Hanzlick & Koponen, 1994: 168-173). در حقوق کیفری ایران نیز هر چند قانون‌گذار تعریف جامع و صریحی از سببیت ارائه نکرده، اما ساختار مواد مربوط به تسبیب در جنایت نشان

می‌دهد که معیار انتساب نتیجه بر پایهٔ استناد عرفی و نقش مؤثر سبب استوار است و در این چارچوب می‌توان رفتارهای غیرفیزیکی را نیز در صورت احراز اثر غالب در شمار اسباب مسئولیت‌آور قرار داد (الیاسی، ۱۴۰۱: ۷۶). در مقابل، ارادهٔ بزه‌دیده متغیری است که می‌تواند هم در جهت تقویت و هم در جهت تضعیف انتساب نتیجه عمل کند. اگر اقدام به خودکشی ناشی از تصمیمی آزاد سنجیده و منفک از سلطهٔ روانی مرتکب باشد اصل بر آن است که ارادهٔ مباشرانهٔ بزه‌دیده رابطهٔ سببیت را قطع می‌کند، اما هرگاه ثابت شود که این اراده در اثر آزار مستمر تهدید فرسایش شخصیت یا وضعیت آسیب‌پذیری شناخته‌شده دچار اختلال جدی شده است دیگر نمی‌توان آن را اراده‌ای کامل و مستقل تلقی کرد. در این فرض نقش مرتکب از سطح تأثیر اخلاقی فراتر می‌رود و می‌تواند در قلمرو مسئولیت کیفری مؤثر واقع شود (Panczak et al., 2013: 28-36). در بستر روابط نزدیک تصمیم به مرگ در مواردی محصول انباشت فشار و سلطه است نه انتخابی جدا از زمینهٔ رابطه‌ای و همین یافته‌ها برای حقوق کیفری اهمیت دارد، زیرا ارزیابی استقلال ارادهٔ بزه‌دیده را از حالت انتزاعی خارج می‌کند و به واقعیت‌های روان‌شناختی و اجتماعی نزدیک می‌سازد (Logan et al., 2019:1693-1706).

معیار درست در انتساب نتیجه آن است که دادگاه به جای تمرکز صوری بر این گزاره که فعل نهایی از سوی بزه‌دیده انجام شده است به سنجش حقوقی کیفیت ارادهٔ او بپردازد و بررسی کند که آیا این اراده در زمان اقدام هنوز واجد استقلال متعارف بوده یا در نتیجهٔ رفتار مرتکب به حدی مخدوش شده که کارکرد قاطع خود را ازدست داده است. بر پایهٔ این مبنا در حقوق کیفری ایران با توجه به مواد ۴۹۲ و ۵۰۶ قانون مجازات اسلامی هرگاه رفتار مرتکب عرفاً سبب جنایت شناخته شود و اقدام بزه‌دیده ناشی از ارادهٔ آزاد و بریده از فرایند سلطهٔ روانی نباشد، انتساب نتیجهٔ مرگ به مرتکب از حیث تسبیب قابل دفاع است و در فروض خاص با اجتماع شرایط مادهٔ ۲۹۰ حتی می‌تواند به بحث دربارهٔ عمد نیز راه یابد. با این حال توسعهٔ عنوان قتل بدون احراز دقیق اختلال اراده و غلبهٔ سبب خارجی با اصول تفسیر مضیق و شخصی بودن مسئولیت کیفری سازگار نیست و از همین جهت سنجش رابطهٔ سببیت در این حوزه باید مبتنی بر معیارهای سخت‌گیرانهٔ اثباتی و ارزیابی منضبط قضائی باشد.

۲. تحلیل فقهی و حقوقی انتساب قتل در مرگ‌های ناشی از سوق‌دادن به خودکشی

۲ـ۱. بررسی مبانی فقهی و حقوقی مباشرت، تسبیب و معاونت در خودکشی

در تحلیل مرگ ناشی از خودکشی برانگیخته، نخست باید تقابل میان دو قاعدهٔ فقهی «المباشر اقوی من السبب» و «تسبیب در جنایت» با دقت روشن شود، زیرا در این حوزه همواره این پرسش مطرح است که آیا رفتار شخص ثالث در حد ایجاد زمینه و مقدمه باقی مانده است یا آنکه از نظر عرف و ضوابط انتساب، به مرتبه‌ای رسیده که نتیجهٔ مرگ را باید به او مستند دانست (شفیعی مازندرانی، ۱۳۸۹: ۳۹). در فقه امامیه، مباشرت ناظر به وضعیتی است که جنایت بی‌واسطه به فعل مرتکب تحقق یابد و تسبیب بر موردی حمل می‌شود که مرتکب، سبب وقوع جنایت را فراهم سازد (ذبیحی‌ریزی، ۱۳۹۸: ۹۸). اصل اولی در فقه و حقوق کیفری آن است که با ورود مباشر (بزه‌دیده که خودکشی می‌کند)، رابطهٔ سببیت میان رفتار سبب (فشار روانی مرتکب) و نتیجه (مرگ) قطع می‌شود، چراکه ارادهٔ آزاد مباشر، به‌مثابهٔ یک «عامل معترض»، مانع از استناد نتیجه به سبب می‌شود (حسین‌زاده، ۱۳۹۹: ۸۸). با این حال، این اصل مطلق نیست؛ نوآوری نظری پژوهش حاضر در این است که براساس «قاعدهٔ تسبیب» و مفهوم «استناد عرفی»، هرگاه ارادهٔ مباشر در اثر «اکراه معنوی شدید» یا «تغریر روانی»، به مرتبهٔ «مسلوب‌الاختیار شدن» یا «اضطرار شدید» برسد، مباشر فیزیکی (بزه‌دیده) به‌مثابهٔ «آلت دست» یا «واسطهٔ فاقد ارادهٔ مستقل» تلقی شده و قاعدهٔ «السبب اقوی من المباشر» حاکم می‌شود (علیزاده، ۱۴۰۰: ۱۵۹ـ ۱۶۹).

بر همین مبنا، اگر ارادهٔ بزه‌دیده در اثر فشار روانی شدید، تحقیر مستمر یا سلطهٔ عاطفی به گونه‌ای فرسوده شود که اقدام نهایی او استقلال متعارف نداشته باشد، از منظر قواعد اصولی، ارادهٔ او دیگر «علت تامه» محسوب نمی‌شود، بلکه تنها «مجرای تحقق ارادهٔ مرتکب» قرار می‌گیرد. ساختار قانون مجازات اسلامی ظرفیت بررسی این وضعیت را در چهارچوب تسبیب در جنایت فراهم کرده است. مادهٔ ۴۹۲ قانون مجازات اسلامی، جنایت را در صورت «استناد عرفی» به رفتار مرتکب، قابل انتساب می‌داند. این واژه «استناد عرفی»، گویای آن است که قانون‌گذار از نگاه مادی‌گرایانهٔ صرف فاصله گرفته و به معیارهای کیفی و قضاوتی روی آورده است. همچنین مادهٔ ۵۰۶ نیز در باب اجتماع مباشر و سبب، معیار «اقوی بودن سبب از مباشر» را مطرح می‌کند. در مرگ‌های ناشی از فشار روانی، «اقوی بودن» نه به معنای قدرت فیزیکی، بلکه به معنای «سیطرهٔ روانی و سلب قدرتِ

تصمیم‌گیری عقلانی» از بزه‌دیده است. درواقع، زمانی که مرتکب با «تحقیر مستمر»، بزه‌دیده را به «بن‌بست روانی» می‌کشاند، او را در وضعیتی قرار می‌دهد که مرگ را تنها راه گریز می‌بیند؛ در این حالت، «اراده» که رکن اساسی مباشرت است، مخدوش شده و تسبیب تقویت می‌شود (کوشا و علی‌نژاد، ۱۳۹۲: ۱۵۱ـ ۱۷۰).

از سوی دیگر، معاونت در جرم به‌موجب مادهٔ ۱۲۶ همان قانون، زمانی محقق است که شخص بدون انجام عنصر مادی اصلی، نقش تبعی ایفا کند. با این وصف، در موضوع خودکشی برانگیخته، اگر رفتار مرتکب صرفاً در حد تشویق مقطعی باشد، سخن گفتن از معاونت نیز با دشواری روبه‌روست، زیرا خودکشی در حقوق ایران جرم‌انگاری مستقل نشده است. اما هرگاه رفتار از سطح ترغیب ساده عبور کند و به «ایجاد وضعیت سلطه» بینجامد، موضوع از قالب معاونت خارج می‌شود. بنابراین، نباید با تقلیلِ این رفتارها به معاونت، از مسئولیت اصلی مرتکب در جایگاه «سبب مغلوب‌کنندهٔ اراده» غفلت کرد. مبانی فقهی همچون «قاعدهٔ غرور» و «قاعدهٔ لاضرر» نیز مؤید این است که هرگاه شخصی با ابزارهای روانی، دیگری را در معرض هلاکت قرار دهد، ضامن است (احسان‌پور، ۱۴۰۰: ۱۱ـ ۲۸). نتیجه آنکه اگر مرتکب با علم به وضعیت خاص بزه‌دیده و با اعمال سلطهٔ روانی مداوم، قدرت تصمیم‌گیری آزاد را به نحو جدی مختل کند، اقدام نهایی بزه‌دیده را نمی‌توان «اراده‌ای مستقل» تلقی کرد که رابطهٔ سببیت را قطع می‌کند. در چنین فرضی، تحلیل قضیه در سطح تسبیب در جنایت از جهت حقوقی استوارتر از توسل به مفهوم معاونت است، زیرا در تسبیب، برخلاف معاونت، بر «رابطهٔ علیت میان رفتار و نتیجه» تأکید می‌شود، نه صرفاً همکاری در فعل غیر. در موارد استثنایی که نقش رفتار مرتکب بر ارادهٔ بزه‌دیده غلبهٔ کامل دارد، حتی می‌توان از نوعی مباشرت حکمی سخن گفت، مشروط بر آنکه «معیار عرفی» براساس اوضاع و احوال، فعل بزه‌دیده را مستقیماً به فشار روانی مرتکب نسبت دهد.

۲ـ ۲. معیارهای تمایز میان معاونت در خودکشی، تسبیب در جنایت و قتل

تمایز میان معاونت در خودکشی تسبیب در جنایت و قتل در گام نخست به ماهیت نقش مرتکب در فرایند منتهی به مرگ باز می‌گردد، زیرا همهٔ اشکال مداخله در خودکشی دیگری از حیث شدت تأثیر و درجهٔ انتساب در یک مرتبه قرار نمی‌گیرند. هرگاه رفتار شخص ثالث صرفاً در حد ترغیب تشویق

یا تقویت روانی تصمیمی باشد که بزه‌دیده هنوز آن را با ارادهٔ مستقل و قدرت انتخاب متعارف اتخاذ می‌کند سخن از قتل یا حتی تسبیب در جنایت با دشواری جدی روبه‌روست. در این فرض مداخلهٔ مرتکب از نظر تحلیلی به قلمرو معاونت نزدیک می‌شود هرچند در حقوق ایران از آنجا که خودکشی عنوان مجرمانهٔ مستقل ندارد معاونت در آن نیز به معنای مصطلح قابل تحقق نیست و به همین جهت اتکای صرف به مفاهیم عام معاونت همیشه پاسخ‌گو نخواهد بود. برعکس هرگاه رفتار مرتکب از حد تشویق لفظی فراتر رود و با ایجاد وضعیت روانی مستمر و فرساینده، قدرت تصمیم‌گیری متعارف بزه‌دیده را متزلزل سازد موضوع وارد قلمرو تسبیب می‌شود، زیرا در اینجا مرتکب تنها مشوق نیست، بلکه سازندهٔ مسیری است که به مرگ می‌انجامد (نادری، ۱۴۰۳: ۹۳).

معیار اساسی در تسبیب، استناد عرفی نتیجه به رفتار مرتکب است و این استناد زمانی قوت می‌گیرد که چند عنصر در کنار هم احراز شود: استمرار رفتارهای آزارنده، آگاهی مرتکب از آسیب‌پذیری خاص بزه‌دیده، قابلیت پیش‌بینی مرگ و نقش غالب فشار روانی در سلب یا اختلال شدید اراده. در چنین فرضی، اقدام نهایی بزه‌دیده دیگر لزوماً حلقه‌ای مستقل و قاطع در زنجیرهٔ سببیت تلقی نمی‌شود، بلکه ممکن است جلوهٔ پایانی فرایندی باشد که عامل اصلی آن مرتکب بوده است. مادهٔ ۴۹۲ قانون مجازات اسلامی در انتساب جنایت به رفتار مرتکب بر معیار استناد تکیه دارد و مادهٔ ۵۰۶ نیز در فرض اجتماع سبب و مباشر حکم به مسئولیت سبب اقوی از مباشر داده است. این دو حکم در کنار مادهٔ ۲۹۰ همان قانون نشان می‌دهد که حقوق کیفری ایران در صورت احراز سببیت قوی و سوء نیت لازم ظرفیت عبور از تحلیل ساده‌انگارانهٔ معاونت را دارد. بنابراین تسبیب در جنایت در این حوزه زمانی قابل دفاع است که فشار روانی از یك عامل حاشیه‌ای به سبب مؤثر و غالب در وقوع مرگ تبدیل شده باشد (همان: ۹۰). قتل در شدیدترین سطح انتساب زمانی قابل طرح است که رفتار مرتکب نه فقط سبب‌ساز بلکه از منظر حقوقی و عرفی در حکم عامل اصلی سلب حیات ارزیابی شود در این مرحله باید ثابت شود که مرتکب یا قصد نتیجه را داشته یا با علم به وضعیت ویژهٔ بزه‌دیده رفتاری را ادامه داده که نسبت به آن شخص نوعاً کشنده بوده است. بند پ مادهٔ ۲۹۰ قانون مجازات اسلامی از همین منظر اهمیت دارد، زیرا جنایت عمدی را در فرض آگاهی مرتکب به وضعیت خاص مجنی علیه و نوعاً کشنده بودن رفتار نسبت به او قابل تحقق می‌داند. از این رو اگر بزه‌دیده در وضعیت شکنندهٔ روانی قرار داشته و مرتکب با علم به این وضعیت به تهدید

تحقیر و سلطهٔ مخرب ادامه داده باشد می‌توان در موارد استثنایی از عنوان قتل سخن گفت، هرچند این تفسیر نیازمند احتیاط مضاعف است و نباید به توسعهٔ بی‌ضابطهٔ قلمرو قتل بینجامد. درواقع مرز میان تسبیب و قتل در شدت انتساب و درجهٔ احراز عنصر معنوی نهفته است؛ یعنی هرچه نقش مرتکب در زوال اراده و تحقق مرگ مسلط‌تر و آگاهانه‌تر باشد تحلیل به سوی قتل عمدی نزدیک‌تر می‌شود (شریفی خضارتی، ۱۴۰۰: ۸۷).

معیار نهایی برای تفکیک این سه عنوان نه شکل ظاهری رفتار بلکه میزان سلطهٔ علّی و روانی مرتکب بر فرایند منتهی به مرگ است. هرجا بزه‌دیده با ارادهٔ آزاد و مستقل تصمیم نهایی را اتخاذ کرده باشد توسعهٔ عنوان قتل فاقد مبنای حقوقی است و حتی تسبیب نیز باید با احتیاط پذیرفته شود، اما هرگاه مرتکب با رفتاری نظام‌مند و مستمر، اختیار متعارف بزه‌دیده را تحلیل ببرد و مرگ به نحو قابل پیش‌بینی از همان وضعیت ناشی شده باشد، استناد نتیجه به او در قالب تسبیب یا در فروض شدیدتر در قالب قتل قابل دفاع خواهد بود؛ به بیان دقیق‌تر معاونت ناظر به تأثیر تبعی است، تسبیب ناظر به ایجاد یا تقویت سبب مؤثر است و قتل ناظر به استیلا بر فرایند سلب حیات در سطحی است که اقدام ظاهری بزه‌دیده استقلال حقوقی خود را ازدست می‌دهد. این تفکیک با اصول قانون مجازات اسلامی و منطق تفسیر مضیق سازگارتر است و از خلط میان مداخلهٔ اخلاقاً نکوهیده و مسئولیت کیفری شدید جلوگیری می‌کند.

۲ـ۳. امکان‌سنجی انتساب عنوان قتل در حقوق کیفری ایران

امکان‌سنجی انتساب عنوان قتل در حقوق کیفری ایران در مرگ‌های ناشی از فشار روانی مستمر، مستلزم تطبیق این رفتارها با ساختار قانونی جنایات علیه نفس، به‌ویژه جنایت عمدی است. در نظام حقوقی ایران بر پایهٔ مادهٔ ۲۸۹ قانون مجازات اسلامی، جنایات بر نفس به عمدی، شبه‌عمدی و خطای محض تقسیم می‌شوند و برای تحقق هر یک از این عناوین، احراز رفتار مادی، انتساب نتیجه و عنصر روانی ضروری است. در مواردی که مرتکب بدون صدمهٔ فیزیکی و از طریق اعمال خشونت روانی شدید، زمینه‌ساز مرگ بزه‌دیده می‌شود، انتساب عنوان قتل عمدی با دشواری‌های تفسیری مواجه است. با این حال، بند «پ» مادهٔ ۲۹۰ قانون مجازات اسلامی مقرر می‌دارد هرگاه مرتکب کار نوعاً غیرکشنده‌ای انجام دهد که نسبت به بزه‌دیده به‌علت بیماری، پیری، ناتوانی یا وضعیت خاص او نوعاً موجب جنایت شود و مرتکب به آن وضعیت آگاهی داشته باشد، جنایت عمدی

خواهد بود (حسین‌زاده، ۱۳۹۹: ۱۳۲). در تحلیل این بند، باید میان «بیماری و ناتوانی جسمی» و «وضعیت خاص روانی» تفکیک قائل شد. شکنندگی شدید روانی بزه‌دیده، از نظر علمی می‌تواند به‌عنوان «وضعیت خاص» تفسیر شود؛ اما از منظر تفسیری، تسری این عنوان به وضعیت‌های روانی مبهم بدون وجود سابقهٔ درمانگاهی یا اختلالات روانی ثبت‌شده، با مانع روبه‌روست. استمرار رفتارهای آزاردهندهٔ روانی تنها در صورتی در قلمرو رفتارهای نوعاً کشنده قرار می‌گیرد که مرتکب با «علم پیشینی و مؤثر» به این شکنندگی خاص، رفتاری را پیش بگیرد که به‌طور مستقیم به فروپاشی روانی بزه‌دیده بینجامد.

با وجود این ظرفیت نظری، اعمال عنوان قتل عمدی در رویهٔ قضائی با موانع جدی روبه‌روست. نخستین مانع، اصل تفسیر مضیق قوانین کیفری و لزوم حفظ مرز میان اخلاق و حقوق جزاست، زیرا اثبات کارکرد سلب‌کنندهٔ حیات در رفتارهای غیرمادی همواره با تردید همراه است. درواقع، تسری رفتارهای غیرفیزیکی به بند «پ» مادهٔ ۲۹۰، به‌دلیل فقدان تصریح مقنن درخصوص «رفتارهای روانی»، ممکن است به توسعهٔ غیرقانونی دامنهٔ شمول جرم قتل عمدی منجر شود. مانع دوم، لزوم احراز رابطهٔ سببیت بی‌واسطه یا متعارف میان رفتار مرتکب و خودکشی بزه‌دیده است؛ به گونه‌ای که بتوان اقدام به خودکشی را فاقد وصف ارادهٔ مستقل دانست. در فقه امامیه نیز هرگاه مباشر در انجام جنایت دارای ارادهٔ آزاد باشد، مسئولیت به او منتسب می‌شود و انتساب نتیجه به سبب تنها در صورتی پذیرفته است که سبب اقوی از مباشر باشد. در راستای اعمال این قاعدهٔ فقهی، مفهوم «اقوی بودن سبب» در امور روانی باید با تکیه بر «معیارهای سنجش‌پذیر» تحلیل شود؛ بدین معنا که آیا فشار روانی اعمال‌شده به حدی بوده است که از نظر عرفی، «اختیار تصمیم‌گیری متعارف» را از فرد سلب کند یا خیر. بر این اساس، در حقوق کیفری ایران، انتساب عنوان قتل در فرضی که بزه‌دیده خود اقدام به سلب حیات می‌کند، تنها زمانی امکان‌پذیر خواهد بود که اثبات شود اراده و اختیار بزه‌دیده در اثر رفتارهای مستمر مرتکب به‌طور کامل زایل شده یا به گونه‌ای مخدوش گردیده که اقدام او فاقد ارزش حقوقی به‌عنوان انتخاب آزادانه بوده است (خسروی‌زاد، ۱۳۹۶: ۵۱).

انتساب عنوان قتل عمدی در حقوق کیفری ایران به مرگ‌های ناشی از فشار روانی، هرچند از حیث نظری و با استناد به بند «پ» مادهٔ ۲۹۰ قانون مجازات اسلامی ناممکن نیست، اما در عمل نیازمند اثبات استانداردهای بسیار سخت‌گیرانه است. این انتساب تنها زمانی با اصول حقوق جزا

سازگار خواهد بود که دادگاه بر پایهٔ ادلهٔ قطعی ازجمله گزارش‌های تخصصی روان‌پزشکی قانونی و مستندات دیجیتال، احراز کند مرتکب با سوءنیت خاص یا علم به وضعیت شکنندهٔ بزه‌دیده، رفتاری مستمر و فرساینده اعمال کرده که به‌طور مستقیم ارادهٔ آزاد او را زایل ساخته است (میرزایی، ۱۳۹۹: ۳۳ـ ۴۹). در غیاب چنین استانداردهای اثباتی محکمی، تمسک به قتل عمدی اساساً فاقد وجاهت قانونی است. بنابراین، در مواجهه با چالش‌های اثباتی عنصر روانی و مادی، راهکار منصفانه‌تر و منطبق بر اصول حقوقی، تفکیک میان فروض است؛ بدین ترتیب که در موارد عدم احراز زوال کامل اراده، رفتار مرتکب حسب مورد در قالب «تسبیب در جنایت غیرعمدی» (موضوع مواد ۴۹۲ و ۵۰۶) یا حتی «معاونت در خودکشی» (در صورت انطباق با بندهای مادهٔ ۱۲۶) تحلیل شود. افزون بر این، برای پر کردن خلأ قانونی موجود، پیگیری اصلاحات قانون‌گذاری جهت «جرم‌انگاری مستقل خشونت روانی شدید» و «سوق دادن به خودکشی» به‌عنوان جرائم خاص علیه تمامیت روان‌شناختی اشخاص، رویکردی اصولی‌تر و سازگارتر با اصل قانونی بودن جرائم و مجازات‌ها به‌شمار می‌رود.

۳. چالش‌های اثباتی در مرگ‌های ناشی از فشار روانی

۳ـ۱. چالش‌های اثبات فشار روانی، تحقیر مستمر و زوال اراده

در حقوق کیفری ایران، اثبات اینکه فشار روانی یا تحقیر مستمر به مرتبه‌ای رسیده که ارادهٔ بزه‌دیده را مختل یا زایل کرده، با دشواری‌های جدی روبه‌روست. نخست آنکه قانون‌گذار عنوان مستقلی با نام خشونت روانی یا تحقیر مستمر پیش‌بینی نکرده و به همین سبب، رفتارهای مزبور ناگزیر باید ذیل عناوین پراکنده‌ای چون توهین موضوع مادهٔ ۶۰۸، تهدید موضوع مادهٔ ۶۶۹، مزاحمت و سایر رفتارهای موهن تحلیل شود. از این رو، دادرس در مقام رسیدگی نه با یک عنوان کیفری منسجم، بلکه با مجموعه‌ای از رفتارهای متنوع و گاه پراکنده مواجه است که اثبات پیوستگی و استمرار آن‌ها نیازمند ادله‌ای فراتر از ادعای صرف شاکی است. در چنین وضعی، استناد به مادهٔ ۱۶۰ قانون مجازات اسلامی و ادله‌ای مانند شهادت، اسناد و امارات، تنها زمانی کارآمد خواهد بود که قرائن موجود بتواند الگوی مستمر آزار، تحقیر و فشار را به نحو منقح و منسجم آشکار سازد. علاوه بر این، در مقام اثباتِ استمرار و سازمان‌یافتگی رفتار، دادرسان کیفری ناگزیر از تمسک به «امارات قضائی متواتر» هستند تا بتوانند عنصر مادیِ مرکب و مستمرِ این پدیده را احراز کنند؛ چراکه هر یک از

رفتارهای مرتکب به‌تنهایی ممکن است واجد وصف مجرمانه مستقل یا مؤثر در سلب حیات نباشد، اما تجمیع و هم‌افزایی آن‌ها در طول زمان، موجدِ یک خطر مستمر و مرگبار است.

چالش دوم، اثبات رابطه میان این رفتارها و زوال اراده است. در حقوق کیفری، زوال یا اختلال اراده غالباً در مباحثی مانند اکراه، اجبار، اضطرار، جنون و فقدان قوهٔ تمییز بررسی می‌شود و انتقال این مفاهیم به قلمرو فشار روانی مستمر، نیازمند دقتی مضاعف است. صرف اندوه، درماندگی، ترس یا فرسایش عاطفی برای احراز زوال اراده کفایت نمی‌کند؛ بلکه باید احراز شود که رفتار مرتکب به گونه‌ای مستمر، هدفمند و فرساینده بوده که در نتیجهٔ آن، استقلال تصمیم‌گیری بزه‌دیده به‌طور مؤثر مخدوش شده است. از منظر تحلیلِ اصولی و فقهی، زوال اراده در این فروض نباید با «جنون فقهی» خلط شود، بلکه مقصود از آن، «مسلوب‌الاختیار شدن عرفی» یا ایجاد وضعیت «اضطرار شدیدِ غیرقابل تحمل» است که در آن، بزه‌دیده فاقد «ارادهٔ مؤثر و مستقل» در اتخاذ تصمیمات متعارف قلمداد می‌شود. به عبارت دیگر، ارادهٔ مادی بزه‌دیده باقی است، اما ارادهٔ حقوقی و تصمیم‌گیری آزادانهٔ او تحت سیطرهٔ مطلق روانی مرتکب، محو شده است. در پرونده‌های مربوط به مرگ ناشی از خودکشی برانگیخته، این دشواری دوچندان است، زیرا دادگاه باید میان یک تصمیم ظاهراً خودخواسته و اثری که فشار مداوم بر ساختار روانی قربانی بر جای گذاشته، تفکیک کند. در این میان، نظریهٔ پزشکی قانونی، سوابق درمانی، پیام‌ها، مکاتبات، شهادت اشخاص مطلع و اوضاع و احوال رابطهٔ طرفین، نقش تعیین‌کننده دارند و بدون تجمیع این قرائن، انتساب رفتار مرتکب به نتیجهٔ مرگ با مانع جدی مواجه می‌شود. تکوین این رابطهٔ استنادِ حقوقی مستلزم ارائهٔ تصویری روشن از «فروپاشی تدریجی سیستم دفاع روانی» قربانی است که کارشناسان روان‌پزشکی قانونی باید به‌طور دقیق، رابطهٔ علیت فرایندی میان رفتارهای مرتکب و زوال قوای تصمیم‌گیری بزه‌دیده را تأیید کنند؛ در غیر این صورت، رابطهٔ سببیت به‌دلیل دخالت ارادهٔ مادیِ بزه‌دیده قطع‌شده تلقی خواهد شد.

۳ـ ۲. نقش ادلهٔ کارشناسی، روان‌پزشکی، روان‌شناسی و ادلهٔ دیجیتال

در پرونده‌های مربوط به مرگ‌های ناشی از فشار روانی، ادلهٔ کارشناسی مهم‌ترین ابزار برای عبور از سطح ادعا و ورود به مرحلهٔ احراز قضائی است. از آنجا که آثار آزار روانی، تحقیر مستمر و فرسایش اراده غالباً در قالب نشانه‌های ظاهری مستقیم بروز نمی‌کند، دادرس ناگزیر است به نظریه‌های تخصصی روان‌پزشکی قانونی و روان‌شناسی استناد کند تا هم وضعیت پیشین بزه‌دیده و هم آثار

تدریجی رفتار مرتکب روشن شود. در این میان، روان‌پزشکی بیشتر ناظر بر تشخیص اختلالات بالینی، افسردگی، اضطراب شدید، افکار خودکشی و امکان انتساب یا تشدید آن‌ها به رفتارهای بیرونی است، در حالی که روان‌شناسی بر الگوی رابطه، تداوم آزار، سازوکارهای سلطه، وابستگی عاطفی، و فرسایش تدریجی تصمیم‌گیری متمرکز می‌شود. از منظر حقوقی، این نظریه‌ها به خودی خود دلیل مستقل بر انتساب کیفری نیستند، اما در کنار ادلهٔ مندرج در مادهٔ ۱۶۰ قانون مجازات اسلامی و در پرتو علم قاضی، می‌توانند حلقهٔ اتصال میان رفتار آزارنده و نتیجهٔ مرگ را تقویت کنند. به‌ویژه هنگامی که گزارش کارشناسی بر وجود نشانه‌های مکرر ترس، انزوا، تحقیر، یا درماندگی روانی دلالت داشته باشد، امکان تحلیل دقیق‌تر رابطهٔ سببیت فراهم می‌شود (احمدی، ۱۴۰۴: ۸۰).

در کنار ادلهٔ کارشناسی، ادلهٔ دیجیتال جایگاهی تعیین‌کننده دارد، زیرا بخش مهمی از خشونت روانی در بستر ارتباطات الکترونیکی رخ می‌دهد. پیامک‌ها، گفت‌وگوهای شبکه‌های اجتماعی، فایل‌های صوتی، تصاویر، تماس‌های ثبت‌شده، سوابق حذف یا تکرار مزاحمت، و نیز داده‌های فنی مربوط به زمان و مکان ارتباط، می‌توانند استمرار، شدت و جهت‌گیری رفتار مرتکب را آشکار کنند. در این زمینه، مادهٔ ۱۲ قانون تجارت الکترونیکی، دادهٔ پیام را در حکم نوشته دانسته و قابلیت استناد آن را در فرایند دادرسی تقویت کرده است. بنابراین، چنانچه اصالت و انتساب داده‌ها از طریق کارشناسی فنی احراز شود، این ادله می‌توانند نقش مهمی در اثبات آزار مستمر و تهدید یا تحقیر ایفا کنند. با این حال، ارزش اثباتی ادلهٔ دیجیتال هنگامی کامل می‌شود که همراه با قرائن بیرونی مانند شهادت شهود، سوابق درمانی، گزارش‌های اورژانس اجتماعی و نظر متخصصان روان‌پزشکی و روان‌شناسی ارزیابی شود، زیرا متن یک پیام به‌تنهایی برای اثبات زوال اراده کافی نیست، اما در کنار سایر قرائن می‌تواند الگوی فشار مستمر و هدفمند را به نحو قابل قبول نشان دهد (رضایی، ۱۳۹۷: ۹۲).

در این گونه پرونده‌ها کارآمدترین شیوهٔ اثبات، اتکا به یک دلیل منفرد نیست، بلکه تجمیع منظم ادلهٔ تخصصی و دیجیتال در چارچوب یک زنجیرهٔ استدلالی منسجم است. دادگاه زمانی می‌تواند از حد ظن و احتمال عبور کند که نظریهٔ کارشناسی، محتوای داده‌های دیجیتال و اوضاع و احوال رابطهٔ طرفین، همدیگر را تأیید کنند و نشان دهند که رفتار مرتکب صرفاً موجب رنج عاطفی گذرا نبوده، بلکه به فرسایش تدریجی سلامت روان و تضعیف جدی اراده منتهی شده است. در غیر این صورت، تکیه بر برداشت‌های کلی از فشار روانی، برای انتساب نتیجهٔ مرگ کفایت ندارد و تحلیل پرونده باید در چارچوب عناوین متعارف کیفری و با رعایت اصل تفسیر مضیق قوانین جزایی انجام گیرد.

۳ـ۳. ارزیابی قضائی ادله و دشواری‌های احراز سوءنیت و سببیت

در مرگ‌های ناشی از فشار روانی، ارزیابی قضائی ادله صرفاً به شمارش دلایل محدود نمی‌شود، بلکه دادگاه باید پیوند منطقی میان رفتار انتسابی، وضعیت روانی بزه‌دیده و نتیجهٔ مرگ را احراز کند. مطابق مادهٔ ۱۶۰ قانون مجازات اسلامی، ادلهٔ اثبات در امور کیفری شامل اقرار، شهادت، قسامه، سوگند در موارد مقرر قانونی و علم قاضی است و در چنین پرونده‌هایی، علم قاضی معمولاً از مجموعه قرائن، اسناد، گزارش‌های کارشناسی، داده‌های دیجیتال، شهادت اشخاص مطلع و اوضاع و احوال رابطهٔ طرفین حاصل می‌شود. دشواری اصلی آن است که فشار روانی غالباً در قالب رفتارهای تدریجی، پراکنده و غیرجسمانی مانند تحقیر، تهدید، طرد عاطفی، کنترل‌گری، تخریب حیثیت یا ایجاد ناامنی روانی بروز می‌کند و هر یک از این رفتارها، به‌تنهایی ممکن است برای انتساب نتیجهٔ مرگ کافی نباشد. از این رو، دادگاه باید بررسی کند که آیا این رفتارها درمجموع، الگوی مستمر و هدفمند آزار را تشکیل داده‌اند یا صرفاً نشانهٔ اختلاف، تنش یا سوء معاشرت بوده‌اند. در این مسیر، نظریهٔ روان‌پزشکی قانونی و روان‌شناسی اهمیت ویژه دارد، زیرا می‌تواند وضعیت روانی قربانی، میزان آسیب‌پذیری، سابقهٔ افسردگی یا افکار خودکشی و تأثیر رفتار مرتکب بر تضعیف اراده را برای مرجع قضائی روشن سازد (مصلح، ۱۴۰۴: ۶۵). احراز سوءنیت و سببیت در این پرونده‌ها با معیارهای سخت‌گیرانهٔ حقوق کیفری سنجیده می‌شود. براساس مواد ۲۸۹ و ۲۹۰ قانون مجازات اسلامی، جنایت بر نفس زمانی عمدی تلقی می‌شود که مرتکب قصد ایراد جنایت داشته باشد یا رفتاری انجام دهد که نوعاً موجب جنایت شود، یا با علم به وضعیت خاص بزه‌دیده، عملی را مرتکب شود که نسبت به او نوعاً کشنده محسوب گردد. در مرگ ناشی از خودکشی برانگیخته، اثبات این عناصر دشوارتر است، زیرا آخرین فعل مادی توسط خود بزه‌دیده انجام می‌شود و همین امر، رابطهٔ سببیت را با تردید مواجه می‌سازد. بنابراین، دادگاه باید احراز کند که رفتار مرتکب صرفاً یکی از عوامل زمینه‌ای نبوده، بلکه در زنجیرهٔ علیت، نقش مؤثر و غالب داشته است. همچنین باید روشن شود که مرتکب از وضعیت آسیب‌پذیر قربانی آگاه بوده و با وجود این آگاهی، رفتارهای فرساینده را ادامه داده است. در غیر این صورت، انتساب نتیجهٔ مرگ به او با اصولی مانند تفسیر مضیق قوانین کیفری، اصل شخصی بودن مسئولیت کیفری و ضرورت احراز رابطهٔ سببیت متعارف سازگار نخواهد بود (نادری، ۱۴۰۳: ۱۱۲).

باید میان تأثیر روانی رفتار مرتکب و سببیت کیفری منتهی به مرگ تفکیک دقیق صورت گیرد. هر رفتار تحقیرآمیز یا آزارنده، هرچند از جهت اخلاقی و حتی در مواردی از جهت کیفری قابل تعقیب باشد، لزوماً سبب حقوقی مرگ محسوب نمی‌شود. انتساب چنین نتیجهٔ سنگینی زمانی قابل دفاع است که دادگاه بر پایهٔ ادلهٔ معتبر احراز کند فشار روانی اعمال‌شده، مستمر، هدفمند، قابل پیش‌بینی و متناسب با وضعیت خاص بزه‌دیده بوده و ارادهٔ او را به نحوی مؤثر از استقلال خارج کرده است. در فقدان این سطح از اثبات، مسئولیت مرتکب باید در حدود عناوین مسلم‌تر مانند توهین، تهدید، افترا، مزاحمت یا سایر جرائم قابل انطباق بررسی شود و توسعهٔ عنوان قتل یا سببیت مرگ، بدون پشتوانهٔ اثباتی کافی، با مبانی مسلم حقوق جزا سازگار نیست.

نتیجه‌گیری

پژوهش حاضر در بررسی امکان انتساب قتل در مرگ‌های ناشی از فشار روانی، تحقیر مستمر و سوق دادن بزه‌دیده به خودکشی، به این جمع‌بندی می‌رسد که اگرچه در حقوق کیفری ایران نص صریحی که این وضعیت را به‌طور مستقیم در قالب قتل عمد تنظیم کرده باشد، مشاهده نمی‌شود، ظرفیت تحلیلی برخی مقررات قانون مجازات اسلامی مصوب ۱۳۹۲، به‌ویژه در حوزهٔ انتساب نتیجه و سببیت، امکان صورت‌بندی محدود و مشروط این بحث را فراهم می‌سازد. با این حال، پذیرش چنین انتسابی منوط به آن است که از یک سو رفتار مرتکب واجد چنان شدت، تکرار و جهت‌مندی باشد که از سطح فشار روانی متعارف فراتر رود و در زمرهٔ خشونت روانی شدید قرار گیرد، و از سوی دیگر، رابطهٔ میان این رفتار و مرگ بزه‌دیده، بر پایهٔ معیارهایی عینی و قابل احراز، به نحو متعارف و حقوقی اثبات شود. در همین چارچوب، مقاله نشان می‌دهد که صرف ادعای تحقیر، تهدید یا آزار روانی برای انتساب نتیجهٔ مرگ کافی نیست، بلکه دادگاه باید مجموعه‌ای از شاخص‌های عملی را احراز کند؛ ازجمله استمرار و تراکم رفتار آزاردهنده در یک بازهٔ زمانی معنادار، هدفمند بودن رفتارها در جهت تخریب شخصیت، انقیاد روانی یا فروپاشی عاطفی بزه‌دیده، وجود قرائن روشن از تأثیر شدید این رفتارها بر کارکردهای شناختی و ارادی قربانی، و نیز نبود عامل مستقل و قاطع دیگری که نتیجهٔ مرگبار را توضیح دهد. به بیان دیگر، زوال اراده زمانی قابل احراز است که ادلهٔ کارشناسی، به‌ویژه نظر روان‌پزشکی قانونی، نشان دهد بزه‌دیده در اثر فشارهای وارده، توان تصمیم‌گیری آزاد و

متعارف خود را به نحو جدی از دست داده و رفتار نهایی او، نه محصول انتخابی مستقل، بلکه برآیند وضعیت روانی برساخته به‌وسیلهٔ رفتار مستمر مرتکب بوده است.

بر این اساس، رابطهٔ سببیت عرفی نیز تنها در صورتی قابل پذیرش است که میان رفتار مرتکب و نتیجهٔ نهایی، پیوندی روشن، مستمر و غیرگسسته برقرار باشد؛ به نحوی که عرف و تحلیل قضائی، مرگ را نتیجهٔ دور یا اتفاقی رفتار ندانند، بلکه آن را محصول قابل انتساب همان فرایند آزار روانی قلمداد کنند. در این مسیر، بررسی سابقهٔ روانی بزه‌دیده، وضعیت آسیب‌پذیری او، محتوای پیام‌ها، گفتارها و تعاملات ثبت‌شده، شهادت نزدیکان، گزارش‌های تخصصی پزشکی قانونی، و تحلیل زمان‌بندی میان تشدید آزارها و وقوع نتیجه، نقشی اساسی در احراز دعوا دارد. بنابراین، مقاله در پاسخ به ایراد مربوط به فقدان معیارهای اجرایی، بر این نکته تأکید می‌کند که مرز میان فشار روانی متعارف و خشونت روانی شدید، نه بر مبنای برداشت‌های ذهنی، بلکه بر پایهٔ شدت، استمرار، هدف‌مندی، آثار قابل سنجش روانی و انحصار نسبی علت قابل تعیین است. درنهایت، نتیجهٔ تحقیق آن است که انتساب قتل در این قلمرو باید استثنایی، مضیق و مبتنی بر ادلهٔ فنی و قضائی متقن باشد و تنها در فرضی پذیرفتنی است که زوال اراده و رابطهٔ سببیت، به نحو روشن و اقناع‌کننده احراز شود؛ در غیر این صورت، توسعهٔ عنوان قتل به این موارد، با اصل تفسیر مضیق قوانین کیفری و الزامات قطعیت در انتساب کیفری سازگار نخواهد بود.

حامی مالی:

این مقاله هیچ حامی مالی ندارد.

مشارکت نویسندگان:

زینب باقری‌نژاد: مفهوم‌سازی، نظارت بر داده‌ها، اعتبارسنجی، مدیریت پروژه، منابع.

میلاد چکاو و مرجان محرم: روش‌شناسی، تحلیل، نوشتن بررسی و ویرایش، تحقیق و بررسی، پیش‌نویس اصلی.

تعارض منافع:

بنا بر اظهار نویسندگان این مقاله تعارض منافع ندارد.

ملاحظات اخلاقی:

این پژوهش بر پایهٔ مطالعهٔ اسناد، قوانین، رویه‌های قضائی و منابع کتابخانه‌ای انجام شده و در آن هیچ‌گونه مطالعه‌ای بر روی انسان، حیوان یا داده‌های شخصی صورت نگرفته است؛ بنابراین، اخذ تأییدیهٔ کمیتهٔ اخلاق برای این پژوهش ضروری نبوده است. با این حال، نویسنده اصول امانت‌داری علمی، صداقت پژوهشی، استناددهی صحیح و رعایت حقوق مالکیت فکری را در تمامی مراحل پژوهش رعایت کرده است.

در تهیهٔ این مقاله از ابزارهای هوش مصنوعی مولد صرفاً برای کمک به ویرایش زبانی، بهبود ساختار نگارش و ارتقای خوانایی متن استفاده شده است. این ابزارها در طراحی پژوهش، تحلیل علمی، تفسیر یافته‌ها، استنتاج نتایج یا تصمیم‌گیری‌های پژوهشی نقشی نداشته‌اند و مسئولیت کامل صحت، اصالت و محتوای نهایی مقاله بر عهدهٔ نویسنده/ نویسندگان است.

موافقت نویسندگان:

تمامی نویسندگان نسخهٔ نهایی مقاله را مطالعه و تأیید کرده‌اند و با انتشار آن موافقت دارند.

منابع

احمدی، علیرضا (۱۴۰۴)، بررسی خودکشی در فقه امامیه و حقوق موضوعهٔ ایران، تهران: چشم‌انداز قطب.

احسان‌پور، سید رضا (۱۴۰۰)، «تحلیل موجهات خودکشی از منظر فقه امامیه و حقوق کیفری ایران»، فصلنامهٔ پژوهش‌های فقه و حقوق اسلامی، ۶۳، ۱۱_۲۸

الیاسی، سامان (۱۴۰۱)، بررسی فقهی حقوقی جرم‌شناسی خودکشی، شروع و معاونت در آن با رویکرد تطبیقی، پایان‌نامهٔ کارشناسی ارشد، مؤسسهٔ آموزش عالی روزبهان، دانشکدهٔ علوم انسانی.

حسین‌زاده، پیمان (۱۳۹۹)، خودکشی؛ از تحریم فقهی تا تجریم حقوقی، تهران: میزان.

خسروی‌زاد، افشار (۱۳۹۶)، بررسی خودکشی در حقوق کیفری ایران، تهران: وارش.

رضایی، حمزه (۱۳۹۷)، معاونت در خودکشی در قانون ایران و انگلستان، تهران: پشوتن.

شریفی خضارتی، امیر (۱۴۰۰)، خودکشی (مطالعهٔ جرم‌شناسی، فقهی و حقوقی)، تهران: اندیشهٔ سبز نوین.

شفیعی مازندرانی، سید محمد (۱۳۸۹)، «ممنوعیت خودکشی از دیدگاه فقه اسلامی»، پژوهش‌های فقهی، ۱، ۳۹.

ذبیحی‌ریزی، سلمان (۱۳۹۸)، خودکشی از دیدگاه فقه جزایی، تهران: کاشف علم.

علیزاده، یعقوب (۱۴۰۰)، «تحریک دیگری به خودکشی از منظر فقه و حقوق کیفری»، فقه و حقوق تطبیقی کیفری، ۱، ۱۵۹-۱۶۹.

کیخا، حسن (۱۳۹۵)، خودکشی در حقوق جنایی، تهران: خرسندی.

کوشا، جعفر و علی‌نژاد، آذر (۱۳۹۲)، «تحریک به خودکشی؛ جرم‌انگاری یا جرم‌زدایی»، تحقیقات حقوقی، ۶۴، ۱۵۱-۱۷۰.

مصلح، زینب (۱۴۰۴)، تحلیل ابعاد حقوقی، فقهی، سیاسی، فرهنگی، اجتماعی، اقتصادی، روان‌شناسی، پزشکی پدیدهٔ شوم خودکشی و بررسی دیدگاه‌های حقوقی مخالفان و موافقان حق مرگ و راهکارهایی جهت کاهش آن، تهران: گارسه.

میرزایی، سمیرا (۱۳۹۹)، «بررسی حکم خودکشی و معاونت در آن از نظر شریعت و حقوق ایران»، رهیافت‌های نوین در مطالعات اسلامی، ۳، ۳۳ـ۴۹.

نادری، صحبت (۱۴۰۳)، خودکشی و علل حقوقی آن، تهران: آرون.

References

Binder, G., & Chiesa, L. E. (2019), "The Puzzle of Inciting Suicide", *American Criminal Law Review*, *56*, 65-133.

Bourget, D., Gagné, P., & Moamai, J. (2000), "Spousal homicide and suicide in Quebec", *Journal of the American Academy of Psychiatry and the Law*, *28*(2), 179-182.

Flynn, S., Gask, L., Appleby, L., & Shaw, J. (2016), "Homicide-suicide and the role of mental disorder: a national consecutive case series", *Social Psychiatry and Psychiatric Epidemiology*, *51*(6), 877-884.

Flynn, S., Swinson, N., While, D., Hunt, P., Roscoe, A., Rodway, C., Windfuhr, K., Kapur, N., & Appleby, L. (2009), "Homicide followed by suicide: a cross-sectional study", *The Journal of Forensic Psychiatry and Psychology*, *20*(2), 306-321.

Greenfield, P., Calcia, M., McCree, C., Sahota, M., Thomas, H., Kirkpatrick, K., Vagi, R., Howard, L., Markham, S., & Bhavsar, V. (2025), "Identifying, assessing and responding to perpetration of domestic abuse: practice guide for mental health professionals", *BJPsych Advances*, *31*(1), 8-19.

Hannah, S., Turf, E., and Fierro, M. (1998), "Murder-suicide in central Virginia: a descriptive epidemiologic study and empiric validation of Hanzlick-Koponen typology", *American Journal of Forensic Medicine and Pathology*, *19*(3), 275-283.

Hanzlick, R., & Koponen, M. (1994), "Murder-suicide in Fulton County, Georgia, 1988-1991. Comparison with a recent report and proposed

typology", *American Journal of Forensic Medicine and Pathology*, *15*(2), 168-173.

Henrion, R. (2014), "Domestic violence: any progress?", *Bulletin de l'Académie Nationale de Médecine*, *198*(4-5), 893-903.

Logan, J., Ertl, A., & Bossarte, R. (2019), "Correlates of Intimate Partner Homicide among Male Suicide Decedents with Known Intimate Partner Problems", *Suicide and Life-Threatening Behavior*, *49*(6), 1693-1706.

Marzuk, P., Tardiff, K., & Hirsch, Ch. (1992), "The Epidemiology of Murder-Suicide", *Journal of the American Medical Association*, *267*(23), 3179-3190.

Oram, H., Flynn, S., Shaw, J., Appleby, L., & Howard, L. (2013), "Mental illness and domestic homicide: a population-based descriptive study", *Psychiatric Services*, *64*(10), 1006-1011.

Panczak, R., Geissbühler, M., Zwahlen, M., Killias, M., Tal, K., & Egger, M. (2013), "Homicide-suicides compared to homicides and suicides: systematic review and meta-analysis", *Forensic Science International*, *233*(1-3), 28-36.

Pawłowska-Muc, A., Pilewska-Kozak, A., Stadnicka, G., Kęsik, J., & Dobrowolska, B. (2023), "Satisfaction with the life of Polish women experiencing domestic violence", *Frontiers in Public Health*, *11*(1073612), 1-10.

Pereira, A., Vieira, D., & Magalhães, T. (2013), "Fatal intimate partner violence against women in Portugal: a forensic medical national study", *Journal of Forensic and Legal Medicine*, *20*(8), 1099-1107.

Pottinger, A., Bailey, A., & Passard, N. (2019), "Archival data review of intimate partner homicide-suicide in Jamaica, 2007-2017: focus on mental health and community response", *Revista Panamericana de Salud Pública*, *43*(e99), 1-8.

Journal Website

Legal Innovation Quarterly

Spring 2026

Volume 2, Issue 3

E-ISSN: 3115-8498

A Comparative Analysis of the Right to Privacy of Children in the Age of Artificial Intelligence and the Digital Environment in the Legal Systems of Iran and Canada

Mansooreh Hosseini* [1], Mojtaba Farahmand [2]

1. Ph.D. Student in Criminal Law and Criminology, Faculty of Law and Humanities, Shahrekord Branch, Islamic Azad University, Shahrekord, Iran (Corresponding Author)*
2. Assistant Professor, Department of Criminal Law and Criminology, Faculty of Law, Isfahan (Khorasgan) Branch, Islamic Azad University, Isfahan, Iran.

***Corresponding author email address:** mansoureh.hosseini1404@gmail.com

Extended Abstract

1. Introduction

In the age of information technology, children are exposed to various risks, including unauthorized access to personal data, the dissemination of private images, and the commercial exploitation of personally identifiable information. The principal research question is how existing laws in Iran and Canada protect children's right to privacy in digital environments and which legal system adopts a more comprehensive approach. The protection of the privacy of children and adolescents is significant from the perspectives of criminal law and criminology, because violations of privacy may give rise to primary and secondary victimization of children. Furthermore, weaknesses in oversight mechanisms and the absence of specific criminal sanctions in this area have created a gap in criminal policy.

Received: December 31, 2025 - **Accepted:** February 6, 2026 - **Published:** March 21, 2026

Hosseini, Mansoureh; and Farahmand, Mojtaba. (2026). "A Comparative Analysis of Children's Right to Privacy in the Age of Artificial Intelligence and Digital Space under the Legal Systems of Iran and Canada." *Legal Innovation Quarterly*, 2(3), pp. 83–106.
Doi: https://doi.org/10.22034/lir.2026.2087769.1034

© 2026 The Authors. Published by Legal Innovation Research Institute, Tehran, Iran. This is an open access article distributed under the terms of the Creative Commons Attribution 4.0 International (CC BY 4.0) License.

In other words, given the increase in cybercrime against children, the absence of specific legislation on the protection of children's data in Iran, and the diversity of protective legislation in Canada, including federal and provincial laws concerning the protection of personal information, alignment of Iran's criminal policy with the international standards established by the Convention on the Rights of the Child is essential.

2. Research Methodology

This study, conducted using a descriptive-analytical-comparative method, is grounded in theories such as the theory of protective victimology, which emphasizes the need for differentiated protection of children; the theory of data security and the right to control personal information, as reflected in Canadian legal instruments; and the principle of safeguarding human dignity in Iranian jurisprudence and law, as reflected in Articles 252 and 582 of the Islamic Penal Code, which has served as a basis for privacy protection under domestic law. The objectives pursued in this article are to identify the legal and criminological challenges arising from violations of children's privacy in Iran and Canada; to compare the legal policies of the two countries concerning the protection of children's personal data and digital content; and to put forward legislative reform proposals for drafting a law on the protection of children's data in Iran.

3. Research Findings

This study examines, from a comparative perspective, the legal safeguards for the protection of children's privacy under the legal systems of Iran and Canada. The findings indicate that the Canadian legal system has established a more effective framework for safeguarding children's data, drawing on comprehensive data protection laws, transparency requirements, parental consent, and a proactive approach to emerging technologies. By contrast, the Iranian legal system has yet to establish a coherent and dedicated framework for children's personal data, platform accountability, and oversight of artificial intelligence applications, while existing protections remain fragmented and lack a specialized focus. Through a comparative analysis of laws, criminal policies, international instruments, and relevant ethical standards, this study presents measures to strengthen criminal protection, regulate technology, and ensure children's privacy in the age of artificial intelligence and the digital environment.

Children and adolescents are among the victims of the use of cyberspace and artificial intelligence, have no awareness of privacy protection, and may readily be exploited by offenders. In other words, children may lack awareness or possess limited literacy skills that prevent them from fully understanding their right to privacy and the potential long-term risks and effects of data sharing and artificial intelligence processing. They therefore have a limited capacity to assess the associated risks. In this regard, the government should

implement protective and preventive measures through educating parents, children, and adolescents about the use of cyberspace, and appropriate legal action should be taken against offenders in this area.

A comparative analysis of the two legal systems concerning the protection of the privacy of children and adolescents in Iran and Canada led to the conclusion that Canada has a more advanced system of criminal protection and preventive regulations, whereas the establishment of a comprehensive data protection system remains on Iran's agenda. The principal differences between the two systems lie in the extent of their supervisory institutions, criminal sanctions, and data-driven policymaking. In other words, although artificial intelligence and the digital environment create opportunities, they may also pose a serious threat to children's privacy. The principal differences between Iran and Canada lie in the levels of legislative development, oversight, and public education; however, no country is immune to these challenges. Furthermore, to reduce the threats arising from the use of artificial intelligence and the digital environment and to protect children and adolescents, governments should cooperate in this area, technology companies should act with greater accountability, and families should increase their awareness and keep the online environment safe for their children and adolescents.

4. Recommendations

The proposals that may be advanced in this regard include drafting a comprehensive law in Iran on the "Protection of Children's Personal Data," drawing on the Canadian model; establishing a specialized unit within Iran's Cyber Police (FATA) to investigate offences involving violations of children's privacy; and formally acceding to the Optional Protocol, with the aim of taking more substantial steps towards improving children's circumstances in cyberspace and in connection with the use of artificial intelligence, and protecting their rights in this domain.

5. Conclusion

Measures that may be considered to address the challenges threatening children and adolescents who use artificial intelligence and cyberspace in Canada include restricting targeted advertising directed at children; exercising stricter control over facial recognition technology; strengthening regulations governing artificial intelligence in education; using privacy settings; teaching children the skill of saying "no" in digital environments; engaging in active, dialogue-based supervision; and using parental control tools. Furthermore, the drafting of a comprehensive law on the protection of children's data, the imposition of an obligation on platforms to ensure transparency in the use of data, the development of digital literacy education programmes, the establishment of an independent supervisory body, the use of privacy settings,

the teaching of the skill of saying “no” in digital environments to children, active and dialogue-based supervision, and the use of parental control tools are measures that may be considered in relation to the challenges that threaten children and adolescents who use artificial intelligence and cyberspace in Iran.

Keywords: Children’s privacy; digital environment; artificial intelligence; criminal protection; Iranian legal system; Canadian legal system; data protection.

Funding
This article has no financial support or funding.

Authors' Contributions
Mansooreh Hosseini: Methodology, formal analysis, writing – review & editing, investigation, writing – original draft.
Mojtaba Farahmand: Conceptualization, data curation, validation, project administration, and resources.

Conflict of Interest
According to the authors’ declaration, there is no conflict of interest regarding this article.

Ethical Considerations
This study was conducted based on the analysis of legal documents, statutes, judicial decisions, and library-based sources. It did not involve human participants, animals, or personal data; therefore, ethical approval from an institutional ethics committee was not required. Nevertheless, the authors adhered to the principles of academic integrity, research honesty, proper citation practices, and respect for intellectual property rights throughout all stages of the research.
Generative artificial intelligence (AI) tools were used solely to assist with language editing, improving the structure of the manuscript, and enhancing the readability of the text. These tools did not contribute to the study design, scientific analysis, interpretation of findings, drawing of conclusions, or any research-related decision-making. The author(s) assume full responsibility for the accuracy, originality, and final content of the manuscript.

Authors' Approval
All authors have reviewed and approved the final version of the manuscript and agree to its publication.

بهار ۱۴۰۵
دوره ۲، شمارهٔ ۳
شاپای الکترونیکی:
۳۱۱۵-۸۴۹۸

فصلنامه نوآوری حقوقی

وبسایت مجله

تحلیل تطبیقی حق حفظ حریم خصوصی کودکان در عصر هوش مصنوعی و فضای دیجیتال در نظام‌های حقوقی ایران و کانادا

منصوره حسینی [۱*]، مجتبی فرهمند [۲]

۱. دکتری حقوق کیفری و جرم‌شناسی، دانشکدهٔ حقوق و علوم انسانی، واحد شهرکرد، دانشگاه آزاد اسلامی، شهرکرد، ایران (نویسندهٔ مسئول)
۲.استادیار گروه حقوق کیفری و جرم‌شناسی، دانشکدهٔ حقوق، واحد خوراسگان اصفهان، دانشگاه آزاد اسلامی، اصفهان، ایران.

*ایمیل نویسندهٔ مسئول: mansoureh.hosseini1404@gmail.com

چکیده

رشد فزایندهٔ فناوری‌های ارتباطی، هوش مصنوعی و رسانه‌های اجتماعی، ابعاد نوینی از حریم خصوصی کودکان را در معرض تهدید قرار داده است. کودکان در فضای دیجیتال نه‌تنها به‌عنوان کاربران فعال، بلکه به‌عنوان بزه‌دیدگان بالقوه در برابر گردآوری بی‌رویهٔ داده‌ها، پروفایل‌سازی، ردیابی رفتاری و سوءاستفادهٔ احتمالی از اطلاعات شخصی قرار دارند. پژوهش حاضر با رویکرد تطبیقی به بررسی حمایت‌های قانونی در دو نظام حقوقی ایران و کانادا در زمینهٔ حفظ حریم خصوصی کودکان می‌پردازد. یافته‌ها نشان می‌دهد که نظام حقوقی کانادا، با تکیه بر قوانین جامع حفاظت از داده‌ها، الزامات شفافیت، رضایت والدین و رویکرد پیش‌دستانه در مواجهه با فناوری‌های نوپدید، ساختاری کارآمدتر برای صیانت از داده‌های کودکان ایجاد کرده است. در مقابل، در نظام حقوقی ایران هنوز چارچوب منسجم و ویژه‌ای برای داده‌های شخصی کودکان، مسئولیت‌پذیری پلتفرم‌ها و نظارت بر کاربردهای هوش مصنوعی شکل نگرفته و حمایت‌ها پراکنده و غیرتخصصی باقی مانده است. این مطالعه با تحلیل تطبیقی قوانین، سیاست‌های جنایی، اسناد بین‌المللی و معیارهای اخلاقی مرتبط، راهکارهایی برای تقویت حمایت کیفری، تنظیم‌گری فناوری و تضمین حریم خصوصی کودکان در عصر هوش مصنوعی و فضای دیجیتال ارائه می‌دهد.

واژگان کلیدی: حریم خصوصی کودکان، فضای دیجیتال، هوش مصنوعی، حمایت کیفری، نظام حقوقی ایران، نظام حقوقی کانادا، حفاظت از داده‌ها.

دریافت‌شده در تاریخ: ۱۰ دی ۱۴۰۴ - **پذیرش‌شده در تاریخ:** ۱۷ بهمن ۱۴۰۴- **منتشرشده در تاریخ:** ۱ فروردین ۱۴۰۵

حسینی، منصوره؛ فرهمند، مجتبی. (۱۴۰۵). «تحلیل تطبیقی حق حفظ حریم خصوصی کودکان در عصر هوش مصنوعی و فضای دیجیتال در نظام‌های حقوقی ایران و کانادا». فصلنامه نوآوری حقوقی، دوره ۲، شماره ۳، صص ۸۳- ۱۰۶.

Doi: https://doi.org/10.22034/lir.2026.2087769.1034

© 2026 The Authors. Published by Legal Innovation Research Institute, Tehran, Iran. This is an open access article distributed under the terms of the Creative Commons Attribution 4.0 International (CC BY 4.0) License.

مقدمه

نقشی که هوش مصنوعی در جامعه ایفا می‌کند، رو به افزایش است و تأثیر آن بر زندگی کودکان نیز رو به افزایش است. همه‌گیری کووید ـ ۱۹ این گذار دیجیتال را تسریع کرده است. از سال ۲۰۲۰ واقعیت‌های فاصله‌گذاری اجتماعی، فعالیت‌های برخط کودکان را از یادگیری گرفته تا بازی و مراقبت‌های بهداشتی، بیشتر از پیش تغییر داد و باعث پذیرش سریع و گستردهٔ فناوری‌های مبتنی بر هوش مصنوعی شد. این تغییرات قابل توجه هستند. ظهور هوش مصنوعی این پتانسیل را دارد که زندگی کودکان را راحت‌تر و در برخی موارد عادلانه‌تر کند. با این حال، هوش مصنوعی خطرات قابل توجهی را نیز برای حریم خصوصی کودکان ایجاد می‌کند، خطراتی که کمتر مورد بررسی کارشناسان و پژوهشگران قرار گرفته‌اند. برخی از تجربیات جدید کودکان که با هوش مصنوعی همراه هستند، کاملاً مشهود هستند. قابل توجه است که کودکان امروزه می‌توانند در کنار دوستان خیالی خود با اسباب‌بازی‌های هوشمند صحبت کنند. با این حال، برخی از مهم‌ترین پیامدهای آن در زیر سطح قرار دارند، به روش‌هایی که هوش مصنوعی داده‌های تولیدشده توسط روال‌های آشنا در زندگی روزمرهٔ کودکان ثبت، ذخیره و استفاده می‌کند. عکس‌های مدرسه که از طریق اینترنت، به جای پست، به اشتراک گذاشته می‌شوند، می‌توانند تجزیه و تحلیل شوند و از طریق فناوری تشخیص چهره برای شناسایی افراد استفاده شوند. کودکان کنجکاوی که به جای والدین، از یک بلندگوی هوشمند اطلاعات می‌خواهند، نه‌تنها به خودشان آموزش می‌دهند، بلکه به هوش مصنوعی نیز می‌آموزند که صدای آن‌ها را تشخیص دهد. نمره‌دهی الگوریتمی به این معنی است که نمرهٔ ضعیف در تنها یک آزمون ریاضی فقط یک بخش عادی از یادگیری نیست، بلکه می‌تواند به‌عنوان یک نقطهٔ داده برای پیش‌بینی عملکرد و فرصت‌های آیندهٔ کودک استفاده شود. هوش مصنوعی می‌تواند از اطلاعات کودکان برای تصمیم‌گیری درمورد آن‌ها استفاده کند که بر محتوایی که می‌بینند و فرصت‌هایی که می‌توانند به آن‌ها دسترسی داشته باشند، تأثیر می‌گذارند؛ علی‌رغم این خطرات، واکنش‌های سیاسی، عمدتاً بزرگ‌سالان‌محور بوده‌اند و توجه کمی به تأثیر عمیق و متمایز هوش مصنوعی بر کودکان داشته‌اند.

به عبارت دیگر در عصر فناوری اطلاعات، کودکان در معرض خطرات متنوعی چون دسترسی غیرمجاز به داده‌های شخصی، انتشار تصاویر خصوصی و بهره‌برداری تجاری از اطلاعات هویتی قرار گرفته‌اند. پرسش اصلی این است که چگونه قوانین موجود در ایران و کانادا از حق حریم

خصوصی کودکان در محیط‌های دیجیتال حمایت می‌کنند و کدام نظام حقوقی برخورد جامع‌تری دارد؟ بحث حفظ حریم خصوصی کودکان و نوجوانان از دیدگاه حقوق جزا و جرم‌شناسی اهمیت دارد، زیرا نقض حریم خصوصی می‌تواند زمینه‌ساز بزه‌دیدگی اولیه و بزه‌دیدگی ثانویه در کودکان شود. از سوی دیگر، ضعف سازوکارهای نظارتی و نبود ضمانت اجراهای کیفری مشخص در این حوزه، سیاست جنایی را با خلأ روبه‌رو کرده است. به عبارتی با افزایش بزهکاری سایبری علیه کودکان و نبود قانون اختصاصی حفاظت از داده‌های کودکان در ایران همچنین تنوع قوانین حمایتی در کانادا (مانند قوانین فدرال و استانی در زمینهٔ حفاظت از اطلاعات شخصی) همسویی سیاست جنایی ایران با استانداردهای جهانی کنوانسیون حقوق کودک ضروری است. این پژوهش که به روش تحلیلی ـ توصیفی ـ تطبیقی انجام شده بر پایهٔ نظریه‌هایی چون نظریهٔ بزه‌دیده‌شناسی حمایتی که بر ضرورت حمایت افتراقی از کودکان تأکید دارد، نظریهٔ امنیت داده‌ها و حق کنترل شخصی بر اطلاعات که در اسناد حقوقی کانادا نمود یافته است همچنین بر اصل صیانت از حیثیت انسانی در فقه و حقوق ایران طبق مواد ۲۵۲ و ۵۸۲ قانون مجازات اسلامی، که مبنای حریم خصوصی در قوانین داخلی بوده، استوار است. اهدافی که در این مقاله به دنبال آن هستیم عبارت‌اند از: شناسایی چالش‌های قانونی و جرم‌شناختی نقض حریم خصوصی کودکان در ایران و کانادا، مقایسهٔ سیاست‌های قانونی دو کشور در حفظ داده‌های شخصی و محتوای دیجیتال کودکان، ارائهٔ پیشنهادهای اصلاحی برای تدوین قانون حمایت از داده‌های کودکان در ایران.

۱. مفاهیم

۱ـ۱. مفهوم کودکان و نوجوانان در حقوق ایران و کانادا

صرف نظر از اختلاف عقایدی که درخصوص سن مسئولیت کیفری و به‌تبع در تعریف طفل وجود دارد،طبق قانون حمایت از اطفال و نوجوانان مصوب ۱۳۹۹ مفهوم طفل در بند (الف) مادهٔ یک این‌گونه تعریف شده که: «طفل، هر فرد که به سن بلوغ شرعی نرسیده است» و سن بلوغ شرعی در کشور ایران برای دختر نه سال و برای پسر پانزده سال تمام هجری است.

براساس قانون حمایت از اطفال و نوجوانان مصوب ۱۳۹۹ مفهوم نوجوان در بند (ب) مادهٔ یک بدین نحو تعریف شده است: «نوجوان فردی است که به بلوغ شرعی رسیده اما به سن هجده سال تمام نرسیده است». البته مطابق مادهٔ دو این قانون تمام افرادی که به سن هجده سال تمام شمسی

نرسیده‌اند مشمول این قانون هستند و به‌نظر می‌رسد این تقسیم‌بندی کودک و نوجوان محلی از اعراب نداشته باشد.

مطابق با مادهٔ یک کنوانسیون حقوق کودک سازمان ملل متحد (CRC, 1989)، عمداً از اصطلاح «کودک» هنگام اشاره به «هر انسانی که زیر هجده سال سن دارد، مگر اینکه طبق قانون قابل اجرا در مورد کودک، سن بلوغ زودتر حاصل شود» استفاده خواهم کرد. از آنجایی که کانادا کنوانسیون حقوق کودک را در سال ۱۹۹۲تصویب کرد و از آنجایی که در کانادا سن بلوغ زودتر حاصل نمی‌شود، سن قانونی که کودکان کانادایی از آن حمایت می‌شوند، هجده سال است. با این حال، اصطلاحات رایج مورد استفاده برای کودکان درگیر در سیستم عدالت کیفری، یعنی «نوجوان، جوان، خردسال» و همچنین اصطلاحات انگ‌زننده «نوجوان بزهکار و مجرم جوان»، کودکان را از حقوقی که هم تحت کنوانسیون حقوق کودک و هم قانون کانادا به آن‌ها اعطا شده است، محروم می‌کنند، در حالی که آن‌ها را از «حقوق بزرگسال» برخوردار نمی‌سازند. نام سه قانون اصلی عدالت کودکان کانادا در این زمینه گویاست: قانون بزهکاران نوجوان ۱۹۰۸، قانون جوانان قانون مجرمان ۱۹۸۵ و قانون عدالت کیفری جوانان ۲۰۰۲. این مبحث اصطلاح‌شناسی بین‌المللی، قوانینی که در سه قانون و دستورالعمل سازمان ملل متحد برای کودکان درگیر در دادرسی‌های قضائی مشهود است: قوانین حداقل استاندارد برای اجرای عدالت نوجوانان ۱۹۸۵، قوانین حمایت از نوجوانان محروم از آزادی ۱۹۹۰ و دستورالعمل‌های پیشگیری از بزهکاری نوجوانان۱۹۹۰ (Chapdelaine, 2007: 268).

۲-۱. مفهوم هوش مصنوعی

به‌طور کلی به یک سیستم مبتنی بر ماشین اشاره دارد که با توجه به مجموعه‌ای از اهداف تعریف‌شده، می‌تواند وظایفی را که معمولاً به هوش انسانی نیاز دارد، مانند پیش‌بینی‌ها و تصمیم‌گیری‌ها، انجام دهد. قابل توضیح است که هوش مصنوعی نقش بسیاری در زندگی کودکان ایفا می‌کند و اساساً تجربیات و مکان‌های روزمرهٔ آن‌ها را از خانه‌هایشان گرفته تا مدارسشان و سایر خدمات و فضاهای عمومی تغییر شکل می‌دهد. در حالی که کاربرد هوش مصنوعی به سرعت گسترش یافته است، ابزارهایی برای پرداختن به چالش‌هایی که هوش مصنوعی می‌تواند برای حریم خصوصی کودکان ایجاد کند، به سرعت پیشرفت نکرده‌اند (راهنمای متخصصان حریم خصوصی برای هوش مصنوعی و یادگیری ماشین (https://fpf.org).

۱-۳. مفهوم حق بر حریم خصوصی کودکان

حق بر حریم خصوصی یکی از شاخه‌های بنیادین حقوق بشر است که در اسناد بین‌المللی همچون مادهٔ ۱۲ اعلامیهٔ جهانی حقوق بشر و مادهٔ ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی مورد شناسایی قرار گرفته است. درخصوص کودکان، مادهٔ ۱۶ کنوانسیون حقوق کودک (CRC) به‌صراحت بر حق کودک نسبت به حریم خصوصی، مکاتبات و احترام به آبرو و حیثیت تأکید دارد. حریم خصوصی کودک، گستره‌ای از اطلاعات شخصی، رفتارهای برخط و داده‌های زیستی او را دربر می‌گیرد که امروزه با ورود هوش مصنوعی، امکان تحلیل، پردازش و حتی پیش‌بینی آن‌ها فراهم شده است.

۲. تهدیدات عصر هوش مصنوعی و فضای دیجیتال برای حریم خصوصی کودکان در ایران و کانادا

با توجه به اینکه امروزه رشد سریع تکنولوژی‌های دیجیتال، شبکه‌های اجتماعی و ابزارهای مبتنی بر هوش مصنوعی، فرصت‌های بی‌سابقه‌ای برای آموزش، سرگرمی و ارتباطات کودکان فراهم کرده، اما همین تکنولوژی تهدیدات جدی برای حریم خصوصی، امنیت داده‌ها و سلامت روانی کودکان به‌وجود آورده است.

به‌علت ناآگاهی کودکان از پیامدهای انتشار اطلاعات شخصی، در برابر سوءاستفاده‌های دیجیتال آسیب‌پذیرتر از بزرگسالان بوده و به همین دلیل این چالش در کشورهای مختلف، با توجه به سطح قوانین، زیرساخت‌ها و فرهنگ دیجیتال، ابعاد مختلفی را به دنبال دارد.

زمانی که کودکان و نوجوانان از هوش مصنوعی بدون رعایت چارچوب‌های اخلاقی استفاده کنند، حریم خصوصی‌شان نقض می‌شود، در نتیجهٔ این امر ممکن است به خطرات امنیتی و تبعیض در تصمیم‌گیری‌های آموزشی منجر شود. واضح است که تدوین سیاست‌های شفافی در زمینهٔ بحث مورد نظر توسط مسئولان، آموزش معلمان و دانش‌آموزان در راستای استفادهٔ درست از هوش مصنوعی و طراحی الگوریتم‌های منصفانه و امن بسیار اهمیت دارد (بویری منجی و زارعی، ۱۴۰۴: ۱).

تأثیر هوش مصنوعی در نقض یا تهدید حریم خصوصی کودکان را می‌توان در سه سطح، دسته‌بندی کرد: سطح اول که گردآوری گستردهٔ داده‌های کودکان است، هوش مصنوعی با پروفایل‌سازی و ردیابی دیجیتال، ریسک افشای اطلاعات زیستی و مکانی، حریم خصوصی کودکان و نوجوانان را تهدید می‌کند. در سطح مذکور داده‌ها را از طریق سامانه‌های هوشمند در بازی‌های

برخط، اپلیکیشن‌های آموزشی یا شبکه‌های اجتماعی داده‌های رفتاری، صوتی و چهرهٔ کودکان، ذخیره می‌کنند؛ در سطح دوم هوش مصنوعی از طریق تولید محتوای جعلی دست به اقدامات مخرب می‌زند که این کار را با استفاده از تصاویر جعلی از کودکان، شبیه‌سازی صدای کودکان و نوجوانان، ساخت هویت جعلی از آن‌ها انجام می‌دهد. این اقدام به هوش مصنوعی امکان می‌دهد تا بتواند از کودکان و نوجوانان یا خانواده‌های آنان باج‌گیری، آزار سایبری و سوءاستفاده کند یا از آن برای تبلیغات هدفمند یا پیش‌بینی رفتار استفاده می‌کند؛ در سطح سوم هوش مصنوعی با در اختیار داشتن اطلاعات شخصی و محرمانهٔ کودکان ریسک افشای اطلاعات زیستی و مکانی را برای کودکان و نوجوانان به‌وجود می‌آورد که این تهدید با استفاده از ابزارهای هوشمند خانگی مانند دستیارهای صوتی و دوربین‌های هوشمند، گاه بدون رضایت آگاهانهٔ والدین ذخیرهٔ اطلاعات محیطی و گفت‌وگوهای خانگی برایش مقدور می‌شود؛ در سطح چهارم هوش مصنوعی با استفاده از الگوریتم‌های اعتیادآور یا پلتفرم‌هایی که با استفاده از هوش مصنوعی ارائه می‌شود، محتوایی را نمایش می‌دهند که بیشترین زمان ماندگاری کودک را تضمین کند. درنتیجه برای کودک یا نوجوان وابستگی دیجیتال، کاهش تمرکز و آسیب‌های روانی ایجاد می‌کند؛ در سطح پنجم هوش مصنوعی به ردیابی آموزشی کودکان و نوجوانان می‌پردازد، به‌گونه‌ای که بسیاری از پلتفرم‌های ارائه‌شده در دوران آموزش برخط می‌تواند وسیله‌ای باشد که رفتار یادگیری، سرعت پاسخ‌دهی و میزان توجه کودکان و نوجوانان را ثبت و تحلیل می‌کند. هوش مصنوعی با این داده‌ها به طبقه‌بندی یا برچسب‌گذاری کودکان دست می‌زند.

به عبارت دیگر، کودکان و نوجوانان حق دارند تا از فضای مناسب در جهت آموزش و رشد استفاده کنند، با این حال استفاده از هوش مصنوعی در فضای پویای فناوری و اینترنت حریم خصوصی آن‌ها را به خطر می‌اندازد که با توجه حق آموزش و رعایت حریم خصوصی، آزادی بیان و منع تبعیض مسائل و حقوق مهمی برای کودکان توجه مسئولان و متولیان این امر، ضروری است.

> استفادهٔ نامناسب از هوش مصنوعی درحق بر آموزش کودکان به نقض حریم خصوصی و آسیب داده‌های کودکان منجر شده و موجب نگرانی‌های امنیتی می‌شود. همچنین نقض تعامل انسانی موجب کاهش ارتباطات انسانی و احساساتی کودکان است. افزایش نابرابری، تبعیض، محدودیت آزادی بیان کودکان ازجمله حقوقی است که در رابطه با حق برآموزش کودکان مورد نقض جدی قرار می‌گیرد (صفاری‌نیا، ۱۴۰۳: ۱).

به سخن دیگر،

> والدین نیز در کنار استقبال از امکانات آموزشی نوین، نسبت به کاهش مرزهای بین خانه و مدرسه، نامشخص بودن نحوهٔ ذخیره و تحلیل داده‌های فرزندان، ناامنی اطلاعاتی و تضعیف استقلال و هویت کودک در مواجهه با سیستم‌های هوشمند دغدغه‌های قابل توجهی بیان کرده‌اند. تحلیل پدیدارشناسانهٔ داده‌ها آشکار می‌سازد که چالش‌های اخلاقی ادراک‌شده، بیشتر به عدم شفافیت در کارکردهای هوش مصنوعی، ناآگاهی از پیامدهای بلندمدت آن بر فرایند جامعه‌پذیری کودکان، و محدودیت معلمان و والدین در مدیریت رفتار دیجیتال کودکان بازمی‌گردد. قلمرو کودکی در عصر هوش مصنوعی نیازمند بازتعریف اصول اخلاقی، اصلاح سازوکارهای حفظ حریم خصوصی، و توانمندسازی والدین و معلمان در استفادهٔ آگاهانه از فناوری‌های هوشمند است (خلیلی و سوادی، ۱۴۰۴: ۱).

در نظام حقوقی ایران، قانون جامع و اختصاصی برای حفاظت از داده‌های مربوط به کودکان و حفظ حریم خصوصی‌شان وضع نشده که این مسئله یک چالش قانونی در رابطه با تهدیدات عصر هوش مصنوعی و فضای دیجیتال محسوب می‌شود. چارچوب‌های قانونی موجود پراکنده و کلی و محدودیت‌هایی که در نظارت بر عملکرد پلتفرم‌های خارجی وجود دارد از دیگر چالش‌های این حیطه است. همچنین بخش زیادی از کودکان ایرانی از پلتفرم‌هایی استفاده می‌کنند که سرورهای آن‌ها خارج از کشور است که این مسئله به انتقال داده به خارج از کشور، نبود شفافیت دربارهٔ نحوهٔ استفاده از داده‌ها و دشواری پیگیری حقوقی منجر می‌شود. از مشکلات دیگر در ایران آگاهی پایین دیجیتال کودکان و نوجوانان در بسیاری از خانواده‌هاست، به گونه‌ای که سواد رسانه‌ای والدین محدود است و کنترل والدین بر روی استفاده از هوش مصنوعی و فضای دیجیتال به صورت نظام‌مند نیست، بنابراین کودکان بدون آموزش کافی وارد فضای مجازی می‌شوند.

در مقابل در نظام حقوقی کانادا، که یکی از کشورهایی است که در زمینهٔ حفاظت از داده پیشرو است و چارچوب‌های قوی‌تری داشته، قانون حفاظت از اطلاعات شخصی و اسناد الکترونیکی وضع شده است (Montgomery et al., 2017: 14). همچنین قانونگذار این کشور در ایالت‌های کانادا، قوانین استانی چون قانون حفظ حریم خصوصی کبک و تمرکز ویژه بر رضایت آگاهانه و حفاظت از کودکان کانادایی وضع کرده است. با وجود وضع قوانین قوی، همچنان مشکلاتی در این نظام حقوقی به‌چشم می‌خورد که از جملهٔ آن‌ها می‌توان به نفوذ شرکت‌های بزرگ فناوری به اطلاعات

شخصی کودکان و نوجوانان، تبلیغات هدفمند برای نوجوانان، چالش اجرای قوانین در برابر شرکت‌های فراملی اشاره کرد. در رابطه با رویکرد آموزشی در کشور کانادا، آموزش سواد دیجیتال در مدارس به صورت جدی‌تری نسبت به ایران صورت می‌پذیرد و همچنین کمپین‌های آگاهی‌بخشی برای والدین فعالیت می‌کنند و نهادهای ناظر مستقل در استفادهٔ کودکان و نوجوان از هوش مصنوعی وجود دارد (Barassi, 2020: 17).

استفادهٔ کودکان و نوجوانان از هوش مصنوعی و فضای مجازی پیامدهای اجتماعی و روانی به دنبال دارد. این پیامدها ممکن است شکل‌گیری ردپای دیجیتال دائمی از سنین پایین، تهدید هویت و امنیت شخصی، افزایش آزار سایبری و فشار روانی ناشی از مقایسهٔ اجتماعی را به دنبال داشته باشد. همچنین در بلندمدت، داده‌های جمع‌آوری‌شده می‌تواند بر فرصت‌های تحصیلی و شغلی آیندهٔ کودک تأثیر بگذارد.

۳. حق حفظ حریم خصوصی کودکان در عصر هوش مصنوعی و فضای دیجیتال در نظام حقوقی ایران

حمایت کیفری از حق حفظ حریم خصوصی کودکان از نظر حقوقی عبارت است از تدابیری که قانونگذار برای جلوگیری از تعرض به زندگی خصوصی کودکان و شخصیت معنوی آنان در قانون در نظر داشته و تجاوز به آن مستلزم حمایت از بزه‌دیده و اعمال مجازات بر فرد متجاوز بر حریم خصوصی است (انصاری، ۱۳۹۱: ۱۰). ضروری است تا با اقدامات تقنینی و با ابزارهایی چون فناوری‌های اطلاعات و ارتباطات، از کودکان و نوجوانان در فضای مجازی و در برابر هوش مصنوعی موجود در فضای مجازی، حمایت شود و با جرم‌انگاری رفتارهای بزهکارانه و جبران خسارات جسمی و روحی واردشده به کودکان و نوجوانان بزه‌دیده از هتک حیثیت این قشر جلوگیری شود (پورمسجدیان و ابراهیمی، ۱۳۹۹: ۸۲). قانون حمایت از کودکان و نوجوانان ۱۳۹۹ که حریم خصوصی دیجیتال را به‌طور مستقیم پوشش نمی‌دهد، قانون اساسی، قانون مجازات اسلامی، قانون آیین دادرسی کیفری، قانون احترام به آزادی‌های مشروع و حقوق شهروندی مصوب ۱۳۸۳، قانون جرائم رایانه‌ای اصلاحی سال ۱۳۹۹، قانون تجارت الکترونیک و مصوبات و بخشنامه‌های دیگر در زمرهٔ قوانین و مقرراتی هستند که مقنن گاه تلاش می‌کند تا به‌طور ضمنی و گاه صریحاً از برخی مصادیق حریم خصوصی حمایت نماید. در نظام حقوقی ایران به‌طور عمومی محل سکونت و سایر

ابعاد جسمانی و خانوادگی اشخاص در قانون مجازات اسلامی و سایر قوانین متفرقه از تعرض مصون مانده، اما ابعاد ذهنی مورد مصونیت قرار نگرفته است.

براساس اصل ۲۲ قانون اساسی، حیثیت، جان، مال، حقوق، مسکن و شغل اشخاص از تعرض مصون است، مگر در مواردی که قانون تجویز کند. در توضیح اصل مذکور می‌توان گفت، کودکان و نوجوانان نیز به‌عنوان شهروندانی که دارای حقوق و آزادی‌های طبیعی و انسانی در جامعهٔ امروزی هستند، بایستی شرایط زندگی امن در جامعه به گونه‌ای برایشان فراهم شود تا نسبت به جان، مال، مسکن، تمام حقوق فردی خود و... هیچ گونه بیم و هراسی نداشته باشند یا به عبارتی قشر مذکور در امنیت کامل زندگی کنند. درواقع با استفاده از این اصل می‌توان از اتخاذ تدابیر و تصمیمات ضعیف توسط حکومت که زمینه هرگونه تعرض به جان، مال و حقوق و مسکن و شغل و... را فراهم کرده است، جلوگیری کرد.

همچنین براساس اصل ۲۵ قانون اساسی، بازرسی و نرساندن نامه‌ها، ضبط و فاش کردن مکالمات تلفنی، افشای مخابرات تلگرافی و تلکس، سانسور، عدم مخابره و نرساندن آن‌ها، استراق سمع و هرگونه تجسس ممنوع است مگر به حکم قانون. در تشریح اصل فوق‌الذکر، در نظام حقوقی ایران، حریم خصوصی کودکان و نوجوانان را می‌توان در چهار عنوان مسکن و محل تحصیل خصوصی، اطلاعات جسمانی، اطلاعات شخصی و ارتباطات خصوصی معرفی کرد. بر این اساس، اطلاعات و اسرار شخصی قشر مورد بحث، اساساً باید از تعرض مصون باشد و هیچ شخصی مجوز دسترسی به آن‌ها را ندارد، این اصل مأموران دولتی و اشخاص دیگر را نیز شامل می‌شود. هیچ شخصی حق ندارد اطلاعات کودکان و نوجوانان را به مجرد وجود نفع برای خود، به دادگاه ارائه دهد مگر در زمان اضطراری اصل ۷۹ قانون اساسی و دیگری کشف و تعقیب جرائم. در عصر تکنولوژی کنونی، اصل مصونیت اطلاعات شخصی کودکان و نوجوانان با ظهور فضای مجازی و هوش مصنوعی با یک خطر جدی مواجه شده است، از این رو ضرورت دارد تا مقررات دقیقی از طرف دولت در رعایت اصل حفظ حریم خصوصی وضع شود. به‌طور کلی دو اصل ۲۲ و ۲۵ قانون اساسی به حمایت ضمنی از حریم خصوصی پرداخته است.

براساس مواد قانونی که در فصل پنجم قانون جرائم رایانه‌ای اصلاحی مصوب سال ۱۳۹۹، به‌عنوان هتک حیثیت و نشر اکاذیب، قانونگذار بیشتر بر محتوای مستهجن تمرکز دارد، نه حفاظت داده‌های کودکان. به گونه‌ای که در مادهٔ ۱۶ مقرر داشته، هرکس به وسیلهٔ سامانه‌های رایانه‌ای یا

مخابراتی، فیلم یا صوت یا تصویر دیگری را تغییر دهد یا تحریف کند و آن را منتشر یا با علم به تغییر یا تحریف منتشر کند، به نحوی که عرفاً موجب هتک حیثیت او شود، به حبس از ۹۱ روز تا دو سال یا جزای نقدی از پنج میلیون (۵.۰۰۰.۰۰۰) ریال تا چهل میلیون (۴۰.۰۰۰.۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد. علاوه بر آن در تبصرهٔ همین ماده بیان داشته که چنانچه تغییر یا تحریف به صورت مستهجن باشد، مرتکب به حداکثر هر دو مجازات مقرر محکوم خواهد شد.

با بررسی مادهٔ فوق می‌توان گفت مادهٔ ۱۶ قانون جرائم رایانه‌ای وضع شد تا از حریم شخصی و حیات خصوصی افراد از سوی قانون گذاران حمایت شود؛ بنابراین اگر شخصی با سامانه‌های رایانه‌ای یا مخابراتی مرتکب تعرض به حریم خصوصی اشخاص شوند و اقدامات وی به نشر اطلاعات خانوادگی و شخصی طرف مقابل منجر شود، مستوجب مجازات می‌شود. در تحقق رفتار مادی جرائم مبتنی بر توزیع و انتشار، مالکیت مرتکب بر محتوا یا اشیای مستهجن شرط نیست؛ بنابراین واسطگان و اشخاصی که با انگیزهٔ تحصیل مال، عملیات توزیع یا فروش را محقق می‌سازند، مستوجب مسئولیت کیفری مباشرتی ناشی از مادهٔ فوق خواهند بود (میرکمالی و صالح احمدی، ۱۴۰۰: ۵۶).

همچنین بر اساس مادهٔ ۱۷ قانون جرائم رایانه‌ای، هر کس به وسیلهٔ سامانه‌های رایانه‌ای یا مخابراتی صوت یا تصویر یا فیلم خصوصی یا خانوادگی یا اسرار دیگری را بدون رضایت او جز در موارد قانونی منتشر کند یا در دسترس دیگران قرار دهد، به نحوی که به ضرر یا عرفاً موجب هتک حیثیت او منجر شود، به حبس از ۹۱ روز تا دو سال یا جزای نقدی از پنج میلیون (۵.۰۰۰.۰۰۰) ریال تا چهل میلیون (۴۰.۰۰۰.۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد.

با نگاهی عمیق در مادهٔ ۱۷ قانون جرائم رایانه‌ای درمی‌یابیم که این ماده با هدف جرم‌انگاری در دسترس قرار دادن صوت، تصویر، فیلم‌های خصوصی یا خانوادگی و یا اسرار دیگری وضع شده است. عنصر مادی این جرم دارای دو بخش بوده که بخش اول آن، اظهار اکاذیب است. به‌طوری که مرتکب، مطالبی خلاف واقعیت را از عمد و دانسته (عامداً و عالماً) به اشخاصی نسبت دهد؛ در صورتی که عمل مرتکب به وارد شدن ضرر مادی یا معنوی به مجنی علیه منجر بشوند یا خیر. بخش دوم این جرم به نظر قانونگذار به جرم‌انگاری افشای اسرار مردم عادی بستگی دارد. با توجه به اینکه در جرم نشر اکاذیب توجه بر روی مقامات رسمی است، اما براساس مادهٔ فوق و با توجه به پیشرفته شدن و پیچیده‌تر شدن تکنولوژی وسایل الکترونیکی و رایانه‌ای، قانونگذار در مقام جرم‌انگاری

افشای حریم خصوصی اشخاص دیگر نیز آمده است. همچنین با توجه به اینکه افشای اطلاعات و داده‌های خصوصی اشخاص زیان‌های معنوی مختلفی را ممکن است به همراه داشته باشد، این گونه جرائم را در دستهٔ جرائم عمومی برشمرده‌اند که گذشت شاکی ممکن است صرفاً موجب تخفیف مجازات شود.

در مادهٔ ۱۸ قانون فوق‌الذکر نیز بیان داشته که هر کس به قصد اضرار به غیر یا تشویش اذهان عمومی یا مقامات رسمی به‌وسیلهٔ سامانهٔ رایانه‌ای یا مخابراتی اکاذیبی را منتشر کند یا در دسترس دیگران قرار دهد یا با همان مقاصد اعمالی را برخلاف حقیقت، رأسا یا به‌عنوان نقل قول، به شخص حقیقی یا حقوقی به‌طور صریح یا تلویحی نسبت دهد، اعم از اینکه از طریق یادشده به نحوی از انحا ضرر مادی یا معنوی به دیگری وارد شود یا نشود، افزون بر اعادهٔ حیثیت (در صورت امکان)، به حبس از ۹۱ روز تا دو سال یا جزای نقدی از ۰۰۰ /۰۰۰ /۲۰ تا ۰۰۰ /۰۰۰ /۱۵۰ ریال یا هر دو مجازات محکوم خواهد شد.

با بررسی مادهٔ ۱۸ این برداشت می‌شود که با وجود اینکه جرم نشر اکاذیب قبلاً توسط قانونگذار جرم‌انگاری شده بود، اما از آنجایی که نشر اکاذیب به‌وسیلهٔ سامانه‌های رایانه‌ای یا مخابراتی یا استفاده از هوش مصنوعی در نظر گرفته نشده بود، قانونگذار با اختیار و قدرتی که در تعقیب و مجازات اشخاصی که از این طریق به نشر اکاذیب مبادرت می‌ورزند، به وضع مادهٔ ۱۸ قانون جرائم رایانه‌ای اقدام کردند. در صورتی که جرم نشر اکاذیب را می‌بایست جزء جرائم قابل گذشت درنظر گرفت، اما در رابطه با جرم نشر اکاذیب از طریق سامانه‌های رایانه‌ای و مخابراتی یا استفاده از هوش مصنوعی، به نظر برخی کارشناسان این حوزه باید جرم مذکور را دارای جنبهٔ عمومی دانسته و گذشت شاکی ممکن است فقط از جهات تخفیف محسوب شود. با توجه به موارد ذکرشده، فقدان حفاظت از داده‌های کودکان در قوانینی که در نظام حقوقی ایران قانونگذار وضع نموده به چشم می‌خورد.

علاوه بر قوانین فوق در مادهٔ ۹ قانون حمایت از اطفال و نوجوانان مصوب سال ۱۳۹۹، هرگونه دسترسی یا انتشار اطلاعات خصوصی کودک را بدون رضایت یا حکم قانونی، جرم‌انگاری کرده است. همچنین براساس سند سیاست‌های کلی شبکهٔ ملی اطلاعات مصوب سال ۱۳۹۵، نیز بر لزوم صیانت از کودکان در فضای مجازی تأکید دارد. با وجود این، هنوز در ایران قانون مستقل و جامع حمایت از داده‌های شخصی کودکان مشابه مقررات عمومی حفاظت از داده‌ها در اتحادیهٔ

اروپا وضع نشده است. بنابراین، نواقص حقوقی در حوزهٔ داده‌های دیجیتال، الگوریتم‌های هوش مصنوعی، و نظارت بر زیرساخت‌های کودک‌محور مشاهده می‌شود.

به جهت ارتقای سطح حمایت از حریم خصوصی کودکان و نوجوانان و حفظ حریم خصوصی کودکان در عصر هوش مصنوعی و فضای دیجیتال، اقداماتی چون تدوین قانون ویژهٔ حفظ داده‌های شخصی کودکان، تأسیس کمیسیون حفاظت از داده‌های کودکان در جهت نظارت بر شرکت‌ها و الگوریتم‌های هوش مصنوعی فعال در ایران، ترویج سواد رسانه‌ای و سواد داده‌ای خانواده‌ها، بومی‌سازی چارچوب‌های بین‌المللی، بایستی در دستور کار مسئولان این امر قرار گیرد.

۴. حق حفظ حریم خصوصی کودکان در عصر هوش مصنوعی و فضای دیجیتال در نظام حقوقی کانادا

حقوق بشر صرف نظر از سن، به‌طور مساوی برای همه اعمال می‌شود. با این حال، سازمان ملل متحد تصمیم گرفت که باید درمورد حقوق کودکان (افراد زیر هجده سال) دقیق‌تر عمل کند. این سازمان اذعان می‌کند که کودکان نیازها و موقعیت ویژه‌ای دارند که نسبت به بزرگسالان در برابر استثمار آسیب‌پذیرترند. بنابراین سازمان ملل متحد در سال ۱۹۵۹ سندی را به نام اعلامیهٔ جهانی «حقوق کودک» تصویب کرد که این سند ده حق مهم کودک (منظور از کودک، کودکان و نوجوانان هستند) مانند حق محافظت در برابر بی‌توجهی و ظلم، حق بقا، حق مراقبت، حق در امان ماندن از آسیب دیگران، حق مشارکت کامل در زندگی خانوادگی، فرهنگی و اجتماعی را فهرست می‌کند و کانادا ازجمله کشورهایی است که موافقت کرده است تا به مفاد این سند پای‌بند باشد. گفتنی است که این کنوانسیون در کانادا قانون نیست، اما سندی مهم است تا در راستای کمک به کودکان و نوجوانان مفید واقع شود. امروزه در قانون کانادا در راستای محافظت و حمایت از شهروندان خود ازجمله قشر آسیب‌پذیری چون کودکان و نوجوانان، عموماً در سه سطح دولتی قوانینی وضع کرده‌اند که عبارت‌اند از: قوانین فدرال، شهرداری و قوانین سرزمینی/ استانی. در کانادا قوانینی وجود دارد که از تعدادی از حقوق و آزادی‌ها محافظت می‌کند و به افراد ذی‌نفع اجازه می‌دهد که در صورت عدم رعایت این حقوق و آزادی‌ها، رسماً شکایت کنند.

وقتی به حقوق بشر در کانادا اشاره می‌شود، معمولاً منظور آن دسته حقوق و آزادی‌هایی است که توسط چندین قانون محافظت می‌شوند. اولین مورد منشور حقوق و آزادی‌های کانادا، که شامل

حمایت‌هایی در موارد، آزادی‌های اساسی مانند مذهب، حقوق دموکراتیک مانند حق رأی و نامزدی برای مناصب دولتی، حق حفظ حریم خصوصی اشخاص، حقوق قانونی مانند حق عدم بازداشت یا زندانی شدن خودسرانه و درنهایت حقوق برابری که اشخاص را در برابر قوانینی که به‌طور ناعادلانه علیه گروه خاصی از مردم تبعیض قائل می‌شوند. حقوق از جنبهٔ دیگری نیز مشروط هستند؛ حقوق فردی باید در برابر حقوق دیگران سنجیده شود. به‌طور مثال حق آزادی بیان شخص به این معنی نیست که می‌تواند مطالبی را منتشر کند که هدف آن نفرت‌پراکنی علیه گروه خاصی از مردم باشد. در چنین مواردی دولت می‌تواند حقوق و آزادی‌های اساسی را محدود کند، اما تنها در صورتی که بتواند ثابت کند که این محدودیت در یک جامعهٔ آزاد و دموکراتیک، منطقی و بنا به صلاح‌دید و حفظ و تضمین حقوق و آزادی‌های دیگر اشخاص جامعه است.

منشور حقوق بشر بخشی از قانون کاناداست؛ این بدان معناست که تمام قوانین دیگر کانادا باید به حقوق و آزادی‌هایی که در آن آمده است، احترام بگذارند. قوانین حقوق بشر نیز از حقوق اساسی حمایت می‌کند. در کانادا، قوانین حقوق بشر توسط دولت‌های استانی، منطقه‌ای و فدرال برای محافظت در برابر تبعیض تصویب شده‌اند (اخوان و همکاران، ۱٤۰۰: ٦٥).

از منظر دیگر باید درنظر داشت که کانادا یکی از پیشروترین کشورها در زمینهٔ حفاظت از اطلاعات شخصی و حقوق دیجیتال محسوب می‌شود. اما با گسترش هوش مصنوعی، یادگیری ماشین، و ابزارهای هوشمند، چالش‌های مرتبط با حریم خصوصی کودکان در این کشور نیز رو به افزایش است. کودکان کانادایی در مدرسه، فضای مجازی، بازی‌ها، شبکه‌های اجتماعی و حتی وسایل هوشمند خانگی با فناوری‌هایی تعامل دارند که حجم عظیمی از داده‌های رفتاری، زیستی، مکانی و تحلیلی آن‌ها را جمع‌آوری و پردازش می‌کند.

در این رابطه، نظام حقوقی کانادا تلاش کرده است با ترکیبی از قوانین فدرال، قوانین استانی، و چارچوب‌های اخلاقی نوین، از این حق بنیادین پشتیبانی کند. این گونه نیز می‌توان گفت که کانادا به‌جای یک قانون واحد، چندین قانون کلیدی برای حفاظت از اطلاعات شخصی دارد که کودکان نیز ذیل آن‌ها حمایت می‌شوند. همان‌گونه که قبلاً اشاره شد مهم‌ترین قانون فدرال در زمینهٔ حفاظت از اطلاعات شخصی در حوزهٔ خصوصی بوده و نکات مهمی در این زمینه ارائه داشته است. نکتهٔ اولی که در قانون مذکور به‌چشم می‌خورد رضایت باید «آگاهانه و معتبر» باشد، است؛ با این توضیح که برای کودکان، دریافت رضایت والدین الزامی است، مگر در مواردی که کودک قادر باشد اثرات

مثبت یا منفی جمع‌آوری داده را درک کند. نکتهٔ بعدی اینکه جمع‌آوری داده باید حداقلی و متناسب باشد، با این توضیح که شرکت‌ها موظف‌اند روش‌های شفاف برای اطلاع‌رسانی به والدین دربارهٔ نحوهٔ پردازش دادهٔ کودکان ارائه دهند (Teresa, 2020: 11).

در برخی از ایالات کانادا قوانین استانی مهم، جامع‌تر و سخت‌گیرانه‌تری نسبت به دیگر ایالات وضع شده است، مانند قانون حریم خصوصی در بریتیش کلمبیا، قانون حریم خصوصی در آلبرتا، قانون حفاظت از اطلاعات شخصی در انتاریو در بخش سلامت. همچنین قانون کبک صراحتاً پردازش داده‌های کودکان را حساس دانسته و محدودیت‌های بیشتری اعمال کرده است.

با وجود قوانین قوی همچون قانون حفاظت از اطلاعات شخصی و اسناد الکترونیکی[1] که یکی از مهم‌ترین قوانین فدرال کانادا در حوزهٔ حفاظت از داده‌های شخصی است و قوانین استانی برای عصر هوش مصنوعی، خلأهای قانونی‌ای در این حوزه به‌چشم می‌خورد. چالش‌هایی ازقبیل ناتوانی قوانین در مدیریت یادگیری الگوریتمی، نبود مقررات اختصاصی دربارهٔ داده‌های بیومتریک کودکان، پوشش ناکافی آموزش برخط و فناوری‌ها، محدودیت در مقابله با پروفایل‌سازی مبتنی بر هوش مصنوعی.

معضل دیگر در این زمینه، گستردگی داده‌هایی است که کودکان ناخواسته تولید می‌کنند. هوش مصنوعی سعی می‌کند تا تمام رفتارهای کودک به دادهٔ تحلیل‌پذیر تبدیل کند که این امر دولت کانادا را به‌شدت نگران کرده است. همچنین سازمان‌های کانادایی بارها از اینکه شرکت‌های فرامرزی از داده‌های کودکان سوءاستفاده می‌کنند، شکایت کرده‌اند، اما اعمال جریمه یا کنترل عملی دشوار است که این امر چالشی پیچیده برای رقابت با شرکت‌های فناوری بزرگ ایجاد کرده است.

کانادا در مواجهه با این شرایط اقدامات و رویکردهای اصلاحی خاصی را درنظر گرفته است. یکی از این اصلاحات قانون پیشنهادی C-27[2] است که این قانون با هدف اصلاح PIPEDA مطرح شده و شامل مواردی چون ایجاد قانون جدید[3]، ایجاد قانون داده و هوش مصنوعی[4] جهت تنظیم و کنترل بهتر هوش مصنوعی، افزایش شدید جریمه‌ها، تعریف دادهٔ کودکان به‌عنوان دادهٔ بسیار حساس

1. PIPEDA
2. Canada’s Digital Charter Implementation Act (2022–2024)
3. CPPA (Consumer Privacy Protection Act)
4. AI and Data Act

است. اگر قوانین فوق‌الذکر در کانادا به تصویب نهایی برسد، این کشور یکی از پیشروترین نظام‌های حفاظت از کودکان خواهد بود.

علاوه بر موارد ذکرشده دربارهٔ کودکان داده‌های کودکان که همیشه «حساس» محسوب می‌شود دفتر کمیسیونر حریم خصوصی کانادا،[1] که مسئول حفاظت از حریم خصوصی افراد و نظارت بر اجرای قوانین مرتبط با داده‌های شخصی بوده، دستورالعمل‌های خاصی ارائه کرده است که این دستورالعمل‌ها شامل موارد زیر است: جمع‌آوری نباید بیش از نیاز باشد، کودکان نباید هدف‌گذاری الگوریتمی شوند، پروفایل‌سازی پرخطر باید محدود شود (Valerie & Bailey, 2015: 15).

همچنین سیاستگذاران کشور کانادا در جهت بهبود وضعیت حریم خصوصی کودکان و نوجوانان در محیط‌ها و پلتفرم‌های آموزشی در حال تدوین الزامات جدید هستند تا نه‌تنها برای افزایش سطح امنیت اهداف آموزشی بلکه برای اهداف تجاری و نه برای آموزش الگوریتم‌های دیگر گامی مؤثر بردارند.

در کل می‌توان به این نتیجه دست یافت که حق حفظ حریم خصوصی کودکان در کانادا، به‌عنوان یکی از اصول بنیادین حقوق بشر دیجیتال، با تهدیدهای جدی عصر هوش مصنوعی روبه‌روست. اگرچه نظام حقوقی کانادا یکی از پیشرفته‌ترین و سختگیرانه‌ترین نظام‌ها در حوزهٔ حفاظت از داده است، سرعت پیشرفت فناوری‌های هوش مصنوعی باعث ایجاد خلأهای مهمی در حفاظت از کودکان شده است.

۵. حمایت قانون فدرال از کودکان و نوجوانان

قانون فدرال CVRA به قربانیان حق خاصی برای شنیده شدن در توافقات اقرار به جرم و همچنین حق عمومی برای مشورت با دادستان‌ها را می‌دهد. همچنین به قربانیان اجازه می‌دهد، در صورت نقض حق شنیده‌شدنشان از طریق ماندامو‌س،[2] درخواست بازگشایی مجدد توافق‌نامه را بدهند. اکثر

1. Office of the Privacy Commissioner of Canada (OPC)

۲. در نظام حقوقی کانادا، درخواست ماندامو‌س، نوعی درخواست به دادگاه فدرال است که از دادگاه می‌خواهد یک مقام یا ارگان دولتی را وادار کند تا به وظیفهٔ خود عمل کند و این امر باعث تسریع در روند رسیدگی به پرونده می‌گردد؛ به عبارت دیگر ماندامو‌س دستوری از یک مقام بالاتر به زیردستان است که آن‌ها را موظف می‌کند وظیفهٔ خود را در یک بازهٔ زمانی معین و به‌درستی انجام دهند.

ایالت‌ها به‌طور مشابه دارای یک قانون یا مادهٔ قانون اساسی هستند که به قربانیان حق عمومی مشورت یا مشاوره با دادستان (که مسلماً شامل توافقات اقرار به جرم نیز می‌شود) یا حق خاصی برای شنیده شدن قبل از پذیرش درخواست توسط دادگاه را می‌دهند. دادگاه‌ها برای رد توافقات اقرار به جرم یا بازگشایی غیررسمی جلسات رسیدگی به درخواست جرم، برای اطمینان از رعایت تمام حقوق قربانیان، آزاد بوده‌اند (Alan et al., 2021: 27).

۶. در معرض خطر قرار گرفتن حریم خصوصی کودکان و نوجوانان کانادایی در برابر هوش مصنوعی

ظرفیت و شرایط کودکان برای اعمال حریم خصوصی خود با بزرگ‌سالان متفاوت است. کودکان ممکن است فاقد آگاهی باشند یا مهارت‌های سوادآموزی محدودی داشته باشند که بتوانند حق خود برای حفظ حریم خصوصی را به‌طور کامل درک کنند و خطرات و تأثیرات بالقوهٔ بلندمدت اشتراک‌گذاری داده‌ها و پردازش هوش مصنوعی را درک کنند. در حالی که کودکان و نوجوانان عموماً از نظر فناوری ماهر هستند و می‌خواهند حریم خصوصی خود را حفظ کنند، تمایل دارند تصور محدودتر و کم‌انتقادتری از حریم خصوصی دیجیتال داشته باشد. کودکان تمایل دارند حریم خصوصی را به شیوه‌های بین فردی یا بین خود و سایر افراد یا گروه‌های درنظر بگیرند. آن‌ها (مانند اکثر بزرگ‌سالان) برای درک حریم خصوصی خود در قالب‌های انتزاعی‌تر، تجاری یا نهادی (مانند نحوهٔ ردیابی یا استنتاج داده‌هایشان توسط هوش مصنوعی) تلاش می‌کنند، بنابراین ظرفیت محدودی برای ارزیابی خطرات مرتبط دارند. جعبهٔ سیاه یا همان هوش مصنوعی ارتباطات را بیشتر مبهم می‌سازد و بین ورودی‌ها و نتایج، ارزیابی ریسک حریم خصوصی را برای کودکان دشوارتر می‌کند.

حریم خصوصی کودکان چند وجهی است؛ شامل توانایی آن‌ها در کنترل داده‌هایشان، حرکت در فضاها با استقلال، برقراری ارتباط بدون رهگیری و تصمیم‌گیری مستقل می‌شود. همچنین به زمینه و رابطه بسیار وابسته است؛ ترجیحات حریم خصوصی کودکان شامل ملاحظات متعددی است، ازجمله اینکه چه چیزی درمورد زندگی خصوصی آن‌ها شناخته شده است، توسط چه کسی، برای چه اهدافی و با چه عواقبی. هوش مصنوعی با جمع آوری داده‌های کودکان و وارد کردن اطلاعات به الگوریتم‌ها برای دستیابی به عملکردهای مختلف با نظارت محدود، ممکن است خطرات بالقوه‌ای را برای همهٔ این جنبه‌های حریم خصوصی کودکان ایجاد کند. سه دستهٔ اصلی از

خطرات مربوط به حریم خصوصی کودکان از جانب هوش مصنوعی وجود دارد: خطرات داده‌ای، خطرات عملکردی و خطرات نظارتی (Zon & Lipsey, 2020: 14).

نتیجه

کودکان و نوجوانان ازجمله قربانیان استفاده از فضای مجازی و هوش مصنوعی هستند و هیچ گونه اطلاعی از حفظ حریم خصوصی ندارند و به راحتی ابزار دست مجرمان می‌شوند. به عبارت دیگر، کودکان ممکن است فاقد آگاهی باشند یا مهارت‌های سوادآموزی محدودی داشته باشند که بتوانند حق خود برای حفظ حریم خصوصی را به‌طور کامل درک کنند و خطرات و تأثیرات بالقوهٔ بلندمدت اشتراک‌گذاری داده‌ها و پردازش هوش مصنوعی را درک کنند. بنابراین ظرفیت محدودی برای ارزیابی خطرات مرتبط دارند. در این رابطه نیز دولت بایستی تدابیر حمایتی و پیشگیرانه در قالب آموزش والدین و کودکان و نوجوانان در استفاده از فضای مجازی اعمال کنند و با مجرمان در این زمینه برخورد قانونی مناسب صورت گیرد.

با مقایسهٔ تطبیقی دو نظام حقوقی در رابطه با حفظ حریم خصوصی کودکان و نوجوانان در ایران و کانادا، این نتیجه حاصل شد که کانادا دارای نظام پیشرفته‌تری در زمینهٔ حمایت کیفری و مقررات پیشگیرانه است، در حالی که ایران هنوز راه‌اندازی نظام جامع حفاظت داده را در دستور کار دارد. تفاوت اصلی دو نظام در میزان نهادهای نظارتی، ضمانت اجراهای کیفری، و سیاست‌گذاری داده‌محور است. به عبارت دیگر هوش مصنوعی و فضای دیجیتال، همان‌قدر که فرصت‌ساز هستند، می‌توانند تهدیدی جدی برای حریم خصوصی کودکان باشند. تفاوت اصلی میان ایران و کانادا در سطح قانون‌گذاری، نظارت و آموزش عمومی است، اما هیچ کشوری از این چالش مصون نیست. همچنین در جهت کاهش تهدیدات استفاده از هوش مصنوعی و فضای دیجیتال و حفاظت از کودکان و نوجوانان بایستی دولت‌ها در این زمینه همکاری کنند، همچنین فعالیت شرکت‌های فناوری با مسئولیت‌پذیری بیشتری عمل کنند و نهایتاً خانواده‌ها با افزایش آگاهی خود، محیط مجازی را برای کودکان و نوجوانانشان امن نگه دارند.

پیشنهاداتی که در این زمینه می‌توان مطرح کرد این است که با تدوین قانون جامع در رابطه با «حمایت از داده‌های شخصی کودکان» در ایران با تکیه بر مدل کانادایی و همچنین با ایجاد واحد تخصصی در پلیس فتا برای رسیدگی به جرائم نقض حریم کودکان و علاوه بر آن با الحاق رسمی به

پروتکل اختیاری سعی شود که در بهبود شرایط کودکان در فضای مجازی و استفاده از هوش مصنوعی و حمایت از حقوق آنان در این حوزه گامی جدی‌تر برداشته شود.

راهکارهایی را که در رابطه با چالش‌هایی که کودکان و نوجوانانی که در کانادا از هوش مصنوعی و فضای مجازی استفاده می‌کنند، تهدید می‌کند، می‌توان به محدودسازی تبلیغات هدفمند برای کودکان، کنترل سخت‌گیرانه‌تر فناوری تشخیص چهره، تقویت مقررات مرتبط با هوش مصنوعی در آموزش، استفاده از تنظیمات حریم خصوصی، آموزش مهارت «نه گفتن دیجیتال» به کودک، نظارت فعال و گفت‌وگو محور، استفاده از ابزارهای کنترل والدین اشاره کرد. همچنین تدوین قانون جامع حفاظت از داده‌های کودکان، الزام پلتفرم‌ها به شفافیت در استفاده از داده، توسعهٔ برنامه‌های آموزش سواد دیجیتال، ایجاد نهاد نظارتی مستقل، استفاده از تنظیمات حریم خصوصی، آموزش مهارت «نه گفتن دیجیتال» به کودک، نظارت فعال و گفت‌وگومحور، استفاده از ابزارهای کنترل والدین راهکارهایی هستند که در رابطه با چالش‌هایی که کودکان و نوجوانانی را که در ایران از هوش مصنوعی و فضای مجازی استفاد می‌کنند، تهدید می‌کند، می‌توان درنظر داشت.

حامی مالی:

این مقاله هیچ حامی مالی ندارد.

مشارکت نویسندگان:

منصوره حسینی: روش‌شناسی، تحلیل، نوشتن بررسی و ویرایش، تحقیق و بررسی، پیش‌نویس اصلی.

مجتبی فرهمند: مفهوم‌سازی، نظارت بر داده‌ها، اعتبارسنجی، مدیریت پروژه، منابع.

تعارض منافع:

بنا بر اظهار نویسندگان این مقاله تعارض منافع ندارد.

ملاحظات اخلاقی:

این پژوهش بر پایهٔ مطالعهٔ اسناد، قوانین، رویه‌های قضائی و منابع کتابخانه‌ای انجام شده و در آن هیچ‌گونه مطالعه‌ای بر روی انسان، حیوان یا داده‌های شخصی صورت نگرفته است؛ بنابراین، اخذ

تأییدیهٔ کمیتهٔ اخلاق برای این پژوهش ضروری نبوده است. با این حال، نویسنده اصول امانت‌داری علمی، صداقت پژوهشی، استناددهی صحیح و رعایت حقوق مالکیت فکری را در تمامی مراحل پژوهش رعایت کرده است.

در تهیهٔ این مقاله از ابزارهای هوش مصنوعی مولد صرفاً برای کمک به ویرایش زبانی، بهبود ساختار نگارش و ارتقای خوانایی متن استفاده شده است. این ابزارها در طراحی پژوهش، تحلیل علمی، تفسیر یافته‌ها، استنتاج نتایج یا تصمیم‌گیری‌های پژوهشی نقشی نداشته‌اند و مسئولیت کامل صحت، اصالت و محتوای نهایی مقاله بر عهده نویسنده/ نویسندگان است.

موافقت نویسندگان:

تمامی نویسندگان نسخهٔ نهایی مقاله را مطالعه و تأیید کرده‌اند و با انتشار آن موافقت دارند.

منابع

اخوان، بهار، بینا،احمد و گودرزی، ساناز (۱٤۰۰)، گور حقوق بشر در پرتوی منشور حقوق و آزادی‌های کانادا، تهران: مؤسسهٔ صیانت از حقوق زنان، چاپ اول.

انصاری، باقر (۱۳۹۱)، «مطالعهٔ تطبیقی مسئولیت مدنی ناشی از نقض حقوق مربوط به شخصیت در رسانه‌ها»، نشریهٔ حقوق خصوصی، ۲، ٦۷-۹۹.

بویری منجی، معصومه و زارعی، مریم (۱٤۰٤)، «چالش‌های اخلاقی استفاده از هوش مصنوعی در مدارس ـ حریم خصوصی،امنیت داده‌ها و خطرات و سوگیری الگوریتمی»، اولین همایش بین‌المللی معلمان پیشرو در عصر پژوهش‌های تحول‌آفرین.

پورمسجدیان، فاطمه و ابراهیمی، سیدنصراله (۱۳۹۹)، «واکاوی حقوقی حمایت از حریم خصوصی کودک در فضای مجازی با نگاهی به قوانین ایران و معاهدات بین‌المللی»، نشریهٔ مطالعات زن و خانواده، ٤، ۸۲.

خلیلی، فاطمه و سوادی، زهرا (۱٤۰٤)، «قلمرو کودکی در عصر هوش مصنوعی: از کلاس‌های هوشمند تا نگرانی‌های خانه؛ مطالعهٔ پدیدارشناسانهٔ چالش‌های حریم خصوصی و اخلاقی کودکان از دیدگاه معلمان و والدین»، همایش بین‌المللی آموزش و پرورش در قرن بیست و یکم.

صفاری‌نیا، مهزاد (۱۴۰۳)، «هوش مصنوعی و حق بر آموزش کودکان»، فصلنامهٔ مطالعات فقه و حقوق رسانه، ۱، ۱۳۳-۱۵۲.

میرکمالی، سیدعلیرضا و صالح احمدی، سحر (۱۴۰۰)، قانون مجازات اسلامی در نظم حقوقی کنونی، تهران: انتشارات گالوس، چاپ چهارم، جلد دوم.

قوانین

قانون اساسی ایران.

قانون حمایت از اطفال و نوجوان مصوب ۱۳۹۹.

قانون جرائم رایانه‌ای اصلاحی مصوب سال ۱۳۹۹.

قانون مجازات اسلامی.

قانون حمایت از کودکان و نوجوانان و خانواده‌ها کانادا، مصوب ۲۰۲۰.

منشور حقوق بشر و آزادی‌های کانادا ۲۰۲۵.

References

Young, A. N., & Dhanjal, K. (2021). *Victims' Rights in Canada in the 21st Century*. Ottawa: Department of Justice Canada.

Barassi, V. (2020), *Child Data Citizen: How Tech Companies Are Profiling Us from before Birth*, MIT Press.

Chapdelaine.C. (2007), Child Justice in Canada and The Four Ps: Protection, Prosection, Prevention and Participation, Springer Science+Business Media B.V, P.268.

Montgomery, K., Chester, J., & Milosevic, T. (2017), *Ensuring young people's digital privacy as a fundamental right*, International Data Privacy Law.

Teresa, S. (2020), "Privacy and the Open Internet in Canada", *Journal: Canadian Journal of Law and Technology*, vol18, no1, CanLIIDocs 4179.

Valerie, S., & Bailey, J. (2015), *Privacy and the Digital Generation*, Published in: University of Ottawa Press.

Zon, N., & Lipsey, A. (2020), STANDARDS RESEARCH Children's Safety and Privacy in the Digital Age, Springboard Policy, p.14.

https://fpf.org/wp-content/uploads/2018/10/FPF_Artificial-Intelligence_Digital.pdf

United Nations, *Convention on the Rights of the Child*, 20 November 1989, United Nations, Treaty Series, vol. 1577, p. 3, OHCHR - Convention on the Rights of the Child.

Journal Website

Legal Innovation Quarterly

Spring 2026

Volume 2, Issue 3

E-ISSN: 3115-8498

Artificial Intelligence and Criminal Justice Processes: Manifestations and Applications

Majid Ghourchibeigi [1], Ghulamali Andishwar [2*]

1. Associate Professor, Department of Criminal Law and Criminology, Faculty of Law and Political Science, Kharazmi University, Tehran, Iran.
2. Ph.D. Student in Criminal Law and Criminology, Faculty of Law and Political Science, Kharazmi University, Tehran, Iran (Corresponding Author)

***Corresponding author email address:** ghulamali.andishwar@gmail.com

Extended Abstract

1. Introduction

Contemporary criminal justice systems continue to encounter significant structural and operational deficiencies that affect both their effectiveness and legitimacy. These deficiencies include failures in crime detection and prevention, unjustified deprivation of liberty, insufficient prosecutorial or investigative capacity to substantiate criminal charges, and judicial errors that may culminate in wrongful convictions or acquittals. Such shortcomings not only impair the proper administration of justice but also erode public trust in legal institutions and undermine confidence in the rule of law. Against this background, the emergence of artificial intelligence represents a significant technological development with the potential to transform multiple stages of criminal proceedings.

Received: December 21, 2025 - **Accepted:** March 1, 2026 - **Published:** March 21, 2026

Ghorchibeigi, Majid; and Andishvar, Gholamali. (2026). "Artificial Intelligence and Criminal Justice Processes: Manifestations and Applications." *Legal Innovation Quarterly*, 2(3), pp. 107-134
Doi: https://doi.org/10.22034/lir.2026.2086077.1032

© 2026 The Authors. Published by Legal Innovation Research Institute, Tehran, Iran. This is an open access article distributed under the terms of the Creative Commons Attribution 4.0 International (CC BY 4.0) License.

Artificial intelligence systems, by virtue of their capacity to process extensive datasets, identify patterns, generate probabilistic assessments, and support complex analytical tasks, are increasingly being considered for application in criminal justice. Such applications include predictive policing, facial recognition, digital surveillance, forensic analysis, risk assessment, document review, and decision-support tools for prosecutors and judges. In principle, these tools may enhance efficiency, improve the management of complex evidentiary materials, reduce certain forms of human error, and promote greater consistency in decision-making. In legal systems burdened by case backlogs, limited institutional capacity, or increasingly sophisticated forms of criminality, the application of these technologies may be particularly attractive.

Nevertheless, the incorporation of artificial intelligence into criminal justice gives rise to significant legal, ethical, and procedural concerns. Criminal procedure is not merely an administrative framework for the efficient processing of cases; rather, it constitutes a rights-oriented system designed to preserve human dignity, ensure due process, safeguard equality before the law, and secure the guarantees of a fair trial. Accordingly, the use of artificial intelligence in this field raises fundamental questions concerning the appropriate limits of technological intervention, the legitimacy of relying on algorithmic systems for decisions traditionally entrusted to human decision-makers, and the compatibility of automated tools with the core principles of procedural justice. Concerns relating to algorithmic bias, discriminatory outcomes, the opacity of automated reasoning, limited explainability, intrusions into privacy, and diminished accountability are particularly acute in criminal matters, where decisions may directly affect individual liberty, reputation, and other fundamental rights.

The present study examines whether, and to what extent, artificial intelligence affects the fairness of criminal proceedings and how the benefits and risks associated with its application should be assessed within the framework of criminal procedure. The principal hypothesis is that, although artificial intelligence may enhance efficiency, analytical capacity, consistency, and relative accuracy in criminal justice, its use may also jeopardize fair-trial guarantees unless subject to robust standards of transparency, explainability, accountability, non-discrimination, and meaningful human oversight.

2. Methodology

In terms of its purpose, this study is applied and adopts a descriptive-analytical approach. The legal dimension of the study is examined through a doctrinal methodology grounded in an analysis of the principles of criminal procedure, legal scholarship, and relevant regulatory and comparative approaches to the use of artificial intelligence in criminal justice. The study also draws on interdisciplinary literature at the intersection of law, technology, ethics, and

governance to situate artificial intelligence within broader debates concerning legitimacy, responsibility, and the protection of rights in judicial processes.
The study employs qualitative analysis and inferential interpretation of legal materials and scholarly arguments. For analytical clarity, the role of artificial intelligence in criminal procedure is examined in four principal domains: crime detection and prevention; criminal investigation and evidentiary analysis; adjudication and judicial decision support; and the broader advantages, limitations, and risks associated with the integration of artificial intelligence into criminal proceedings. This framework enables an assessment of artificial intelligence not merely as a technical instrument but also as a normative and institutional phenomenon with significant implications for procedural fairness, judicial legitimacy, and the protection of fundamental rights.

3. Findings

The findings indicate that artificial intelligence has considerable potential to improve the functioning of criminal justice systems in several respects. In the field of crime detection, artificial intelligence may strengthen the capacity of law enforcement authorities to identify suspicious patterns, process large volumes of surveillance and digital data, and detect correlations that may not be readily discernible to human investigators. During the investigative phase, artificial intelligence may facilitate the organization, classification, and analysis of extensive evidentiary materials, including electronic communications, financial records, biometric data, and forensic evidence. These functions may contribute to faster processing, improved evidentiary assessment, and more informed prosecutorial decision-making.

In adjudication, artificial intelligence may also serve as a supplementary decision-support tool, assisting judges in reviewing voluminous case files, identifying relevant legal authorities, structuring legal issues, and summarizing evidentiary records. Such applications may enhance procedural consistency and reduce certain risks associated with cognitive overload, oversights, or inconsistencies in human decision-making. In jurisdictions facing heavy caseloads or institutional inefficiencies, artificial intelligence may therefore offer significant practical benefits.

Nevertheless, the findings also demonstrate that these advantages are accompanied by substantial risks. One of the most significant concerns is the potential of artificial intelligence systems to reproduce, reinforce, or amplify existing social and institutional biases. Where algorithmic models are trained on historically biased or incomplete datasets, their outputs may disproportionately disadvantage particular groups on the basis of race, ethnicity, socioeconomic status, gender, or geographic location. In criminal proceedings, such distortions may undermine equality before the law, weaken the presumption of innocence, and compromise judicial impartiality.

A further challenge concerns algorithmic opacity, commonly characterized as the “black box” problem. In many instances, neither defendants nor legal professionals are able to understand how a particular artificial intelligence system generates a recommendation, classification, or risk assessment. This lack of transparency poses serious obstacles to challenging decisions informed by artificial intelligence, evaluating the reliability of evidence, and ensuring effective judicial scrutiny. The rights of the defense may be materially weakened where an accused person is unable to challenge the reasoning underlying a technological output that influences arrest, detention, the bringing of charges, adjudication, or sentencing.

The findings also reveal concerns relating to privacy, data protection, cybersecurity, and institutional accountability. Artificial intelligence systems used in criminal justice may be vulnerable to technical errors, manipulation, or misuse, while responsibility for harmful outcomes may become diffused among software developers, public authorities, investigators, prosecutors, and judges. Such diffusion is particularly problematic in criminal justice, where the exercise of coercive state power must remain identifiable, legally attributable, and subject to review. Accordingly, the use of artificial intelligence cannot be justified solely on grounds of efficiency or innovation; it must also satisfy the normative requirements of procedural fairness and legal accountability.

4. Conclusion and Recommendations

Conclusion

This study concludes that artificial intelligence should be regarded as a supportive and complementary instrument in criminal justice, rather than as a substitute for human judgment and legal responsibility. Although artificial intelligence may enhance administrative efficiency, analytical capacity, and relative consistency, it cannot replace the interpretive, evaluative, and moral reasoning that is central to criminal adjudication. Decisions concerning guilt, innocence, liberty, and punishment must remain under the effective control of human decision-makers who are legally and ethically accountable for their determinations.

Accordingly, the legitimate use of artificial intelligence in criminal procedure depends on strict adherence to fundamental legal principles, particularly fairness, transparency, explainability, accountability, proportionality, non-discrimination, and effective human oversight. Artificial intelligence should be deployed only in contexts in which its outputs can be meaningfully reviewed, understood, challenged, and corrected within the legal process. The use of opaque or insufficiently auditable systems in core judicial functions should therefore be approached with the utmost caution and should be avoided altogether in certain contexts.

5. Recommendations

On this basis, the study recommends the adoption of clear and comprehensive legal and regulatory frameworks governing the design, deployment, and use of artificial intelligence in criminal justice; the development of explainable, auditable, and rights-sensitive artificial intelligence systems to reduce algorithmic opacity and facilitate meaningful review; the provision of specialized training for judges, prosecutors, lawyers, investigators, and other legal practitioners to enable the critical assessment and proper interpretation of outputs generated by artificial intelligence; the establishment of mechanisms for continuous oversight, independent evaluation, and human rights impact assessment to prevent discriminatory, arbitrary, or unjust outcomes; and the preservation of the principle that artificial intelligence must remain subordinate to human judgment and must not function as an autonomous determinant of criminal liability or punishment.

Accordingly, the future role of artificial intelligence in criminal justice should be shaped not solely by technological optimism, but by a principled balance between innovation and the protection of procedural justice. Only within such a framework may artificial intelligence contribute constructively to criminal proceedings without undermining the essential guarantees of a fair trial.

Keywords: Artificial intelligence; criminal justice; intelligent judicial system; technology in justice.

Funding
This article has no financial support or funding.

Authors' Contributions
Majid Ghourchibeigi: Conceptualization, data curation, validation, project administration, and resources.
Ghulamali Andishwar: Methodology, formal analysis, writing – review & editing, investigation, writing – original draft.

Conflict of Interest
According to the authors' declaration, there is no conflict of interest regarding this article.

Ethical Considerations
This study was conducted based on the analysis of legal documents, statutes, judicial decisions, and library-based sources. It did not involve human participants, animals, or personal data; therefore, ethical approval from an institutional ethics committee was not required. Nevertheless, the authors adhered to the principles of academic integrity, research honesty, proper

citation practices, and respect for intellectual property rights throughout all stages of the research.

Generative artificial intelligence (AI) tools were used solely to assist with language editing, improving the structure of the manuscript, and enhancing the readability of the text. These tools did not contribute to the study design, scientific analysis, interpretation of findings, drawing of conclusions, or any research-related decision-making. The author(s) assume full responsibility for the accuracy, originality, and final content of the manuscript.

Authors' Approval

All authors have reviewed and approved the final version of the manuscript and agree to its publication.

بهار ۱۴۰۵
دوره ۲، شماره ۳
شاپای الکترونیکی:
۳۱۱۵-۸۴۹۸

فصلنامه نوآوری حقوقی

وبسایت مجله

هوش مصنوعی و فرایندهای عدالت کیفری: جلوه‌ها و کاربردها

مجید قورچی بیگی[۱]، غلامعلی اندیشور*[۲]

۱. دانشیار گروه حقوق جزا و جرم‌شناسی، دانشکدهٔ حقوق و علوم سیاسی، دانشگاه خوارزمی، تهران، ایران
۲ . دانشجوی دکتری حقوق جزا و جرم‌شناسی، دانشکدهٔ حقوق و علوم سیاسی، دانشگاه خوارزمی، تهران، ایران (نویسندهٔ مسئول)

*ایمیل نویسندهٔ مسئول: ghulamali.andishwar@gmail.com

چکیده

نظام‌های عدالت کیفری معاصر در مواجهه با تحولات اجتماعی، گسترش جرائم سازمان‌یافته و پیچیدگی داده‌های جرم با چالش‌هایی مانند ناکامی در کشف جرم، دشواری شناسایی مظنونان، اطالهٔ دادرسی و خطاهای انسانی روبه‌رو هستند؛ مشکلاتی که می‌توانند کارایی و مشروعیت عدالت کیفری و حقوق متهمان را تضعیف کنند. ظهور هوش مصنوعی با تحلیل داده‌محور و پردازش سریع اطلاعات، استفاده از فناوری برای بهبود دادرسی عادلانه را مطرح کرده است. مسئلهٔ اصلی پژوهش، بررسی تأثیر هوش مصنوعی بر فرایند دادرسی عادلانه و ارزیابی ظرفیت‌ها و مخاطرات آن در کشف جرم، تحقیق و محاکمه است. پرسش اصلی این است که هوش مصنوعی چگونه می‌تواند دادرسی عادلانه را ارتقا دهد و چه تهدیدهایی برای حقوق دفاعی ایجاد می‌کند. فرضیهٔ پژوهش بر آن است که استفادهٔ ضابطه‌مند از هوش مصنوعی، در چارچوب اصول دادرسی عادلانه، می‌تواند نارسایی‌های موجود را کاهش دهد، مشروط بر آنکه جایگزین تصمیم‌گیری انسانی نشود. پژوهش از نظر ماهیت، توصیفی ـ تحلیلی ثانوی و کاربردی است و داده‌های آن از طریق مطالعهٔ کتابخانه‌ای، بررسی متون حقوقی و جرم‌شناختی و تحلیل قوانین و اسناد مرتبط گردآوری شده است. یافته‌ها نشان می‌دهد هوش مصنوعی در کشف جرم می‌تواند با تحلیل داده‌های رفتاری، مکانی و زمانی به شناسایی الگوهای مجرمانه کمک کند؛ در تحقیق نیز داده‌های دیجیتال، ارتباطات الکترونیکی و تصاویر را سریع پردازش کند و خطاهای انسانی را کاهش دهد. در محاکمه، فناوری می‌تواند با تحلیل سوابق و آرای مشابه، نقش دستیار قضائی را ایفا کند و افزایش هماهنگی میان نهادهای قضائی و اجرایی را ممکن سازد. با این حال، جعبهٔ سیاه الگوریتمی، سوگیری داده‌ها، تبعیض، دست‌کاری سامانه‌ها و تضعیف شفافیت و حقوق دفاعی مهم‌ترین مخاطرات آن است. نتیجه آنکه هوش مصنوعی باید به‌عنوان ابزار حمایتی و تحلیلی، تحت نظارت انسانی، شفافیت الگوریتمی، مسئولیت‌پذیری و کنترل مستمر به‌کار گرفته شود. تدوین مقررات جامع، توسعهٔ مدل‌های توضیح‌پذیر و آموزش قضات و متخصصان نیز ضروری است.

واژگان کلیدی: هوش مصنوعی، عدالت کیفری، سیستم قضای هوشمند، فناوری در عدالت.

دریافت شده در تاریخ: ۳۰ آذر ۱۴۰۴ - **پذیرش‌شده در تاریخ:** ۱۰ اسفند ۱۴۰۴- **منتشرشده در تاریخ:** ۱ فروردین ۱۴۰۵

قورچی بیگی، مجید؛ اندیشور، غلامعلی. (۱۴۰۵). «هوش مصنوعی و فرایندهای عدالت کیفری: جلوه‌ها و کاربردها». فصلنامه نوآوری حقوقی، دوره ۲، شماره ۳، صص. ۱۰۷-۱۳۴

Doi: https://doi.org/10.22034/lir.2026.2086077.1032

© 2026 The Authors. Published by Legal Innovation Research Institute, Tehran, Iran. This is an open access article distributed under the terms of the Creative Commons Attribution 4.0 International (CC BY 4.0) License.

مقدمه

در نظام عدالت کیفری، مجازات به‌عنوان یکی از ابزارهای اصلی تحقق عدالت و حفظ نظم اجتماعی تلقی می‌شود و با اهداف متعددی توجیه می‌گردد. هرچند سزادهی خود یکی از اهداف نظام عدالت کیفری به‌شمار می‌آید، اما اعمال آن علیه بزهکاران با هدف تقویت کارکردهای اصلاحی و بازدارنده در سطح فردی و اجتماعی انجام می‌شود. کنشگران نظام عدالت کیفری که درپی تأمین منافع بزه‌دیده و تحقق رسیدگی منصفانه در راستای منافع عمومی هستند، همواره تلاش می‌کنند تا با بهره‌گیری از ابزارهای کارآمد، عدالت کیفری را به شکلی مؤثر اجرا کنند. دستیابی به چنین اهدافی مستلزم استفاده از روش‌ها و ابزارهای علمی و نوین است که در این میان، هوش مصنوعی می‌تواند به‌عنوان یکی از ابزارهای مؤثر و کارآمد در تحقق اهداف نظام عدالت کیفری مورد توجه قرار گیرد.

بی‌تردید ظهور هوش مصنوعی یکی از مهم‌ترین تحولات فناورانه در جهان معاصر محسوب می‌شود که توانسته است بسیاری از ساختارهای سنتی را دگرگون سازد. هوش مصنوعی[1] شاخه‌ای از علوم کامپیوتر و فناوری‌های پیشرفته است که به طراحی و توسعهٔ سیستم‌ها و برنامه‌هایی می‌پردازد که قادرند وظایفی را انجام دهند که معمولاً نیازمند هوش انسانی است. شکل‌گیری این حوزهٔ علمی به اوایل قرن بیستم بازمی‌گردد (صوفی و صالح‌نژاد، ۱٤۰۲: ۲). جان مک‌کارتی ازجمله نخستین دانشمندانی بود که مفهوم هوش مصنوعی را به‌عنوان علم و مهندسی ساخت ماشین‌های هوشمند مطرح کرد (مصطفوی اردبیلی و همکاران، ۱٤۰۱: ٤).

امروزه هوش مصنوعی در حوزه‌های مختلفی ازجمله صنعت، پزشکی، اقتصاد، علوم اجتماعی و مدیریت مورد استفاده قرار می‌گیرد. با توجه به روند رو به رشد توسعهٔ این فناوری، انتظار می‌رود که در آیندهٔ نزدیک کاربردهای آن به‌صورت گسترده‌تری در جنبه‌های مختلف زندگی بشر گسترش یابد و تحولات قابل توجهی در عرصه‌های گوناگون ایجاد کند (همان: ۲). یکی از حوزه‌های مهمی که در سال‌های اخیر توجه پژوهشگران را به خود جلب کرده است، کاربرد هوش مصنوعی در فرایند دادرسی کیفری است. درواقع، امکان بهبود کارایی و دقت نظام‌های عدالت کیفری از طریق استفاده از فناوری‌های هوشمند به‌طور فزاینده‌ای مورد توجه قرار گرفته است. از آنجا که قدرت دولت در زمان صدور احکام کیفری بیشترین تأثیر را بر زندگی شهروندان دارد، بهره‌گیری از فناوری‌های نوین در

1. Artificial Intelligence (AI)

چنین تصمیم‌گیری‌هایی می‌تواند نقش مهمی در ارتقای کیفیت و دقت تصمیمات قضائی ایفا کند (Ryberg, 2024: 2).

دادرسی عادلانه و منصفانه یکی از اهداف بنیادین نظام عدالت کیفری است که بر مجموعه‌ای از اصول و قواعد اساسی استوار است. ازجمله مهم‌ترین این اصول می‌توان به اصل تساوی افراد در برابر قانون، اصل بی‌طرفی و استقلال قضائی، اصل رعایت حقوق متهم، اصل برائت و همچنین رعایت حریم خصوصی در جریان دادرسی کیفری اشاره کرد (مصدق، ۱٤۰۲: ۲۵).

با وجود مزایا و ظرفیت‌های قابل توجه هوش مصنوعی، استفاده از این فناوری در نظام عدالت کیفری با چالش‌ها و انتقاداتی نیز مواجه شده است. یکی از انتقادات مطرح‌شده این است که سیستم‌های هوش مصنوعی عمدتاً بر پایهٔ پردازش داده‌های عددی و منطق دوگانه (صفر و یک) عمل می‌کنند و ممکن است درک پیچیدگی‌های انسانی و شرایط خاص هر پرونده برای آن‌ها دشوار باشد. در مقابل، برخی پژوهشگران معتقدند که بسیاری از فرایندهای شناختی انسان نیز به‌نوعی مبتنی بر الگوهای دوگانه در سیستم عصبی هستند و هوش مصنوعی می‌تواند با تحلیل حجم عظیمی از داده‌ها، الگوهای تصمیم‌گیری دقیق‌تری ارائه دهد (اسحاقی، ۱٤۰۲: ٤).

از سوی دیگر، تصمیم‌گیری انسانی ممکن است تحت تأثیر عواملی مانند خستگی، احساسات، تعصب یا جانبداری قرار گیرد. این امر می‌تواند احتمال بروز خطا در برخی تصمیمات قضائی را افزایش دهد. در مقابل، سیستم‌های مبتنی بر هوش مصنوعی می‌توانند بدون تأثیرپذیری از چنین عوامل انسانی، داده‌ها و اطلاعات را تحلیل کند و در فرایند تصمیم‌گیری به‌عنوان ابزار کمکی مورد استفاده قرار گیرند. به همین دلیل، برخی پژوهشگران بر این باورند که استفادهٔ صحیح و کنترل‌شده از هوش مصنوعی می‌تواند به ارتقای کارایی و دقت نظام عدالت کیفری کمک کند (شیخوند و همکاران، ۱٤۰۲: ۱۳۹_۱٤۰).

با این حال، استفاده از هوش مصنوعی در دادرسی کیفری پرسش‌های مهمی را نیز مطرح می‌کند. ازجمله اینکه: هوش مصنوعی چه تأثیری بر اصول بنیادین عدالت کیفری، مانند حق دادرسی عادلانه و اصل برائت دارد؟ آیا استفاده از این فناوری با موازین حقوق بشر سازگار است؟ چگونه می‌توان میان کارآمدی هوش مصنوعی و تضمین حقوق متهم در فرایند دادرسی کیفری تعادل برقرار کرد؟ همچنین چه چالش‌های حقوقی و اخلاقی در استفاده از هوش مصنوعی در این حوزه وجود دارد و پذیرش تصمیمات مبتنی بر این فناوری تا چه اندازه می‌تواند بر اعتماد عمومی نسبت به نظام عدالت

کیفری تأثیر بگذارد؟ در عین حال، بسیاری از پژوهش‌ها نشان می‌دهد که هوش مصنوعی می‌تواند در مراحل مختلف دادرسی کیفری نقش حمایتی و تکمیلی ایفا کند و به تقویت اصول بنیادین دادرسی عادلانه کمک نماید.

۱. فرایند دادرسی کیفری: بی‌عدالتی در نظام عدالت کیفری ممکن است به اشکال گوناگونی بروز کند. گاهی افراد بی‌گناه به جرائمی که مرتکب نشده‌اند محکوم می‌شوند و در مقابل، ممکن است برخی مجرمان واقعی از مجازات بگریزند. همچنین امکان دارد تبرئه‌های نادرست رخ دهد یا مجرمان بیش از حد استحقاق خود مجازات شوند، یا برعکس، مجازاتی کمتر از میزان استحقاقشان دریافت کنند. علاوه بر این، در برخی موارد برخوردهای تبعیض‌آمیز مبتنی بر نژاد یا قومیت نیز مشاهده می‌شود که از مصادیق آشکار بی‌عدالتی محسوب می‌شود. بسیاری از مردم رنج کشیدن یک فرد بی‌گناه در زندان را بدتر از آزاد بودن یک مجرم می‌دانند (Roberts, 1954: 20).

در نظام عدالت کیفری، فرایند دادرسی کیفری با تحقق یکی از اسباب تحریک دعوای جزایی آغاز می‌شود که در مادۀ ٥٦ قانون اجراآت جزایی سال ۱۳۹۲ افغانستان پیش‌بینی شده است. براساس این ماده، اسباب تحریک دعوای جزایی عبارت‌اند از: مشاهدۀ جرم در هنگام ارتکاب و سایر حالات جرم مشهود، استغاثه و درخواست کمک، اطلاع از وقوع جرم، شکایت اشخاص یا مراجع، درخواست مراجع رسمی، اطلاع ادارات و مؤسسات از ارتکاب جرم، مشاهدۀ آثار و علائم جرم توسط سارنوال، نشر مطالب مبنی بر ارتکاب جرم و همچنین اظهارات شخص علیه خود.

همچنین مطابق مواد ۸۰، ۸۱ و ١٤٥ قانون اجراآت جزایی (۱۳۹۲) افغانستان و مادۀ ۲۲ قانون آیین دادرسی کیفری (۱۳۹۲) جمهوری اسلامی ایران، دادرسی کیفری شامل کشف جرم، تعقیب متهم، انجام تحقیقات، حفظ حقوق عمومی و اقامۀ دعوای لازم است که انجام این وظایف عمدتاً در صلاحیت و مسئولیت نهادهایی مانند پلیس و دادسرا قرار دارد.

۱. تعاریف

هوش مصنوعی ترکیبی از دو کلمۀ «هوش» و «مصنوعی» است که هر کدام را می‌توان به‌صورت جدا تعریف کرد. نخست هوش: برخی هوش را توانایی کسب تجربه، ادارک و انتخاب مناسب در برابر تغییرات محیطی می‌دانند. اما برخی دیگر هوش را عبارت از توانایی یافتن سریع راه‌حل مناسب در فضای اطلاعاتی عظیم می‌دانند. هوش مصنوعی: سیستم‌های هوش‌مند است که از طریق تجزیه

و تحلیل داده‌های بزرگ و «محاسبات ابری» یاد می‌گیرند، اجرا می‌کنند و انواع جدید از نرم‌افزارها و رُبات‌ها را توان‌مند می‌سازند تا به‌صورت بسیار مستقل از تصمیمات سازندگان و اپراتورها عمل کنند (مصطفی و همکاران، ۱٤۰۱: ٤).

هوش مصنوعی به‌لحاظ قدرت تصمیم‌گیری به چهار نسل تقسیم می‌شود: نسل اول: واکنش‌گرا؛ نسل دوم: محدود؛ نسل سوم: ذهنی؛ و نسل چهارم: خودآگاه دانسته می‌شود. این دسته‌بندی اهمیت فراوان دارد، زیرا نقش هوش مصنوعی که در فرایند دادرسی کیفری به‌کار می‌رود خیلی مهم است و باید دارای قدرت والا از درک و فهم انسانی باشد، تا تأثیرپذیری آن بر دادرسی کیفری منصفانه باشد. باید دقت کرد که عملکرد هوش‌مندانه و تجزیه و تحلیل داده‌ها در سیستم‌های ماشینی بدون دانستن نقشهٔ راه عملی میسر نیست و این نقشه الگوریتم نام دارد. الگوریتم: مجموعهٔ متناهی از دستورالعمل‌هاست که به ترتیب خاص اجرا می‌شوند و مسئله را حل می‌کنند یا الگوریتم روش گام به گام برای حل مسله یا پرونده است (همان).

۲. مرحلهٔ کشف جرم و تعقیب متهم

کشف جرم و تعقیب متهم از مراحل آغازین فرایند دادرسی کیفری است که از وظایف اساسی پلیس و دادستان به‌شمار می‌رود. بر اساس مادهٔ ۲۲ قانون آیین دادرسی کیفری ایران و مواد ۸۰ و ۸۱ قانون اجراآت جزای افغانستان، پلیس و دادستان مکلف‌اند برای کشف جرم، تعقیب متهم و جمع‌آوری ادله از هر وسیله‌ای که قانون اجازه می‌دهد استفاده کنند. در این میان، این پرسش مطرح می‌شود که آیا استفاده از هوش مصنوعی در این حوزه امکان‌پذیر است و چه تأثیری می‌تواند بر فرایند کشف جرم و تعقیب متهم داشته باشد.

با توجه به پیشرفت‌های سریع فناوری، به‌کارگیری هوش مصنوعی در کشف جرائم، تعقیب متهمان و جمع‌آوری ادله نه‌تنها امکان‌پذیر است، بلکه می‌تواند تحول قابل توجهی در نظام عدالت کیفری ایجاد کند. هوش مصنوعی قادر است حجم گسترده‌ای از داده‌ها را در مدت زمان کوتاه تحلیل کند و الگوهای پنهان را شناسایی نماید. با این حال، استفاده از این فناوری باید در چارچوب اصول بنیادین حقوق کیفری، به‌ویژه اصل برائت و حق بر حریم خصوصی افراد، صورت گیرد، زیرا هرگونه استفادهٔ غیرقانونی یا غیرمتناسب از داده‌ها می‌تواند به نقض حقوق و آزادی‌های اساسی شهروندان منجر شود.

۲ـ۱. تحلیل داده‌های بزرگ و الگوهای جرم

پس از وقوع جرم، انتظار عمومی از پلیس آن است که در کوتاه‌ترین زمان ممکن بزهکار را شناسایی و دستگیر کند. با این حال، در بسیاری از موارد پلیس به‌دلیل محدودیت منابع، پیچیدگی جرائم یا فقدان اطلاعات کافی در شناسایی مظنونان با دشواری مواجه می‌شود (Clarke & Eck, 2008: 5). در چنین شرایطی، هوش مصنوعی می‌تواند با تحلیل داده‌های گسترده و پیچیده به کشف جرم کمک کند.

۲ـ۱ـ۱. پیش‌بینی جرم

موفقیت نهادهای کشفی در کشف جرم تا حد زیادی به کیفیت اطلاعات و سرعت تصمیم‌گیری آن‌ها وابسته است؛ از این رو پیش‌بینی جرم اهمیت زیادی دارد (محبی و همکاران، ۱۴۰۰: ۲). الگوریتم‌های هوش مصنوعی قادرند حجم عظیمی از داده‌های مرتبط با جرائم، ازجمله زمان، مکان، نوع جرم و سوابق جنایی را تحلیل کرده و الگوهای پنهان را شناسایی کنند. این تحلیل‌ها می‌توانند مناطق و زمان‌هایی را که احتمال وقوع جرم در آن‌ها بیشتر است پیش‌بینی کنند.

به همین دلیل، رویکرد «پلیس مبتنی بر پیش‌بینی»[1] در بسیاری از نظام‌های عدالت کیفری مورد توجه قرار گرفته است. یکی از مهم‌ترین مزیت‌های هوش مصنوعی در این حوزه، توانایی آن در تحلیل داده‌های گسترده و ناهمگون است؛ قابلیتی که می‌تواند در بررسی پرونده‌های پیچیدهٔ کیفری بسیار سودمند باشد (مقدم و همکاران، ۱۴۰۲: ۴).

هوش مصنوعی این امکان را فراهم می‌کند که اطلاعات حقوقی، سوابق قضائی، داده‌های اجتماعی و حتی داده‌های رسانه‌ای به صورت هم‌زمان تحلیل شوند و نتایج آن برای پیشگیری از جرم و کشف آن مورد استفاده قرار گیرد (Rigano, 2019: 7). توانایی پردازش حجم عظیمی از داده‌ها باعث می‌شود که الگوهای پیچیده و پنهان در رفتارهای مجرمانه شناسایی شود و اطلاعات ارزشمندی برای پیش‌بینی جرائم آینده فراهم آید (صوفی و صالح‌نژاد، ۱۴۰۲: ۵).

درواقع پیش‌بینی جرم با بررسی داده‌های تاریخی و تحلیل الگوهای گذشته، امکان پیش‌بینی وقوع جرم در آینده را براساس عواملی مانند مکان، زمان، روز، فصل و سال فراهم می‌کند (Kumar & Irshad, 2022: 16). پیامد چنین رویکردی می‌تواند کاهش میزان جرائم، افزایش امنیت عمومی و تقویت اعتماد شهروندان به نظام عدالت کیفری باشد.

---

1. predictive policing

۲-۱-۲. شناسایی شبکه‌های جنایی

یکی دیگر از کاربردهای مهم هوش مصنوعی در کشف جرم، شناسایی شبکه‌های جنایی است. الگوریتم‌های تحلیل شبکه می‌توانند روابط میان افراد، مکان‌ها و رویدادهای مجرمانه را بررسی کرده و ساختار سازمان‌های مجرمانه را شناسایی کنند. این فناوری می‌تواند برای کشف ارتباطات پنهان میان اعضای باندهای جنایی، گروه‌های تروریستی یا شبکه‌های قاچاق مورد استفاده قرار گیرد (Europol, 2020:15).

تحلیل داده‌ها به نهادهای مجری قانون این امکان را می‌دهد که فعالیت‌های سازمان‌های مجرمانه را شناسایی کرده و برای مختل کردن یا پیگرد قانونی آن‌ها اقدام کنند. همچنین، الگوریتم‌های هوش مصنوعی می‌توانند با شناسایی الگوهای رفتاری مجرمان بالقوه، به پیشگیری از وقوع جرم کمک کنند و درنهایت موجب افزایش امنیت عمومی و اعتماد جامعه به نظام عدالت کیفری شوند (Rigano, 2019: 8).

۲-۱-۳. تحلیل داده‌های مالی

از دیگر کاربردهای مهم هوش مصنوعی در کشف جرم، تحلیل تراکنش‌های مالی است. بسیاری از جرائم سازمان‌یافته مانند پول‌شویی، کلاه‌برداری و فساد مالی از طریق شبکه‌های پیچیدهٔ مالی انجام می‌شوند و کشف آن‌ها با روش‌های سنتی دشوار است. هوش مصنوعی با تحلیل حجم عظیمی از داده‌های مالی می‌تواند الگوهای مشکوک را شناسایی کند.

الگوریتم‌های تشخیص تقلب با مقایسه ویژگی‌های شناخته‌شدهٔ تقلب با تراکنش‌های جاری، فعالیت‌های مشکوک را شناسایی می‌کنند و الگوریتم‌های پیش‌بینی نیز تلاش می‌کنند وقوع تقلب را پیش از تحقق آن پیش‌بینی نمایند (Akbarossadat, 2021: 24). استفاده از این فناوری می‌تواند به نهادهای قضائی و نهادهای نظارتی در کشف جرائم مالی و تعقیب مرتکبان آن‌ها کمک قابل توجهی کند.

۲ـ۲. بهبود تحقیقات پلیس

تشخیص چهره: سرویس‌های تشخیص چهره[1] از فناوری‌های هوش مصنوعی و یادگیری ماشین برای شناسایی و تحلیل چهره‌ها بهره می‌برند. ابزارهای «FR» معمولاً نیازمند تطبیق مجدد با یک تصویر هستند تا دقت و سازگاری نتایج با الزامات قانونی افزایش یابد. در کاربردهای حقوقی، الزامات فنی مرتبط با «FR» در موارد متعدد به‌دلیل کیفیت پایین تصاویر یا زوایای نامناسب با چالش مواجه می‌شوند و این امر موجب کاهش صحت شناسایی می‌گردد. در چنین شرایطی، تصاویر چهره با استفاده از فناوری‌های «FR» به‌صورت مؤثرتر پردازش و تنظیم می‌شوند. به‌کارگیری ابزارهای مبتنی بر هوش مصنوعی نه‌تنها قابلیت اطمینان فرایندهای شناسایی را افزایش می‌دهد، بلکه به متخصصان امکان دستیابی به دقت و توازن بیشتر در تصمیم‌گیری‌ها را نیز می‌دهد؛ افزون بر این، اصول و معیارهای مبتنی بر عدالت می‌توانند توجیهات حقوقی لازم را برای بهبود مشروعیت تصمیمات فراهم سازند (Carlson & Colleagues, b.t. 4).

هوش مصنوعی قادر است در شناسایی چهرهٔ مظنونان و مجرمان مورد استفاده قرار گیرد. با به‌کارگیری مدل‌های پیشرفتهٔ تشخیص چهره و شبکه‌های عصبی، می‌توان دقت شناسایی مظنونان و مجرمان را به‌طور قابل توجهی افزایش داد (حیدپور و همکاران، ۱۴۰۲: ۹).

تشخیص اثرانگشت تغییریافته: با استفاده از هوش مصنوعی، سیستم‌های «AFIS» که مبتنی بر الگوریتم‌های یادگیری ماشین و شبکه‌های عصبی هستند، می‌توانند برای تشخیص و تطبیق اثر انگشت‌ها به‌کار گرفته شوند. از آنجا که برخی افراد همواره در تلاش‌اند تا از شناسایی توسط این سامانه‌ها اجتناب کنند و روش‌های تغییر ویژگی‌های بیومتریک خود را توسعه می‌دهند، ضروری است که سیستم تشخیص اثر انگشت از طریق قابلیت یادگیری در زمان واقعی، سرعت و دقت خود را حفظ کند (Carlson & Colleagues, b.t. 6). این یکی از اثرات مثبت بهره‌گیری از هوش مصنوعی در فرایندهای دادرسی کیفری به‌شمار می‌رود

تحلیل صوت‌ها و فیلم‌ها: یکی از قابلیت‌های کلیدی هوش مصنوعی، تحلیل داده‌هاست و می‌تواند منابع صوتی و تصویری را برای استخراج نتایج دقیق و معتبر بررسی کند. این توانایی در فرایند کشف جرم و شناسایی مجرمان نقشی حیاتی دارد. با استفاده از مدل‌های یادگیری ماشین و شبکه‌های عصبی، امکان تحلیل فیلم‌های دوربین‌های مداربسته فراهم می‌شود. همچنین می‌توان از طریق

1. face recognition services

تحلیل دقیق صداهای مختلف مانند صدای تلفن، برخورد اجسام، تیراندازی و ...، به نتایج مؤثر رسید (حیدپور و همکاران، ۱۴۰۲: ۵).

تحلیل صحنهٔ جرم: هوش مصنوعی با قدرت و دقت بالای محاسباتی خود، در حوزه‌هایی چون تشخیص الگوها، پردازش تصویر و صدا، ترجمهٔ زبان و شناسایی افراد مشکوک، عملکردی فراتر از توان انسان دارد (صوفی و صالح‌نژاد، ۱۴۰۲: ۵). به‌واسطهٔ توان بالای پردازش داده، الگوریتم‌های پیشرفته قادرند مشخصات افراد مشکوک را تشخیص دهند و آثار و علائم موجود در صحنهٔ جرم را تجزیه و تحلیل کنند؛ سپس اطلاعات مرتبط را در اختیار مأموران پلیس و نهادهای امنیتی قرار دهند تا وضعیت کنونی افراد مظنون را ارزیابی کنند. افزون بر این، هوش مصنوعی می‌تواند با تحلیل داده‌های صحنهٔ جرم، الگوهای رفتاری و تعاملات افراد را شناسایی کند و در صورت مشاهدهٔ تغییرات غیرمعمول، هشدارهای لازم را به پلیس ارائه دهند (حیدپور و همکاران، ۱۴۰۲: ۲۰).

۳. مرحلهٔ تحقیق جرم

مرحلهٔ تحقیق جرم از مهم‌ترین مراحل فرایند دادرسی کیفری است، زیرا هدف اصلی آن کشف حقیقت، احراز وقوع یا عدم وقوع جرم، شناسایی مرتکب یا مرتکبان احتمالی و فراهم‌سازی دلایل لازم برای اتخاذ تصمیم قضائی است. مطابق مادهٔ ۹۲ قانون آیین دادرسی کیفری ایران، انجام تحقیقات مقدماتی در همهٔ جرائم، جز جرائم موضوع مادهٔ ۳۰۲ همان قانون، اصولاً بر عهدهٔ بازپرس است؛ با این توضیح که شروع و انجام این تحقیقات منوط به ارجاع دادستان، به‌عنوان مقام تعقیب، خواهد بود. بنابراین، پس از کشف جرم و گردآوری اولیهٔ دلایل، دادستان و بازپرس مکلف‌اند با بررسی همه‌جانبهٔ واقعه، اعتبار داده‌ها، قرائن و ادلهٔ موجود را ارزیابی کنند و زمینهٔ اثبات یا نفی اتهام را برای دادگاه فراهم سازند. در این مرحله، هر ابزاری که بتواند دقت، سرعت و جامعیت تحلیل اطلاعات را افزایش دهد، می‌تواند در کشف حقیقت و کاهش خطای انسانی نقش مؤثری ایفا کند.

در این چارچوب، استفاده از هوش مصنوعی در مرحلهٔ تحقیق جرم می‌تواند تأثیر قابل توجهی بر کیفیت و کارآمدی تحقیقات مقدماتی داشته باشد. هوش مصنوعی، به‌ویژه از طریق شبکه‌های عصبی مصنوعی، قادر است داده‌های گسترده و متنوع را پردازش، طبقه‌بندی و تحلیل کند. شبکه‌های عصبی مصنوعی از مجموعه‌ای از پردازشگرهای کوچک و مرتبط با یکدیگر تشکیل شده‌اند که با الهام از ساختار عصبی مغز انسان عمل می‌کنند. این شبکه‌ها دارای ورودی، خروجی و حافظهٔ

داخلی هستند و می‌توانند داده‌های دریافتی را پردازش و ذخیره کنند. بر این اساس، هوش مصنوعی با ارزیابی داده‌ها و اطلاعات محیطی، می‌تواند به‌صورت مستقل و کارآمد، مناسب‌ترین راه‌حل را برای دستیابی به نتیجه انتخاب و آن را تثبیت کند (همان: ۵).

کاربرد هوش مصنوعی در تحقیقات کیفری را می‌توان در چند محور اصلی بررسی کرد: نخست، هوش مصنوعی توانایی پردازش حجم عظیمی از داده‌ها را دارد؛ داده‌هایی که ممکن است شامل گزارش‌های پلیسی، تصاویر دوربین‌های مداربسته، داده‌های مخابراتی، سوابق کیفری، اطلاعات شبکه‌های اجتماعی، داده‌های مکانی، اسناد مالی و سایر آثار دیجیتال باشد. تحلیل دستی چنین داده‌هایی، به‌ویژه در جرائم پیچیده، سازمان‌یافته یا سایبری، بسیار زمان‌بر و گاه غیرممکن است. الگوریتم‌های هوش مصنوعی می‌توانند میان داده‌های پراکنده ارتباط برقرار سازند، الگوهای پنهان را شناسایی کنند و سرنخ‌هایی را در اختیار مقام تحقیق قرار دهند که در روش‌های سنتی ممکن است از دید انسان پنهان بماند. از همین رو، گفته شده است که الگوریتم‌های هوش مصنوعی با بهره‌گیری از منابع قانونی، داده‌های اجتماعی و اطلاعات رسانه‌ای، در شناسایی مرتکبان جرم و افراد دارای ریسک بالا نقش مؤثری ایفا می‌کنند (Carlson & colleagues, n.d.7).

به‌واسطهٔ قدرت بالای پردازش و تحلیل داده‌ها، دادستان می‌تواند با بهره‌گیری از هوش مصنوعی، دلایل و مدارک گردآوری‌شده را تجزیه‌وتحلیل کند و حقیقت وقوع یا عدم وقوع جرم، همچنین بی‌گناهی یا گناه‌کاری مظنون را کشف سازد. هوش مصنوعی در پیش‌بینی جرم، تشخیص چهره و تحلیل اطلاعات جنایی توانایی چشمگیری دارد و می‌تواند در کوتاه‌ترین زمان ممکن، مقام تحقیق را به نتیجه برساند (Ibid).

٤. مراحل محاکمه و اصدار حکم

کاربرد هوش مصنوعی در مرحلهٔ محاکمه و صدور حکم مستلزم دقت و احتیاط بیشتری است، زیرا خطا در بررسی پرونده یا تعیین مجازات می‌تواند کارایی کل نظام عدالت کیفری را تضعیف و حتی امنیت عمومی را تهدید کند.

به باور برخی پژوهشگران، نقش‌آفرینی هوش مصنوعی در اثبات جرم و تعیین مجازات می‌تواند با بهره‌گیری از پایگاه داده‌ای جامع و الگوریتم‌های منطقی مبتنی بر قواعد «اگر ـ آنگاه» انجام شود. چنین سیستمی قادر است با دقت و انسجام بالا، مراحل مرتبط با تشدید، تخفیف یا اعمال نهادهای

ارفاقی را در پرونده‌های مشابه به‌صورت یکپارچه اجرا کند و در کوتاه‌ترین زمان ممکن حکم صادر نماید؛ تصمیمی که به‌دلیل نبود عوامل انسانی نظیر خطای شناختی یا عاطفی، احتمال خطا در آن بسیار پایین است و امکان صدور کیفرهای مشابه در جرائم مشابه را فراهم می‌آورد (شیخوند و همکاران، ۱۴۰۲: ۱۴۳). مقام قضائی از هوش مصنوعی برای گردآوری اطلاعات و دریافت خروجی یا پیشنهاد استفاده می کند و از این جهت مقام قضائی مختار خواهد بود تا به خروجی یا پیشنهاد ارائه‌شده توسط هوش مصنوعی ترتیب اثر دهد یا مستقلاً رأی صادر کند (کوشا و باقری، ۱۴۰۳: ۲۴۴).

درخصوص تعیین مجازات توسط هوش مصنوعی سه رویکرد کلی وجود دارد:

۱. رویکرد جایگزینی کامل: در این دیدگاه، هوش مصنوعی به‌صورت مستقل و با لحاظ تمام خصوصیات پرونده، اصول حقوقی و دستورالعمل‌های مربوط، حکم صادر می‌کند و نیازی به تشکیل جلسهٔ دادگاه نیست.

۲. رویکرد جایگزینی مشروط: مشابه رویکرد پیشین، الگوریتم جایگزین قاضی می‌شود، اما فقط در صورتی که طرفین دعوا رضایت داشته باشند. در غیر این صورت، قاضی انسانی باید رأی صادر کند.

۳. رویکرد حمایتی: در این روش، هوش مصنوعی به‌عنوان ابزار کمکی در خدمت قاضی عمل می‌کند و با تحلیل سوابق قضائی و الگوهای مشابه، امکان صدور احکام منسجم‌تر و مطمئن‌تر را فراهم می‌سازد.

به‌نظر می‌رسد رویکرد سوم، عملی‌تر و مورد پذیرش بیشتری در نظام‌های حقوقی باشد (شیخوند و همکاران، ۱۴۰۲: ۱۴۳-۱۴۴).

۵. مزیت‌ها و چالش‌ها

به‌صورت کلی استفاده از هوش مصنوعی در فرایند دادرسی کیفری دارای مزیت‌ها و چالش‌های مختلف است که در ذیل به بررسی برخی از آن‌ها می‌پردازیم:

اتوماتیک‌سازی و تسریع در فرایند دادرسی: استفاده از هوش مصنوعی، یادگیری ماشین و سیستم‌های اطلاعاتی برای بهبود کارایی و سرعت در فرایند قضائی مهم است، زیرا این رویکرد قادر است در صرفه‌جویی زمان، افزایش دقت و تقلیل خطاهای انسانی به ما کمک کند.

مدیریت مستندات و شواهد: یکی از کار بردهای مهم فناوری در حوزه‌های حقوقی، قضائی و اداری، مدیریت مستندات و شواهد با استفاده از هوش مصنوعی است. با استفاده از الگوریتم‌های پیش‌رفته می‌توان فرایند مرتبط با جمع‌آوری، سازمان‌دهی، تحلیل و بازیابی مستندات و شواهد را به‌طور چشمگیر بهبود بخشید، زیرا جمع‌آوری و سازماندهی مستندات و شواهد از منابع مختلف به‌صورت خودکار از قابلیت‌های هوش مصنوعی است که با اسکن و دیجتالی‌سازی، طبقه‌بندی مستندات براساس نوع، موضوع، تاریخ و سایر معیارهای مرتبط و برچسب‌گذاری هوشمند انجام می‌شود.

تحلیل و استخراج اطلاعات: هوش مصنوعی قادر به استخراج اطلاعات کلیدی از مستندات و تحلیل آن‌هاست که شامل تبدیل تصاویر اسناد به متن قابل جست‌وجو، شناسای و استخراج اطلاعات خاص، مانند نام، تاریخ، مبالغ یا مفاهیم حقوقی و بررسی مستندات برای شناسایی الگوها، تناقضات یا اطلاعات مرتبط با پرونده است.

جست‌وجو و بازیابی مستندات: با استفاده از هوش مصنوعی بسیار سریع می‌توان جست‌وجو و بازیابی مستندات را انجام داد، چون هوش مصنوعی ب‌عنوان یک فناوری کمپوتری از سرعت عمل بسیار بالا برخوردار خواهد بود، بنابراین با ورود داده‌ها و انجام آموزش‌های سالم به هر حجمی که اطلاعات وجود داشته باشد در مدت بسیار کم مستندات موردنظر را بازیابی و در اختیار شما قرار می‌دهد. این سرعت پردازش محاکمه را تسریع می‌نماید (محمودی و کاظمی، ۱۴۰۲: ۶۱).

بهبود شفافیت و کاهش تبعیض: استفاده از هوش مصنوعی (AI) در فرایند دادرسی کیفری می‌تواند به بهبود شفافیت و کاهش تبعیض کمک کند، اما این مسئله نیازمند دقت بالا با توجه به چالش‌های مرتبط است، اما استفاده از آن دارای مزیت‌های ذیل است:

شفافیت بیشتر: گفتمان‌های انتقادی درمورد هوش مصنوعی و یادگیری ماشینی دربارهٔ عدالت، پاسخ‌گوی و شفافیت وجود دارد. به همین منظور اروپا شفافیت را یکی از هفت الزام کلیدی برای تحقق «هوش مصنوعی قابل اعتماد» ذکر کرده است (Larsson & Heintz, 2020: 2). بدون تردید با شفافیت در رسیدگی‌های کیفری در نتیجهٔ تحلیل داده‌های بزرگ و ارائهٔ گزارش‌های دقیق، هوش مصنوعی می‌تواند فرایند تصمیم‌گیری را شفاف تر کند، زیرا این سیستم‌ها قادرند مستندات و شواهد را به‌صورت عینی بررسی کند و از این طریق احتمال خطای انسانی را کاهش دهد. گاهی شفافیت ناظر بر فرایند طی‌شده توسط هوش مصنوعی است که به‌عنوان شفافیت الگوریتم خوانده می‌شود. اگر الگوریتم و داده‌های ورودی به سیستم هوشمند از شفافیت کافی برخوردار نباشد نمی‌توان انتظار

مناسب از عملکرد هوش مصنوعی برای کاربر داشت (حسینی و همکاران، ۱۴۰۲: ۷۳). ولی به همین راحتی هم نیست، زیرا برخی از الگوریتم‌های هوش مصنوعی از یادگیری عمیق استفاده می‌کنند و ممکن است به‌عنوان «جعبهٔ سیاه» (Lersson, 2020: 5) عمل کنند؛ یعنی ممکن است تصمیمات آن‌ها برای انسان قابل درک نباشد (توسعه‌دهندگان باید سعی کنند تا الگوریتم‌ها هوش مصنوعی را به گونه‌ای طراحی کنند که تصمیمات آن‌ها برای کاربران قابل درک باشد).

کاهش تبعیض: اگر داده‌های آموزشی هوش مصنوعی ناقص یا متعصبانه باشند، ممکن است سیستم تصمیمات تبعیض‌آمیز و ناعادلانه اتخاذ کند که این امر به جای کاهش تبعیض می‌تواند به تشدید آن بینجامد. به سه دلیل AI می‌تواند نتایج جانبدارانه تولید کند: اول، طرف‌داری ازپیش‌موجود که در کدنویسی و طراحی سیستم مورد استفاده قرار می‌گیرد؛ دوم، طرف‌داری فنی که از محدودیت‌های سامانه ناشی می‌شود؛ سوم، طرف‌داری برآیند، که در نتیجهٔ درگیر شدن کاربران با هوش مصنوعی اتفاق می‌افتد (رهبر و شعبانپور، ۱۴۰۱: ۴۳۰). اگر هوش مصنوعی به درستی طراحی و آموزش داده شود، می‌تواند بدون توجه به عوامل ناخودآگاه مانند، نژاد، جنسیت یا موقعیت اجتماعی، تصمیمات عادلانه اتخاذ کند که این امر می‌تواند به کاهش تبعیض در فرایند دادرسی کیفری کمک کند.

۵ـ۱. دقت و پیش‌بینی دقیق‌تر حکم‌ها

تحلیل داده‌های قضائی: با استفاده از الگوریتم‌های یادگیری ماشینی، می‌توان داده‌های تاریخی مربوط به پروندهٔ قضائی را تحلیل کرد و الگوهایی را شناسی کرد که به پیش‌بینی نتایج احتمالی پرونده‌ها کمک می‌کند. آنچه مهم است شفافیت در الگوریتم‌هاست تا بتوانند به درستی داده‌ها را تحلیل کنند، زیرا برای تحقق این امر لازم است در هوش مصنوعی فرایندی طی شود که خروجی خاص حاصل شود و این خروجی مورد نظر به شفافیت در عملکرد الگوریتم ها بستگی دارد (حسینی و همکاران، ۱۴۰۲: ۷۷).

پیش‌بینی احکام: سیستم‌های هوش مصنوعی قادرند با تحلیل پرونده‌های مشابه، پیش‌بینی‌هایی درمورد احتمال صدور حکم خاصی ارائه دهند و این پیش‌بینی‌ها می‌تواند به قضات، وکلا و طرفین پرونده کمک کند تا تصمیم بهتری اتخاذ کنند. هوش مصنوعی می‌تواند حجم زیادی از پرونده‌ها و تمام اسناد و احکام دادگاه را که در گذشته توسط قضات تا به امروز که در ارتباط به یک پروندهٔ مرتبط

است، همراه با زیادی از انواع دیگر داده‌ها عمومی بررسی کند، این می‌تواند در تصمیم‌گیری قضای مفید باشد (محمودی و بحر کاظمی، ۱۴۰۲: ۶۲).

افزایش دقت در تصمیم‌گیری قضائی: استفاده از هوش مصنوعی می‌تواند موجب کاهش خطاهای ناشی از قضاوت‌های انسانی شود، این ابزار می‌تواند با تحلیل دقیق‌تر شواهد و مدارک، دقت تصمیم‌گیری‌ها را افزایش دهد و در استانداردسازی فرایندهای قضائی کمک کند تا تصمیمات قضائی براساس اطلاعات و شواهد منطقی گرفته شود (همان: ۵۷).

دسترس‌پذیری و عدالت برای افراد ناتوان: استفاده از هوش مصنوعی در فرایند دادرسی کیفری می‌تواند نقش اساسی در دسترس‌پذیری عدالت برای مردم به‌خصوص افراد ناتوان ایفا کند (همان: ۵۷) که در ذیل بررسی می‌کنیم:

ترجمهٔ خودکار و تفسیر زبان اشاره: هوش مصنوعی می‌تواند به افراد ناشنوا یا کم‌شنوا کمک کند تا از طریق ترجمهٔ خودکار زبان اشاره به محتوای جلسات دادگاه دسترسی پیدا کنند.

تبدیل متن به گفتار و گفتار به متن: برای افراد نابینا یا بی‌سواد، سیستم‌های تبدیل متن به گفتار و گفتار به متن، می‌توانند محتوای دادگاه را قابل فهم‌تر کنند.

دسترسی به اطلاعات حقوقی: استفاده از هوش مصنوعی می‌تواند به افراد ناتوان کمک کند تا اطلاعات حقوقی را به شیوه‌های ساده و قابل فهم دریافت کنند. همچنان هوش مصنوعی می‌تواند به افراد ناتوان مشاوره‌های حقوقی اولیه ارائه دهد و آن‌ها را در فرایند دادرسی راهنمای کند.

۵ـ۲. چالش‌های هوش مصنوعی به‌عنوان قاضی

به‌نظر می رسد کاربرد هوش مصنوعی در نقش قاضی چندان بی‌دردسر نیست و ایرادات جدی را به همراه دارد. یکی از ایرادات AI در زمینهٔ استدلال حقوقی است. ممکن است AI در استدلال‌های صوری موفق عمل کند، اما در پرونده‌های بدیع و دشوار، با چالش‌هایی مواجه است، زیرا پرونده‌های بدیع فاقد سابقهٔ قضائی‌اند؛ در اغلب نظام‌های حقوقی راهکاری برای این معضل سنجیده شده، مانند نظام حقوقی ایران که اصل ۱۶۷ قانون اساسی و مادهٔ ۳ آیین دادرسی مدنی آمده است که قاضی باید با ابتکار و با استفاده از اصول حقوقی دعوای مطروحه را حل کند. همچنین در مادهٔ ۲ قانون مدنی افغانستان آمده است: در مواردی که حکمی در قانون یا فقه حنفی موجود نبود، محکمه مطابق با عرف عمومی که مناقض احکام قانون و اساسات عدالت نباشد، حکم صادر کند.

اما پرسشی که مطرح می‌شود این است که آیا هوش مصنوعی قادر به رسیدگی چنین پرونده‌هایی است؟ حل و فصل چنین پرونده‌هایی خلاقیت حقوقی می‌طلبد، هوش مصنوعی به‌دلیل عدم درک از ارزش‌های اجتماعی و اخلاقی، قادر به تولید قاعدهٔ حقوقی نیست، زیرا ایجاد یک قاعدهٔ حقوقی براساس عدالت، انصاف و سیاست‌گذاری‌های عمومی شکل می‌گیرد (رهبری و شعبانپور، ۱۴۰۱: ۴۲۱). اگر هوش مصنوعی فاقد چنین قابلیتی باشد، چگونه می‌تواند به‌عنوان قاضی در چنین پرونده‌هایی نقش بازی کند؟ درپرونده‌های بدیع موقعیتی مطرح می‌شود که رویهٔ قضائی به حد کافی در موضوع مورد مناقشه غنی نیست که هوش مصنوعی بتواند الگوبرداری کند، لذا اعمال صلاحیت قضائی نیازمند ارزیابی آن پرونده با دیدگاه تازه است که از صلاحیت یادگیری ماشینی بیرون است. اما برخلاف این ادعاها گروهی از صاحب‌نظران معتقدند هوش مصنوعی در مواجهه با موارد بدیع موفق عمل می‌کند و البته این بیشتر در زمینه‌های پزشکی به اثبات رسیده و در زمینهٔ حقوقی چنین موفقیت هنوز در مرحلهٔ امیدواری قرار دارد (همان: ۴۲۲).

نکتهٔ مورد اهتمام دیگر در منصب قضائی صلاح‌دید قاضی است. دادرسان در مواردی ناچار به اعمال صلاح‌دید خود است. در پرونده‌های بدیع و دشوار که در قانون و شرع حکمی موجود نباشد و رویهٔ قضائی هم خالی باشد یا حتی در موارد ممکن است پیروی کورکورانه از قانون خلاف عدالت، انصاف و نتایج غیرعقلانی را درپی داشته باشد، قاضی ناگزیر است با صلاح‌دید خود عمل کند تا حقی ضایع و ستمی بر پا نشود. در چنین موقعیتی هوش مصنوعی نمی‌تواند مناقشه را حل کند و گروهی از متخصصان بر این باورند که بهتر است این وظیفهٔ مهم برعهدهٔ قضات انسانی باقی بماند. گروهی از محققان به این باورند که حل پرونده‌های بدیع و دشوار مستلزم برقراری موازنه میان ارزش‌هاست، ولی هوش مصنوعی قادر به درک ارزش‌های انسانی و اخلاقی نیست (همان: ۴۲۸) .

مشروعیت کاربرد AI در نقش قاضی از دیدگاه اسلام: به‌صورت اختصاری می‌توانیم با اتکا به دلایل از کتاب و سنت، مشروعیت یا عدم مشروعیت استفاده از هوش مصنوعی را در نقش قاضی تبیین کنیم.

نخست آنکه قضاوت امری مشروع و غایت نهایی آن تأمین عدالت، صلح و برابری است. قرآن کریم به تکرار بر این امر تأکید کرده است که می‌توان به آیهٔ ۵۸ سورهٔ نساء، ۴۲ سورهٔ المائده، ۱۰ سورهٔ الحجرات، ۸ سورهٔ الممتحنه و... اشاره کرد، هر کدام از این آیات بر تأمین عدالت، صلح و احقاق زِحق اهتمام ورزیده است. سیرهٔ نبی اکرم (ص) سرشار از تأکیدات، ارشادات واجرای عدالت

است. نبی اکرم (ص) می‌فرماید: لاضرر و لاضرار فی الاسلام. در این ترید نیست که فلسفهٔ بعثت پیامبر اکرم (ص) نجات بشریت از گمراهی و تأمین عدالت و احقاق صاحب حق بوده است. با هر وسیلهٔ ممکن که بتوانیم عدالت را تأمین و حق را به صاحب آن بازگردانیم، از ضرر به خود و دیگران جلوگیری کنیم و این غایت نهایی احکام الهی است. در فقه امامیه دو نظریه به قول طباطبایی مطرح است: نخست استفاده از هوش مصنوعی را در نقش قاضی منوط به حکم حاکم شرع می‌دانند و دوم استفاده از آن را مشروط به صحت داده‌ها می‌دانند که بتواند برای قاضی در مقام حکم مفید باشد (طباطبایی و بینش بهنیا، ۱۴۰۱: ۱۲). اما سؤال این است که به‌کار گرفتن هوش مصنوعی در نقش قاضی می‌تواند عدالت را تأمین و حق را به زِحق حُکم نماید؟ با توجه به قدرت و توانایی‌ای که امروزه در هوش مصنوعی وجود دارد می‌توان پاسخ داد که این ظرفیت و اطمینان شاید به‌صورت کلی و همه‌جانبه هنوز به میان نیامده، ولی می‌توان از هوش مصنوعی در منصب قضائی به‌عنوان مشاور قضائی و حتی در قضایای کم‌اهمیت‌تر به‌عنوان قاضی حکم استفاده کرد. اما بی‌ایراد هم نیست، خیلی‌ها استفاده از هوش مصنوعی در امر قضاوت را ناجایز دانسته و به شروط انتخاب قاضی و شرایط علمیت قاضی اشاره می‌کنند که البته جای تأمل دارد و نمی‌توان ادعای آن‌ها را کاملاً منتفی دانست، ولی به نظر نویسنده استفاده از هوش مصنوعی در نقش قاضی بعد از اثبات توانایی آن در امر قضاوت نه‌تنها مشکلی نمی‌تواند داشته باشد که انسان را در امر رسیدن به عدالت و اجرای منصفانه و عادلانهٔ قانون یاری می‌رساند و این همان غرض آیات الهی است. چنانچه در کشورهای مثل استونی اجازه داده شده تا در پرونده‌های به ارزش ۸۰۰۰ دلار هوش مصنوعی در نقش قاضی بازی کند، یا در استرالیا نیز اجازه داده شده از هوش مصنوعی برای پیش‌بینی نتایج اختلافات در مناقشات ملکی، خانوادگی، با استدلال‌های مبتنی بر قانون و شبکه‌های عصبی استفاده کند (رجبی و همکاران، ۱۴۰۲: ۳۷۵).

۶. ملاحظات حقوقی در استفاده از هوش مصنوعی

با وجود مزایای فراوان هوش مصنوعی در کشف جرم، استفاده از این فناوری باید با رعایت اصول اساسی حقوق کیفری همراه باشد. یکی از مهم‌ترین این اصول، اصل برائت است. براساس این اصل، هر شخصی بی‌گناه فرض می‌شود مگر اینکه جرم او در دادگاه صالح و براساس ادلهٔ قانونی اثبات

شود. بنابراین، نتایج حاصل از تحلیل‌های هوش مصنوعی نباید به‌عنوان دلیل قطعی مجرمیت تلقی شود، بلکه باید صرفاً به‌عنوان ابزار کمکی برای تحقیقات کیفری مورد استفاده قرار گیرد.

از سوی دیگر، استفادهٔ گسترده از داده‌ها و فناوری‌های نظارتی ممکن است به نقض حریم خصوصی شهروندان منجر شود. بسیاری از سیستم‌های هوش مصنوعی برای تحلیل رفتارهای مجرمانه از داده‌های شخصی مانند اطلاعات ارتباطی، داده‌های مکانی یا فعالیت‌های برخط استفاده می‌کنند. در صورت نبود نظارت قانونی و سازوکارهای شفاف، این امر می‌تواند به سوءاستفاده از داده‌ها و نقض حقوق اساسی افراد منجر شود (Oswald, 2018: 15).

از این رو، قانون‌گذاران باید چارچوب‌های قانونی مشخصی برای استفاده از هوش مصنوعی در نظام عدالت کیفری تدوین کنند تا ضمن بهره‌گیری از مزایای این فناوری، از حقوق بنیادین شهروندان نیز حمایت شود. رعایت اصولی مانند تناسب، ضرورت، شفافیت و نظارت قضائی می‌تواند به ایجاد تعادل میان کارایی فناوری و حمایت از حقوق و آزادی‌های فردی کمک کند.

نتیجه‌گیری

هوش مصنوعی یکی از نوآورانه‌ترین و تحول‌آفرین‌ترین پدیده‌های علم و فناوری معاصر است که توانسته است ظرفیت‌های گسترده و شگفت‌انگیزی را در عرصه‌های مختلف به نمایش بگذارد. ریشه‌های نظری این فناوری به اوایل قرن بیستم بازمی‌گردد و بسیاری، جان مک‌کارتی را از نخستین اندیشمندانی می‌دانند که هوش مصنوعی را در قالب یک حوزهٔ مستقل علمی و مهندسی مطرح ساخت. امروزه هوش مصنوعی در حوزه‌های گوناگون، ازجمله پزشکی، صنعت، حمل‌ونقل، امور نظامی و غیرنظامی، کاربردهای فراوانی یافته و به‌تدریج دامنهٔ نفوذ آن به علوم انسانی، به‌ویژه حوزهٔ عدالت کیفری، نیز گسترش یافته است. بررسی‌ها نشان می‌دهد که این فناوری می‌تواند در مراحل مختلف فرایند کیفری، از کشف جرم تا محاکمه و صدور حکم، نقشی مؤثر و تحول‌آفرین ایفا کند.

نخست، در مرحلهٔ کشف جرم و تعقیب متهم، بهره‌گیری از هوش مصنوعی می‌تواند فرایندهای دشوار، پیچیده و زمان‌بر مربوط به شناسایی جرائم و تعقیب مظنونان را تسهیل سازد. یافته‌های این پژوهش نشان می‌دهد که هوش مصنوعی از توانایی بالایی در تحلیل کلان‌داده‌های جنایی، شناسایی الگوهای رفتاری و جرمی، پیش‌بینی جرم، کشف شبکه‌های جنایی، تحلیل داده‌های مالی، تشخیص چهره، شناسایی اثر انگشت‌های تغییریافته، تحلیل صوت و تصویر و نیز بررسی صحنهٔ جرم

برخوردار است. این قابلیت‌ها به ضابطان عدلی و نهادهای کشفی امکان می‌دهد تا با سرعت، دقت و کارآمدی بیشتری به کشف جرم، شناسایی مرتکبان و ارائهٔ آنان به مراجع ذی‌صلاح اقدام کنند.

دوم، در مرحلهٔ تحقیق جرم، با توجه به اینکه در نظام‌های حقوقی افغانستان و ایران، دادستان و بازپرس مسئولیت انجام تحقیقات مقدماتی و بررسی اتهام را بر عهده دارند، هوش مصنوعی می‌تواند به‌عنوان ابزاری کمکی و مؤثر در اختیار این مقامات قرار گیرد. توانایی این فناوری در تحلیل هم‌زمان قوانین، سوابق کیفری، رویه‌های قضائی، اسناد و مدارک پرونده، می‌تواند مقامات تحقیق را در دستیابی سریع‌تر و دقیق‌تر به حقیقت یاری رساند. درنتیجه، استفاده از هوش مصنوعی نه‌تنها موجب تسریع در فرایند تحقیق و اثبات حقیقت می‌شود، بلکه می‌تواند احتمال بروز خطاهای انسانی، غفلت‌های تحلیلی و تصمیم‌گیری‌های شتاب‌زده را نیز کاهش دهد.

سوم، در مرحلهٔ محاکمه و صدور حکم، هرچند کاربرد هوش مصنوعی در برخی کشورها تجربه شده و این فناوری از قابلیت‌هایی همچون تحلیل پرونده، تطبیق قواعد حقوقی و حتی پیشنهاد مجازات برخوردار است، اما استفاده از آن در این مرحله مستلزم احتیاط و ملاحظهٔ بیشتری است. درخصوص نقش هوش مصنوعی در تعیین مجازات و صدور حکم، سه رویکرد عمده قابل شناسایی است: رویکرد نخست، مبتنی بر جایگزینی کامل هوش مصنوعی به‌جای قاضی انسانی است؛ رویکرد دوم، مبتنی بر جایگزینی مشروط است، به‌گونه‌ای که مگر در صورت درخواست طرفین برای قاضی انسانی، تصمیم الگوریتمی معتبر تلقی شود؛ و رویکرد سوم، استفاده از هوش مصنوعی به‌عنوان ابزار حمایتی و کمکی برای قاضی است. به‌نظر می‌رسد از میان این سه رویکرد، رویکرد سوم از حیث انطباق با اصول دادرسی منصفانه، حفظ نقش قاضی انسانی و کاهش مخاطرات ناشی از تصمیم‌گیری کاملاً ماشینی، قابل‌قبول‌تر و واقع‌بینانه‌تر باشد.

چهارم، با وجود مزایای قابل توجه هوش مصنوعی، به‌کارگیری آن در جایگاه تصمیم‌گیر قضائی با چالش‌های مهمی نیز همراه است. رسیدگی به پرونده‌های بدیع، پیچیده و فاقد پیشینهٔ قانونی یا قضائی روشن، مستلزم نوعی خلاقیت حقوقی، درک عمیق از ارزش‌های اخلاقی و اجتماعی و توجه به سیاست‌های عمومی حاکم بر جامعه است؛ عناصری که هنوز به‌طور کامل در قلمرو توانمندی‌های هوش مصنوعی قرار نگرفته‌اند. از این رو، هرچند این فناوری در تحلیل داده‌ها و ارائهٔ پیشنهادهای مبتنی بر الگوهای پیشین بسیار توانمند است، اما در مواجهه با پرونده‌های نوپدید و استثنایی، همچنان نیاز به مداخله و قضاوت انسانی به قوت خود باقی است.

حامی مالی:

این مقاله هیچ حامی مالی ندارد.

مشارکت نویسندگان:

مجید قورچی بیگی: مفهوم‌سازی، نظارت بر داده‌ها، اعتبارسنجی، مدیریت پروژه، منابع.

غلامعلی اندیشور: روش‌شناسی، تحلیل، نوشتن بررسی و ویرایش، تحقیق و بررسی، پیش‌نویس اصلی.

تعارض منافع:

بنا بر اظهار نویسندگان این مقاله تعارض منافع ندارد.

ملاحظات اخلاقی:

این پژوهش بر پایهٔ مطالعهٔ اسناد، قوانین، رویه‌های قضائی و منابع کتابخانه‌ای انجام شده و در آن هیچ‌گونه مطالعه‌ای بر روی انسان، حیوان یا داده‌های شخصی صورت نگرفته است؛ بنابراین، اخذ تأییدیهٔ کمیتهٔ اخلاق برای این پژوهش ضروری نبوده است. با این حال، نویسنده اصول امانت‌داری علمی، صداقت پژوهشی، استناددهی صحیح و رعایت حقوق مالکیت فکری را در تمامی مراحل پژوهش رعایت کرده است.

در تهیهٔ این مقاله از ابزارهای هوش مصنوعی مولد صرفاً برای کمک به ویرایش زبانی، بهبود ساختار نگارش و ارتقای خوانایی متن استفاده شده است. این ابزارها در طراحی پژوهش، تحلیل علمی، تفسیر یافته‌ها، استنتاج نتایج یا تصمیم‌گیری‌های پژوهشی نقشی نداشته‌اند و مسئولیت کامل صحت، اصالت و محتوای نهایی مقاله بر عهده نویسنده/ نویسندگان است.

موافقت نویسندگان:

تمامی نویسندگان نسخهٔ نهایی مقاله را مطالعه و تأیید کرده‌اند و با انتشار آن موافقت دارند.

منابع

اسحاقی، شقایق (۱۴۰۲)، «هوش مصنوعی در آموزش و پرورش (مزایا و معایب آن)»، ماهنامهٔ عملی تخصصی پایا شهر، ۱ـ۱۰.

قانون اساسی جمهوری اسلامی ایران (۱۳۵۸)، تهران.

قانون آیین دادرسی کیفری (مصوب ۴ اسفند ۱۳۹۲) (۱۳۹۲)، تهران.

حسینی، سیداحمد، عبدخدائی، زهره و شریف‌خانی، محمد (۱۴۰۲)، «کاربرد هوش مصنوعی در رسیدگی‌های قضایی». دیدگاه‌های حقوقی قضائی، ۲۸(۱۰۱)، ۶۷-۹۰.

حیدرپور، حمیدرضا، شهانقی، محمد و مهرآرا، ژیلا (۱۴۰۲)، «کاربرد هوش مصنوعی در جرم‌یابی»، تمدن حقوقی، ۶(۱۸)، ۱۷۳-۱۹۴.

رجبی، فرشید، ایزدی فرد، علی‌اکبر، زارعی، محمدمهدی و جهانی، علی‌اکبر (۱۴۰۲)، «مشروعیت به‌کارگیری هوش مصنوعی در قضاوت»، مطالعات فقه اقتصادی، ۵(۵)، ۳۷۳-۳۸۶.

رهبری، ابراهیم و شعبانپور، علی (۱۴۰۱)، «چالش‌های کاربردی هوش مصنوعی به‌عنوان قاضی»، تحقیقات حقوقی ویژه‌نامهٔ حقوق و فناوری، ۴۱۹- ۴۴۴.

سوشینا، تاتینا و آندری، سوبنین (۱۴۰۲)، «هوش مصنوعی در نظام عدالت کیفری: روندها و احتمالات پیشِ رو»، ترجمهٔ سالار صادقی، تمدنی حقوقی، ۶(۱۸)،۹۱-۱۰۲.

شیخوند، محمدصادق، کرد علیوند، روح‌الدین، مینایی، بهروز، آشوری، محمد و مهدوی ثابت، محمدعلی (۱۴۰۲)، «هوش مصنوعی و صدور احکام کیفری؛ تصمیم‌سازی یا تصمیم‌گیری»، پژوهش‌های حقوقی تطبیقی، ۲۷(۴)، ۱۳۸-۱۶۷.

صوفی، سارا و صالح‌نژاد بهرستاقی، صابر (۱۴۰۲)، «تأثیر هوش مصنوعی در ارتکاب جرایم سایبری»، مطالعات حقوقی، ۱۱(۵)،۱-۱۸.

طباطبایی، سیده فاطمه و بینش به‌نیا، الهه، (۱۴۰۱)، «حکم تکلیفی به‌کارگیری هوش مصنوعی به عنوان قاضی»، حقوق اسلامی، ۱۹(۷۵)،

عدلیه، وزارت (۱۳۹۲)، قانون اجراآت جزایی افغانستان (شمارهٔ ۱۱۳۲)، کابل: مطبعهٔ دولتی.

کاظمی‌فر، محمد (۱۴۰۳)، قانون مجازات اسلامی ایران، تهران: سروشگان.

کبرسادات، سید مجید (۱۴۰۱)، مروری بر روش‌های کشف تقلب بانکی با استفاده از هوش مصنوعی، تهران: مؤسسهٔ آموزش عالی فردوس، ۲(۶)، ۲۰- ۴۱

کوشا، ارسلان و باقری، مژگان (۱۴۰۳)، «تأثیر به‌کارگیری هوش مصنوعی در جمع‌آوری ادلهٔ کیفری»، مطالعهٔ علوم سیاسی حقوق و فقه، ۱۰(۴)، ۲۴۱- ۲۵۳.

محبی، سمیه، حمیدی‌زاده محمدرضا و فدای‌نژاد، محمداسماعیل (۱۴۰۰)، «الگوریتم انتخاب ویژگی‌های مناسب به‌منظور پیش‌بینی شاخص بورس اوراق بهادار تهران چشم‌انداز مدیریت مالی»، نشریهٔ چشم‌انداز مدیریت مالی، ۱۱(۳۴)، ۳۵-۶۷.

محمودی، امیررضا و بحرکاظمی، مریم (۱۴۰۲)، «هوش مصنوعی و تأثیر آن بر سیستم قضایی»، تمدن حقوقی، ۱۸، ۵۵-۷۲.

مصدق، محمد (۱۴۰۲)، آیین دادرسی کیفری، تهران: جنگل.

مصطفوی اردبیلی، سیدمحمدمهدی، تقی‌زاده انصاری، مصطفی، و رحمتی‌فر، سمانه (۱۴۰۱)، «کارکردهای هوش مصنوعی از منظر دادرسی منصفانه»، حقوق فناوری‌های نوین، ۳(۶)، ۴۷-۶۰.

مقدم، حکمتی، سادات، فاطمه و عبداللهی، نگار (۱۴۰۳)، «نگاهی به کاربردهای هوش مصنوعی در فرایند دادرسی»، نشریهٔ عدلیه، ٦، ۳۲-۳۶.

نظری علوم، مهدی، محمدی، غلام رضاشاه، دعاگویان، داود و کریمی، روح‌الله (۱۴۰۳)، «شناسایی متهمین جرایم جنایی و امنیتی»، مطالعات امنیت داخلی، ٦، ۱۴۷-۱۷۶.

References

Akbarossadat, S. (2021). Artificial intelligence and financial fraud detection. *Journal of Financial Crime, 28(3),* 1–25.

Carlson, C. A., Hemby, J. A., Wooten, A. R., Jones, A. R., Lockamyeir, R. F., Carlson, M. A., Dias, J. L., & Whittington, J. E. (2021). Testing encoding specificity and the diagnostic feature-detection theory of eyewitness identification, with implications for showups, lineups, and partially disguised perpetrators. Cognitive Research: Principles and Implications, 6, Article 14.

IJIS Technology and Architecture Committee (ITAC). (2019). Artificial intelligence in justice and public safety. IJIS Institute.

Clarke, R. V., & Eck, J. E. (2005). *Crime analysis for problem solvers in 60 small steps*. U.S. Department of Justice, Office of Community Oriented Policing Services.

Delponte, L. (2018). European artificial intelligence (AI) leadership: The path for an integrated vision. European Parliament, Policy Department for Economic, Scientific and Quality of Life Policies, Directorate-General for Internal Policies. PE 626.074.

Kumar, A., & Irshad, M. (2022). Crime prediction using machine learning techniques. International Journal of Computer Applications, *184*(12), 10–18.

Larsson, S., & Heintz, F. (2020). Transparency in artificial intelligence. Internet Policy Review, 9(2), 1-16.

Larsson, S. (2020). On the governance of artificial intelligence through ethics guidelines. Asian Journal of Law and Society, 7(3), 437–451.

Oswald, M. (2018). Algorithm-assisted decision-making in the public sector. Philosophical Transactions of the Royal Society A, 376(2128), 1–16.

Rigano, C. (2019). Using artificial intelligence to address criminal justice needs. *NIJ Journal*, *280*, 5-11.

Ryberg, J. (2024). Sentencing, artificial intelligence, and condemnation. *Criminal Justice Ethics*, *43*(2), 131–145.

Journal Website

Legal Innovation Quarterly

Spring 2026

Volume 2, Issue 3

E-ISSN: 3115-8498

Iran's Criminal Policy on Digital Violence Against Women's Mental Health: With Reference to the World Health Organization's Approach

Jamal Beigi *[1], Zahra Eghbali [2]

1. Professor, Department of Criminal Law and Criminology, Law Research Center, Maragheh Branch, Islamic Azad University, Maragheh, Iran (Corresponding Author)*
2. Ph.D. Student, Department of Criminal Law and Criminology, Researcher at the Law Research Center, Maragheh Branch, Islamic Azad University, Maragheh, Iran

***Corresponding author email address:** jamal_beigi@iau.ac.ir

Extended Abstract

1. Introduction

The rapid growth of digital technologies over the past decade has transformed the traditional structure of human relationships and gender relations and has created new arenas for the manifestation of violence. In this context, women are more exposed than other groups to hidden and overt forms of digital violence; although this violence occurs without physical contact, its profound psychological intensity threatens their psychological security, freedom of expression, self-esteem, and social functioning. This phenomenon has become an emerging crisis, particularly in the post-COVID era and with the increase in dependence on online platforms. In Iran, likewise, statistics on cases related to online harassment, the dissemination of private images, and cyber threats against women are on the rise.

Received: 17 January 2026 - **Accepted:** 18 March 2026 - **Published:** 21 March 2026

Beigi, Jamal; and Eghbali, Zahra. (2026). "Iran's Criminal Policy on Digital Violence Against Women's Mental Health: With a Focus on the World Health Organization's Approach." Legal Innovation Quarterly, 2(3), pp. 135-174
Doi: https://doi.org/10.22034/lir.2026.2085421.1031

© 2026 The Authors. Published by Legal Innovation Research Institute, Tehran, Iran. This is an open access article distributed under the terms of the Creative Commons Attribution 4.0 International (CC BY 4.0) License.

The principal issue addressed by the present study is the existing gap between Iran's criminal policy approach and global standards. Iran's criminal policy is primarily focused on penal responses and punishment-oriented measures and pays less attention to preventive mechanisms based on mental health and subsequent support. By contrast, the World Health Organization (WHO), adopting a holistic approach, regards digital violence as part of "gender-based violence" and as a serious threat to public health. The researcher's principal concern is to examine the extent to which Iran's current policies are aligned with mental health components and what reforms are necessary to enhance their effectiveness. Accordingly, the present study seeks to answer the following questions: To what extent is Iran's criminal policy aligned with global standards for combating digital violence, and which mental health components have been overlooked in this policymaking?

2. Research Methodology

The research method adopted in this study is descriptive-analytical. To this end, data concerning Iran's domestic laws, including the Computer Crimes Law and the Islamic Penal Code, as well as the documents and guidelines of the World Health Organization, have been collected through library-based and documentary research. Subsequently, adopting a comparative approach, the theoretical foundations and operational strategies of both fields have been assessed and evaluated. The analysis focuses on identifying the gap between Iran's exclusively legal-criminal approach and the WHO's health-oriented approach.

3. Research Findings

The research findings can be classified under two main headings: "Analysis of Criminological Manifestations" and "Contrast Between Policy Approaches."

1. Typology of Digital Violence and Its Legal Status in Iran

The analyses indicate that three categories of offenses have posed the greatest threats to women in Iranian cyberspace.

*Pornography and Image Abuse (Revenge Pornography): Under Articles 742 to 746 of the Islamic Penal Code, the dissemination of private images has been criminalized. However, the findings indicate that these offenses are often committed with the aim of infringing reputation and assassinating character, and that women, owing to their gender-specific characteristics, are the principal victims of this phenomenon. Although the current law criminalizes the conduct, it does not pay sufficient attention to the aspects of "structural victimization" or to the remediation of psychological harm resulting from the violation of dignity.

*Cyber Trafficking and Sexual Exploitation: Cyberspace has provided a platform for the "identification," "recruitment," and "deception" of women by human trafficking networks. Although the Law on Combating Human

Trafficking (2004) exists, establishing the role of digital intermediaries and combating networks that use cryptocurrencies remain challenging.

*Online Harassment and Symbolic Violence: Cyber harassment, approximately 90 percent of which is directed against women, creates an environment filled with anxiety and insecurity. In addition, the study refers to a novel form of violence termed "symbolic violence" or "the imposition of beauty ideals." Unregulated advertising for cosmetic surgery in Iranian cyberspace places women under psychological pressure to change their bodies, which constitutes harm to public health but has not been expressly criminalized under criminal law [cite: 380–385].

2. The Contrast Between the Health-Oriented Paradigm (WHO) and the Security-Oriented Paradigm (Iran)

The comparative findings indicate that the World Health Organization regards digital violence as an extension of gender-based violence and as a "public health" crisis with consequences such as chronic anxiety, depression, and post-traumatic stress disorder (PTSD). The Organization's strategy is based on "primary prevention" (education and media literacy), "secondary prevention" (risk screening and psychological intervention), and "tertiary support" (victim empowerment) [cite: 408–412].

In contrast, Iran's criminal policy is primarily based on the paradigms of "moral security" and "criminalization." Existing laws focus more on the conduct of the offender than on the psychological condition of the victim. Iran lacks national protocols for the psychological support of victims of cyber violence and does not have a targeted educational system for the prevention of these offenses. This policy gap has resulted in persistently high rates of psychological harm and non-reporting among women, despite police and judicial responses.

4. Conclusion and Recommendations

The present study concluded that Iran's criminal policy toward digital violence against women, although active in the punitive dimension and in responding to clear manifestations (such as the dissemination of images), has serious gaps in the preventive and supportive dimensions. The current situation indicates the predominance of a one-dimensional penal approach that regards digital violence merely as a security disorder, whereas, according to WHO standards, this phenomenon is a public health problem.

The absence of a precise definition of gender-based cyber violence, the lack of enforcement mechanisms to address symbolic violence (such as harmful beauty advertising), and the absence of a link between the judicial system and the mental health system have been identified as the main challenges. To move beyond the current situation and enhance the effectiveness of criminal policy, the following recommendations are proposed:

1. Integration of Penal Policy and a Health-Oriented Approach: A transition from a purely reactive approach to an approach in which therapeutic and counseling interventions form part of the judicial proceedings. The establishment of psychological service centers specifically for victims of digital violence and the design of a national counseling protocol are necessary.

2. Legal Reforms: The criminalization of emerging forms, such as "gender-based deepfakes" and "beauty-related symbolic violence," and the legal definition of gender-based digital violence.

3. Social and Educational Prevention: A focus on digital literacy and cyber safety education for women and girls in order to increase psychological resilience, in accordance with WHO recommendations on primary prevention.

4. Development of Supportive Infrastructure: The establishment of safe and confidential reporting systems for vulnerable women and the requirement for domestic platforms to comply with user security standards.

Ultimately, effective criminal policy requires health and mental health institutions, alongside the police and the Judiciary, to play an active role in the process of prevention and treatment so that women's psychological security in the digital environment is ensured.

Keywords: Digital violence; women; mental health; criminal policy; World Health Organization; victim-centered approach.

Funding
This article has no financial support or funding.

Authors' Contributions
Jamal Beigi: Conceptualization, data curation, validation, project administration, and resources.
Zahra Eghbali: Methodology, formal analysis, writing – review & editing, investigation, writing – original draft.

Conflict of Interest
According to the authors' declaration, there is no conflict of interest regarding this article.

Ethical Considerations
This study was conducted based on the analysis of legal documents, statutes, judicial decisions, and library-based sources. It did not involve human participants, animals, or personal data; therefore, ethical approval from an institutional ethics committee was not required. Nevertheless, the authors adhered to the principles of academic integrity, research honesty, proper citation practices, and respect for intellectual property rights throughout all stages of the research.Generative artificial intelligence (AI) tools were used solely to assist with language editing, improving the structure of the manuscript, and enhancing the readability of the text. These tools did not

contribute to the study design, scientific analysis, interpretation of findings, drawing of conclusions, or any research-related decision-making. The author(s) assume full responsibility for the accuracy, originality, and final content of the manuscript.

Authors' Approval

All authors have read and approved the final version of the manuscript and consent to its publication.

بهار ۱۴۰۵
دوره ۲، شمارهٔ ۳
شاپای الکترونیکی:
۳۱۱۵-۸۴۹۸

فصلنامه نوآوری حقوقی

وبسایت مجله

سیاست جنایی ایران در قبال خشونت دیجیتالی علیه سلامت روانی زنان با نگاهی بر رویکرد سازمان بهداشت جهانی

جمال بیگی[*۱]، زهرا اقبالی[۲]

۱. استاد گروه حقوق کیفری و جرم‌شناسی، مرکز تحقیقات حقوق، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران (نویسندهٔ مسئول).
۲. دانشجوی دکتری تخصصی گروه حقوق کیفری و جرم‌شناسی، پژوهشگر مرکز تحقیقات حقوق، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران.

[*] ایمیل نویسندهٔ مسئول: jamal_beigi@iau.ac.ir

چکیده

خشونت دیجیتال علیه زنان صرفاً صورت الکترونیکی جرائم سنتی نیست، بلکه به‌واسطهٔ ویژگی‌هایی مانند قابلیت تکثیر و بازنشر سریع، ماندگاری داده، ناشناس‌مانی نسبی، امکان دسترسی فرامرزی، ترکیب رفتارهای متعدد در یک فرایند واحد و پیوند آن با سازوکارهای پلتفرمی، می‌تواند دامنه و استمرار آسیب را افزایش دهد. مسئلهٔ اصلی پژوهش حاضر آن است که آیا سیاست جنایی ایران، در مواجهه با مصادیقی چون انتشار بدون رضایت تصاویر خصوصی، تحریف و انتشار محتوای تصویری، تهدید و مزاحمت برخط و بهره‌کشی جنسی تسهیل‌شده با فناوری، از ظرفیت لازم برای حمایت مؤثر از سلامت روانی زنان برخوردار است یا خیر. پژوهش با روش توصیفی ـ تحلیلی و رویکرد تطبیقی، نخست مفهوم خشونت دیجیتال را به‌صورت عملیاتی تفکیک می‌کند؛ سپس مقررات کیفری ایران، به‌ویژه مواد ۷۴۴، ۷۴۵ و ۷۴۶ قانون مجازات اسلامی (تعزیرات) و مقررات مرتبط را از منظر عناصر جرم، قلمرو حمایت، قابلیت انطباق با فناوری‌های نوظهور و آثار حمایتی بررسی می‌کند؛ در ادامه، مؤلفه‌های سلامت‌محور مورد تأکید سازمان جهانی بهداشت را به معیارهای قابل سنجش برای ارزیابی سیاست جنایی تبدیل می‌کند. نوآوری مقاله در ارائهٔ «مدل سیاست جنایی چهارحلقه‌ای خشونت دیجیتال» است که پاسخ کیفری را در کنار پیشگیری، حمایت سلامت‌محور و حکمرانی/ پاسخ‌گویی نهادی قرار می‌دهد و برای هر حلقه شاخص‌های حقوقی و اجرایی پیشنهاد می‌کند. یافته‌ها نشان می‌دهد که حقوق کیفری ایران در برخی رفتارهای مشخص، ازجمله انتشار غیرمجاز محتوای خصوصی و تحریف تصویر یا صوت، ابزار جرم‌انگاری دارد؛ اما این پوشش، معادل شناسایی جامع خشونت دیجیتال به‌عنوان یک پدیدهٔ آسیب‌زا برای سلامت روان نیست. خلأ اصلی نه فقط در فقدان عنوان مجرمانهٔ مستقل، بلکه در نبود پیوند نظام‌مند میان جرم‌انگاری، پیشگیری، خدمات سلامت روان، سازوکارهای گزارش‌دهی امن، حذف سریع محتوای زیان‌بار، ثبت داده‌های تفکیک‌شده و ارزیابی اثربخشی سیاست‌هاست. از این رو، مقاله به‌جای توصیهٔ کلی به تقویت قوانین، اصلاحات مشخصی را در سه سطح تقنینی، اجرایی و داده‌ای پیشنهاد می‌کند.

واژگان کلیدی: خشونت دیجیتال، زنان، سلامت روان، سیاست جنایی، سازمان جهانی بهداشت، بزه‌دیده‌محوری.

دریافت‌شده در تاریخ: ۲۷ دی ۱۴۰۴ - **پذیرش‌شده در تاریخ:** ۲۷ اسفند ۱۴۰۴- **منتشرشده در تاریخ:** ۱ فروردین ۱۴۰۵

بیگی، جمال؛ اقبالی، زهرا. (۱۴۰۵). «سیاست جنایی ایران در قبال خشونت دیجیتالی علیه سلامت روانی زنان با نگاهی بر رویکرد سازمان بهداشت جهانی». فصلنامه نوآوری حقوقی، دوره ۲، شماره ۳، صص ۱۳۵-۱۷۴.

Doi: https://doi.org/10.22034/lir.2026.2085421.1031

© 2026 The Authors. Published by Legal Innovation Research Institute, Tehran, Iran. This is an open access article distributed under the terms of the Creative Commons Attribution 4.0 International (CC BY 4.0) License.

مقدمه

رشد شتابان فناوری‌های دیجیتال ساختار سنتی روابط انسانی و جنسیتی را دگرگون کرده و میدان‌های نوینی برای بروز خشونت فراهم آورده است. زنان بیش از سایر گروه‌ها در معرض اشکال پنهان و آشکار خشونت دیجیتال قرار دارند؛ خشونتی که بدون تماس فیزیکی، اما با شدت روانی عمیق، امنیت ذهنی، آزادی بیان، عزت‌نفس و کارکردهای اجتماعی آنان را تهدید می‌کند. این پدیده در کشورهای مختلف به‌عنوان یک بحران نوظهور مطرح شده و به‌ویژه در دوران کرونا و پساکرونا، با افزایش وابستگی به بسترهای برخط، بُعد تازه‌ای یافته است. در ایران نیز آمار رو به افزایشی از پرونده‌های مرتبط با آزار و اذیت برخط، تهدیدهای سایبری، انتشار تصاویر خصوصی و حملات سازمان‌یافتهٔ دیجیتال علیه زنان وجود دارد. با این حال، سیاست جنایی کشور همچنان بر پاسخ کیفری متمرکز است و کمتر به سازوکارهای پیشگیرانه مبتنی بر سلامت روان، حمایت‌های پسینی و مداخلات چندرشته‌ای توجه شده است. در مقابل، سازمان بهداشت جهانی با رویکردی کل‌نگر، خشونت دیجیتال را بخشی از «خشونت مبتنی بر جنسیت» و تهدیدی جدی برای سلامت عمومی تلقی می‌کند و راهبردها و دستورالعمل‌های مشخصی برای حمایت روانی، پیشگیری جمعیت‌محور، سیاست‌گذاری دیجیتال ارائه داده است.

اهمیت این پژوهش در آن است که برای نخستین‌بار، سیاست جنایی ایران را در پرتو استانداردهای سلامت‌محور سازمان بهداشت جهانی بررسی می‌کند و شکاف میان رویکرد حقوقی ـ کیفری ایران و رویکرد سلامت‌محورWHO[1] را نشان می‌دهد. این تحقیق با تلفیق دیدگاه‌های جرم‌شناسی، سلامت عمومی و حقوق دیجیتال، تلاش می‌کند تصویری دقیق از وضعیت کنونی و نیازهای اصلاحی ارائه دهد تا زمینه برای سیاست‌گذاری منسجم، پیشگیرانه و زن‌محور فراهم شود. درخصوص پیشینهٔ تحقیق مطالعات ارزشمندی صورت گرفته است. فلین[2] و همکاران (2020) در پژوهشی به قربانی‌شناسی خشونت جنسی تسهیل‌شده با فناوری پرداخته‌اند. هنری و پاول[3] (2018) نیز در کتاب خود رویکردی چندرشته‌ای به جرائم خشونت جنسی دیجیتال داشته‌اند. در منابع داخلی ارجمند و شریفی (۱۴۰۳) چالش‌های قانونی جرائم سایبری علیه زنان را بررسی کرده‌اند.

---

۱. سازمان بهداشت جهانی

2. Flynn
3. Henry & Powell

با این حال، وجه تمایز پژوهش حاضر در تمرکز بر شکاف میان رویکرد صرفاً کیفری ایران و رویکرد سلامت‌محور سازمان بهداشت جهانی است که تاکنون به‌صورت تطبیقی و با تأکید بر سلامت روان مورد واکاوی دقیق قرار نگرفته است. این مطالعه با طرح پرسش‌هایی چون «سیاست جنایی ایران تا چه حد با استانداردهای جهانی مقابله با خشونت دیجیتال علیه زنان همسویی دارد؟»، «کدام مؤلفه‌های سلامت روانی در سیاست‌گذاری ایران مغفول مانده‌اند؟»، «چه اصلاحاتی می‌تواند پاسخ ایران را کارآمدتر سازد؟» به مقایسهٔ تطبیقی می‌پردازد و در پایان چارچوبی پیشنهادی برای سیاست جنایی تقویت‌شده ارائه خواهد کرد.

۱. پیشینهٔ پژوهش و جایگاه نوآوری

مطالعات داخلی و خارجی پیشین عمدتاً در سه مسیر حرکت کرده‌اند: توصیف اشکال خشونت فناوری‌تسهیل‌شده؛ تحلیل حمایت کیفری از حریم خصوصی، حیثیت و امنیت زنان؛ و بررسی آثار روانی آزار و خشونت برخط. پژوهش‌های پیشین موجود در نسخهٔ اولیهٔ مقاله نیز بر قربانی‌شناسی، جرائم جنسی تسهیل‌شده با فناوری و چالش‌های قانونی جرائم سایبری علیه زنان تمرکز داشته‌اند. با این حال، صرف جمع کردن این مطالعات، خلأ نظری را پر نمی‌کند.

نوآوری این پژوهش در «انتقال معیارهای سلامت‌محور از سطح توصیه‌های کلی به سطح ابزار ارزیابی سیاست جنایی» است. در این مدل، سیاست جنایی مطلوب زمانی کامل تلقی می‌شود که چهار حلقه به یکدیگر متصل باشند: ۱. جرم‌انگاری و پاسخ قضائی؛ ۲. پیشگیری و کاهش خطر؛ ۳. حمایت بزه‌دیده‌محور و سلامت روان؛ ۴. حکمرانی داده، پاسخ‌گویی نهادی و ارزیابی نتیجه. بنابراین، پرسش مقالهٔ دیگر صرفاً این نیست که آیا رفتاری جرم‌انگاری شده است؟، بلکه این است که آیا نظام حقوقی می‌تواند از مرحلهٔ شناسایی رفتار تا کاهش آسیب و بازگشت بزه‌دیده به وضعیت ایمن، زنجیره‌ای مؤثر ایجاد کند؟

۲. روش‌شناسی و چارچوب تحلیلی پژوهش

این پژوهش از حیث هدف، کاربردی و از حیث روش، توصیفی ـ تحلیلی با رویکرد تطبیقی و تحلیل هنجاری است. واحد تحلیل، «سیاست جنایی در قبال خشونت دیجیتال علیه زنان است»، نه یک جرم منفرد. داده‌های پژوهش از سه دسته تشکیل می‌شود: نخست، قوانین و مقررات کیفری ایران؛

دوم، اسناد سیاستی و راهنماهای سازمان جهانی بهداشت؛ و سوم، مطالعات علمی و داده‌های رسمی یا گزارش‌های عمومی دربارهٔ جرائم سایبری. در بخش تجربی، اصل احتیاط رعایت شده است: هرجا دادهٔ ملی اختصاصی دربارهٔخشونت جنسیتی دیجیتال وجود ندارد، از تبدیل آمار عمومی جرائم سایبری به ادعای شیوع خشونت علیه زنان خودداری می‌شود.

برای عملیاتی کردن مقایسه، پنج معیار استخراج شده است: شناسایی و جرم‌انگاری، پیشگیری، حمایت و سلامت روان، پاسخ نهادی و دسترسی به عدالت و داده و ارزیابی معیارهای مزبور با توجه به تأکید WHO بر تولید شواهد، و سلامت (WHO, 2026a; WHO, 2022).

۳. مدل پیشنهادی: چارچوب چهارحلقه‌ای سیاست جنایی سلامت‌محور

مدل پیشنهادی مقاله بر این فرض استوار است که پاسخ کیفری، شرط لازم اما به‌تنهایی شرط کافی برای مقابله با خشونت دیجیتال نیست. چهار حلقه مدل عبارت‌اند از: حفاظت حقوقی، پیشگیری، ترمیم و سلامت، و حکمرانی و یادگیری. ویژگی نوآورانهٔ مدل آن است که خروجی هر حلقه، ورودی حلقهٔ بعدی است، برای مثال ثبت شکایت باید به ارجاع امن به خدمات سلامت منجر شود و دادهٔ حاصل از پرونده‌ها باید در طراحی سیاست پیشگیری مورد استفاده قرار گیرد.

جدول ۱: مدل چهارحلقه‌ای سیاست جنایی سلامت‌محور و شاخص‌های ارزیابی آن

پیشنهاد	خلأ قابل مشاهده در ایران	شاخص ارزیابی	کارکرد	حلقه
تعریف قانونی/ سیاستی خشونت دیجیتال و تکمیل مقررات برای مصادیق نوظهور	پوشش رفتارهای مشخص وجود دارد، اما پدیده به صورت جامع تعریف نشده	وضوح عنوان مجرمانه، سرعت حفظ ادله، تناسب پاسخ	جرم‌انگاری، تعقیب، ادله و جبران	۱. حفاظت حقوقی
برنامهٔ ملی پیشگیری و استانداردهای ایمنی پلتفرمی	تمرکز غالب بر واکنش پسینی	آموزش، سواد دیجیتال، طراحی ایمن	کاهش خطر پیش از وقوع	۲. پیشگیری

پروتکل ارجاع و خدمات محرمانه و رایگان/ قابل دسترس	پیوند ضعیف میان پلیس/ قضاء و خدمات سلامت روان	غربال‌گری، ارجاع، مشاوره، محرمانگی	کاهش آسیب و بازگشت بزه‌دیده به وضعیت ایمن	۳. ترمیم و سلامت
سامانهٔ دادهٔ مشترک با شاخص‌های جنسیتی و سلامت	فقدان دادهٔ عمومی تفکیک شده دربارهٔ جنسیت و نوع خشونت	دادهٔ تفکیک‌شده، گزارش سالانه، ارزیابی نتیجه	ثبت داده و اصلاح مستمر سیاست	۴. حکمرانی و یادگیری

این مدل به‌جای آنکه «مدل جهانی وارداتی» تلقی شود، ابزاری تحلیلی برای بومی‌سازی استانداردهای سلامت‌محور است. درنتیجه، ادعای نوآوری مقاله در «ساخت مدل» نیست، بلکه در پیوند دادن سه حوزه‌ای است که معمولاً جداگانه بررسی می‌شوند: حقوق کیفری، سلامت روان و حکمرانی داده‌های دیجیتال.

٤. گونه‌شناسی خشونت دیجیتال و آثار حقوقی ـ روانی آن

۴ـ۱. انتشار بدون رضایت تصاویر و اطلاعات خصوصی

مادهٔ ۷۴۵ قانون مجازات اسلامی (تعزیرات)، که معادل مادهٔ ۱۷ قانون جرائم رایانه‌ای است، انتشار یا در دسترس قرار دادن صوت، تصویر، فیلم خصوصی یا خانوادگی یا اسرار دیگری بدون رضایت را، مشروط به تحقق ضرر یا هتک حیثیت عرفی، جرم‌انگاری کرده است. این ماده از مهم‌ترین ابزارهای کیفری موجود برای مقابله با انتشار غیررضایی تصاویر خصوصی است. با این حال، از منظر سیاست سلامت‌محور، سه نکته قابل توجه است: نخست، تمرکز عنصر قانونی بر «انتشار یا در دسترس قرار دادن» است و نه کل چرخهٔ تهدید به انتشار، اجبار، اخاذی و بازنشرهای بعدی؛ دوم، معیار ضرر یا هتک حیثیت عرفی می‌تواند نیازمند تفسیر منطبق با اشکال نوین آسیب باشد؛ سوم، جرم‌انگاری به‌تنهایی سازوکار فوری و تخصصی برای حذف محتوا و حمایت روانی از قربانی ایجاد نمی‌کند.

در نسخهٔ اولیه، برخی عبارات دربارهٔ ویژگی‌های جسمانی یا روانی زنان می‌توانست ناخواسته به سرزنش بزه‌دیده منجر شود. در تحلیل علمی حاضر، علت افزایش آسیب‌پذیری نه «لطافت» یا ویژگی ذاتی زنان، بلکه عوامل ساختاری مانند نابرابری قدرت، تهدید به افشای اطلاعات، وابستگی اقتصادی یا عاطفی، دسترسی نابرابر به حمایت و سازوکارهای جنسیت‌مند آزار در فضای دیجیتال تلقی می‌شود.

٤ـ٢. تحریف، دستکاری و محتوای جعلی

مادهٔ ۷۴۴ انتشار صوت، تصویر یا فیلم تغییریافته یا تحریف‌شده را در صورتی که عرفاً موجب هتک حیثیت شود، جرم‌انگاری می‌کند. این حکم برای دستکاری سنتی تصویر قابل استفاده است، اما تحول فناوری‌های تولید محتوای مصنوعی و deepfake پرسش‌های جدیدی دربارهٔ احراز «تحریف» انتساب عمل، سرعت انتشار و مسئولیت اشخاص متعدد ایجاد می‌کند. بنابراین، خلأ اصلی الزاماً فقدان هرگونه عنوان کیفری نیست، بلکه فقدان سازوکار تخصصی برای تشخیص و واکنش سریع به محتوای مصنوعی و تعیین تکلیف بازنشرهای زنجیره‌ای است.

٤ـ٣. تهدید، مزاحمت و تعقیب برخط

مزاحمت و تهدید دیجیتال ممکن است از یک پیام ساده آغاز و به تعقیب مستمر، افشای دادهٔ شخصی، تهدید به انتشار تصاویر، اخاذی و سرایت به زندگی فیزیکی منتهی شود. مشکل سیاست جنایی در این حوزه، گسست میان «رفتارهای متعدد» و «آسیب واحد» است: هر پیام ممکن است در خلأ کم‌اهمیت به‌نظر برسد، اما مجموعه رفتارها می‌تواند الگویی از کنترل و ارعاب ایجاد کند. بنابراین ارزیابی خطر باید بر مبنای الگوی رفتاری و تداوم آن انجام شود، نه‌فقط واقعه‌ای منفرد.

٤ـ٤. بهره‌کشی و قاچاق تسهیل‌شده با فناوری

فضای دیجیتال می‌تواند برای شناسایی، جذب، فریب و کنترل قربانیان قاچاق انسان استفاده شود. در اینجا مسئلهٔ اصلی، انطباق قواعد موجود قاچاق انسان با ابزارهای فناورانه و دسترسی فرامرزی است. با این حال، نباید هر نوع فریب برخط را بدون احراز عناصر قانونی، «قاچاق سایبری» نامید. تحلیل دقیق باید میان تبلیغ فریبنده، تسهیل جابه‌جایی، بهره‌کشی و سازمان‌یافتگی تمایز بگذارد.

٤ـ٥. خشونت نمادین و فشارهای مرتبط با بدن و زیبایی

فشارهای دیجیتال دربارهٔ بدن و زیبایی را نمی‌توان بدون دلیل کافی در زمرهٔ جرائم کیفری قرار داد. این پدیده بیشتر در سطح پیشگیری، تنظیم تبلیغات، سواد رسانه‌ای و حمایت سلامت روان قابل تحلیل است؛ مگر آنکه رفتار مشخصی مانند تبلیغ گمراه‌کننده، مداخلهٔ غیرمجاز پزشکی، تهدید یا اخاذی واجد عناصر جرم باشد. این تفکیک برای پرهیز از توسعهٔ بی‌ضابطهٔ قلمرو کیفری ضروری است.

۵. تحلیل ماده‌محور حقوق کیفری ایران

چه رفتاری جرم است؟ چه منفعتی حمایت می‌شود؟ چه خلأیی باقی می‌ماند؟ و چه اصلاحی قابل پیشنهاد است؟

جدول ۲: تحلیل ماده‌محور مقررات کیفری ایران در حوزهٔ خشونت دیجیتال و پیشنهادهای اصلاحی

پیشنهاد اصلاحی	خلأ/ چالش	نقطهٔ قوت	رفتار تحت پوشش	مقرره
تدوین قواعد اثباتی و حمایتی ویژهٔ محتوای مصنوعی؛ پیش‌بینی سازوکار حذف فوری در موارد خطرناک	ابهام در deepfake، بازنشرهای زنجیره‌ای و انتساب فنی	پوشش دستکاری محتوای تصویری	تغییر یا تحریف صوت، تصویر یا فیلم و انتشار آن با هتک حیثیت	مادهٔ ۷۴۴
تکمیل حمایت برای تهدید، بازنشر و اخاذی؛ دستور قضایی سریع برای توقف دسترسی و حفظ ادله	عدم پوشش جامع تهدید به انتشار و چرخهٔ بازنشر؛ فقدان پیوند با خدمات حمایتی	حمایت از حریم خصوصی و حیثیت	انتشار/ دسترسی بدون رضایت به محتوای خصوصی یا اسرار با ضرر/ هتک حیثیت	مادهٔ ۷۴۵
تفسیر مضیق و حفظ آزادی بیان همراه با حمایت	مرز میان نقد، خبر، ادعا و نشر اکاذیب نیازمند	امکان واکنش به برخی حملات حیثیتی	انتشار اکاذیب با قصد اضرار یا تشویش	مادهٔ ۷۴۶

مؤثر در موارد احراز عناصر جرم	دقت؛ مادهٔ سلامت روان را مستقیماً هدف نمی‌گیرد			
تدوین دستورالعمل قضائی برای ارزیابی الگوی آزار و تداوم رفتار	ماهیت جمعی و تکرارشوندهٔ آزار دیجیتال همیشه در قالب رفتار منفرد دیده نمی‌شود	امکان استفاده برای برخی آزارهای برخط	تهدید/ اهانت، حسب مورد	مقررات تهدید و توهین در قانون تعزیرات
پروتکل فوری حفظ ادله، درخواست حذف/ مسدودسازی محتوای زیان‌بار و حمایت از محرمانگی بزه‌دیده	سرعت حذف محتوا از پلتفرم و همکاری فرامرزی چالش‌برانگیز است	امکان حفظ داده و تحقیق تخصصی	حفظ و تحصیل ادلهٔ دیجیتال	آیین دادرسی جرائم رایانه‌ای

۵ـ۱. تحلیل انتقادی: خلأ اصلی «فقدان جرم» نیست، بلکه «فقدان زنجیرهٔ حمایت» است

بررسی ماده‌محور نشان می‌دهد که تصویر «فقدان کامل قانون» دقیق نیست. قانونگذار برخی رفتارهای اصلی را جرم‌انگاری کرده است. درنتیجه، تحلیل علمی باید از ادعای کلی «خلأ قانونی» فاصله بگیرد و خلأ را در سه سطح تفکیک کند: خلأ مفهومی، خلأ اجرایی و خلأ حمایتی. خلأ مفهومی به فقدان تعریف یا طبقه‌بندی جامع خشونت دیجیتال بازمی‌گردد؛ خلأ اجرایی به دشواری کشف، انتساب، حفظ ادله و توقف سریع انتشار؛ و خلأ حمایتی به نبود پیوند نهادی میان فرایند کیفری و سلامت روان و حمایت اجتماعی.

این تمایز، نتیجهٔ اصلی تحلیلی مقاله است. اگر صرفاً عنوان مجرمانهٔ جدیدی ایجاد شود، اما قربانی همچنان برای حذف محتوا، دریافت حمایت روانی، حفاظت از دادهٔ شخصی و پیگیری قضائی مجبور به عبور از مسیرهای متعدد باشد، سیاست جنایی جدید الزاماً کارآمدتر نشده است.

بنابراین معیار کارآمدی باید از «تعداد عناوین مجرمانه» به کاهش آسیب قابل اندازه‌گیری منتقل شود.

۵ـ۲. رویکرد سازمان جهانی بهداشت و معیارهای سلامت‌محور

WHO خشونت علیه زنان را مسئله‌ای با پیامدهای جدی جسمی و روانی می‌داند و بر خدمات جامع، ازجمله حمایت‌های سلامت روان، آموزش کارکنان، تولید داده، هماهنگی میان سلامت و عدالت و سیاست‌گذاری مبتنی بر شواهد تأکید دارد. در حوزهٔ محیط‌های دیجیتال نیز WHO تصریح می‌کند که فناوری‌های دیجیتال می‌توانند هم فرصت و هم خطر برای سلامت روان ایجاد کنند و ازجمله خطرات، خشونت برخط، استثمار جنسی و انزوای اجتماعی است. از این رو، نسبت دادن رویکرد WHO به یک الگوی صرفاً درمانی نیز دقیق نیست؛ رویکرد مزبور ترکیبی از پیشگیری، خدمات، داده، سیاست و همکاری بین‌بخشی است (WHO, 2026).

راهنمای RESPECT Women نیز در نسخهٔ دوم خود، پیشگیری از خشونت علیه زنان را در هفت راهبرد شامل تقویت مهارت‌های رابطه‌ای، توانمندسازی زنان، تضمین خدمات، کاهش فقر، ایمن سازی محیط‌ها، پیشگیری از خشونت علیه کودکان و تغییر نگرش‌ها و هنجارها صورت‌بندی می کند. این چارچوب نشان می‌دهد که پاسخ مؤثر به خشونت، ذاتاً چندسطحی است و نمی‌توان آن را به مجازات مرتکب فروکاست (Ibid).

جدول ۳: مقایسهٔ رویکرد سلامت‌محور WHO با وضعیت حقوق ایران و شکاف‌های سیاستی

شکاف سیاستی	وضعیت قابل استنباط از حقوق ایران	رویکرد سلامت محورWHO	معیار
ضعف یکپارچگی و ارزیابی برنامه‌ها	وجود اقدامات پراکنده، اما فقدان چارچوب جامع ویژهٔ خشونت دیجیتال در متن بررسی‌شده	آموزش، محیط ایمن، تغییر هنجارها و توانمندسازی	پیشگیری
فقدان پروتکل ارجاع و خدمات تخصصی	ابزار کیفری وجود دارد، اما پیوند نظام‌مند با	حمایت survivor-centred و خدمات سلامت روان	خدمات

	سلامت روان روشن نیست		
نبود دادهٔ تفکیک شدهٔ جنسیتی/ نوع خشونت/ پیامد روانی	داده‌های جرائم سایبری غالباً بر دسته های عمومی جرم متمرکز است	پایش، پیمایش و شاخص‌های سلامت	داده
جزیره‌ای بودن پاسخ	نهادهای متعدد وجود دارند، اما زنجیرهٔ ارجاع واحد مشخص نیست	همکاری سلامت، عدالت، خدمات اجتماعی	پاسخ چندنهادی
فاصلهٔ میان جرم‌انگاری و حمایت جامع	جرم‌انگاری برخی مصادیق وجود دارد	قانون مؤثر همراه با اجرا و منابع	قانون

۵ـ۳. شواهد تجربی و محدودیت داده‌های ایران

یکی از ایرادات اساسی داور، اتکای مقاله به گزاره‌های تجربی بدون دادهٔ کافی است. در بازنگری حاضر، این ایراد با اصلاح روش استدلال پاسخ داده شده است. نخست، داده‌های جهانی WHO صرفاً برای نشان دادن اهمیت سلامت‌محور مسئله به‌کار می‌روند و به‌عنوان شاخص وضعیت ایران استفاده نمی‌شوند. دوم، آمار پلیس فتا دربارهٔ جرائم سایبری، با احتیاط تفسیر می‌شود، زیرا ترکیب پرونده‌ها شامل جرائم مالی و سایر جرائم است و از آن نمی‌توان شیوع خشونت جنسیتی دیجیتال را استخراج کرد. سوم، فقدان آمار رسمی تفکیک‌شده به‌عنوان شکاف سیاست‌گذاری معرفی می‌شود.

در گزارشی رسمی/ رسانه‌ای از اظهارات رئیس پلیس فتا دربارهٔ سال ۱۴۰۳، اعلام شده است که حدود ۷۰ درصد پرونده‌های پلیس فتا به کلاهبرداری رایانه‌ای و برداشت غیرمجاز مربوط بوده و دسترسی غیرمجاز به داده‌ها، هتک حیثیت، نشر اکاذیب و مزاحمت اینترنتی نیز در میان موضوعات شکایت قرار داشته‌اند. این داده نشان می‌دهد که جرائم سایبری سبدی ناهمگون است و نمی‌توان بدون تفکیک جنسیت، نوع رفتار و پیامد روانی، از آن دربارهٔ خشونت علیه زنان نتیجه‌گیری کرد. این احتیاط از نظر روش‌شناسی یک امتیاز است نه ضعف مقاله.

از منظر پژوهشی، پیشنهاد می‌شود نظام آماری ایران در آینده چهار متغیر را به‌صورت هم‌زمان ثبت کند: جنسیت بزه‌دیده، نوع رفتار دیجیتال، رابطهٔ بزه‌دیده و مرتکب، و پیامدهای گزارش‌شده ازجمله ترس، اضطراب، اختلال در فعالیت روزمره و نیاز به خدمات سلامت. چنین داده‌ای امکان ارزیابی واقعی سیاست را فراهم می‌کند. WHO نیز بر ضرورت تولید شواهد دربارهٔ میزان و پیامدهای خشونت و استفاده از پیمایش‌های جمعیتی و نظام‌های اطلاعاتی سلامت تأکید دارد.

٦. تحلیل حقوقی ـ جرم‌شناختی جرائم علیه زنان در فضای سایبر

ضروری است جرائمی که در فضای سایبری زنان را تهدید می‌کنند به‌دقت شناسایی شوند و سطح آگاهی عمومی به‌ویژه در میان زنان افزایش یابد. در ادامه، این نوشتار به بررسی و تحلیل سه عنوان مجرمانه‌ای می‌پردازد که بیشترین آمار را در میان خشونت علیه زنان در محیط دیجیتال دارند.

٦ـ١. هرزه نگاری و سوءاستفاده از تصاویر خصوصی

تعریف لغوی «هرزه‌نگاری» یا پورنوگرافی به هر نوع نوشته، تصویر، فیلم یا محتوای مرتبط با امور جنسی گفته می‌شود که از منظر ادبی، هنری، سیاسی یا علمی فاقد هر گونه ارزش و کارکرد است. در حوزهٔ حقوق کیفری، ارتکاب جرم در حوزهٔ پورنوگرافی زمانی محقق می‌شود که شخص، ابزارها یا وسایلی را که حاوی این‌گونه تصاویر و محتواهای هرزه است، تهیه کند، بفروشد، توزیع نماید یا در معرض مشاهدهٔ عموم قرار دهد و دیگران را به مشارکت در این نمایش یا فعالیت‌های مرتبط با پورنوگرافی ترغیب یا تحریک کند (باستانی، ۱۳۸۳: ۵۰). هرزه‌نگاری در فضای سایبر، شامل تولید، انتشار یا معاملهٔ محتوایی است که حاوی نمایش اندام جنسی یا اعمال جنسی باشد. در حقوق کیفری ایران، قانون‌گذار در فصل چهارم قانون جرائم رایانه‌ای (مواد ۷۴۲ تا ۷۴۶ قانون مجازات اسلامی بخش تعزیرات) به این موضوع پرداخته است. به موجب مادهٔ ۷۴۲، هر کس به‌وسیلهٔ سامانه‌های رایانه‌ای یا مخابراتی محتویات مستهجن را منتشر، توزیع یا معامله کند، مجرم شناخته می‌شود. در فضای واقعی نیز جنسیت همواره یکی از عوامل اثرگذار در بزه‌دیدگی بوده است، زیرا الگوهای زیست زنان و مردان، تفاوت‌های شخصیتی و موقعیت‌های اجتماعی آن‌ها، سبب می‌شود که در برخی جرائم، زنان در معرض تهدید بیشتری قرار گیرند. همین قاعده در فضای مجازی نیز دیده می‌شود؛ به‌گونه‌ای که در جرائم سایبری، زنان بیش از مردان با خطر بزه‌دیدگی مواجه‌اند. یکی از چالش‌های

اصلی در این حوزه، پدیدهٔ «انتقام‌جویی پورنوگرافیک» است؛ وضعیتی که در آن تصاویر خصوصی زنان بدون رضایت آن‌ها و با هدف هتک حیثیت یا اخاذی منتشر می‌شود. برخلاف دیدگاه‌های سنتی که گاه قربانی را به‌دلیل «بی‌احتیاطی» یا «ویژگی‌های جنسیتی» مقصر می‌انگاشتند، جرم‌شناسی نوین بر «بزه‌دیدگی ساختاری» تأکید دارد. در این جرائم، مرتکب با سوءاستفاده از اعتماد قبلی یا هک سیستم‌ها، امنیت روانی زن را نشانه می‌گیرد. مادهٔ ۷۴۵ قانون مجازات اسلامی (مادهٔ ۱۷ قانون جرائم رایانه‌ای) صراحتاً انتشار صوت، تصویر یا فیلم خصوصی یا خانوادگی دیگری را بدون رضایت او جرم‌انگاری کرده است که گامی مهم اما ناکافی در حمایت از قربانیان محسوب می‌شود. هرزه‌نگاری زنان ازجمله جرائمی است که به‌دلیل ویژگی‌های خاص زنان چه از حیث خصوصیات جسمانی و جذابیت‌های ظاهری و چه از جهت ویژگی‌های روانی مانند لطافت، مهربانی یا حساسیت بیشتر زمینهٔ بزه‌دیدگی آنان را در محیط مجازی تشدید می‌کند. در عمل، زنانی که در فضای سایبر با انگیزهٔ دوستی، ارتباط، گفت‌وگو یا حتی بیان مشکلات شخصی حضور پیدا می‌کنند، در چشم برخی مرتکبان به‌مثابهٔ «دعوت‌نامه‌ای برای ارتکاب جرم جنسی» تلقی می‌شوند و همین امر احتمال بزه‌دیدگی آنان را افزایش می‌دهد. در این دسته از جرائم که غالباً حول محور جنسیت و محتوای هرزه‌نگارانه شکل می‌گیرند، بزهکار فردی است که تحت تأثیر تمایلات غریزی و با اتکا به خلوت و آزادی عمل در فضای سایبری مرتکب رفتار مجرمانه می‌شود. در چنین مواردی، می‌توان از یک «گرایش کیفری تعدیل‌شده» سخن گفت؛ بدین معنا که ارتکاب جرم مرتبط با محتوا ازجمله هرزه‌نگاری زنان کمتر تحت تأثیر ارادهٔ آزاد قرار دارد و بیش از آنکه محصول تصمیم‌گیری عقلانی باشد، از شرایط اجتماعی، انگیزه‌های غریزی، خلأ نظارت و کنترل، محیط‌های بی‌قاعده ناشی می‌شود. بر این اساس، مرتکب در این حوزه لزوماً فردی سودمحور یا محاسبه‌گر نیست و ارادهٔ او غالباً تحت تأثیر عوامل درونی و بیرونی قرار می‌گیرد.

از منظر حقوقی و جرم‌شناسی، هرزه‌نگاری زنان در فضای مجازی شامل تولید، انتشار یا معاملهٔ محتوایی است که دارای مضمون نمایش اندام جنسی زنان یا نمایش صریح اعمال جنسی اعم از میان انسان‌ها یا میان انسان و حیوان از طریق سیستم‌های رایانه‌ای و مخابراتی باشد. این محتوا می‌تواند به‌صورت فردی یا جمعی تولید یا منتشر شود. رفتارهای مجرمانه مرتبط با هرزه‌نگاری که سابقه‌ای طولانی در جرائم سنتی نیز دارد، با پیشرفت فناوری‌های رایانه‌ای و اینترنت وارد حوزهٔ دیجیتال شده و به‌دلیل گستره وسیع انتشار، به‌صورتی بی‌سابقه گسترش یافته است. نمونه‌های آن را

می‌توان در وجود صندوق‌های پستی الکترونیک، وب‌سایت‌ها و کانال‌هایی مشاهده کرد که به تبلیغ، توزیع و فروش تصاویر یا فیلم‌های هرزه می‌پردازند و هر نوع محتوای جنسی مورد تقاضا را عرضه می‌کنند (همان: ۵۰).

بزه‌دیدگی در جرم هرزه‌نگاری تنها محدود به زنی که تصویر او منتشر می‌شود نیست، بلکه جامعه به‌ویژه سایر زنان نیز به‌عنوان بزه‌دیدگان ثانویه آسیب می‌بینند. هرچند ممکن است در نگاه نخست، زنِ نمایش‌داده‌شده در محتوای هرزه بیش از دیگران آسیب‌پذیر به‌نظر برسد، اما تأثیر این تصاویر بر نگرش عمومی نسبت به زنان و روابط جنسی نیز بسیار عمیق و گسترده است. بسیاری از پژوهشگران، تبلیغ آزادانهٔ روسپی‌گری و محتوای هرزه در شبکه‌های ماهواره‌ای و اینترنتی را از مهم‌ترین عوامل نقض حقوق جنسی زنان می‌دانند؛ زنانی که نه تمایلی به مشاهده یا اجرای چنین محتوایی دارند و نه فشار شریک جنسی را می‌پذیرند. تحقیر شخصیت زن در فیلم‌های مبتذل، نمایش آمادگی روسپیان برای اعمال تحقیرآمیز، استفادهٔ ابزاری از مانکن‌ها برای تبلیغات با تأکید بر بدن زن، عادی‌سازی روابط جنسی خشونت‌آمیز و گروهی که همگی مصداق بارز خشونت علیه زنان هستند، نمونه‌هایی روشن از آموزش اجتماعی خشونت جنسی به‌شمار می‌روند. این روند نه‌تنها در رسانه‌های ماهواره‌ای و اینترنتی، بلکه در بسیاری از شبکه‌های تلویزیونی و مطبوعات جهانی نیز مشاهده می‌شود (السان، ۱۳۸۴: ۱۵۰). درمجموع، رسانه‌ها از دو مسیر خاص، به افزایش خشونت جنسی علیه زنان دامن می‌زنند. نخست، تبدیل زن به کالا از طریق استفادهٔ تبلیغاتی از زیبایی زنان در پیام‌های تجاری و نمایش روابط خصوصی جنسی به‌عنوان صحنه‌ای طبیعی در فیلم‌ها، تئاترها و مستندها. دوم، عادی جلوه دادن تعرض جنسی بدون وجود رابطهٔ قانونی میان طرفین (همان: ۱۵۱). ماهیت اینترنت به‌عنوان رسانه‌ای تأثیرگذار، امکان بروز مجموعه‌ای از رفتارهای صحیح و ناصحیح را فراهم کرده است. این فضا به‌دلیل ویژگی‌های خاص خود که پیش‌تر نیز اشاره شد هم فرصت مشارکت اجتماعی، توانمندسازی و حضور برابر زنان در جامعهٔ اطلاعاتی را فراهم می‌کند و هم بستری تهدیدآمیز برای خشونت جنسی و بزه‌دیدگی آنان ایجاد می‌کند. مهم‌ترین نمود این بزه‌دیدگی، گسترش هرزه‌نگاری زنان در فضای مجازی است که امروز به یکی از چالش‌های جدی سیاست جنایی و سلامت روانی زنان تبدیل شده است.

٦ـ۲. تحلیل ماده‌محور و شکاف حمایتی در انتشار محتوای خصوصی

در حقوق کیفری ایران، مادهٔ ۷۴۵ قانون مجازات اسلامی (تعزیرات) که متناظر با مادهٔ ۱۷ قانون جرائم رایانه‌ای مصوب ۱۳۸۸ است، انتشار، توزیع یا در دسترس قرار دادن صوت، تصویر یا فیلم خصوصی یا خانوادگی دیگری یا اسرار او را، بدون رضایت وی، در صورتی که موجب ضرر یا عرفاً موجب هتک حیثیت شود، جرم‌انگاری کرده است. اهمیت این حکم در آن است که حریم خصوصی و حیثیت را در محیط دیجیتال مورد حمایت قرار می‌دهد؛ با این حال، تحلیل سیاستی نشان می‌دهد که حمایت کیفری موجود لزوماً تمام چرخهٔ خشونت را پوشش نمی‌دهد.

نخست، در بسیاری از موارد، آسیب از «تهدید به انتشار» آغاز می‌شود و پیش از تحقق انتشار، آثار روانی و محدودکنندهٔ آن بر قربانی ایجاد می‌گردد. دوم، پس از انتشار، بازنشر سریع و چندلایهٔ محتوا می‌تواند دامنهٔ زیان را افزایش دهد و کنترل قربانی بر تصویر یا اطلاعات شخصی خود را عملاً ازبین ببرد. سوم، در مواردی انتشار با اخاذی، تهدید، تعقیب و آزار مستمر همراه می‌شود و عنوان واحد انتشار محتوای خصوصی نمی‌تواند تمام ابعاد رفتار را توضیح دهد. از این منظر، خلأ سیاستی نه لزوماً فقدان جرم‌انگاری، بلکه فقدان یک زنجیرهٔ منسجم از جرم‌انگاری، توقف فوری انتشار، حمایت از قربانی و جبران آثار زیان است.

پیشنهاد تقنینی مقاله در این بخش، ایجاد سازوکار صریح و سریع برای دستور موقت حذف یا توقف دسترسی به محتوای خصوصی زیان‌بار، پیش‌بینی تدابیر حمایتی برای جلوگیری از تماس و تهدید مجدد مرتکب با بزه‌دیده، و تقویت امکان مطالبهٔ خسارت مادی و معنوی است. چنین اصلاحی باید با تضمین‌های دادرسی و اصل تناسب همراه باشد تا میان حمایت از حریم خصوصی و سایر حقوق بنیادین تعادل برقرار شود.

٦ـ۳. قاچاق سایبری زنان و بهره‌کشی جنسی

با وجود لغو رسمی برده‌داری در قرن‌های هجدهم و نوزدهم، پدیدهٔ برده‌داری در دو قرن اخیر به شکل نوینی تحت عنوان قاچاق انسان ظاهر شده است. امروزه بهره‌کشی و سوءاستفاده از افراد، به‌ویژه زنان و کودکان، نه‌تنها کاهش نیافته، بلکه در قالب قاچاق انسان گسترده‌تر و پیچیده‌تر شده و جغرافیای آن فراتر از گذشته است. در گذشته، برده‌فروشان عمدتاً نیروی کار بردگان را هدف قرار می‌دادند، اما در حال حاضر، استفاده از اعضا و بدن افراد نیز مورد توجه قاچاقچیان قرار گرفته است؛

به همین دلیل، این پدیده را می‌توان شکل مدرن برده‌داری دانست (حبیب‌زاده و مکاران، ۱۳۸۸: ۱۰۱). فضای مجازی ابزارهای نوینی را در اختیار شبکه‌های قاچاق انسان قرار داده است. امروزه مراحل «شناسایی»، «جذب» و «فریب» قربانیان از طریق پلتفرم‌های دیجیتال و با وعده‌های دروغین (مانند مدلینگ، استخدام یا مهاجرت) صورت می‌گیرد. این پدیده که تحت عنوان «قاچاق سایبری» شناخته می‌شود، مشمول «قانون مبارزه با قاچاق انسان مصوب ۱۳۸۳» است. هرچند قانون مذکور در مادهٔ ۱، قاچاق انسان را شامل عبور دادن فرد از مرز با اجبار یا فریب تعریف کرده است، اما چالش اصلی در اثبات نقش واسطه‌های دیجیتال است. شبکه‌های سازمان‌یافته با استفاده از رمزارزها و بسترهای رمزنگاری‌شده، ردپای مالی و ارتباطی خود را پنهان می‌کنند. در این بستر، زنان قربانی اغلب در چرخه‌ای از بهره‌کشی جنسی[1] گرفتار می‌شوند که فراتر از مرزهای جغرافیایی است و مقابله با آن نیازمند همکاری‌های قضائی بین‌المللی است. قاچاق زنان و دختران توسط شبکه‌های بین‌المللی، از نقاط مختلف جهان، ابعاد گسترده‌ای یافته است. قاچاقچیان با وعدهٔ شغل مناسب و درآمد بالا، زنان و دختران جویای کار را فریب می‌دهند و همانند بردگان دوران گذشته، آن‌ها را در کشتی‌ها و مکان‌های مخفی پنهان می‌کنند تا به کشورهای مقصد منتقل شوند. بسیاری از این مهاجران غیرقانونی در مسیر خود به دست باندهای مافیایی می‌افتند و سرانجام به مراکز فساد و استثمار کشیده می‌شوند. سود سرشار حاصل از قاچاق زنان و دختران، این پدیده را به یک فاجعهٔ جهانی تبدیل کرده است (اشتری، ۱۳۸۵: ۲۸). به‌دلیل اهمیت این موضوع، ابتدا به تعریف کلی قاچاق می‌پردازیم و سپس جنبه‌های مختلف قاچاق زنان را بررسی خواهیم کرد. در ادامه، نقش اینترنت و فضای مجازی در گسترش این نوع جرم و تأثیر آن بر بزه‌دیدگی زنان مورد بحث قرار می‌گیرد. لغت «قاچاق» از واژهٔ ترکی «قاماق» گرفته شده و به معنای گریز، فرار یا ترک وطن است (حبیب‌زاده و مکاران، ۱۳۸۸: ۱۰۳). به‌طور کلی، قاچاق عبارت است از انتقال پنهانی یک شیء یا انسان از مکانی به مکان دیگر، به گونه‌ای که با استفاده از روش‌های مختلف پنهان‌سازی انجام می‌شود. بسته به نوع مورد انتقال، می‌توان از قاچاق مواد مخدر، انسان، سلاح، مواد هسته‌ای یا اعضای بدن سخن گفت، اما در همهٔ این موارد، اصل انتقال غیرقانونی پنهانی، عنصر مشترک است (معظمی، ۱۳۸۴: ۹۶).

---

1. sexual exploitation

درخصوص قاچاق انسان، دو مفهوم بین‌المللی وجود دارد که هنوز به‌طور دقیق و متمایز به فارسی ترجمه نشده‌اند: «Trafficking» و«Smuggling». به‌طور ساده، «Smuggling» به انتقال غیرقانونی مهاجران با هدف منافع مالی اشاره دارد، در حالی که «Trafficking» شامل انتقال انسان‌ها به منظور نگهداری تحت شرایط شبیه بردگی یا بهره‌کشی جنسی است. به عبارت دیگر، در «Trafficking»افراد به زور یا فریب، به‌ویژه زنان و کودکان، برای اهداف سودآور قاچاق می‌شوند، در حالی که در «Smuggling» گروه‌های مجرمان، مهاجران داوطلب را صرفاً به مقصد می‌رسانند و پس از رسیدن به مقصد نیز ممکن است استثمار شوند (همان: ۱۰۲). مسئلهٔ قاچاق انسان معمولاً در قالب عناوینی مانند قاچاق زنان، قاچاق زنان و کودکان یا قاچاق برای اهداف بهره‌کشی جنسی مطرح می‌شود، زیرا زنان و کودکان به‌دلیل آسیب‌پذیری، بیشترین قربانیان این پدیده هستند. درمجموع، قاچاق انسان عبارت است از انتقال انسان با استفاده از اغفال، اجبار، تهدید یا روش‌های مشابه، به‌منظور بهره‌کشی، به‌ویژه بهره‌کشی جنسی (حبیب‌زاده و مکاران، ۱۳۸۸: ۱۰۴). مسئلهٔ قاچاق زنان در ادبیات حقوق بین‌الملل، با وجود پیشینهٔ طولانی آن، در سدهٔ اخیر با تعاریف دقیق‌تر و هنجاری‌تری از سوی نهادهای جهانی همراه شده است. نخستین تعریف رسمی، در سال ۱۹۹۴ از سوی مجمع عمومی سازمان ملل ارائه شد. در این تعریف، قاچاق زنان به‌عنوان انتقال پنهانی و غیرقانونی افراد از مرزهای ملی ـ عمدتاً از کشورهای در حال توسعه یا اقتصادهای در حال گذار ـ با هدف واداشتن زنان و دختران به شرایط استثمار جنسی یا اقتصادی و کسب سود برای قاچاقچیان و شبکه‌های جنایت‌ساز معرفی شده است. این تعریف همچنین مواردی همچون کار اجباری خانگی، ازدواج صوری، استخدام پنهانی و فرزندخواندگی ساختگی را نیز در زمرهٔ مصادیق مرتبط با قاچاق قرار داده است (اشتری، ۱۳۸۵: ۱۷). گام بعدی در تبیین استانداردهای جهانی، «پروتکل پیشگیری، سرکوب و مجازات قاچاق اشخاص به‌ویژه زنان و کودکان» کنوانسیون پالرمو[1] (United Nations, 2000) بود. مادهٔ ۳ این پروتکل، تعریف جامع‌تری ارائه می‌دهد و قاچاق را شامل استخدام، جابه‌جایی، انتقال، پناه دادن یا دریافت افراد از طریق تهدید، استفاده از زور، انواع اجبار، ربایش، تقلب، فریب، سوءاستفاده از ضعف یا آسیب‌پذیری، یا پرداخت و دریافت منافع جهت کسب رضایت شخصی می‌داند که کنترل فرد دیگری را در اختیار دارد. این اقدامات زمانی در قالب قاچاق قرار می‌گیرند که

1 . United Nations Convention against Transnational Organized Crime (Palermo Convention)

هدف آن‌ها بهره‌کشی باشد. بهره‌کشی نیز طیفی از رفتارها را شامل می‌شود: بهره‌کشی جنسی، روسپی‌گری اجباری، کار یا خدمت اجباری، بردگی یا شیوه‌های مشابه آن، بیگاری و برداشت اعضای بدن (اشتری، ۱۳۸۵: ۱۸).

بررسی تاریخی نشان می‌دهد که قاچاق زنان، از دوران برده‌داری تا امروز، پیامدهای عمیق و جبران‌ناپذیری بر زنان و ساختار اجتماعی بر جای گذاشته است. این پدیده غالباً زمینه‌ساز جرائم دیگری مانند روسپی‌گری اجباری، خشونت جنسی و گردشگری جنسی می‌شود. یکی از ریشه‌های اصلی آسیب‌پذیری زنان در برابر شبکه‌های قاچاق، «زنانه شدن فقر» است. در شرایطی که ۷۰ درصد جمعیت ۳/۱ میلیارد نفری فقیر جهان را زنان و کودکان تشکیل می‌دهند، نابرابری در دسترسی به آموزش رسمی و فرصت‌های شغلی، بسیاری از زنان را ناگزیر یا فریب‌خورده به سوی باندهای قاچاق سوق می‌دهد (السان، ۱۳۸۴: ۳۴۴). در عصر حاضر، قاچاق زنان ابعاد پیچیده‌تری یافته است. با گسترش اینترنت و فضای سایبری، شبکه‌های سازمان‌یافتهٔ قاچاق به بستری تازه و کارآمد برای شناسایی، فریب و جذب قربانیان دست یافته‌اند. وعده‌هایی چون اشتغال مناسب، دریافت اقامت کشورهای اروپایی یا دسترسی به بورسیه‌های دانشگاهی، ابزارهای معمول برای شکار زنان و دختران‌اند. فناوری اطلاعات و ارتباطات، در کنار مزایای گسترده، امکان بهره‌برداری مجرمانه را نیز فراهم کرده و فضای مجازی را به یکی از مهم‌ترین عرصه‌های ارتکاب جرائم سازمان‌یافته، ازجمله قاچاق جنسی، تبدیل کرده است (زندی، ۱۳۸۹: ۱۶۵). قاچاق جنسی از مهم‌ترین مصادیق جرائم سازمان‌یافتهٔ فراملی است و دلیل اصلی سازمان‌یافتگی آن، سود اقتصادی بسیار کلان این بازار سیاه است. شبکه‌هایی که در این حوزه فعالیت می‌کنند، ساختاری چندلایه دارند و ممکن است صدها فرد در فرایندهای مختلف آن درگیر باشند: شناسایی و جذب طعمه، فریب یا تهدید، نگهداری، انتقال و درنهایت بهره‌کشی جنسی. این شبکه‌ها امکانات و تسهیلات لازم را برای کنترل و بهره‌برداری از قربانیان فراهم می‌کنند و گاه حتی به قربانی اجازهٔ کوچک‌ترین مقاومت یا فرار را نمی‌دهند (السان، ۱۳۸۴: ۳۳۴). اگرچه قاچاق زنان سابقه‌ای طولانی پیش از ظهور اینترنت دارد، اما فضای سایبری امکان‌های تازه‌ای برای دسترسی، اغفال، ناشناس ماندن و مدیریت شبکه‌ای فراهم کرده که فعالیت قاچاقچیان را بسیار تسهیل کرده است. آنان از ابزارهای دیجیتال برای برقراری ارتباط، فریب، انتقال اطلاعات و حتی فروش قربانیان بهره می‌برند (راودراد، ۱۳۸۴: ۷۶). هر ساله هزاران زن و دختر در سراسر جهان به صورت قاچاق، از وطن خود به مقاصدی غیرقانونی منتقل می‌شوند که عمدتاً برای

بهره‌کشی جنسی و اقتصادی مورد استفاده قرار می‌گیرند. بررسی‌ها نشان می‌دهد که بیش از ۲۰۰ میلیون نفر در جهان تحت کنترل یا سلطهٔ شبکه‌های قاچاق انسان هستند. در سال ۲۰۰۰، ایالات متحده قانونی را تصویب کرد که به قاچاق انسان نگاه فراملی داشت و آمارها نشان می‌دادند حدود ۷۰۰ هزار زن و کودک به‌طور سالانه قاچاق می‌شوند که از این تعداد نزدیک به ۵۰ هزار نفر به آمریکا منتقل می‌شوند. بیشتر این افراد با فریب، تهدید یا اجبار وارد چرخهٔ بهره‌کشی می‌شوند و در معرض فحشا، انتشار تصاویر مستهجن و سایر خدمات جنسی قرار می‌گیرند. اما قاچاق انسان تنها به صنعت سکس محدود نمی‌شود، بلکه شامل کار اجباری و نقض آشکار معیارهای حقوق بشر، سلامت عمومی و قوانین کار در سطح جهانی نیز می‌گردد. شبکه‌های قاچاق با سوءاستفاده از وضعیت‌های نابسامان زنان مانند فقر، محرومیت از آموزش، بیکاری، تبعیض و محدودیت فرصت‌های اقتصادی در کشور مبدأ آن‌ها را با وعده‌های دروغین استخدام در مشاغلی مانند پرستاری، خدمتکاری، کار در کارخانه، رستوران یا فروشندگی فریب می‌دهند (معظمی، ۱۳۸۴: ۱۰۱). ساده‌ترین دلیل رشد قاچاق زنان در سال‌های اخیر، سودآوری بالای این فعالیت است. قاچاقچیان با اطلاع از اینکه بهره‌برداری مکرر از یک فرد قاچاق‌شده سود قابل توجهی دارد و احتمال تعقیب آنان کم است، انگیزهٔ بالایی برای ادامهٔ فعالیت دارند (اشتری، ۱۳۸۵: ۲۳۸). طبق گزارش سازمان بین‌المللی مهاجرت، سالانه قاچاق زنان و دختران حدود ۸ میلیارد دلار درآمد ایجاد می‌کند. سود سرشار این تجارت موجب شده شبکه‌های فعال در قاچاق مواد مخدر و اسلحه نیز وارد این عرصه شوند، زیرا برخلاف مواد مخدر و اسلحه که تنها یک بار فروخته می‌شوند، افراد قاچاق‌شده را می‌توان چندین بار بهره‌برداری کرد (حبیب‌زاده و مکاران، ۱۳۸۸: ۱۰۲). فضای مجازی و اینترنت نیز شرایط جدیدی برای فعالیت قاچاقچیان فراهم کرده است. امنیت ناکافی فناوری‌های ارتباطی و امکان پنهان ماندن هویت کاربران، فرصت مناسبی برای سوءاستفاده و جذب قربانیان ایجاد می‌کند (باستانی، ۱۳۸۳: ۵۸). قاچاقچیان از طریق اتاق‌های گفت‌وگو، وب‌سایت‌ها و شبکه‌های اجتماعی مانند فیسبوک و یاهو، با زنان آشنا می‌شوند و پس از مدتی مذاکره و ارائهٔ وعده‌های پوشالی، آنان را به مسیر قاچاق و بهره‌کشی هدایت می‌کنند. بزه‌دیدگی زنان در این زمینه ابعاد گسترده و پیامدهای زیان‌بار دارد. زنان به‌دلیل تبعیض‌های جنسیتی و ضعف نسبی جسمی، آسیب‌پذیرتر از مردان هستند و قربانی قاچاق انسان به‌ویژه برای بهره‌کشی جنسی می‌شوند (حبیب‌زاده و مکاران، ۱۳۸۸: ۱۱۲). آنان از جنبه‌های جسمی، روحی و مالی بزه‌دیده می‌شوند، شامل خشونت جسمی مانند تجاوز، بیگاری، ضرب و

جرح، احساس پوچی و رهاشدگی، سوءاستفادهٔ مالی توسط وعده‌های پوشالی و درنهایت طرد اجتماعی یا گوشه‌گیری از سوی خانواده و جامعه.

٤-٦- آزار و اذیت اینترنتی زنان[1]

مزاحمت اینترنتی هنوز تعریف واحد و دقیقی ندارد، اما معمولاً به هرگونه استفاده از اینترنت، ایمیل یا ابزارهای ارتباطی الکترونیک برای ایجاد اذیت و آزار دیگران اشاره دارد. این نوع مزاحمت شامل رفتارهای مکرر تهدیدآمیز یا آزاردهنده است که یک فرد علیه فرد دیگر اعمال می‌کند. اگرچه شکل‌های مختلفی از آزار و تهدید کامپیوتری وجود دارد، مزاحمت اینترنتی از نظر ماهیت شباهت زیادی با مزاحمت در دنیای واقعی دارد؛ بسیاری از مزاحمان اینترنتی همانند مزاحمان سنتی قصد کنترل قربانیان خود را دارند و رفتارهای مشابهی بروز می‌دهند. شواهد گزارش‌شده در سال ۱۹۹۹ توسط دادستانی کل آمریکا نشان می‌دهد که اغلب مزاحمان اینترنتی مرد و قربانیان عمدتاً زنان هستند (راودراد، ۱۳۸۴: ۷۸).

مزاحمت در فضای مجازی، برخلاف مزاحمت فیزیکی، نیازمند تماس مستقیم با قربانی نیست، اما همچنان می‌تواند باعث ایجاد ترس، اضطراب و آسیب روانی در قربانی اغلب زنان شود. از این رو، می‌توان استدلال کرد که یافته‌های مرتبط با آزارهای دنیای واقعی تا حد زیادی قابل تعمیم به جرائم اینترنتی هستند (زررخ، ۱۳۸۹: ۱۳۳).

جرم آزار و اذیت اینترنتی عمدتاً علیه زنان رخ می‌دهد و در این گونه جرائم، زن نقش قربانی را ایفا می‌کند. مطالعات نشان می‌دهد که تقریباً ۹۰ درصد این نوع آزارها توسط مردان نسبت به زنان انجام می‌شود. چنین رفتارهایی فضایی مملو از اضطراب، ترس، تردید و فشارهای روانی و روحی برای زنان فعال در محیط اینترنت ایجاد می‌کند (راودراد، ۱۳۸۴: ۸۹). با گسترش اینترنت در زندگی روزمره و حرفه‌ای افراد، مزاحمان می‌توانند از سهولت دسترسی به اطلاعات شخصی و قابلیت ارسال پیام‌های یک‌طرفه و ناشناس بهره‌برداری کنند. این ویژگی‌ها سبب می‌شود موانع مواجههٔ مستقیم با قربانی کاهش یافته و احتمال اعمال مزاحمت افزایش یابد. درواقع، مزاحمان ممکن است در مواجههٔ حضوری یا تلفنی با قربانی دچار تردید شوند، اما در فضای مجازی ارسال پیام‌های تهدیدآمیز و آزاردهنده برای آن‌ها آسان‌تر است. این نوع آزار می‌تواند مشابه مزاحمت فیزیکی، مقدمه‌ای برای

1. online harrasment

رفتارهای خشونت‌آمیزتر باشد (همان: ۷۸). روش‌های اعمال مزاحمت اینترنتی نسبت به زنان متفاوت و متنوع است. برخی مزاحمان با نفوذ به کامپیوتر یا اینترنت قربانی، وی را مجبور به مشاهده یا توزیع محتوای پورنوگرافی می‌کنند، یا با افشای اطلاعات شخصی او و انتشار پیام‌های تحریک‌آمیز در سایت‌ها و اتاق‌های گفت‌وگو، دیگران را نیز به آزار قربانی تشویق می‌کنند (باستانی، ۱۳۸۳: ۵۰). مزاحمان پیشرفته می‌توانند با استفاده از نرم‌افزارهای اتوماتیک، پیام‌های تهدیدآمیز و آزاردهنده را به صورت منظم یا نامنظم ارسال کنند، بدون اینکه شخصاً هر بار پشت کامپیوتر حضور داشته باشند. این قابلیت، شناسایی و مقابله با مزاحمت را برای قربانی دشوار می‌کند (راودراد، ۱۳۸۴: ۷۹). مزاحمت‌های اینترنتی گاهی به صورت افترا نیز بروز می‌کنند. افترا، فارغ از شکل کلاسیک آن که معمولاً شامل انتشار اسناد یا اظهارات نادرست در جمع یا رسانه‌هاست، می‌تواند در فضای دیجیتال نیز رخ دهد. در این حالت، افترا ممکن است از طریق ایمیل، فایل‌های الکترونیک یا سایر ابزارهای برخط منتشر شود. برای مثال، ارسال مطالب توهین‌آمیز یا فحاشی از طریق ایمیل، یا انتشار محتوایی که می‌تواند افراد را ناراحت کند یا اعتبارشان را خدشه‌دار سازد، در قالب مزاحمت اینترنتی قابل پیگرد است. حتی ارسال پیام‌های ناخواسته یا اسپم نیز در این دسته قرار می‌گیرد. نکتهٔ مهم آن است که برای تحقق جرم مزاحمت اینترنتی، لزوماً محتوای منفی یا زیان‌آور بودن پیام ضروری نیست؛ کافی است دریافت‌کننده بدون رضایت مورد آزار قرار گیرد (دزیانی، ۱۳۸۴: ۵۸).

مزاحمت‌های اینترنتی را می‌توان به دو نوع کلی تقسیم کرد:

۱. مزاحمتی که صرفاً در فضای مجازی رخ می‌دهد و در همان محیط ادامه می‌یابد.

۲. مزاحمتی که از فضای مجازی آغاز می‌شود و به زندگی واقعی قربانی سرایت می‌کند، برای مثال زمانی که مزاحم تلاش می‌کند اطلاعاتی مانند شماره تلفن یا آدرس منزل قربانی را به‌دست آورد (راودراد، ۱۳۸۴: ۸۱).

انواع مزاحمان اینترنتی نیز متفاوت است و شامل موارد زیر می‌شود:

۱. مزاحم معمولی یا عاشق بی‌خطر: این فرد معتقد است رابطه‌اش با قربانی قطع شده و اغلب با یک علاقه‌مند ساده اشتباه گرفته می‌شود.

۲. مزاحم روان‌پریش اینترنتی: این فرد تصور غلطی دارد که قربانی او را دوست دارد، حتی اگر هیچ‌گاه او را ندیده باشد. این مزاحمان اغلب افراد منزوی‌اند و قربانیان خود را معمولاً از میان زنان متأهل یا فعالان اجتماعی مانند معلمان انتخاب می‌کنند. مقابله با این نوع مزاحمت دشوار است.

۳. مزاحم انتقام‌جو: این نوع فرد به دلایلی واقعی یا خیالی عصبانی است و قصد انتقام‌گیری از قربانی را دارد، برای مثال، برخی کارکنان اخراج‌شده ممکن است خود را قربانی بدانند و بخواهند از کارفرما یا افراد مرتبط انتقام بگیرند. درمورد زنان، این مزاحمت ممکن است از سوی همسران پیشین نیز صورت گیرد (همان: ۸۱).

پژوهش‌ها نشان می‌دهد افرادی که در فضای مجازی دست به آزار دیگران می‌زنند، انگیزه‌های گوناگونی دارند؛ انگیزه‌هایی که گاه در زندگی واقعی نیز ریشه دارند و در محیط برخط فقط شکل تازه‌ای به خود می‌گیرند. در مقالهٔ «مسائل اجتماعی زنان در اینترنت» نوشتهٔ اعظم راودراد (همان: ۸۲)، چهار دسته از این انگیزه‌ها توضیح داده شده است:

۱. انگیزه‌های جنسی

این نوع آزار، در فضای دیجیتال پدیده‌ای دور از انتظار نیست؛ همان‌طور که در روابط روزمره نیز بارها مشاهده می‌شود. پنهان بودن هویت در اینترنت، راه را برای کسانی که قصد سوءاستفاده دارند هموار می‌کند و احساس مصونیت در آنان ایجاد می‌کند. بنابراین فرد مزاحم بدون ترس از شناخته شدن، می‌تواند رفتارهای جنسی ناخواسته را نسبت به زنان تکرار کند.

۲. دلبستگی‌های افراطی و روابطِ از کنترل‌خارج‌شده

گاه مزاحمت از دل یک ارتباط عاطفی برخط آغاز می‌شود. ممکن است یکی از طرفین بخواهد رابطه را پایان دهد، اما دیگری نتواند این تصمیم را بپذیرد. چالش اصلی این‌گونه مزاحمت‌ها آن است که رابطه معمولاً با اعتماد آغاز شده و اطلاعات شخصی بسیاری میان طرفین مبادله شده است. همین اطلاعات، پس از قطع رابطه، ابزار آزاردهی در دست فرد متعصب می‌شود. تهدیدهای مکرر، ارسال پیام‌های آزارنده یا حتی پیام‌های حاوی تهدید به مرگ، معمولاً از همین نقطه شکل می‌گیرد.

۳. انتقام‌جویی یا بروز خشم و کینه

در مواردی، فرد مزاحم به‌سبب سخنی، نقدی یا اختلافی در فضای مجازی تصمیم به انتقام می‌گیرد. گاهی حتی هیچ ارتباط قبلی میان مزاحم و قربانی وجود ندارد و فرد تنها برای تخلیهٔ خشم خود، شخصی را به‌طور تصادفی انتخاب می‌کند. در چنین وضعی، قربانی تنها به‌دلیل «در مسیر بودن» هدف قرار می‌گیرد و بار خشم بی‌دلیل یک فرد ناشناس را تحمل می‌کند.

۳. نمایش قدرت و خودنمایی دیجیتال

دسته‌ای از مزاحمان نه به دنبال انتقام‌اند و نه مسئله‌ای شخصی با قربانی دارند؛ آنان صرفاً می‌خواهند توانایی خود در دستکاری، نفوذ یا آزار دیگران را به رخ بکشند. این رفتار نوعی «قدرت‌نمایی کودکانه» در محیط اینترنت است؛ جایی که فرد با کمترین امکانات می‌تواند حس توانمندی کاذب پیدا کند.

افرادی که پیام‌های تهدیدآمیز دریافت می‌کنند اغلب تصور می‌کنند مزاحم فردی خطرناک یا حرفه‌ای است، در حالی که در بسیاری موارد، مزاحم حتی توان انجام کمترین آسیب واقعی را هم ندارد.

همچنین گسترش فناوری‌های ارتباطی، دسترسی افراد به یکدیگر را بدون سختی فراهم کرده است. کافی است مزاحم یک رایانه، یک اتصال ساده و حداقل دانش فنی داشته باشد تا بتواند فرد موردنظر را آزار دهد. سرعت ارتباطات مجازی باعث می‌شود حتی فردی در فاصله‌ای بسیار دور بتواند در چند لحظه موجی از اذیت و تهدید را روانهٔ قربانی کند (نوروزی و افراخته، ۱٤۰۰: ۲۷۰).

پنهان ماندن هویت نیز به‌خودیِ خود نوعی آزار روانی ایجاد می‌کند. در دنیای واقعی، قربانی می‌داند چه کسی آزارش داده و احتمال پیگیری حقوقی وجود دارد، اما در اینترنت، مزاحم می‌تواند با تغییر سرویس‌دهنده، ساختن حساب‌های متعدد و استفاده از نام‌های گوناگون، خود را پشت پرده‌ای از ناشناسی پنهان کند. این وضعیت، احساس بی‌پناهی و آسیب‌پذیری مضاعفی برای قربانی ایجاد می‌کند. ناشناس ماندن، مزاحم را در یک موقعیت برتر قرار می‌دهد. وی در حالی که برای هدف قربانی غیر قابل شناسایی است، می‌تواند در مکانی دیگر، یا همان اطراف یا در اتاق مجاور در محل کار باشد. ناتوانی قربانی در شناسایی مهاجم و ناشناس ماندن وی ممکن است مزاحم را به ادامهٔ این گونه اعمال تشویق کند. به علاوه برخی متهمان با اطمینان از ناشناس‌ماندنشان مکن است بیشتر بخواهند که قربانی را در محل کار و یا منزل تعقیب کنند و اینترنت اطلاعات جامعی را برای این هدف در اختیار آنان قرار خواهد داد.

٦ـ۵. تفکیک خشونت دیجیتال از عناوین مجرمانهٔ سنتی

یکی از نتایج تحلیلی این پژوهش آن است که «خشونت دیجیتال» یک عنوان مجرمانهٔ واحد نیست، بلکه مفهومی جرم‌شناختی و سیاستی برای توصیف مجموعه‌ای از رفتارهاست که ممکن است تحت عناوین کیفری متفاوت قرار گیرند. از این رو، نباید از نبود عنوان مستقل با عنوان «خشونت دیجیتال

علیه زنان» نتیجه گرفت که تمام رفتارهای مزبور فاقد پاسخ کیفری‌اند. در مقابل، وجود عناوین پراکنده نیز به‌تنهایی به معنای کفایت حمایت نیست. مسئلهٔ اصلی، میزان پوشش رفتاری، دسترسی قربانی به حمایت و توان نظام برای پاسخ سریع به رفتارهای ترکیبی است.

بر این اساس، مقاله میان سه وضعیت تمایز می‌گذارد: الف) رفتارهایی که عنوان کیفری نسبتاً روشن دارند؛ ب) رفتارهایی که از طریق ترکیب چند عنوان کیفری قابل تعقیب‌اند، اما حمایت فوری و متناسب برای آن‌ها پیش‌بینی نشده است؛ و ج) رفتارهای نوظهوری که در مرز میان آسیب اجتماعی، نقض حقوق مدنی و جرم قرار می‌گیرند و نیازمند ارزیابی دقیق اصل قانونی بودن جرم و مجازات پیش از جرم‌انگاری جدید هستند. این تفکیک از جرم‌انگاری شتاب‌زده جلوگیری می‌کند و اصلاح سیاست جنایی را به سمت پاسخ متناسب و مبتنی بر شواهد سوق می‌دهد.

۶-۶. خشونت نمادین و استانداردهای تحمیلی زیبایی

یکی از نوظهورترین اشکال خشونت دیجیتال علیه زنان، خشونت مبتنی بر «الگوسازی تحمیلی زیبایی» در فضای مجازی است. در این نوع خشونت، بدن طبیعی زنان به‌طور مستمر در معرض مقایسه با الگوهای غیرواقعی، دستکاری‌شده و تجاری‌سازی‌شده قرار می‌گیرد. شبکه‌های اجتماعی، به‌ویژه پلتفرم‌های تصویرمحور، با ترویج چهره‌ها و بدن‌های یکسان‌سازی‌شده، نوعی «بی‌ارزش‌سازی بدن طبیعی» را بازتولید می‌کنند که مستقیماً بر عزت‌نفس زنان تأثیر می‌گذارد. این پدیده که می‌توان آن را «خشونت زیبایی‌شناختی» نامید، زنان را تحت فشار روانی برای تغییر بدن خود از طریق جراحی‌های زیبایی قرار می‌دهد. فقدان نظارت قانونی بر تبلیغات پزشکی در فضای مجازی و فعالیت آزادانهٔ اینفلوئنسرهای غیرمتخصص، مصداقی از رهاشدگی فضای سایبر است که سلامت جسم و روان زنان را تهدید می‌کند. اگرچه این مورد صراحتاً در قوانین کیفری جرم‌انگاری نشده، اما ذیل بحث «مداخلهٔ غیرمجاز در امور پزشکی» و «آسیب به سلامت عمومی» قابل تحلیل است. در این فرایند، تبلیغ گستردهٔ جراحی‌های زیبایی، فیلرها، تزریق‌ها و مداخلات پزشکی زیبایی در بستر فضای مجازی آن هم بدون نظارت مؤثر حقوقی و پزشکی به شکل‌گیری نوعی اجبار پنهان اجتماعی منجر می‌شود؛ اجباری که زنان را به سوی تغییر بدن خود برای کسب پذیرش اجتماعی سوق می‌دهد. این سازوکار را می‌توان شکل خاصی از «خشونت نمادین» دانست؛ خشونتی که نه از طریق ضرب و جرح، بلکه از طریق تحقیر خاموش بدن زن و القای حس «ناکافی بودن» به او اعمال

می‌شود. پیامدهای این شکل از خشونت، در کاهش اعتماد به نفس، افزایش اختلالات اضطرابی، افسردگی، نارضایتی از بدن و گرایش به رفتارهای پرخطر روانی و جسمانی در میان زنان، به‌ویژه دختران جوان، کاملاً مشهود است.

۷. رویکرد سازمان بهداشت جهانی،چالش‌ها و راهبردهای سیاست جنایی نوین

۷ـ۱. رویکرد سازمان بهداشت جهانی و چالش‌های سیاست جنایی ایران

برای درک دقیق شکاف موجود میان استانداردهای جهانی و وضعیت کنونی سیاست جنایی داخلی ضروری است که مبانی نظری و عملیاتی هر دو حوزه مورد واکاوی تطبیقی قرار گیرد. سازمان بهداشت جهانی با رویکردی کل‌نگر خشونت دیجیتال را فراتر از جرم رایانه‌ای صرف و به‌عنوان بخشی از خشونت مبتنی بر جنسیت و بحران سلامت عمومی می‌نگرد که نیازمند مداخله‌های چندوجهی است. درمقابل، سیاست جنایی ایران با تکیه بر مبانی سنتی و قوانین موضوعه عمدتاً بر جنبه‌های کیفری، مجازات‌محوری و حفظ اخلاق عمومی تمرکز دارد و کمتر به ابعاد روان‌شناختی و حمایتی بزه‌دیدگان توجه نشان داده است. در این بخش تلاش می‌شود با تحلیل اسناد بین‌المللی و قوانین داخلی تقابل این دو رویکرد در دو محور «مبانی پارادایمی» و «راهبردهای پیشگیری» تبیین شود تا چالش‌های ساختاری و کاستی‌های سیاست جنایی ایران در مواجهه با خشونت دیجیتال علیه زنان آشکار گردد.

۷ـ۲. پارادایم سلامت‌محور در برابر رویکرد امنیت‌مدار

۷ـ۲ـ۱. معیارهای عملیاتی همسویی با رویکرد سلامت‌محور

برای جلوگیری از استفادهٔ کلی و غیرعملیاتی از مفهوم «رویکرد سازمان بهداشت جهانی»، در این پژوهش همسویی با رویکرد سلامت‌محور براساس پنج معیار بررسی می‌شود: ۱. پیشگیری اولیه و کاهش عوامل خطر؛ ۲. دسترسی قربانیان به خدمات سلامت و سلامت روان؛ ۳. پاسخ چندبخشی و هماهنگ میان نهادهای قضائی، انتظامی، بهداشتی و اجتماعی؛ ۴. تولید داده‌های قابل تفکیک برای شناخت الگوی خشونت و ارزیابی سیاست؛ و ۵. توجه به پیامدهای کوتاه‌مدت و بلندمدت خشونت در طراحی مداخله. این معیارها مبنای مقایسهٔ ایران و رویکرد سلامت‌محور قرار می‌گیرند.

براساس این معیارها، شکاف ایران را باید «شکاف نهادی ـ سیاستی» دانست، نه صرفاً «شکاف تقنینی». قانون کیفری عمدتاً رفتار مرتکب را تعریف و مجازات می‌کند، در حالی که سیاست سلامت‌محور باید برای مسیر بزه‌دیده نیز پاسخ طراحی کند: گزارش امن، ارزیابی خطر، توقف یا کاهش مواجهه با محتوای زیان‌بار، ارجاع به خدمات سلامت روان، حمایت اجتماعی و پیگیری نتایج. بنابراین، اصلاح قانون بدون اصلاح سازوکارهای اجرایی و حمایتی، به‌تنهایی قادر به پر کردن شکاف شناسایی‌شده نیست.

سازمان بهداشت جهانی طی سال‌های اخیر خشونت دیجیتال را امتداد پیچیده‌تر و چندلایه‌تر خشونت مبتنی بر جنسیت دانسته و آن را تهدیدی مستقیم برای سلامت روان زنان معرفی کرده است (Arias & Pankhurst, 2021: 8). در اسناد کلیدی این سازمان، ازجمله

> طرح اقدام جهانی برای تقویت نقش نظام سلامت در مواجهه با خشونت علیه زنان تصریح شده است که خشونت در فضای برخط واجد همان پیامدهای روانی خشونت فیزیکی است، با این تفاوت که شدت و پایداری آسیب در محیط دیجیتال به‌دلیل ماندگاری محتوا و امکان بازنشر گسترده، عمق بیشتری می‌یابد در گزارش‌های پژوهشی WHO، این آسیب‌ها در سه سطح فوری، میان‌مدت و بلندمدت دسته‌بندی شده‌اند و اختلالاتی همچون اضطراب مزمن، افسردگی، آشفتگی هویتی، PTSD[1] به‌عنوان پیامدهای شایع خشونت دیجیتال ذکر شده‌اند (Lami, 2021:145).

سازمان بهداشت جهانی همچنین بر خطرات فزایندهٔ اعمال فشارهای زیبایی‌شناختی در فضای دیجیتال تأکید دارد و آن را یکی از اشکال خشونت ساختاری علیه زنان می‌داند. در حالی که در بسیاری از کشورها، تبلیغات مربوط به مداخلات زیبایی تحت نظارت سخت‌گیرانه قرار دارد، در ایران خلأ جدی در تنظیم‌گری تبلیغات جراحی‌ها و اقدامات زیبایی در بستر شبکه‌های اجتماعی مشاهده می‌شود؛ مسئله‌ای که سلامت روان و جسم زنان را در معرض تهدید مضاعف قرار می‌دهد. سازمان بهداشت جهانی به‌جای تکیه بر رویکرد کیفری، چارچوبی سلامت‌محور ارائه می‌دهد و دولت‌ها را مکلف می‌داند که برای قربانیان خدمات مشاوره‌ای، روان‌درمانی کوتاه‌مدت، غربال‌گری خطر و حمایت اجتماعی فراهم کنند. در این رویکرد تأکید می‌شود که نخستین پاسخ به خشونت دیجیتال باید از سوی نظام سلامت باشد، نه صرفاً نظام کیفری، زیرا ابعاد روانی آسیب، نقطهٔ آغاز مداخله است. این نگاه

---

۱. اختلال اضطراب یا استرس پس از سانحه

سلامت‌محور، شبکهٔ مداخله‌ای چندنهادی شامل وزارت بهداشت، بخش آموزش، پلیس سایبری و نهادهای اجتماعی را ضروری می‌سازد؛ شبکه‌ای که به‌گفتهٔ WHO، بدون آن امکان مدیریت آسیب‌های روانی زنان در محیط دیجیتال فراهم نمی‌شود (Henry & Pawll, 2018a: 69) .

در مقابل، سیاست جنایی ایران عمدتاً بر جرم‌انگاری و واکنش پسینی به رفتار مجرمانه متمرکز است. ساختارهای قانونی مرتبط، همچون قانون جرائم رایانه‌ای و مقررات پراکندهٔ کیفری، بیشتر بر رفتار مرتکب تمرکز دارند تا پیامدهای روانی قربانی (سلیمی قلعه‌ئی و همکاران، ۱٤۰۳: ۵-۷). در بررسی سیاست جنایی ایران مشاهده می‌شود که هدف اصلی، تأمین امنیت اخلاقی و حفظ حیثیت افراد است، نه حمایت فعال از سلامت روان زنان، همین امر موجب می‌شود پیامدهای روانی خشونت دیجیتال به‌عنوان عنصر فرعی و تبعی تلقی شوند (ارجمند و شریفی، ۱٤۰۳: ۱۰۹) این تفاوت در فلسفهٔ تقنینی، یکی از اصلی‌ترین شکاف‌ها میان ایران و استانداردهای ارائه‌شده از سوی سازمان بهداشت جهانی است (Woodlock, 2017: 584-602).

۷ـ۳. راهبردهای پیشگیری و مداخله در سیاست جنایی نوین

۷ـ۳ـ۱. مدل پیشنهادی سیاست جنایی چهارحلقه‌ای

بر مبنای یافته‌های تطبیقی، مدل پیشنهادی مقاله از چهار حلقهٔ مکمل تشکیل می‌شود. حلقهٔ نخست «پاسخ حقوقی» است که شامل جرم‌انگاری موجود، تعیین مسئولیت، ضمانت اجرا و تدابیر فوری برای توقف آسیب است. حلقهٔ دوم «پیشگیری» است که آموزش سواد دیجیتال، ارتقای آگاهی حقوقی، طراحی ایمن پلتفرم‌ها و مداخلات هدفمند برای گروه‌های در معرض خطر را دربرمی‌گیرد. حلقهٔ سوم «حمایت بزه‌دیده‌محور» است که دسترسی به خدمات سلامت روان، حمایت حقوقی، محرمانگی و جلوگیری از بزه‌دیدگی مجدد را محور قرار می‌دهد. حلقهٔ چهارم «حکمرانی داده و ارزیابی» است که ایجاد نظام ثبت و طبقه‌بندی داده، شاخص‌های عملکرد و ارزیابی دوره‌ای سیاست را ضروری می‌داند.

مزیت این مدل در آن است که هر حلقه قابل ارزیابی مستقل است، اما کارآمدی کل سیاست تابع ارتباط میان آن‌هاست. برای مثال، افزایش کشف جرم بدون افزایش دسترسی قربانیان به خدمات حمایتی ممکن است صرفاً ظرفیت سرکوب را بالا ببرد، نه اینکه آسیب روانی یا تکرار خشونت را

کاهش دهد. همچنین آموزش بدون سازوکار گزارش‌دهی و پاسخ سریع، اثر محدودی خواهد داشت. بنابراین، معیار نهایی موفقیت سیاست جنایی باید کاهش خطر، کاهش تکرار خشونت، افزایش دسترسی به حمایت و ارتقای امنیت روانی باشد؛ نه صرفاً افزایش تعداد پرونده‌های کیفری.

در سطح تقنینی، این مدل پیشنهاد می‌کند که در اصلاحات آتی، حمایت از قربانی در کنار حمایت از حیثیت و حریم خصوصی مورد تصریح قرار گیرد؛ برای تهدید و انتشار محتوای خصوصی سازوکارهای فوری و متناسب پیش‌بینی شود؛ دربارهٔ محتوای دستکاری‌شده و مصنوعی، با رعایت اصل قانونی بودن و اصل تناسب، خلأهای موجود شناسایی و در صورت احراز ضرورت تقنینی برطرف شود؛ و در سطح اجرایی، پروتکل مشترکی میان پلیس، مراجع قضائی، خدمات سلامت و نهادهای اجتماعی برای ارجاع و حمایت از بزه‌دیدگان تدوین شود.

جدول ٤: مقایسهٔ وضعیت غالب نظام کیفری ایران با الگوی سلامت‌محور و پیشنهادهای سیاستی

پیشنهاد سیاستی	الگوی سلامت محور	وضعیت غالب در نظام کیفری ایران	معیار ارزیابی
تکمیل پوشش رفتاری و تدابیر فوری	پاسخ متناسب و همراه با حمایت	جرم‌انگاری پراکندهٔ مصادیق	پاسخ کیفری
آموزش، سواد دیجیتال و کاهش عوامل خطر	پیشگیری اولیه و ثانویه	غلبهٔ واکنش پس از وقوع	پیشگیری
پروتکل ارجاع و حمایت روانی ـ حقوقی	خدمات سلامت و حمایت مستمر	تمرکز بیشتر بر رفتار مرتکب	حمایت بزه‌دیده
ثبت تفکیک‌شده بر حسب نوع خشونت و جنسیت	سیاست‌گذاری مبتنی بر شواهد	نبود دادهٔ تفصیلی و یکپارچه	داده و ارزیابی

در تحلیل تطبیقی، مشاهده می‌شود که WHO بر پیشگیری اولیه اتکا دارد؛ یعنی آموزش، سواد رسانه‌ای، آگاهی از امنیت دیجیتال و ایجاد محیط‌های برخط امن. در حالی که سیاست جنایی ایران در این سطح تقریباً فاقد برنامهٔ ملی یا سامانه آموزشی هدفمند دربارهٔ خشونت دیجیتال است

(ارجمند و شریفی، ۱۴۰۳: ۱۲۰). در سطح پیشگیری ثانویه نیز WHO بر ارزیابی خطر، مداخلهٔ روان‌شناختی و حمایت خانواده‌محور تأکید دارد، در حالی که ایران عمدتاً به واکنش پلیسی و قضائی تکیه می‌کند و از لحاظ حمایت روانی فاقد پروتکل‌های مدون ملی است (Citron, 2014: 12) . در پیشگیری ثالثیه نیز WHO مدل‌های توان‌افزایی روانی ـ اجتماعی را توصیه می‌کند تا قربانی بتواند تجربهٔ آسیب را مدیریت کند و بهزیستی روانی خود را بازیابد، اما در ایران چنین مدل‌هایی تنها به‌صورت موردی و محدود وجود دارد و با نظام کیفری نیز پیوند نهادینه ندارد (Henry & Powell, 2018b: 45).

تفاوت‌های دو رویکرد در حوزهٔ جرم‌انگاری نیز برجسته است. ایران بخشی از مصادیق خشونت دیجیتال مانند تهدید، نشر اکاذیب یا انتشار تصاویر خصوصی را جرم‌انگاری کرده، اما بسیاری از مصادیق نوظهور ازجمله deepfake[1] جنسیتی، مزاحمت دیجیتال مستمر[2] و حملات سایبری جنسیت‌محور هنوز فاقد عنوان مستقل یا سازوکار حمایتی ویژه هستند (زندی، ۱۴۰۲: ۲۲۲). درمقابل، WHO بر جرم‌انگاری خاص اصرار ندارد و بیشتر بر استانداردسازی قوانین در راستای حفظ سلامت روان و صیانت از کرامت زنان تأکید می‌کند؛ یعنی هدف نهایی باید کاهش آسیب باشد، نه صرفاً افزایش مجازات (Jane, 2017: 608-622). برآیند این ارزیابی نشان می‌دهد که ایران با وجود برخورد کیفری نسبتاً قوی، هنوز فاقد «سیاست سلامت‌محور» در حوزهٔ خشونت دیجیتال است. این فقدان موجب کاهش نرخ گزارش‌دهی، افزایش ترس از پیگیری قضائی، تعمیق آسیب‌های روان‌شناختی در میان زنان می‌شود (Flynn et al., 2020: 5656-5678). به بیان دیگر، راهبرد ایران در نقطهٔ «واکنش» مستقر است، در حالی که راهبرد WHO در نقطهٔ «پیشگیری و حمایت» توسعه یافته است. همین شکاف مفهومی، مهم‌ترین عامل عدم تناسب میان سیاست‌های کنونی و نیازهای واقعی قربانیان محسوب می‌شود (Lewis, 2017: 718-732).

در مسیر اصلاح، ایران نیازمند سیاستی تلفیقی است که میان پاسخ کیفری و مداخلهٔ سلامت‌محور پیوند برقرار کند. این چارچوب باید خشونت دیجیتال را به‌عنوان تهدید جدی سلامت عمومی زنان شناسایی کند و مداخله‌های آموزشی، روان‌شناختی و اجتماعی را در کنار برخورد کیفری قرار دهد. ایجاد مراکز خدمات روانی ویژهٔ قربانیان خشونت دیجیتال، طراحی پروتکل ملی مشاورهٔ روان‌شناختی، راه‌اندازی سامانهٔ ملی گزارش‌دهی محرمانه، همکاری نهادی میان وزارت

---

۱. جعل عمیق

2. stalking

بهداشت، پلیس فتا و قوهٔ قضائیه از نخستین گام‌های ضروری هستند (فتاحیان، ۱۳۹۶: ۳۱-۳۲). در کنار اصلاحات نهادی، بازنگری قانونی نیز ضرورت دارد؛ ازجمله تعریف قانونی «خشونت دیجیتال جنسیت‌محور»، جرم‌انگاری حملات مبتنی بر فناوری‌های نو مانند deepfake، تدوین نظام حمایتی مناسب برای زنان قربانی. هم‌زمان، سیاست پیشگیرانه باید بر آموزش امنیت دیجیتال، افزایش تاب‌آوری روانی، سواد رسانه‌ای و توانمندسازی زنان تمرکز کند، زیرا این عناصر در رویکرد WHO مؤلفه‌های اساسی برای کاهش آسیب روانی محسوب می‌شوند (Vickery & Everbach, 2018: 7; Mantilla, 2015: 28).

درنهایت، آنچه برای ایران ضرورت دارد، گذار از یک سیاست صرفاً کیفری به سمت سیاست یکپارچه‌ای است که سلامت روان، حمایت اجتماعی و امنیت دیجیتال را به ستون‌های اصلی مقابله با خشونت دیجیتال تبدیل کند؛ سیاستی که بتواند میان حقوق کیفری و نظام سلامت پلی پایدار بنا کند و پاسخ ملی را از واکنش منفعلانه به مداخلهٔ فعال، علمی و انسان‌محور تبدیل سازد (وطنی و اسدی، ۱۳۹۵: ۱۰۱).

۷ـ۴. پیشنهادهای اصلاحی مشخص و قابل تقنین

۷ـ۴ـ۱. پیشنهاد نخست: تعریف و طبقه‌بندی سیاستی خشونت دیجیتال

به‌جای جرم‌انگاری شتاب‌زده همهٔ رفتارهای دیجیتال، پیشنهاد می‌شود در یک سند سیاست جنایی یا قانون جامع، «خشونت دیجیتال مبتنی بر جنسیت» به‌عنوان یک مفهوم سیاستی تعریف و سپس مصادیق کیفری آن به‌صورت احصایی یا تمثیلی مشخص شود. این تعریف باید رفتارهایی مانند انتشار غیررضایی محتوای خصوصی، تهدید به انتشار، تعقیب و آزار مستمر، دستکاری محتوای جنسی/ تحقیرآمیز، اخاذی مبتنی بر دادهٔ خصوصی و برخی اشکال بهره‌کشی تسهیل‌شده با فناوری را از رفتارهای صرفاً نامطلوب اجتماعی تفکیک کند.

۷ـ۴ـ۲. پیشنهاد دوم: تکمیل حمایت از مادهٔ ۷۴۵

حمایت کیفری نباید فقط پس از تحقق انتشار و ورود ضرر فعال شود. در مواردی که تهدید جدی و قابل اثبات به انتشار محتوای خصوصی وجود دارد، امکان اتخاذ تدابیر حمایتی فوری باید پیش بینی شود. همچنین برای بازنشرهای زنجیره‌ای، سازوکارهای سریع حفظ ادله و درخواست توقف

دسترسی باید روشن باشد. این اصلاح می‌تواند از طریق قانون خاص یا دستورالعمل قضائی دقیق، بدون توسعهٔ نامتناسب قلمرو جرم‌انگاری انجام شود.

۷ـ٤ـ۳. پیشنهاد سوم: پاسخ اختصاصی به deepfake و محتوای مصنوعی

در مواردی که محتوای مصنوعی به‌صورت جنسی یا تحقیرآمیز به شخص منتسب می‌شود و با قصد آسیب به حیثیت یا اخاذی انتشار می‌یابد، باید رابطهٔ آن با مواد ۷۴۴ و ۷۴۵ روشن شود. در صورت ناکافی‌بودن تفسیر موجود، قانونگذار می‌تواند عنصر «ایجاد یا انتشار محتوای مصنوعی منتسب به شخص بدون رضایت و با قصد هتک حیثیت / اخاذی» را به‌صورت محدود و دقیق تنظیم کند. پیشنهاد مقاله، جرم‌انگاری عام «دیپ‌فیک» نیست، بلکه جرم‌انگاری رفتار زیان‌بار مشخص با رعایت اصل قانونی بودن جرائم و مجازات‌هاست.

۷ـ٤ـ٤. پیشنهاد چهارم: ایجاد پروتکل ارجاع سلامت روان

برای پرونده‌هایی که با تهدید جنسی، انتشار محتوای خصوصی یا تعقیب مستمر همراهند، پلیس و مرجع قضائی باید بتوانند با رضایت و حفظ محرمانگی، بزه‌دیده را به خدمات سلامت روان ارجاع دهند. این پروتکل باید شامل ارزیابی خطر، حمایت فوری، محرمانگی اطلاعات و منع افشای غیرضروری داده‌های حساس باشد. چنین اقدامی دقیقاً همان نقطه‌ای است که پاسخ کیفری را به پاسخ سلامت‌محور پیوند می‌دهد.

۷ـ٤ـ٥. پیشنهاد پنجم: سامانهٔ داده و شاخص ارزیابی سیاست

پیشنهاد می‌شود سالانه شاخصی با عنوان «شاخص پاسخ سیاست جنایی به خشونت دیجیتال علیه زنان» منتشر شود. این شاخص می‌تواند پنج مؤلفه داشته باشد: تعداد شکایت‌های تفکیک‌شده، زمان متوسط حفظ / حذف محتوای زیان‌بار، نرخ ارجاع به خدمات حمایتی، نتیجهٔ قضائی پرونده ها و میزان دسترسی بزه‌دیدگان به خدمات سلامت. این شاخص، سیاست جنایی را از سطح «وجود قانون» به سطح «نتیجهٔ قابل سنجش» منتقل می‌کند.

۸. بحث و یافته‌های نهایی

یافتهٔ نخست این است که نظام کیفری ایران فاقد ابزار قانونی برای مواجهه با خشونت دیجیتال نیست؛ مواد ۷۴۴ تا ۷۴۶ و مقررات پراکندهٔ دیگر ،ظرفیت واکنش به بخشی از رفتارها را فراهم کرده اند. بنابراین، تعبیر دقیق‌تر از وضعیت موجود، پوشش ناقص و غیریکپارچه است نه فقدان مطلق حمایت کیفری. یافتهٔ دوم آن است که فناوری، آسیب را به فراتر از عنصر مادی جرم منتقل کرده است: ماندگاری و بازتولید محتوا، ترس از افشای مجدد، فشار اجتماعی و اختلال در احساس امنیت می‌تواند حتی پس از توقف رفتار اولیه ادامه یابد. یافتهٔ سوم، که وجه نوآورانهٔ مقاله را تشکیل می‌دهد، این است که پاسخ مؤثر باید زنجیره‌ای باشد و چهار حلقهٔ حفاظت حقوقی، پیشگیری، سلامت و حکمرانی داده را به هم متصل کند.

یافتهٔ چهارم به داده‌های تجربی مربوط است. در وضعیت کنونی، داده‌های عمومی جرائم سایبری برای سنجش خشونت جنسیتی دیجیتال کافی نیستند. بنابراین، ادعای «افزایش» یا «شیوع گسترده» باید فقط در جایی به‌کار رود که مطالعهٔ معتبر یا آمار اختصاصی آن را پشتیبانی کند. این اصلاح، استحکام روش‌شناختی مقاله را افزایش می‌دهد و هم‌زمان نشان می‌دهد که فقدان دادهٔ تفکیک‌شده خود یکی از موانع سیاست‌گذاری مبتنی بر شواهد است.

نتیجه‌گیری

خشونت دیجیتال علیه زنان، در نقطهٔ تلاقی حقوق کیفری، فناوری، سلامت عمومی و سیاست اجتماعی قرار دارد. بررسی تطبیقی نشان داد که رویکرد سلامت‌محور WHO، پاسخ به خشونت را به مجازات مرتکب محدود نمی‌کند، بلکه بر پیشگیری، خدمات survivor-centred، سلامت روان، تولید داده و همکاری بین‌بخشی تأکید دارد. در ایران، قانونگذار در حوزه‌هایی مانند تحریف محتوای تصویری، انتشار غیررضایی محتوای خصوصی و نشر اکاذیب ابزارهای کیفری ایجاد کرده است، اما این ابزارها در قالب یک زنجیرهٔ سیاستی منسجم با پیشگیری و حمایت سلامت‌محور عمل نمی کنند.

بر این اساس، راه‌حل پیشنهادی مقاله، توسعهٔ بی‌رویهٔ جرم‌انگاری نیست. اصلاح مطلوب باید سه سطح را هم‌زمان پوشش دهد: در سطح تقنینی، تکمیل حمایت از قربانیان و روشن کردن وضعیت رفتارهای نوظهور؛ در سطح اجرایی، ایجاد پروتکل سریع حفظ ادله، توقف انتشار و ارجاع

به خدمات سلامت؛ و در سطح حکمرانی، ایجاد نظام دادهٔ تفکیک‌شده و شاخص سالانهٔ ارزیابی سیاست. بر مبنای مدل چهارحلقه‌ای پیشنهادی، سیاست جنایی زمانی کارآمد است که بتواند از «شناسایی رفتار» به «کاهش آسیب» و از «رسیدگی به پرونده» به «یادگیری نهادی» حرکت کند. این جابه‌جایی از سیاست جنایی صرفاً جرم‌محور به سیاست جنایی سلامت‌محور، مهم‌ترین دستاورد تحلیلی پژوهش حاضر است.

محدودیت‌های پژوهش

محدودیت اصلی پژوهش، نبود مجموعه دادهٔ ملی عمومی و تفکیک‌شده دربارهٔ خشونت دیجیتال علیه زنان و پیامدهای سلامت روانی آن است. از این رو، مقاله از تعمیم آمار عمومی جرائم سایبری به خشونت جنسیتی پرهیز کرده است. محدودیت دوم، تفاوت میان مفهوم خشونت دیجیتال در ادبیات اجتماعی و عناوین مجرمانهٔ موجود در حقوق ایران است. این تفاوت موجب می‌شود همهٔ مصادیق اجتماعی، الزاماً واجد وصف کیفری نباشند. پژوهش‌های آینده می‌توانند با روش پیمایشی یا مطالعهٔ پرونده‌های قضائی، مدل پیشنهادی را به‌صورت کمی آزمون کنند.

حامی مالی:
این مقاله هیچ حامی مالی ندارد.

مشارکت نویسندگان:
جمال بیگی: مفهوم‌سازی، نظارت بر داده‌ها، اعتبارسنجی، مدیریت پروژه، منابع.
زهرا اقبالی: روش‌شناسی، تحلیل، نوشتن بررسی و ویرایش، تحقیق و بررسی، پیش‌نویس اصلی.

تعارض منافع:
بنا بر اظهار نویسندگان این مقاله تعارض منافع ندارد.

ملاحظات اخلاقی:
این پژوهش بر پایهٔ مطالعهٔ اسناد، قوانین، رویه‌های قضائی و منابع کتابخانه‌ای انجام شده و در آن هیچ‌گونه مطالعه‌ای بر روی انسان، حیوان یا داده‌های شخصی صورت نگرفته است؛ بنابراین، اخذ

تأییدیه کمیتهٔ اخلاق برای این پژوهش ضروری نبوده است. با این حال، نویسنده اصول امانت‌داری علمی، صداقت پژوهشی، استناددهی صحیح و رعایت حقوق مالکیت فکری را در تمامی مراحل پژوهش رعایت کرده است.

در تهیهٔ این مقاله از ابزارهای هوش مصنوعی مولد صرفاً برای کمک به ویرایش زبانی، بهبود ساختار نگارش و ارتقای خوانایی متن استفاده شده است. این ابزارها در طراحی پژوهش، تحلیل علمی، تفسیر یافته‌ها، استنتاج نتایج یا تصمیم‌گیری‌های پژوهشی نقشی نداشته‌اند و مسئولیت کامل صحت، اصالت و محتوای نهایی مقاله بر عهده نویسنده/نویسندگان است.

موافقت نویسندگان:

تمامی نویسندگان نسخه نهایی مقاله را مطالعه و تأیید کرده‌اند و با انتشار آن موافقت دارند.

منابع

ارجمند، مارال و شریفی، بهدادا (۱٤۰۳)، «جرائم علیه زنان در فضای سایبری: چالش‌های قانونی، خلأهای حقوقی و راهکارهای مقابله»، حقوق سایبری، ۲، ۱۰٤-۱۲٤.

اشتری، بهناز (۱۳۸۵)، قاچاق زنان، چاپ اول، تهران: میزان.

السان، مصطفی (۱۳۸٤)، «قاچاق زنان و کودکان برای بهره‌کشی جنسی از منع جهانی تا حمایت از بزه دیدگان»، نشریهٔ رفاه اجتماعی، ۱٦، ۳۲۹-۳٦٤.

باستانی، برومند (۱۳۸۳)، جرایم کامپیوتری و اینترنتی جلوه‌ای نوین از بزهکاری، چاپ اول، تهران: بهنامی.

حبیب‌زاده، محمدجعفر و همکاران (۱۳۸۸)، «قاچاق انسان در حقوق کیفری ایران»، پژوهش‌های حقوقی تطبیقی، ٤، ۹۹-۱۲۳.

دزیانی، محمدحسن (۱۳۸٤)، «ایمنی در اینترنت ـ راهنمایی برای والدین»، قضاوت، ۳٤، ٥٤-٥٦.

راودراد، اعظم (۱۳۸٤)، «مسایل اجتماعی زنان در اینترنت»، مطالعات فرهنگی و ارتباطات، ۳، ۷۳ ـ ۹۲.

رایجیان اصلی، مهرداد (۱۳۸٤)، بزه‌دیده‌شناسی حمایتی، چاپ اول، تهران: دادگستر.

زندی، محمدرضا (۱۳۸۹)، تحقیقات مقدماتی در جرایم سایبری، چاپ اول، تهران: جنگل و جاودانه.

زررخ، احسان (۱۳۸۹)، بزه‌دیده‌شناسی سایبری، فصلنامهٔ مجلس و پژوهش، ۶۴، ۱۲۷-۱۵۸.

زندی، محمدرضا، حسینی، سیده آمنه و تدین، عباس (۱٤۰۲)، «ضرورت‌سنجی جرم‌انگاری پدیدهٔ قلدری مجازی در حقوق کیفری ایران و آمریکا»، حقوق تطبیقی، ۲۱۹،۱۹-۲٤٤.

سلیمی قلعه‌ئی، احسان، حسین‌زاده قدیم، آیدا و بوذری، سپیده (۱٤۰۳)، «خشونت علیه زنان در شبکه‌های اجتماعی برخط: شناسایی گونه‌ها، صدمات روانی و راهبردهای واکنشی»، حقوق پزشکی، ۵۹، ۱٤۷-۱٦۳.

فتاحیان، مریم (۱۳۹٦)، «بررسی علل جهانی افزایش خشونت سایبری علیه زنان»، قانون یار، ۳، ۲۹-٤۸.

معظمی، شهلا (۱۳۸٤)، جرم سازمان‌یافته و راه‌کارهای جهانی مقابله با آن، چاپ اول، تهران: دادگستر.

نوروزی، زهرا و افراخته، عبدالحمید (۱٤۰۰)، «واکاوی خشونت سایبری زنان و چتر حمایت قانون‌گذاری ملی و بین‌المللی»، پژوهش‌نامهٔ زنان، ۲، ۲۵۹_۲۹۰.

وطنی، امیر و اسدی، حمید (۱۳۹۵)، «سیاست جنایی جمهوری اسلامی ایران در جرائم سایبری با تأکید بر ویژگی‌های خاص این جرائم»، پژوهشنامهٔ حقوق اسلامی، ۱(٤۳)،۹۹-۱۲٦.

References

Arias, E., & Pankhurst, H. (2021), *Digital Gender-Based Violence and Women's Mental Health: A Global Review*, London: Routledge.

Citron, D. K. (2014), *Hate Crimes in Cyberspace. Harvard University Press*, (This book explores the legal and social implications of online harassment, with a focus on gender-based violence against women).

Flynn, A., Henry, N., & Powell, A. (2020), "Technology-facilitated sexual violence victimization: Results from an exploratory survey of young women in Australia", *Journal of Interpersonal Violence*, *35*(23-24), 5656-5678. (Empirical study on prevalence and effects of online sexual violence).

Henry, N., & Powell, A. (2018a), *Technology-Facilitated Sexual Violence*, NewYork: Springer.

Henry, N., & Powell, A. (2018b), *Technology-Facilitated Sexual Violence: A Multidisciplinary Approach to the Crimes of Technology-Facilitated Sexual Violence and Abuse. Routledge*, (Examines forms of digital abuse, including image-based sexual exploitation targeting women).

Jane, E. A. (2017), "Misandry online: 'Incel' anger and the mainstreaming of misogyny", *Continuum: Journal of Media & Cultural Studies*, *32*(5), 608-

622. (Discusses online misogyny and its violent manifestations against women).

Lami, C. (2021), "Digital Harassment and Women's Mental Health: A Public Health Perspective", *Journal of Global Mental Health*, *4*(2), 140–159.

Lewis, R., Rowe, M., & Wiper, C. (2017), "Online abuse, harassment, and discrimination: A study of women's experiences in the workplace", *Journal of Gender Studies*, *26*(7), 718-732. (Analyzes workplace-related cyber violence faced by women).

Mantilla, K. (2015), *Gendertrolling: How Misogyny Went Viral*, Praeger. (Investigates the viral nature of gendered online trolling and its impact on women).

United Nations General Assembly. (2000), *Protocol to prevent, suppress and punish trafficking in persons, especially women and children*, supplementing the United Nations Convention against Transnational Organized Crime (A/RES/55/25). New York: United Nations. United Nations Treaty Series, 2237, 319. https://treaties.un.org/doc/Publication/MTDSG/Volume%20II/Chapter%20XVIII/xviii-12-a.en.pdf.

Vickery, J. R., & Everbach, T. (Eds.). (2018), *Mediating Misogyny: Gender, Technology, and Harassment*, Palgrave Macmillan. (A collection of essays on technology-enabled gender violence).

Woodlock, D. (2017), "The Abuse of Technology in Domestic Violence and Stalking", *Violence Against Women*, *23*(5), 584–602.

World Health Organization. (2026a), *Violence against women* [Fact sheet]. Geneva: World Health Organization. https://www.who.int/news-room/fact-sheets/detail/violence-against-women.

World Health Organization. (2022), *Preventing intimate partner violence improves mental health* [News release]. Geneva: World Health Organization. https://www.who.int/news/item/06-10-2022-preventing-intimate-partner-violence-improves-mental-health.

Journal Website

Legal Innovation Quarterly

Spring 2026

Volume 2, Issue 3

E-ISSN: 3115-8498

A Jurisprudential Examination of Crime Prevention and Punishment, with Emphasis on Clause 5 of Article 156 of the Constitution of the Islamic Republic of Iran

Tahora Norozi *[1], Sayid Mohamad Mahdi Ahmadi[2], Ali Reza Asgari [3]

1. Ph.D. Student in Jurisprudence and Principles of Islamic Law, Faculty of Humanities, Qom Branch, Islamic Azad University, Qom, Iran **(Corresponding Author)***
2. Associate Professor, Department of Jurisprudence and Principles of Law, Faculty of Humanities, Qom Branch, Islamic Azad University, Qom, Iran.
3. Associate Professor, Department of Jurisprudence and Principles of Law, Faculty of Humanities, Qom Branch, Islamic Azad University, Qom, Iran.

***Corresponding author email address:** tnoroziii@iran.ir

Extended Abstract

1. Introduction

The article, "*A Jurisprudential Examination of Crime Prevention and Punishment, with Emphasis on Clause 5 of Article 156 of the Constitution of the Islamic Republic of Iran*," examines the place of crime prevention from the perspective of Islamic jurisprudence and Iranian constitutional law.

2. Research Methodology

In the first section, the concept of crime prevention is explained, and its types, including social, situational, and penal prevention, are introduced. The article explains that social prevention serves to mitigate the conditions conducive to crime by improving cultural, economic, educational, and family conditions, whereas situational prevention prevents the commission of offenses by making opportunities to commit crimes more difficult to exploit and increasing the likelihood of their detection. Penal prevention is likewise pursued through legal sanctions and the proper enforcement of punishments.

Received: 8 January 2026 - **Accepted:** 20 February 2026 - **Published:** 21 March 2026

Norouzi, Tahoura; Ahmadi, Seyed Mohammad Mehdi; and Asgari, Alireza. (2026). "A Jurisprudential Examination of Crime Prevention and Punishment, with Emphasis on Clause 5 of Article 156 of the Constitution of the Islamic Republic of Iran." *Legal Innovation Quarterly*, 2(3), pp. 175-198

Doi: https://doi.org/10.22034/lir.2026.2090411.1040

© 2026 The Authors. Published by Legal Innovation Research Institute, Tehran, Iran. This is an open access article distributed under the terms of the Creative Commons Attribution 4.0 International (CC BY 4.0) License.

The jurisprudential foundations of crime prevention are then examined. By drawing on the Qur'an, the Sunnah, the principle of enjoining good and forbidding wrong, social responsibility, the moral reform of individuals, and religious education, the author demonstrates that, in Islamic jurisprudence, prevention is better than cure. From the perspective of Islam, reducing crime is not possible through punishment alone; rather, the moral reform of individuals, the strengthening of faith, the promotion of social justice, and public responsibility play a fundamental role in prevention.

The role of social institutions, such as the family, education, culture, and society, in crime prevention is then analyzed. The article emphasizes that the family is the first institution of upbringing, and that the proper teaching of moral values, the strengthening of religious beliefs, and the creation of a healthy social environment are considered among the most important factors in reducing criminality.

3. Research Findings

A substantial section of the article is devoted to the analysis of Clause 5 of Article 156 of the Constitution. Under this clause, one of the duties of the Judiciary is "taking appropriate measures to prevent the commission of crime and to reform offenders." By examining this constitutional provision, the author states that the Constitution does not regard prevention merely as an executive measure; rather, it considers prevention a fundamental duty of the Judiciary. It is also emphasized that achieving this objective requires cooperation from the country's other executive, cultural, and social institutions, and that the Judiciary will not be able to fully implement preventive policies on its own.

The article then compares the jurisprudential foundations with Clause 5 of Article 156 and concludes that there is a considerable degree of consistency between Islamic teachings and the Constitution of the Islamic Republic of Iran. Principles such as the moral reform of individuals, justice, social responsibility, and crime prevention are emphasized in both jurisprudential sources and the Constitution. Accordingly, the criminal policy of the Islamic Republic of Iran rests on a solid jurisprudential foundation.

4. Recommendations

Finally, the author refers to the challenges involved in implementing preventive policy, including the lack of coordination among institutions, inadequate planning, a shortage of implementation mechanisms, cultural and social problems, and limited resources.

5. Conclusion

The article concludes that the effective realization of Clause 5 of Article 156 is possible only through cooperation among the Judiciary, the Government, and

cultural and educational institutions, together with public participation, and that the development of preventive policies may have a significant impact on reducing crime, enhancing social security, and achieving justice.
Keywords: Crime prevention; Islamic jurisprudence; Islamic criminal policy; Constitution of the Islamic Republic of Iran; Article 156 of the Constitution.

Funding
This article has no financial support or funding.

Authors' Contributions
Sayid Mohamad Mahdi Ahmadi & Ali Reza Asgari: Conceptualization, data curation, validation, project administration, and resources.
Tahora Norozi: Methodology, formal analysis, writing – review & editing, investigation, writing – original draft.

Conflict of Interest
According to the authors' declaration, there is no conflict of interest regarding this article.

Ethical Considerations
This study was conducted based on the analysis of legal documents, statutes, judicial decisions, and library-based sources. It did not involve human participants, animals, or personal data; therefore, ethical approval from an institutional ethics committee was not required. Nevertheless, the authors adhered to the principles of academic integrity, research honesty, proper citation practices, and respect for intellectual property rights throughout all stages of the research.Generative artificial intelligence (AI) tools were used solely to assist with language editing, improving the structure of the manuscript, and enhancing the readability of the text. These tools did not contribute to the study design, scientific analysis, interpretation of findings, drawing of conclusions, or any research-related decision-making. The author(s) assume full responsibility for the accuracy, originality, and final content of the manuscript.

Authors' Approval
All authors have read and approved the final version of the manuscript and consent to its publication.

بهار ۱۴۰۵
دوره ۲، شمارهٔ ۳
شاپای الکترونیکی:
۳۱۱۵-۸۴۹۸

فصلنامه نوآوری حقوقی

وبسایت مجله

بررسی فقهی پیشگیری از جرم و مجازات با تأکید بر بند ۵ اصل ۱۵۶ قانون اساسی جمهوری اسلامی ایران

طهورا نوروزی*[۱]، سید محمد مهدی احمدی[۲]، علیرضا عسگری[۳]

۱.دانشجوی دکتری رشتهٔ فقه و مبانی حقوق، دانشکدهٔ علوم انسانی، واحد قم، دانشگاه آزاد اسلامی، قم، ایران (نویسندهٔ مسئول)

۲. دانشیار گروه فقه و مبانی حقوق، دانشکدهٔ علوم انسانی، واحد قم، دانشگاه آزاد اسلامی، قم، ایران

۳. دانشیار گروه فقه و مبانی حقوق، دانشکدهٔ علوم انسانی، واحد قم، دانشگاه آزاد اسلامی، قم، ایران،

*ایمیل نویسندهٔ مسئول: tnoroziii@iran.i

چکیده

پیشگیری از جرم یکی از مهم‌ترین اهداف نظام‌های حقوقی معاصر به‌شمار می‌رود و در دهه‌های اخیر در سیاست جنایی کشورها جایگاه ویژه‌ای یافته است. در اندیشهٔ حقوق کیفری جدید، تمرکز صرف بر مجازات مجرمان کافی دانسته نمی‌شود و توجه به عوامل زمینه‌ساز جرم و اتخاذ تدابیر پیشگیرانه، اهمیت بیشتری پیدا کرده است. در فقه اسلامی نیز پیشگیری از جرم از طریق اصلاح فرد و جامعه، تقویت ارزش‌های اخلاقی و ایجاد نظم اجتماعی مورد توجه قرار گرفته است. آموزه‌های قرآنی و روایی با تأکید بر تربیت فردی، مسئولیت اجتماعی و نظارت عمومی، زمینه‌های کاهش جرم و انحراف را فراهم می‌کنند. در نظام حقوقی جمهوری اسلامی ایران نیز پیشگیری از جرم به‌عنوان یکی از وظایف مهم حاکمیت شناخته شده است. قانون اساسی جمهوری اسلامی ایران در اصل ۱۵۶ وظایف قوهٔ قضائیه را بیان کرده و در بند ۵ این اصل، اقدام مناسب برای پیشگیری از وقوع جرم و اصلاح مجرمان را از وظایف اساسی این قوه دانسته است. این امر نشان‌دهندهٔ توجه قانونگذار به نقش پیشگیری در سیاست جنایی کشور است. پژوهش حاضر با روش توصیفی ـ تحلیلی و با استفاده از منابع فقهی، حقوقی و قانونی، به بررسی مبانی فقهی پیشگیری از جرم و مجازات و تحلیل جایگاه آن در بند ۵ اصل ۱۵۶ قانون اساسی می‌پردازد. یافته‌های تحقیق نشان می‌دهد که اصل پیشگیری از جرم در فقه اسلامی ریشه‌ای عمیق دارد و بسیاری از آموزه‌های دینی در جهت کاهش زمینه‌های ارتکاب جرم و اصلاح رفتار افراد جامعه تنظیم شده است. همچنین بررسی‌ها نشان می‌دهد که بند ۵ اصل ۱۵۶ قانون اساسی انعکاسی از این مبانی فقهی است و قانونگذار با الهام از آموزه‌های اسلامی، پیشگیری از جرم را به‌عنوان یکی از وظایف اساسی قوهٔ قضائیه مطرح کرده است. درنتیجه می‌توان گفت که میان مبانی فقهی اسلام و سیاست جنایی تقنینی در قانون اساسی جمهوری اسلامی ایران هماهنگی قابل توجهی وجود دارد و تقویت رویکردهای پیشگیرانه می‌تواند نقش مهمی در کاهش جرم و تأمین امنیت اجتماعی ایفا کند.

واژه‌های کلیدی: پیشگیری از جرم، فقه اسلامی، سیاست جنایی اسلام، قانون اساسی جمهوری اسلامی ایران، اصل ۱۵۶ قانون اساسی.

دریافت‌شده در تاریخ: ۱۸ دی ۱۴۰۴، **پذیرش‌شده در تاریخ:** ۱ اسفند ۱۴۰۴، **منتشرشده در تاریخ:** ۱ فروردین ۱۴۰۵

نوروزی، طهورا؛ احمدی، سید محمد مهدی؛ عسگری، علیرضا. (۱۴۰۵). «بررسی فقهی پیشگیری از جرم و مجازات با تأکید بر بند ۵ اصل ۱۵۶ قانون اساسی جمهوری اسلامی ایران». فصلنامه نوآوری حقوقی، دوره ۲، شماره ۳، صص ۱۷۵- ۱۹۸.

Doi: https://doi.org/10.22034/lir.2026.2090411.1040

© 2026 The Authors. Published by Legal Innovation Research Institute, Tehran, Iran. This is an open access article distributed under the terms of the Creative Commons Attribution 4.0 International (CC BY 4.0) License.

مقدمه

پیشـگیری از جرم یکی از مهم‌ترین موضـوعات در مطالعات حقوق کیفری و جرم‌شـناسـی معاصر به‌شـمار می‌رود. تجربهٔ نظام‌های حقوقی مختلف نشان داده است که اتکای صرف بر مجازات برای مقـابلـه بـا جرم نمی‌تواند به‌تنهایی موجب کاهش پایدار بزهکاری در جامعه شـــود. به همین دلیل بسیاری از نظام‌های حقوقی در دهه‌های اخیر تلاش کرده‌اند با شناسایی عوامل اجتماعی، اقتصادی و فرهنگی مؤثر در شـکل‌گیری جرم، سـیاسـت‌های پیشـگیرانه را در کنار سیاست‌های کیفری مورد توجه قرار دهند. پیشـگیری از جرم درواقع مجموعه اقداماتی اسـت که با هدف کاهش فرصت‌های ارتکاب جرم و اصـلاح شـرایط اجتماعی زمینه‌ساز بزهکاری صورت می‌گیرد. این رویکرد می‌تواند از طریق تقویت ارزش‌های اجتماعی، افزایش نظارت عمومی و ایجاد سازوکارهای حقوقی مناسب به کاهش جرائم در جامعه کمک کند. از این رو امروزه پیشـــگیری از جرم به‌عنوان یکی از مهم‌ترین ابزارهای سـیاسـت جنایی برای تأمین نظم و امنیت اجتماعی شناخته می‌شود و در بسیاری از اسناد حقوقی و قوانین اساسی کشورها مورد توجه قرار گرفته است (سلیمی، ۱۳۸۸: ۲۵).

در سـیاست جنایی سنتی تمرکز اصلی بر مجازات مجرمان و اعمال کیفر پس از وقوع جرم قرار داشـــت. در این دیـدگـاه فرض بر این بود کـه مجازات شـــدید می‌تواند موجب بازدارندگی افراد از ارتکاب جرم شـــود. با این حال تجربهٔ عملی نشـــان داد که اتکای صـــرف به مجازات نه‌تنها قادر به ریشـه‌کن کردن جرم نیسـت، بلکه در بسـیاری از موارد به افزایش هزینه‌های نظام کیفری و گسترش جمعیـت کیفری زنـدان‌ها منجر می‌شـــود. به همین دلیل از نیمهٔ دوم قرن بیســـتم به‌تدریج رویکرد جدیدی در سـیاسـت جنایی شکل گرفت که در آن توجه به پیشگیری از جرم و کنترل عوامل جرم‌زا اهمیت بیشـتری پیدا کرد. در این رویکرد تلاش می‌شود پیش از آنکه جرم واقع شود با اتخاذ تدابیر اجتماعی، فرهنگی و حقوقی مناسـب از شـکل‌گیری شرایط جرم‌زا جلوگیری شود. بنابراین سیاست جنایی جدید به جای تمرکز صـــرف بر مجازات، مجموعه‌ای از اقدامات پیشـــگیرانه، اصـــلاحی و حمایتی را برای کاهش بزهکاری مورد توجه قرار می‌دهد (نجفی ابرندآبادی، ۱۳۹۲: ۷۲).

در اندیشهٔ اسلامی نیز پیشگیری از جرم از جایگاه مهمی برخوردار است و بسیاری از آموزه‌های دینی در جهت اصـــلاح فرد و جامعه و جلوگیری از وقوع جرم تنظیم شـــده اســـت. در منابع فقهی و متون اسـلامی، تأکید فراوانی بر تربیت اخلاقی، تقویت ایمان و ایجاد نظم اجتماعی دیده می‌شـود که همگی در راسـتای کاهش رفتارهای مجرمانه در جامعه قرار دارند. اسـلام با تأکید بر مسـئولیت

فردی و اجتماعی افراد، تلاش می‌کند از طریق تقویت ارزش‌های اخلاقی و نظارت عمومی، زمینه‌های بروز جرم را کاهش دهد. نهادهایی مانند خانواده، جامعه و حکومت اسلامی نیز در این چارچوب نقش مهمی در پیشگیری از جرم ایفا می‌کنند. به عبارت دیگر در فقه اسلامی پیشگیری از جرم نه‌تنها از طریق مجازات مجرمان بلکه از طریق اصلاح شرایط اجتماعی و تربیت افراد جامعه دنبال می‌شود. این رویکرد نشان می‌دهد که آموزه‌های اسلامی در بسیاری از موارد با دیدگاه‌های نوین جرم‌شناسی و سیاست جنایی در زمینهٔ پیشگیری از جرم هماهنگی قابل توجهی دارد (ره‌پیک، ۱۳۹۰: ۷۰).

در نظام حقوقی جمهوری اسلامی ایران نیز پیشگیری از جرم به‌عنوان یکی از اهداف مهم نظام عدالت کیفری مورد توجه قرار گرفته است. قانون اساسی جمهوری اسلامی ایران که به‌عنوان مهم‌ترین سند حقوقی کشور شناخته می‌شود، چارچوب کلی وظایف نهادهای حکومتی را در زمینهٔ تأمین عدالت و امنیت اجتماعی تعیین کرده است. در این میان قوهٔ قضائیه به‌عنوان یکی از ارکان اساسی نظام حاکمیتی وظیفهٔ مهمی در تحقق عدالت و مقابله با جرم بر عهده دارد. اصل ۱۵۶ قانون اساسی وظایف این قوه را بیان می‌کند و در بند ۵ این اصل، اقدام مناسب برای پیشگیری از وقوع جرم و اصلاح مجرمان را ازجمله وظایف اساسی قوهٔ قضائیه دانسته است. درج چنین وظیفه‌ای در قانون اساسی نشان‌دهندهٔ توجه قانونگذار به اهمیت پیشگیری از جرم و نقش آن در حفظ نظم و امنیت اجتماعی است. از این رو می‌توان گفت که قانون اساسی جمهوری اسلامی ایران با الهام از مبانی فقهی و آموزه‌های اسلامی، پیشگیری از جرم را به‌عنوان یکی از اصول اساسی سیاست جنایی کشور مورد توجه قرار داده است (هاشمی، ۱۳۹۰: ۲/ ۳۱۵).

با وجود اهمیت پیشگیری از جرم در نظام حقوقی ایران، بررسی مبانی فقهی این اصل و ارتباط آن با مقررات قانون اساسی ازجمله موضوعاتی است که نیازمند مطالعه و تحلیل دقیق است. بند ۵ اصل ۱۵۶ قانون اساسی به‌طور صریح بر وظیفهٔ پیشگیری از جرم تأکید کرده است، اما برای درک کامل این اصل لازم است مبانی فقهی و نظری آن نیز مورد بررسی قرار گیرد. از این رو پرسش اصلی این پژوهش آن است که پیشگیری از جرم در فقه اسلامی چه مبانی و اصولی دارد و این مبانی تا چه اندازه در بند ۵ اصل ۱۵۶ قانون اساسی انعکاس یافته است. بر همین اساس هدف مقالهٔ حاضر بررسی مبانی فقهی پیشگیری از جرم و مجازات و تحلیل جایگاه آن در بند ۵ اصل ۱۵۶ قانون اساسی جمهوری اسلامی ایران است. این پژوهش با روش توصیفی ـــ تحلیلی و با

استفاده از منابع فقهی، حقوقی و قانونی تلاش می‌کند ضمن تبیین جایگاه پیشگیری در اندیشهٔ اسلامی، میزان هماهنگی آن با سیاست جنایی تقنینی در قانون اساسی جمهوری اسلامی ایران را نیز مورد بررسی قرار دهد (عمید زنجانی، ۱۳۸۵: ۲۰۵).

۱. مبانی فقهی پیشگیری از جرم در اسلام

پیشگیری از جرم در اندیشهٔ اسلامی دارای مبانی عمیق فقهی و دینی است و تنها به مجازات مجرمان پس از وقوع جرم محدود نمی‌شود. در فقه اسلامی هدف اصلی از وضع احکام شرعی، حفظ نظم اجتماعی و تأمین مصالح عمومی جامعه است. از این رو بسیاری از دستورات دینی در جهت جلوگیری از بروز رفتارهای انحرافی و مجرمانه تنظیم شده‌اند. این دستورات با تأکید بر اصلاح فرد، تقویت باورهای دینی، نظارت اجتماعی و مسئولیت‌پذیری افراد، زمینه‌های ارتکاب جرم را کاهش می‌دهند. درواقع اسلام با ارائهٔ مجموعه‌ای از قواعد اخلاقی، اجتماعی و حقوقی تلاش می‌کند شرایطی فراهم آورد که در آن انسان‌ها کمتر به سوی رفتارهای مجرمانه گرایش پیدا کنند. به همین دلیل پیشگیری از جرم در فقه اسلامی مفهومی گسترده دارد و شامل اقدامات فرهنگی، تربیتی و اجتماعی نیز می‌شود. این رویکرد نشان می‌دهد که در اندیشهٔ اسلامی مقابله با جرم تنها از طریق مجازات دنبال نمی‌شود، بلکه اصلاح فرد و جامعه نیز از اهمیت ویژه‌ای برخوردار است (ره‌پیک، ۱۳۹۰: ۷۰).

در منابع فقهی و متون اسلامی توجه فراوانی به عوامل شکل‌گیری جرم و راه‌های جلوگیری از آن دیده می‌شود. اسلام با تأکید بر تربیت اخلاقی، تقویت ایمان و ایجاد حس مسئولیت اجتماعی در افراد تلاش می‌کند زمینه‌های بروز جرم را کاهش دهد. بسیاری از آموزه‌های اسلامی در جهت اصلاح رفتار انسان و تقویت ارزش‌های اخلاقی بیان شده‌اند تا افراد جامعه در برابر وسوسه‌های ارتکاب جرم مقاومت بیشتری داشته باشند. در این دیدگاه انسان موجودی مسئول است که باید در چارچوب ارزش‌های دینی رفتار کند و از هرگونه ظلم و تعدی نسبت به دیگران پرهیز نماید. بنابراین پیشگیری از جرم در فقه اسلامی به معنای ایجاد شرایطی است که در آن افراد جامعه به‌دلیل باورهای دینی و اخلاقی از ارتکاب رفتارهای مجرمانه خودداری کنند. این امر از طریق آموزش ارزش‌های اخلاقی، تقویت ایمان و ایجاد نظارت اجتماعی تحقق می‌یابد (نجفی ابرندآبادی، ۱۳۹۲: ۵۶).

در این چارچوب می‌توان مبانی فقهی پیشگیری از جرم را در منابع اصلی شریعت اسلامی جست‌وجو کرد. قرآن کریم به‌عنوان مهم‌ترین منبع شریعت اسلامی با تأکید بر اصلاح فرد و جامعه تلاش می‌کند انسان را از ارتکاب رفتارهای نادرست باز دارد. سنت پیامبر و ائمهٔ اطهار نیز با تأکید بر مسئولیت اجتماعی و نظارت عمومی، نقش مهمی در کاهش رفتارهای مجرمانه ایفا می‌کند. علاوه بر این، فقهای اسلامی در آثار فقهی خود به نقش حکومت و نهادهای اجتماعی در حفظ نظم عمومی و جلوگیری از وقوع جرم توجه کرده‌اند. مجموعهٔ این آموزه‌ها نشان می‌دهد که پیشگیری از جرم در اندیشهٔ اسلامی دارای مبانی نظری گسترده‌ای است و می‌تواند به‌عنوان یکی از مهم‌ترین ابزارهای حفظ امنیت اجتماعی مورد توجه قرار گیرد (عبدالقادر عوده، ۱۳۷۶: ۲۳۵).

۱ـ۱. پیشگیری از جرم در قرآن

قرآن کریم به‌عنوان مهم‌ترین منبع شریعت اسلامی نقش اساسی در تبیین اصول اخلاقی و اجتماعی دارد. بسیاری از آموزه‌های قرآنی در جهت اصلاح رفتار انسان و جلوگیری از انحرافات اجتماعی مطرح شده‌اند و از این رو می‌توان آن‌ها را از مهم‌ترین مبانی پیشگیری از جرم در اندیشهٔ اسلامی دانست. در قرآن کریم تأکید فراوانی بر اصلاح فرد، تقویت ایمان و ایجاد نظم اجتماعی دیده می‌شود که همگی در راستای کاهش رفتارهای مجرمانه در جامعه قرار دارند. درواقع قرآن کریم با ارائهٔ مجموعه‌ای از دستورات اخلاقی و اجتماعی تلاش می‌کند انسان را به سوی رفتارهای صحیح هدایت کند و از گرایش او به رفتارهای ناهنجار و مجرمانه جلوگیری نماید. این رویکرد نشان می‌دهد که در نگاه قرآن، پیشگیری از جرم بیش از آنکه بر مجازات تکیه داشته باشد بر اصلاح درونی انسان و تربیت اخلاقی او تأکید دارد (نحل: ۹۰؛ اسراء، ۳۲).

یکی از مهم‌ترین عناصر پیشگیری از جرم در قرآن کریم تأکید بر اصلاح فرد است. قرآن کریم در آیات مختلف انسان را به اصلاح رفتار و پرهیز از ظلم و فساد دعوت می‌کند و از او می‌خواهد که در مسیر عدالت و تقوا حرکت کند. این دعوت به اصلاح فردی درواقع زمینه‌ای برای شکل‌گیری جامعه‌ای سالم و عاری از جرم فراهم می‌کند. هنگامی که افراد جامعه از نظر اخلاقی و معنوی اصلاح شوند، احتمال ارتکاب رفتارهای مجرمانه نیز کاهش می‌یابد. از این رو قرآن کریم با تأکید بر ارزش‌هایی مانند عدالت، صداقت، امانت‌داری و پرهیز از ظلم، تلاش می‌کند زمینه‌های بروز جرم را در جامعه ازمیان بردارد و نظم اجتماعی را تقویت کند (جوادی آملی، ۱۳۸۵: ۲۶۵).

تقوا نیز از دیگر مفاهیم اساسی در قرآن کریم است که نقش مهمی در پیشگیری از جرم دارد. تقوا به معنای پرهیز از گناه و رعایت حدود الهی است و در بسیاری از آیات قرآن به‌عنوان یکی از مهم‌ترین معیارهای رفتار صحیح معرفی شده است. فردی که دارای تقوا باشد تلاش می‌کند از ارتکاب اعمال نادرست و رفتارهای زیان‌بار برای خود و دیگران دوری کند. چنین فردی حتی در شرایطی که امکان ارتکاب جرم وجود دارد، به‌دلیل باورهای دینی و احساس مسئولیت اخلاقی از انجام آن خودداری می‌ورزد. بنابراین تقوا می‌تواند به‌عنوان عامل درونی بازدارنده‌ای عمل کند و نقش مهمی در کاهش رفتارهای مجرمانه در جامعه داشته باشد. به همین دلیل قرآن کریم بارها انسان‌ها را به تقوا و پرهیزگاری دعوت کرده است تا از این طریق جامعه‌ای سالم و عاری از فساد شکل گیرد (مکارم شیرازی، ۱۳۸۶: ۱۱۲).

در کنار اصلاح فرد و تقوا، قرآن کریم بر تربیت اخلاقی انسان نیز تأکید فراوانی دارد. بسیاری از آموزه‌های قرآنی با هدف پرورش فضایل اخلاقی در انسان بیان شده‌اند. ارزش‌هایی مانند صداقت، عدالت، گذشت، مسئولیت‌پذیری و احترام به حقوق دیگران ازجمله اصول اخلاقی مهمی هستند که در قرآن مورد تأکید قرار گرفته‌اند. تربیت اخلاقی افراد جامعه می‌تواند زمینه‌های بسیاری از رفتارهای ناهنجار و مجرمانه را ازمیان ببرد. هنگامی که افراد جامعه به اصول اخلاقی پای‌بند باشند و به حقوق دیگران احترام بگذارند، احتمال بروز جرائم مختلف نیز کاهش می‌یابد. به همین دلیل می‌توان گفت که قرآن کریم از طریق تربیت اخلاقی انسان‌ها تلاش می‌کند زمینه‌های پیشگیری از جرم را در جامعه فراهم کند (جوادی آملی، ۱۳۸۵: ۲۶۵).

علاوه بر این، قرآن کریم به بازدارندگی معنوی نیز توجه ویژه‌ای دارد. در بسیاری از آیات قرآن به پیامدهای اخروی اعمال انسان اشاره شده و افراد به پاسخ‌گویی در برابر اعمال خود در روز قیامت هشدار داده شده‌اند. این هشدارها درواقع نوعی بازدارندگی معنوی ایجاد می‌کنند که می‌تواند انسان را از ارتکاب رفتارهای نادرست باز دارد. هنگامی که فرد باور داشته باشد که تمامی اعمال او مورد حسابرسی قرار خواهد گرفت، احتمال ارتکاب جرم و رفتارهای ناهنجار کاهش می‌یابد. بنابراین بازدارندگی معنوی یکی از مهم‌ترین ابزارهای پیشگیری از جرم در قرآن کریم محسوب می‌شود. این شیوه از پیشگیری بر تقویت باورهای دینی و مسئولیت اخلاقی انسان تکیه دارد و تلاش می‌کند از طریق اصلاح درونی افراد، جامعه‌ای سالم و عاری از جرم ایجاد کند (زلزال: ۷ و ۸).

۱-۲. پیشگیری از جرم در سنت و فقه اسلامی

علاوه بر قرآن کریم، سنت پیامبر اسلام و ائمهٔ اطهار نیز نقش مهمی در تبیین اصول پیشگیری از جرم در جامعهٔ اسلامی دارند. در بسیاری از روایات اسلامی بر ضرورت اصلاح جامعه، نظارت عمومی و جلوگیری از گسترش فساد تأکید شده است. یکی از مهم‌ترین ابزارهای پیشگیری از جرم در سنت اسلامی اصل امر به معروف و نهی از منکر است. این اصل به معنای تشویق افراد به انجام کارهای نیک و بازداشتن آنان از رفتارهای نادرست است و نقش مهمی در حفظ سلامت اخلاقی جامعه دارد. امر به معروف و نهی از منکر درواقع نوعی نظارت اجتماعی محسوب می‌شود که از طریق آن افراد جامعه نسبت به رفتار یکدیگر حساسیت نشان می‌دهند و در صورت مشاهدهٔ انحراف تلاش می‌کنند آن را اصلاح کنند. چنین نظارتی می‌تواند بسیاری از رفتارهای مجرمانه را پیش از وقوع کنترل کند (کلینی، ۱۳۶۵: ۵/ ۵۵).

در فقه اسلامی علاوه بر نظارت اجتماعی، بر مسئولیت عمومی افراد جامعه نیز تأکید شده است. براساس آموزه‌های اسلامی هر فرد در برابر جامعهٔ خود مسئول است و باید در حفظ نظم و جلوگیری از فساد مشارکت داشته باشد. این مسئولیت اجتماعی باعث می‌شود افراد جامعه نسبت به رفتارهای ناهنجار بی‌تفاوت نباشند و در صورت مشاهدهٔ انحراف در جهت اصلاح آن اقدام کنند. چنین رویکردی می‌تواند نقش مهمی در پیشگیری از جرم ایفا کند، زیرا هنگامی که افراد جامعه نسبت به یکدیگر احساس مسئولیت داشته باشند، زمینه‌های گسترش رفتارهای مجرمانه نیز کاهش می‌یابد. از این رو در سنت اسلامی مشارکت اجتماعی در حفظ نظم عمومی از اهمیت ویژه‌ای برخوردار است (عبدالقادر عوده، ۱۳۷۶: ۲۳۵).

نقش حکومت اسلامی نیز در پیشگیری از جرم بسیار مهم است. در آثار فقهی و سیاسی اسلام تأکید شده است که یکی از وظایف اصلی حکومت، حفظ نظم عمومی و جلوگیری از گسترش فساد در جامعه است. حکومت اسلامی باید با وضع قوانین عادلانه، ایجاد نظم اجتماعی و نظارت بر اجرای احکام الهی از وقوع جرم جلوگیری کند. درواقع حکومت با ایجاد ساختارهای مناسب اجتماعی و حقوقی می‌تواند شرایطی فراهم آورد که در آن فرصت‌های ارتکاب جرم کاهش یابد. به همین دلیل در اندیشهٔ سیاسی اسلام حکومت نقش مهمی در تأمین امنیت اجتماعی و جلوگیری از رفتارهای مجرمانه برعهده دارد (ماوردی، ۱۳۸۶ق: ۱۲۰).

۱-۳. نقش نهادهای اجتماعی در پیشگیری

در کنار آموزه‌های دینی و نقش حکومت، نهادهای اجتماعی نیز در پیشگیری از جرم اهمیت زیادی دارند. یکی از مهم‌ترین این نهادها خانواده است. خانواده نخستین محیط اجتماعی است که فرد در آن رشد می‌کند و بسیاری از ارزش‌های اخلاقی و اجتماعی را در آن فرا می‌گیرد. اگر خانواده بتواند وظیفهٔ تربیتی خود را به‌درستی انجام دهد، بسیاری از زمینه‌های انحراف و بزهکاری در افراد ازبین خواهد رفت. آموزش ارزش‌های اخلاقی، ایجاد حس مسئولیت‌پذیری و تقویت باورهای دینی در محیط خانواده می‌تواند نقش مهمی در پیشگیری از جرم داشته باشد (ابن خلدون، ۱۳۶۳: ۱۴۵).

علاوه بر خانواده، جامعه نیز در شکل‌گیری رفتار افراد نقش مهمی ایفا می‌کند. محیط اجتماعی می‌تواند بر نگرش‌ها و رفتارهای افراد تأثیر بگذارد و زمینه‌های ارتکاب جرم یا پرهیز از آن را فراهم کند. جامعه‌ای که در آن ارزش‌های اخلاقی مورد احترام قرار گیرد و افراد نسبت به یکدیگر احساس مسئولیت داشته باشند، کمتر با پدیدهٔ جرم مواجه خواهد شد. بنابراین تقویت هم‌بستگی اجتماعی و افزایش مشارکت عمومی در امور اجتماعی می‌تواند نقش مهمی در کاهش رفتارهای مجرمانه داشته باشد (ره‌پیک، ۱۳۹۰: ۷۰).

درنهایت حکومت نیز به‌عنوان یکی از مهم‌ترین نهادهای اجتماعی وظیفه دارد با ایجاد ساختارهای حقوقی و اجتماعی مناسب از وقوع جرم جلوگیری کند. حکومت با تدوین قوانین عادلانه، ایجاد فرصت‌های برابر و نظارت بر اجرای قانون می‌تواند زمینه‌های بسیاری از جرائم را ازمیان بردارد. از این رو در سیاست جنایی اسلام نقش حکومت در پیشگیری از جرم بسیار مهم تلقی می‌شود و این نهاد باید با استفاده از ابزارهای فرهنگی، اجتماعی و حقوقی در جهت کاهش جرم و تأمین امنیت اجتماعی تلاش کند (نجفی ابرندآبادی، ۱۳۹۲: ۵۶).

۲. مفهوم پیشگیری از جرم در سیاست جنایی اسلام

پیشگیری از جرم در سیاست جنایی معاصر به‌عنوان یکی از مهم‌ترین راهکارهای مقابله با بزهکاری شناخته می‌شود. در این رویکرد تلاش می‌شود با شناسایی عوامل زمینه‌ساز جرم و اتخاذ تدابیر مناسب، از وقوع جرم پیش از تحقق آن جلوگیری شود. سیاست جنایی در معنای عام شامل مجموعه تدابیر تقنینی، قضائی، اجرایی و اجتماعی است که به‌منظور کنترل جرم و حفظ نظم عمومی در جامعه به‌کار گرفته می‌شود. در این چارچوب پیشگیری از جرم به‌عنوان یکی از مهم‌ترین

ابزارهای سیاست جنایی مورد توجه قرار می‌گیرد، زیرا هدف آن کاهش فرصت‌های ارتکاب جرم و اصلاح شرایط اجتماعی است. در اندیشهٔ اسلامی نیز سیاست جنایی تنها به تعیین مجازات برای مجرمان محدود نمی‌شود، بلکه مجموعه‌ای از تدابیر فرهنگی، اجتماعی و حقوقی را دربر می‌گیرد که هدف اصلی آن حفظ امنیت و سلامت جامعه است. از این رو پیشگیری از جرم در سیاست جنایی اسلام جایگاه مهمی دارد و بسیاری از آموزه‌های دینی در جهت تحقق این هدف بیان شده‌اند.

۲-۱. تعریف پیشگیری از جرم

در مطالعات جرم‌شناسی و حقوق کیفری، پیشگیری از جرم به مجموعه اقداماتی گفته می‌شود که با هدف جلوگیری از وقوع جرم و کاهش فرصت‌های بزهکاری در جامعه انجام می‌شود. این اقدامات می‌توانند ماهیت اجتماعی، فرهنگی، اقتصادی یا حقوقی داشته باشند و هدف اصلی آن‌ها جلوگیری از شکل‌گیری شرایطی است که به ارتکاب جرم منجر می‌شود. به عبارت دیگر پیشگیری از جرم به معنای اتخاذ تدابیری است که با کاهش عوامل جرم‌زا و تقویت عوامل بازدارنده، احتمال وقوع جرم را در جامعه کاهش می‌دهد. این رویکرد در مقابل سیاست‌های صرفاً کیفری قرار دارد که تمرکز اصلی آن‌ها بر مجازات مجرمان پس از وقوع جرم است. درواقع پیشگیری از جرم تلاش می‌کند قبل از آنکه جرم واقع شود، با اصلاح شرایط اجتماعی و افزایش آگاهی افراد جامعه از بروز رفتارهای مجرمانه جلوگیری کند (سلیمی، ۱۳۸۸: ۲۵).

براساس دیدگاه جرم‌شناسان، پیشگیری از جرم نه‌تنها موجب کاهش میزان بزهکاری می‌شود، بلکه می‌تواند از افزایش هزینه‌های نظام عدالت کیفری نیز جلوگیری کند. هنگامی که جامعه بتواند با اتخاذ تدابیر مناسب از وقوع جرم جلوگیری کند، نیاز به اعمال مجازات‌های سنگین و گسترش نهادهای کیفری نیز کاهش می‌یابد. از این رو بسیاری از نظام‌های حقوقی در دهه‌های اخیر تلاش کرده‌اند سیاست‌های پیشگیرانه را در کنار سیاست‌های کیفری مورد توجه قرار دهند. این رویکرد درواقع نشان‌دهندهٔ تحول در سیاست جنایی معاصر است که در آن توجه به عوامل اجتماعی و فرهنگی جرم اهمیت بیشتری پیدا کرده است. در چنین دیدگاهی پیشگیری از جرم به‌عنوان یکی از مهم‌ترین ابزارهای کنترل اجتماعی شناخته می‌شود و نقش مهمی در حفظ نظم و امنیت جامعه ایفا می‌کند (حبیب‌زاده، ۱۳۹۱: ۴۰).

۲-۲. انواع پیشگیری

در مطالعات جرم‌شناسی پیشگیری از جرم به انواع مختلفی تقسیم می‌شود که هر یک از آن‌ها با استفاده از روش‌های خاصی تلاش می‌کنند از وقوع جرم جلوگیری کنند. یکی از مهم‌ترین این انواع، پیشگیری اجتماعی است. پیشگیری اجتماعی به مجموعه اقداماتی گفته می‌شود که با هدف اصلاح شرایط اجتماعی و فرهنگی جامعه انجام می‌شود تا زمینه‌های بروز جرم کاهش یابد. این نوع پیشگیری بر عواملی مانند آموزش، تربیت، کاهش نابرابری‌های اجتماعی و تقویت ارزش‌های اخلاقی تمرکز دارد. درواقع پیشگیری اجتماعی تلاش می‌کند با اصلاح ساختارهای اجتماعی و تقویت هم‌بستگی اجتماعی، از شکل‌گیری شرایطی که به بزهکاری منجر می‌شود جلوگیری کند. بسیاری از برنامه‌های آموزشی و فرهنگی که در جهت تقویت ارزش‌های اخلاقی و اجتماعی انجام می‌شوند در چارچوب پیشگیری اجتماعی قرار می‌گیرند (نجفی ابرندآبادی، ۱۳۹۲: ۷۲).

نوع دیگر پیشگیری از جرم، پیشگیری وضعی است. پیشگیری وضعی به مجموعه اقداماتی گفته می‌شود که با هدف کاهش فرصت‌های ارتکاب جرم انجام می‌شود. این نوع پیشگیری بر تغییر شرایط محیطی و فیزیکی تمرکز دارد تا ارتکاب جرم برای بزهکاران دشوارتر شود. برای مثال افزایش نظارت در مکان‌های عمومی، استفاده از فناوری‌های امنیتی و طراحی مناسب فضاهای شهری ازجمله اقداماتی هستند که می‌توانند در چارچوب پیشگیری وضعی مورد استفاده قرار گیرند. در این نوع پیشگیری تلاش می‌شود با کاهش فرصت‌های جرم و افزایش احتمال شناسایی بزهکاران، انگیزهٔ ارتکاب جرم کاهش یابد. پیشگیری وضعی در بسیاری از کشورها به‌عنوان یکی از مهم‌ترین ابزارهای کنترل جرم مورد استفاده قرار گرفته است (اردبیلی، ۱۳۹۰: ۱/ ۱۱۵).

نوع سوم پیشگیری از جرم، پیشگیری کیفری است. در این نوع پیشگیری، استفاده از مجازات و ضمانت اجراهای قانونی به‌عنوان ابزاری برای بازدارندگی از جرم مورد توجه قرار می‌گیرد. هدف از پیشگیری کیفری این است که با تعیین مجازات برای رفتارهای مجرمانه، افراد جامعه از ارتکاب جرم باز داشته شوند. درواقع مجازات به‌عنوان یک عامل بازدارنده عمل می‌کند و می‌تواند افراد را از انجام رفتارهای مجرمانه منصرف کند. البته در سیاست جنایی جدید تأکید می‌شود که پیشگیری کیفری باید در کنار سایر روش‌های پیشگیری مورد استفاده قرار گیرد و نباید تنها ابزار مقابله با جرم تلقی شود (نجفی ابرندآبادی، ۱۳۹۲: ۷۲).

۲-۳. جایگاه پیشگیری در سیاست جنایی اسلام

در اندیشهٔ اسلامی پیشگیری از جرم جایگاه بسیار مهمی دارد و بسیاری از آموزه‌های دینی در جهت جلوگیری از بروز رفتارهای مجرمانه در جامعه بیان شـده‌اند. اسلام با تأکید بر اصلاح فرد و جامعه تلاش می‌کند زمینه‌های ارتکاب جرم را کاهش دهد و از گسترش فساد در جامعه جلوگیری کند. در این چارچوب نهادهایی مانند خانواده، جامعه و حکومت اسلامی نقش مهمی در پیشگیری از جرم ایفـا می‌کننـد. آموزه‌هـایی مانند تقوا، امر به معروف و نهی از منکر و مسـئولیت اجتماعی ازجمله ابزارهایی هسـتند که در سـیاسـت جنایی اسلام برای پیشگیری از جرم مورد استفاده قرار می‌گیرند. این آموزه‌هـا بـا تقویـت نظارت اجتماعی و افزایش مسـئولیت‌پذیری افراد جامعه، نقش مهمی در کاهش رفتارهای مجرمانه دارند (رهپیک، ۱۳۹۰: ۱۱۰).

علاوه بر این، در اندیشـهٔ سـیاسـی اسلام حکومت نیز مسئولیت مهمی در پیشگیری از جرم بر عهده دارد. حکومت اسـلامی باید با وضـع قوانین عادلانه، ایجاد نظم اجتماعی و نظارت بر اجرای احکام الهی از گسـترش جرم و فسـاد جلوگیری کند. درواقع هدف از تشـکیل حکومت در اندیشـهٔ اسـلامی تنهـا اجرای مجازات‌ها نیسـت، بلکه ایجاد جامعه‌ای عادلانه و سـالم اسـت که در آن زمینه‌های بروز جرم به حداقل برسـد. از این رو می‌توان گفت که سیاست جنایی اسلام بر ترکیبی از اقدامات پیشـگیرانه و کیفری اسـتوار است و تلاش می‌کند با استفاده از ابزارهای مختلف، امنیت و نظم اجتماعی را در جامعه برقرار سازد (عبدالقادر عوده، ۱۳۷۶: ۲۴۵).

۳. جایگاه پیشگیری از جرم در قانون اساسی جمهوری اسلامی ایران

پیشـگیری از جرم در نظام حقوقی جمهوری اسـلامی ایران از جایگاه ویژه‌ای برخوردار اسـت و در اسـناد قانونی مختلف مورد توجه قرار گرفته است. مهم‌ترین سند حقوقی کشور یعنی قانون اساسی جمهوری اسـلامی ایران نیز به این موضوع توجه کرده و در تعیین وظایف نهادهای حاکمیتی، نقش مهمی برای پیشـگیری از جرم درنظر گرفته اسـت. قانون اساسی با تعیین وظایف قوهٔ قضائیه و سایر نهـادهای مسـئول تلاش می‌کند چارچوبی حقوقی برای مقابله با جرم و حفظ نظم اجتماعی ایجاد کند. در این چارچوب پیشـگیری از جرم به‌عنوان یکی از مهم‌ترین ابزارهای حفظ امنیت و سلامت جامعه مورد توجه قرار گرفته است.

قانون اساسی جمهوری اسلامی ایران با الهام از مبانی فقه اسلامی و اصول عدالت اجتماعی، وظایف مختلفی را برای نهادهای حکومتی در زمینهٔ حفظ نظم و امنیت عمومی تعیین کرده است. در میان این نهادها قوهٔ قضائیه نقش اساسی در تحقق عدالت و مقابله با جرم دارد. این قوه وظیفه دارد با اجرای قوانین، رسیدگی به جرائم و اتخاذ تدابیر مناسب از گسترش بزهکاری در جامعه جلوگیری کند. درواقع قوهٔ قضائیه علاوه بر رسیدگی به جرائم و اعمال مجازات برای مجرمان، باید با اتخاذ سیاست‌های مناسب در جهت پیشگیری از وقوع جرم نیز اقدام کند. این امر نشان‌دهندهٔ آن است که در نظام حقوقی ایران توجه به پیشگیری از جرم به‌عنوان یکی از ارکان سیاست جنایی مورد تأکید قرار گرفته است.

در قانون اساسی جمهوری اسلامی ایران اصول مختلفی به وظایف قوهٔ قضائیه و نقش آن در حفظ نظم اجتماعی اشاره دارند. با این حال مهم‌ترین اصل در این زمینه اصل ۱۵۶ قانون اساسی است که به‌طور مستقیم وظایف و اختیارات قوهٔ قضائیه را بیان می‌کند. در این اصل علاوه بر وظایف سنتی دستگاه قضائی مانند رسیدگی به دعاوی و صدور حکم، بر موضوع پیشگیری از جرم نیز تأکید شده است. درج چنین وظیفه‌ای در قانون اساسی نشان‌دهندهٔ آن است که قانونگذار اهمیت ویژه‌ای برای پیشگیری از جرم قائل بوده و آن را یکی از وظایف اساسی قوهٔ قضائیه دانسته است.

۳-۱. بررسی اصل ۱۵۶ قانون اساسی

اصل ۱۵۶ قانون اساسی جمهوری اسلامی ایران به بیان وظایف و اختیارات قوهٔ قضائیه می‌پردازد و این قوه را به‌عنوان پشتیبان حقوق فردی و اجتماعی معرفی می‌کند. براساس این اصل، قوهٔ قضائیه وظیفه دارد با اجرای عدالت و رسیدگی به دعاوی، از حقوق مردم حمایت کرده و از گسترش ظلم و بی‌عدالتی در جامعه جلوگیری کند. این اصل همچنین بر استقلال قوهٔ قضائیه تأکید دارد و بیان می‌کند که این قوه باید بدون تأثیرپذیری از سایر قوا به وظایف قانونی خود عمل کند.

در اصل ۱۵۶ قانون اساسی چندین وظیفهٔ مهم برای قوهٔ قضائیه تعیین شده است که هر یک نقش مهمی در حفظ نظم و امنیت اجتماعی دارند. از جملهٔ این وظایف می‌توان به رسیدگی به تظلمات و شکایات، احیای حقوق عامه، نظارت بر حسن اجرای قوانین و کشف جرم اشاره کرد. این وظایف نشان می‌دهند که قوهٔ قضائیه علاوه بر رسیدگی به جرائم، نقش مهمی در نظارت بر

اجرای قـانون و حفظ حقوق عمومی دارد. درواقع هدف از این وظایف آن اســت که با اجرای دقیق قوانین و رسیدگی عادلانه به دعاوی، از بروز بی‌نظمی و بی‌عدالتی در جامعه جلوگیری شود.

یکی از نکات مهم در اصـل ۱۵۶ قانون اسـاسـی آن است که این اصل تنها به برخورد با جرائم پس از وقوع آن‌هـا محـدود نمی‌شـود، بلکه به موضـوع پیشـگیری از جرم نیز توجه دارد. درواقع قانونگذار با گنجاندن موضـوع پیشـگیری در این اصـل تلاش کرده است رویکردی جامع نسبت به مقابله با جرم اتخاذ کند. این رویکرد نشان می‌دهد که قانون اساسی جمهوری اسلامی ایران تنها بر مجازات مجرمان تأکید ندارد، بلکه پیشگیری از جرم را نیز به‌عنوان یکی از وظایف مهم قوۀ قضائیه مطرح کرده اسـت. چنین دیدگاهی با رویکردهای نوین سـیاسـت جنایی که بر پیشـگیری از جرم تأکید دارند هماهنگی قابل توجهی دارد (هاشمی، ۱۳۹۰: ۲/ ۳۱۵).

۳-۲. تحلیل بند ۵ اصل ۱۵۶

در میان بندهای مختلف اصـل ۱۵۶ قانون اسـاسـی، بند پنجم این اصـل اهمیت ویژه‌ای در حوزۀ پیشگیری از جرم دارد. در این بند به‌طور صریح بیان شده است که یکی از وظایف قوۀ قضائیه اقدام مناسب برای پیشگیری از وقوع جرم و اصلاح مجرمان است. این عبارت نشان می‌دهد که قانونگذار علاوه بر توجه به مجازات مجرمان، به موضـوع اصـلاح مجرمان و جلوگیری از وقوع جرم نیز توجه داشته است.

تحلیل بند پنجم اصـل ۱۵۶ نشـان می‌دهد که قانون اساسی جمهوری اسلامی ایران رویکردی پیشگیرانه نسبت به مسئلۀ جرم اتخاذ کرده است. در این بند دو مفهوم مهم یعنی پیشگیری از جرم و اصـلاح مجرمان در کنار یکدیگر قرار گرفته‌اند. این موضوع نشان‌دهندۀ آن است که سیاست جنایی مورد نظر قـانونگـذار تنها بر مجازات تأکید ندارد، بلکه اصــلاح افراد و جلوگیری از تکرار جرم نیز مورد توجـه قرار گرفته اســت. چنین رویکردی با مبانی فقه اســلامی نیز هماهنگ اســت، زیرا در آموزه‌های اسلامی نیز اصلاح فرد و جلوگیری از فساد در جامعه اهمیت فراوانی دارد.

از سـوی دیگر عبارت اقدام مناسـب برای پیشـگیری از وقوع جرم نشـان می‌دهد که قوۀ قضائیه بـایـد بـا اســتفاده از ابزارهای مختلف حقوقی، اجتماعی و فرهنگی در جهت کاهش بزهکاری در جامعه اقدام کند. این اقدامات می‌توانند شــامل برنامه‌های آموزشــی، همکاری با ســایر نهادهای اجتماعی و تدوین سـیاسـت‌های مناسـب برای کاهش عوامل جرم‌زا باشند. بنابراین بند پنجم اصل

۱۵۶ قانون اساسی چارچوبی کلی برای اقدامات پیشگیرانهٔ قوهٔ قضائیه فراهم می‌کند و این قوه را موظف می‌سازد در کنار رسیدگی به جرائم، در جهت جلوگیری از وقوع آن‌ها نیز تلاش کند (عمید زنجانی، ۱۳۸۵: ۲۰۵).

۳-۳. نقش قوهٔ قضائیه در پیشگیری از جرم

قوهٔ قضائیه به‌عنوان یکی از ارکان اساسی نظام حکومتی جمهوری اسلامی ایران نقش مهمی در پیشگیری از جرم دارد. این قوه علاوه بر وظیفهٔ رسیدگی به دعاوی و صدور احکام قضایی، مسئولیت دارد با اتخاذ تدابیر مناسب از گسترش جرم و بزهکاری در جامعه جلوگیری کند. درواقع پیشگیری از جرم یکی از مهم‌ترین وظایف این قوه در چارچوب قانون اساسی به‌شمار می‌رود.

برای تحقق این هدف، قوهٔ قضائیه باید از ابزارهای مختلفی استفاده کند. یکی از مهم‌ترین این ابزارها تدوین سیاست‌های مناسب در حوزهٔ عدالت کیفری است. این سیاست‌ها می‌توانند شامل اصلاح قوانین کیفری، توسعهٔ برنامه‌های اصلاحی برای مجرمان و افزایش همکاری با سایر نهادهای اجتماعی باشند. همچنین قوهٔ قضائیه می‌تواند با افزایش آگاهی عمومی نسبت به پیامدهای جرم و تقویت فرهنگ قانون‌مداری در جامعه، نقش مهمی در کاهش بزهکاری ایفا کند.

علاوه بر این قوهٔ قضائیه می‌تواند از طریق همکاری با نهادهای اجرایی و اجتماعی در جهت کاهش عوامل جرم‌زا اقدام کند. بسیاری از جرائم در مشکلات اجتماعی و اقتصادی ریشه دارند و مقابله با آن‌ها نیازمند همکاری میان نهادهای مختلف حکومتی است. در این میان قوهٔ قضائیه می‌تواند با ارائهٔ راهکارهای حقوقی و نظارت بر اجرای قوانین نقش مهمی در کاهش این عوامل ایفا کند. از این رو می‌توان گفت که نقش قوهٔ قضائیه در پیشگیری از جرم تنها به اقدامات قضائی محدود نمی‌شود، بلکه شامل مجموعه‌ای از اقدامات اجتماعی و فرهنگی نیز می‌شود که هدف اصلی آن‌ها حفظ نظم و امنیت جامعه است (حسینی، ۱۳۹۲: ۸۰).

٤. تطبیق مبانی فقهی با بند ۵ اصل ۱۵۶ قانون اساسی

یکی از موضوعات مهم در بررسی سیاست جنایی جمهوری اسلامی ایران، تطبیق مبانی فقهی پیشگیری از جرم با مقررات قانون اساسی است. قانون اساسی جمهوری اسلامی ایران به‌عنوان مهم‌ترین سند حقوقی کشور بر پایهٔ مبانی اسلامی تدوین شده است و بسیاری از اصول آن

انعکاسی از آموزه‌های فقه اسلامی به‌شمار می‌رود. در این میان بند ۵ اصل ۱۵۶ قانون اساسی که بر پیشگیری از وقوع جرم و اصلاح مجرمان تأکید دارد، ازجمله اصولی است که ارتباط نزدیکی با مبانی فقهی و آموزه‌های اسلامی دارد. درواقع پیشگیری از جرم در فقه اسلامی سابقه‌ای طولانی دارد و بسیاری از احکام شرعی در جهت جلوگیری از فساد و انحراف در جامعه تنظیم شده‌اند.

در اندیشهٔ اسلامی پیشگیری از جرم تنها به معنای جلوگیری از ارتکاب رفتارهای مجرمانه نیست، بلکه شامل مجموعه‌ای از اقدامات فرهنگی، اخلاقی و اجتماعی است که با هدف اصلاح فرد و جامعه انجام می‌شود. این اقدامات می‌توانند شامل تربیت اخلاقی، تقویت ایمان، نظارت اجتماعی و ایجاد نظم در جامعه باشند. چنین رویکردی با سیاست جنایی پیشگیرانه که در حقوق معاصر مطرح شده است هماهنگی قابل توجهی دارد. قانون اساسی جمهوری اسلامی ایران نیز با الهام از همین مبانی، پیشگیری از جرم را به‌عنوان یکی از وظایف مهم قوهٔ قضائیه مطرح کرده است. به همین دلیل بررسی ارتباط میان مبانی فقهی پیشگیری از جرم و بند ۵ اصل ۱۵۶ قانون اساسی می‌تواند به درک بهتر سیاست جنایی اسلامی در نظام حقوقی ایران کمک کند.

از سوی دیگر، توجه قانونگذار به پیشگیری از جرم در قانون اساسی نشان می‌دهد که سیاست جنایی جمهوری اسلامی ایران صرفاً بر مجازات مجرمان تکیه ندارد، بلکه تلاش می‌کند با اتخاذ تدابیر مناسب از وقوع جرم جلوگیری کند. این رویکرد درواقع انعکاسی از دیدگاه اسلام دربارهٔ اصلاح جامعه و جلوگیری از گسترش فساد است. با این حال اجرای مؤثر سیاست‌های پیشگیرانه نیازمند بررسی دقیق مبانی فقهی و حقوقی این اصل و همچنین شناسایی چالش‌های موجود در مسیر اجرای آن است. در ادامه به بررسی ریشه‌های فقهی اصل پیشگیری، انطباق دیدگاه اسلام با قانون اساسی و چالش‌های اجرای این اصل پرداخته می‌شود.

٤-١. ریشه‌های فقهی اصل پیشگیری

در فقه اسلامی پیشگیری از جرم در اصول اساسی شریعت ریشه دارد که هدف آن‌ها حفظ نظم اجتماعی و جلوگیری از فساد در جامعه است. بسیاری از احکام شرعی درواقع با هدف جلوگیری از بروز رفتارهای ناهنجار و مجرمانه وضع شده‌اند. برای مثال تأکید اسلام بر تقوا، عدالت، امر به معروف و نهی از منکر و نظارت اجتماعی همگی در جهت جلوگیری از انحرافات اجتماعی و

کاهش رفتارهای مجرمانه در جامعه قرار دارند. این آموزه‌ها نشـان می‌دهند که در اندیشـهٔ اسـلامی اصلاح فرد و جامعه پیش از اعمال مجازات مورد توجه قرار گرفته است.

یکی از مهم‌ترین مبانی فقهی پیشـگیری از جرم اصـل امر به معروف و نهی از منکر است. این اصـل که از مهم‌ترین اصول اجتماعی در اسلام محسوب می‌شود، افراد جامعه را به نظارت بر رفتار یکدیگر و جلوگیری از گسترش فساد دعوت می‌کند. درواقع این اصل نوعی نظارت اجتماعی ایجاد می‌کند که می‌تواند نقش مهمی در پیشـگیری از جرم داشته باشد. هنگامی که افراد جامعه نسبت به رفتارهای نادرسـت حسـاسـیت داشـته باشند و در جهت اصلاح آن‌ها اقدام کنند، احتمال گسترش جرم و فساد در جامعه کاهش می‌یابد.

علاوه بر این، در فقه اسلامی بر نقش حکومت در حفظ نظم عمومی و جلوگیری از فساد تأکید شـده اسـت. حکومت اسـلامی موظف اسـت با وضـع قوانین عادلانه و ایجاد ساختارهای مناسب اجتماعی، زمینه‌های بروز جرم را کاهش دهد. در این چارچوب پیشـگیری از جرم یکی از وظایف مهم حکومت اسـلامی محسـوب می‌شـود. بنابراین می‌توان گفت که اصل پیشگیری از جرم که در بند ۵ اصـل ۱۵۶ قانون اساسی مطرح شده است، در مبانی فقهی و آموزه‌های اسلامی ریشه دارد و درواقع انعکاسـی از دیدگاه اسلام دربارهٔ ضرورت اصلاح جامعه و جلوگیری از گسترش فساد است (ره‌پیک، ۱۳۹۰: ۱۴۰).

٤-۲. انطباق دیدگاه اسلام با قانون اساسی

قانون اساسی جمهوری اسلامی ایران با الهام از مبانی اسلامی تدوین شده است و بسیاری از اصول آن بازتاب‌دهندهٔ آموزه‌های فقه اسـلامی هسـتند. در این میان بند ۵ اصـل ۱۵۶ قانون اساسی که به پیشـگیری از وقوع جرم و اصلاح مجرمان اشاره دارد، نمونه‌ای از این هماهنگی میان فقه اسلامی و نظام حقوقی کشـور است. در اندیشهٔ اسلامی پیشگیری از جرم همواره مورد توجه بوده و بسیاری از آموزه‌های دینی در جهت جلوگیری از گسترش فساد و انحراف در جامعه بیان شده‌اند.

در قانون اسـاسـی جمهوری اسـلامی ایران نیز این رویکرد مورد توجه قرار گرفته و پیشگیری از جرم به‌عنوان یکی از وظایف اسـاسـی قوهٔ قضـائیه معرفی شـده اسـت. این امر نشـان می‌دهد که قانونگذار تلاش کرده اسـت با استفاده از مبانی فقهی و آموزه‌های اسلامی، چارچوبی حقوقی برای مقابله با جرم و حفظ نظم اجتماعی ایجاد کند. درواقع قانون اسـاسـی با تأکید بر پیشگیری از جرم

نشـان می‌دهد که سـیاسـت جنایی جمهوری اسـلامی ایران تنها بر مجازات مجرمان تمرکز ندارد، بلکه تلاش می‌کند با اتخاذ تدابیر مناسب از وقوع جرم نیز جلوگیری کند.

این هماهنگی میان مبانی فقهی و مقررات قانون اساسی نشان‌دهندهٔ آن است که سیاست جنایی جمهوری اسـلامی ایران بر پایهٔ اصـول اسـلامی شکل گرفته است. در این سیاست جنایی، اصلاح فرد و جـامعـه در کنـار اعمـال مجازات مورد توجه قرار دارد. به همین دلیل می‌توان گفت که بند ۵ اصـل ۱۵۶ قانون اساسی درواقع بازتابی از آموزه‌های فقه اسلامی دربارهٔ ضرورت پیشگیری از جرم و حفظ سلامت جامعه است (فیض، ۱۳۷۵: ۱۹۵).

٤-۳. چالش‌های اجرای پیشگیری

با وجود تأکید قانون اسـاسـی بر پیشـگیری از جرم، اجرای مؤثر این اصـل در عمل با چالش‌های مختلفی روبـه‌روسـت. یکی از مهم‌ترین این چالش‌ها نبود هماهنگی کافی میان نهادهای مختلف مسـئول در حوزهٔ پیشـگیری از جرم اسـت. پیشگیری از جرم موضوعی چند بعدی است که نیازمند همکـاری نهـادهای مختلف اجتماعی، فرهنگی و اجرایی اسـت. در صـورتی که میان این نهادها هماهنگی لازم وجود نداشته باشد، اجرای سیاست‌های پیشگیرانه با مشکلات جدی مواجه خواهد شد.

چالش دیگر در این زمینه محدود بودن امکانات و منابع لازم برای اجرای برنامه‌های پیشـگیرانه اسـت. پیشگیری از جرم نیازمند برنامه‌ریزی دقیق، آموزش عمومی و اجرای سیاست‌های اجتماعی گسـترده اسـت که تحقق آن‌ها مستلزم اختصاص منابع کافی است. در بسیاری از موارد تمرکز نظام عدالت کیفری بیشـتر بر رسـیدگی به جرائم پس از وقوع آن‌هاسـت و اقدامات پیشگیرانه کمتر مورد توجه قرار می‌گیرد. این مسئله می‌تواند موجب کاهش کارایی سیاست‌های پیشگیرانه شود.

از سـوی دیگر آگـاهی ناکافی برخی از افراد جامعه نسـبت به اهمیت پیشـگیری از جرم نیز می‌تواند مانعی در مسـیر اجرای این سیاست‌ها باشد. برای تحقق پیشگیری مؤثر از جرم لازم است فرهنگ قانون‌مداری و مسئولیت اجتماعی در جامعه تقویت شود. در صورتی که افراد جامعه نسبت به نقش خود در حفظ نظم اجتماعی آگاهی نداشـته باشند، اجرای برنامه‌های پیشگیرانه با دشواری بیشـتری روبه‌رو خواهد شد. بنابراین لازم است علاوه بر تقویت نهادهای مسئول، اقدامات فرهنگی

و آموزشی گسترده‌ای نیز در این زمینه انجام شود تا سیاست‌های پیشگیری از جرم بتوانند به‌طور مؤثر در جامعه اجرا شوند (رستمی، ۱۳۹۰: ۱۱۰).

نتیجه‌گیری

پیشگیری از جرم یکی از مهم‌ترین موضوعات در سیاست جنایی معاصر است و در بسیاری از نظام‌های حقوقی به‌عنوان راهکاری مؤثر برای کاهش بزهکاری مورد توجه قرار گرفته است. بررسی مبانی فقهی پیشگیری از جرم نشان می‌دهد که این مفهوم در اندیشهٔ اسلامی سابقه‌ای طولانی دارد و بسیاری از آموزه‌های دینی در جهت جلوگیری از گسترش فساد و انحراف در جامعه بیان شده‌اند. در منابع اسلامی به‌ویژه قرآن کریم و سنت پیامبر و ائمهٔ اطهار، تأکید فراوانی بر اصلاح فرد، تقویت ارزش‌های اخلاقی، مسئولیت اجتماعی و نظارت عمومی دیده می‌شود. این آموزه‌ها نشان می‌دهند که اسلام تنها به مجازات مجرمان پس از وقوع جرم توجه ندارد، بلکه تلاش می‌کند با اصلاح شرایط فردی و اجتماعی از بروز رفتارهای مجرمانه جلوگیری کند. درواقع در اندیشهٔ اسلامی پیشگیری از جرم جایگاهی اساسی دارد و به‌عنوان یکی از مهم‌ترین ابزارهای حفظ نظم و سلامت جامعه شناخته می‌شود.

بررسی مبانی فقهی پیشگیری از جرم نشان می‌دهد که در اسلام مجموعه‌ای از عوامل فردی، اخلاقی و اجتماعی برای جلوگیری از بروز جرم مورد توجه قرار گرفته است. اصلاح فرد از طریق تربیت اخلاقی، تقویت ایمان و پرورش فضایل انسانی ازجمله مهم‌ترین این عوامل است. همچنین آموزه‌هایی مانند امر به معروف و نهی از منکر و تأکید بر مسئولیت اجتماعی افراد جامعه نقش مهمی در ایجاد نوعی نظارت عمومی دارند که می‌تواند از گسترش رفتارهای ناهنجار جلوگیری کند. در کنار این عوامل، نقش نهادهای اجتماعی مانند خانواده، جامعه و حکومت نیز در پیشگیری از جرم بسیار مهم است. این نهادها با ایجاد محیطی سالم و مبتنی بر ارزش‌های اخلاقی می‌توانند زمینه‌های ارتکاب جرم را کاهش دهند و از بروز بسیاری از انحرافات اجتماعی جلوگیری کنند.

در نظام حقوقی جمهوری اسلامی ایران نیز پیشگیری از جرم مورد توجه قرار گرفته و در مهم‌ترین سند حقوقی کشور یعنی قانون اساسی جایگاه ویژه‌ای یافته است. اصل ۱۵۶ قانون اساسی وظایف قوهٔ قضائیه را بیان می‌کند و در بند پنجم این اصل بر اقدام مناسب برای پیشگیری از وقوع جرم و اصلاح مجرمان تأکید شده است. درج چنین وظیفه‌ای در قانون اساسی نشان‌دهندهٔ آن

است که قانونگذار اهمیت زیادی برای پیشگیری از جرم قائل بوده و آن را یکی از وظایف اساسی دستگاه قضائی دانسته است. این امر بیانگر آن است که سیاست جنایی جمهوری اسلامی ایران صرفاً بر مجازات مجرمان تمرکز ندارد، بلکه تلاش می‌کند با اتخاذ تدابیر مناسب از وقوع جرم نیز جلوگیری کند.

از سوی دیگر بررسی بند پنجم اصل ۱۵۶ نشان می‌دهد که میان مبانی فقهی اسلام و مقررات قانون اساسی هماهنگی قابل توجهی وجود دارد. در فقه اسلامی نیز همواره بر اصلاح فرد و جامعه و جلوگیری از گسترش فساد تأکید شده است. بنابراین می‌توان گفت که پیشگیری از جرم در قانون اساسی جمهوری اسلامی ایران درواقع انعکاسی از آموزه‌های اسلامی دربارهٔ حفظ نظم اجتماعی و جلوگیری از انحرافات است. این هماهنگی میان مبانی فقهی و مقررات قانونی می‌تواند زمینهٔ مناسبی برای توسعهٔ سیاست‌های پیشگیرانه در نظام حقوقی کشور فراهم کند.

با وجود این، تحقق کامل اهداف پیشگیری از جرم نیازمند تقویت سیاست‌های پیشگیرانه در سطح جامعه است. پیشگیری از جرم موضوعی چند بعدی است که تنها با اقدامات قضائی تحقق پیدا نمی‌کند، بلکه نیازمند همکاری نهادهای مختلف اجتماعی، فرهنگی و اجرایی است. برای دستیابی به این هدف لازم است علاوه بر تقویت نقش قوهٔ قضائیه، سایر نهادهای اجتماعی نیز در زمینهٔ پیشگیری از جرم مشارکت فعال داشته باشند. آموزش عمومی، تقویت ارزش‌های اخلاقی، ارتقای فرهنگ قانون‌مداری و ایجاد هماهنگی میان نهادهای مختلف ازجمله اقداماتی هستند که می‌توانند در جهت کاهش بزهکاری در جامعه مؤثر باشند.

درنهایت می‌توان گفت که پیشگیری از جرم یکی از مهم‌ترین راهکارهای تأمین امنیت اجتماعی و حفظ نظم عمومی در جامعه است. اندیشهٔ اسلامی با تأکید بر اصلاح فرد و جامعه، زمینه‌های نظری لازم برای توسعهٔ سیاست‌های پیشگیرانه را فراهم کرده و قانون اساسی جمهوری اسلامی ایران نیز با توجه به این مبانی، پیشگیری از جرم را به‌عنوان یکی از وظایف اساسی قوهٔ قضائیه مطرح ساخته است. از این رو تقویت سیاست‌های پیشگیرانه و گسترش اقدامات اجتماعی و فرهنگی در این زمینه می‌تواند نقش مهمی در کاهش جرائم و ایجاد جامعه‌ای سالم و امن ایفا کند.

حامی مالی:

این مقاله هیچ حامی مالی ندارد.

مشارکت نویسندگان:

سید محمد مهدی احمدی و علیرضا عسگری: مفهوم‌سازی، نظارت بر داده‌ها، اعتبارسنجی، مدیریت پروژه، منابع.

طهورا نوروزی: روش‌شناسی، تحلیل، نوشتن بررسی و ویرایش، تحقیق و بررسی، پیش‌نویس اصلی.

تعارض منافع:

بنا بر اظهار نویسندگان این مقاله تعارض منافع ندارد.

ملاحظات اخلاقی:

این پژوهش بر پایهٔ مطالعهٔ اسناد، قوانین، رویه‌های قضائی و منابع کتابخانه‌ای انجام شده و در آن هیچ‌گونه مطالعه‌ای بر روی انسان، حیوان یا داده‌های شخصی صورت نگرفته است؛ بنابراین، اخذ تأییدیه کمیتهٔ اخلاق برای این پژوهش ضروری نبوده است. با این حال، نویسنده اصول امانت‌داری علمی، صداقت پژوهشی، استناددهی صحیح و رعایت حقوق مالکیت فکری را در تمامی مراحل پژوهش رعایت کرده است.

در تهیهٔ این مقاله از ابزارهای هوش مصنوعی مولد صرفاً برای کمک به ویرایش زبانی، بهبود ساختار نگارش و ارتقای خوانایی متن استفاده شده است. این ابزارها در طراحی پژوهش، تحلیل علمی، تفسیر یافته‌ها، استنتاج نتایج یا تصمیم‌گیری‌های پژوهشی نقشی نداشته‌اند و مسئولیت کامل صحت، اصالت و محتوای نهایی مقاله بر عهده نویسنده/نویسندگان است.

موافقت نویسندگان:

تمامی نویسندگان نسخه نهایی مقاله را مطالعه و تأیید کرده‌اند و با انتشار آن موافقت دارند.

منابع

قرآن کریم.

ابن خلدون، عبدالرحمن (۱۳۶۳)، مقدمهٔ ابن خلدون، ترجمهٔ محمد پروین گنابادی، تهران: نگاه نشر و ترجمهٔ کتاب.

اردبیلی، محمدعلی (۱۳۹۰)، حقوق جزای عمومی، جلد اول، تهران: میزان.

حبیب‌زاده، محمدجعفر (۱۳۹۱)، بزه‌دیده‌شناسی و سیاست جنایی، تهران: میزان.

حسینی، سیدمحمد (۱۳۹۲)، سیاست جنایی تقنینی در جمهوری اسلامی ایران، تهران: میزان.

ره‌پیک، احمد (۱۳۹۰)، مبانی فقهی حقوق جزا، قم: پژوهشگاه حوزه و دانشگاه.

رستمی، محمد (۱۳۹۰)، سیاست حبس‌زدایی در حقوق کیفری ایران، تهران: میزان.

سلیمی، حسین (۱۳۸۸)، پیشگیری از جرم، تهران: میزان.

عبدالقادر عوده (۱۳۷۶)، التشریع الجنائی الاسلامی، ترجمهٔ اکبر غفوری، تهران: میزان،

عمید زنجانی، عباسعلی (۱۳۸۵)، حقوق اساسی جمهوری اسلامی ایران، تهران: سمت.

فیض، علی‌رضا (۱۳۷۵)، مقارنه و تطبیق در حقوق جزای عمومی اسلام، تهران: وزارت فرهنگ و ارشاد اسلامی.

کلینی، محمد بن یعقوب (۱۳۶۵)، الکافی، تهران: دارالکتب الاسلامیه.

ماوردی، ابوالحسن علی بن محمد (۱۳۸۶ق)، الأحکام السلطانیة والولایات الدینیة، چاپ دوم، قاهره: شرکت کتابخانه و چاپخانهٔ مصطفی البابی الحلبی و اولاد.

نجفی ابرندآبادی، علی‌حسین (۱۳۹۲)، سیاست جنایی، تهران: میزان.

هاشمی، سید محمد (۱۳۹۰)، حقوق اساسی جمهوری اسلامی ایران، جلد دوم، تهران: میزان.

جوادی آملی، عبدالله (۱۳۸۵)، تفسیر تسنیم، قم: اسراء.

مکارم شیرازی، ناصر (۱۳۸۶)، تفسیر پیام قرآن، قم: مدرسهٔ الامام علی بن ابی طالب.

قانون اساسی جمهوری اسلامی ایران.

پژوهشکده نوآوری حقوقی

Legal Innovation Quarterly

Spring 2026 | Volume 2 | Issue 3

List of articles

➢ **Criminalization of Emerging Threats Arising from Artificial Intelligence: An Analysis of the Challenges and Legislative Solutions**
Saeed Ghomashi, Mohammad Reza Kameli, Mojtaba Nikokalam Nadim 1

➢ **Invisible Murder: Assessing the Possibility of Attributing Murder in Deaths Resulting from Psychological Pressure, Sustained Humiliation, and Driving a Victim to Suicide**
Zeynab Bagherinejad, Milad Chakav, Marjan Mahram 55

➢ **A Comparative Analysis of the Right to Privacy of Children in the Age of Artificial Intelligence and the Digital Environment in the Legal Systems of Iran and Canada**
Mansooreh Hosseini, Mojtaba Farahmand 83

➢ **Artificial Intelligence and Criminal Justice Processes: Manifestations and Applications**

Majid Ghourchibeigi, Ghulamali Andishwar 107

➢ **Iran's Criminal Policy on Digital Violence Against Women's Mental Health: With Reference to the World Health Organization's Approach**
Jamal Beigi, Zahra Eghbali 135

➢ **A Jurisprudential Examination of Crime Prevention and Punishment, with Emphasis on Clause 5 of Article 156 of the Constitution of the Islamic Republic of Iran**

Tahora Norozi, Sayid Mohamad Mahdi Ahmadi, Ali Reza Asgari 161