Legal Research, Vol 29, Issue 115, 2026: 131-154 Print ISSN: 1024-0772 Online ISSN: 3060-5911

Journal of Legal Research
https://lawresearchmagazine.sbu.ac.ir/

Orginal Article

Capacities and Challenges of AI-Based Video Surveillance Systems in Situational Crime Prevention; Under the European Union Artificial Intelligence Act of 2024

Amir Hassan Niazpour[1], Mostafa Taqavi[2], Shima Shafiee[3]

Highlights

- AI-based video surveillance systems can strengthen the capacity of situational crime prevention by enabling early intervention.
- The preventive use of these systems requires adherence to the rule of law, proportionality, fundamental rights and freedoms, privacy, transparency, accountability, and human oversight.
- The European Union Artificial Intelligence Act of 2024 imposes stringent restrictions on certain applications of AI-based video surveillance systems, while several other capabilities remain in need of supplementary rules and safeguards.

ABSTRACT

Introduction

Recent developments in artificial intelligence (AI) have provided new instruments for strengthening crime prevention. Among them, AI-based video surveillance systems—a combination of CCTV cameras and video analytics algorithms—play a prominent role in governing public spaces and advancing the goals of situational crime prevention. By relying on capabilities such as facial recognition, person and object tracking, abandoned-object detection, suspicious-behavior detection, emotion recognition, and crowd anomaly detection, these systems can reduce opportunities for a wide range of crimes, from theft and vandalism to violent and terrorist offenses. At the same time, these capacities may generate serious risks for fundamental rights and freedoms, privacy, the rule of law, and the presumption of innocence, potentially fostering mass surveillance and diminishing public trust. Accordingly, this article pursues three objectives. First, it offers an innovative account of the preventive capacities of AI-based video surveillance systems across four categories: scene-oriented monitoring, identity-oriented monitoring, individual-oriented monitoring, and crowd-oriented monitoring. This fourfold classification is significant because, although these capacities all operate within the broader framework of video surveillance, they differ in terms of the subject matter of processing, the degree of interference with individual rights, and their preventive functions; therefore, they cannot be subjected to a uniform legal response. Second, it analyzes the

How to Cite: Niazpour, Amir Hassan, Taqavi, Mostafa, Shafiee, Shima, "Capacities and Challenges of AI-Based Video Surveillance Systems in Situational Crime Prevention; Under the European Union Artificial Intelligence Act of 2024 ", Legal Research, Vol. 29, No. 115, 2026, pp: 131-154.

DOI: https://doi.org/10.48308/jlr.2026.243090.3027 Received: 13/01/2026-Accepted: 18/03/2026

1. Associate Professor, Faculty of Law, Shahid Beheshti University, Tehran, Iran
2. Associate Professor, Department of Philosophy of Science, Sharif University of Technology, Tehran, Iran
3. PhD Candidate, Faculty of Law, Shahid Beheshti University, Tehran, Iran
Corresponding Author Email: s_shafiee@sbu.ac.ir

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

corresponding socio-legal challenges. Finally, it evaluates the legal status of each capacity in light of the risk-based approach adopted by the European Union Artificial Intelligence Act (EU AI Act) of 2024.

Methods
This study is descriptive–analytical and adopts an interdisciplinary approach, focusing simultaneously on the technical foundations of AI-based video surveillance systems and the principles of crime prevention. First, the preventive capacities are classified based on the purpose of processing—ranging from situational and pattern monitoring to identity recognition and crowd analysis. Second, the challenges are identified and examined in five main areas: 1) the rule of law, 2) the principle of proportionality, 3) fundamental freedoms, 4) privacy, 5) institutional accountability, including the necessity of human oversight. In the final step, these capacities and challenges are mapped onto the EU AI Act's risk-based logic to clarify which uses—given the impacts on fundamental rights—fall under prohibitions, strict restrictions, or high-risk system obligations, and which governance mechanisms are required to control their risks. In this analysis, in addition to the technical function of each capacity, its relationship with the objectives of situational crime prevention and its reliance on personal, biometric, or behavioral data are also taken into consideration. Furthermore, in determining their legal status, a distinction is drawn between capacities that are explicitly addressed by the EU AI Act and those that fall only indirectly within the Act's general provisions.

Results and Discussion
The findings indicate that the development of the technical capacities of AI-based video surveillance systems and the real-time processing of data enable these systems to transform ongoing data into alerts and preventive interventions in real time, thereby thereby narrowing the gap between observation, analysis, and preventive action. These capacities can reinforce the core logic of situational crime prevention—namely, increasing risk for potential offenders, increasing effort, reducing rewards, and reducing provocations. However, their legitimacy and effectiveness depend on the quality of regulation and institutional design. In scene-oriented monitoring, person/object tracking and abandoned-object detection enable early warnings regarding intrusions into restricted areas, suspicious stops, or hazardous items. Yet, false positives and false negatives, together with technical constraints (e.g., occlusion, crowd density, lighting variation), may trigger unnecessary preventive interventions. In identity-oriented monitoring, facial recognition—especially when deployed in real time and at a distance—may enhance deterrence and facilitate targeted control of high-risk individuals. Conversely, because it processes biometric data, it heightens risks of discrimination, misidentification, and privacy infringement; moreover, by weakening the presumption of innocence and the rule of law, it may contribute to transforming citizens into "permanent suspects." In individual-oriented monitoring, detecting suspicious or violent behavior can support minimal, situational interventions; nevertheless, distinguishing ordinary behavior from crime-relevant conduct remains persistently difficult. Emotion recognition, as a branch of affective computing (emotional AI), is even more contested in terms of scientific foundation and reliability for preventive purposes, and is particularly vulnerable to undermining human dignity. Finally, crowd-oriented monitoring, through crowd anomaly detection without individual identification, may be useful for congestion management and for reducing criminal opportunities in high-density environments; however, in the absence of clear criteria, it may still lead to group labeling and the normalization of mass surveillance. From a legal perspective, the article argues that responding to these challenges requires a combination of strict enforcement of proportionality (suitability, necessity, and proportionality in a strict sense), strengthening the presumption of innocence, protecting fundamental freedoms and privacy, limiting the scope of surveillance, ensuring transparency and prohibiting covert surveillance, institutionalizing accountability and integrating implementing human oversight. Under the EU AI Act (2024), a substantial share of security-related uses involving biometric recognition are treated as high-risk and must therefore comply with enhanced requirements for risk management, data quality, documentation, event logging, human oversight, and mechanisms for accountability and contestation. By contrast, lower-risk uses may be pursued with fewer legal constraints if the above principles are respected. Nevertheless, the Act does not explicitly address certain AI-based capabilities, potentially leaving gaps in legal protection and oversight for individuals' rights and freedoms.

Conclusion
In conclusion, AI-based video surveillance systems can be an important tool for situational crime prevention, but only when deployed within a clear legal framework and strict institutional controls designed to uphold the rule of law, the presumption of innocence, proportionality, privacy protection, and human oversight. Otherwise, the same preventive capacities may become a threat to fundamental freedoms and human dignity, thereby undermining the legitimacy and effectiveness of crime prevention governance.

Keywords: Crime Prevention, Situational Crime Prevention, Video Surveillance System, Artificial Intelligence (AI), Video Analytics**.**

فصلنامه تحقیقات حقوقی
https://lawresearchmagazine.sbu.ac.ir/

مقاله علمی-پژوهشی

ظرفیت‌ها و چالش‌های سامانه‌های نظارت تصویری هوش‌بنیان در پیشگیری موقعیت‌مدار از جرم؛ در پرتو قانون هوش مصنوعی اتحادیه اروپا مصوب ۲۰۲۴

امیرحسن نیازپور[۱]، مصطفی تقوی[۲]، شیما شفیعی[۳]

نکات برجسته

- سامانه‌های نظارت‌تصویری هوش‌بنیان می‌توانند با فراهم آوردن امکان مداخله زودهنگام، ظرفیت پیشگیری موقعیت‌مدار از جرم را تقویت نمایند.
- کاربست پیشگیرانه این سامانه‌ها مستلزم رعایت حاکمیت قانون، تناسب، حقوق و آزادی‌های بنیادین، حریم خصوصی، شفافیت، مسئولیت‌پذیری و نظارت انسانی است.
- قانون هوش مصنوعی اتحادیه اروپا مصوب ۲۰۲۴ برای برخی کاربردهای سامانه‌های نظارت تصویری هوش‌بنیان محدودیت‌های سخت‌گیرانه مقرر نموده، اما شماری دیگر از ظرفیت‌ها همچنان نیازمند قواعد و سازوکارهای تکمیلی‌اند.

چکیده

تحولات عرصهٔ هوش‌مصنوعی، امکانات و ابزارهای نوین متعددی را برای تقویت برسازهٔ پیشگیری از جرم فراهم آورده است.از مهم‌ترین این ابزارها، سامانه‌های نظارت تصویری هوش‌بنیان است که با تلفیق دوربین‌های مداربسته و الگوریتم‌های تحلیل تصویر پیشرفته، نقش برجسته‌ای در مدیریت فضاهای عمومی از طریق پیشگیری موقعیت‌مدار از جرم ایفا می‌کند. این سامانه‌ها با بهره‌گیری از فناوری‌هایی نظیر شناسایی چهره، تحلیل رفتار و احساسات، ردیابی اشخاص و اشیا و تشخیص ناهنجاری‌های جمعی، از ظرفیت پیشگیری از جرائم متعددی مانند سرقت، خراب‌کاری، جرائم تروریستی، کودک‌ربایی، جرائم خشونت‌آمیز و... برخوردارند. این نوشتار با رویکردی توصیفی تحلیلی و با تمرکز بر ابعاد فنی و حقوقی، به بررسی ظرفیت‌های پیشگیرانه سامانه‌های نظارت تصویری هوش‌بنیان پرداخته و پس از تحلیل چالش‌های حقوقی آن، هریک را با رویکرد ریسک‌محورِ نخستین هنجارِ بایدی در این پهنه، یعنی قانون هوش‌مصنوعی اتحادیه اروپا مصوب ۲۰۲۴میلادی، تطبیق می‌دهد. یافته‌های این پژوهش نشان می‌دهد که به‌کارگیری این فناوری، ضمن کاهش فرصت‌های ارتکاب جرم، می‌تواند ابزاری مهم برای پیشگیری موقعیت‌مدار از جرائم به‌شمار رود؛ مشروط بر آنکه الزامات حقوقی، ساختاری و اجرایی با هدف حفاظت از کرامت انسانی و حقوق و آزادی‌های فردی و جمعی، مورد توجه نهادهای مسئول قرار گیرد.

کلید واژگان: پیشگیری از جرم، پیشگیری موقعیت‌مدار از جرم، سامانه نظارت تصویری، هوش مصنوعی، تحلیل تصویر.

استناد به این مقاله: امیرحسن، نیازپور، تقوی، مصطفی، شفیعی، شیما، «ظرفیت‌ها و چالش‌های سامانه‌های نظارت تصویری هوش‌بنیان در پیشگیری موقعیت‌مدار از جرم؛ در پرتو قانون هوش مصنوعی اتحادیه اروپا مصوب ۲۰۲۴»، فصلنامه تحقیقات حقوقی، دوره ۲۹، شماره ۱۱۵، مهر ۱۴۰۵، صص: ۱۳۱-۱۵۴.

تاریخ دریافت: ۱۴۰۴/۱۰/۲۳ - تاریخ پذیرش: ۱۴۰۴/۱۲/۲۷ DOI: https://doi.org/10.48308/jlr.2026.243090.3027

۱. دانشیار، دانشکده حقوق، دانشگاه شهید بهشتی، تهران، ایران
۲. دانشیار، گروه فلسفه علم، دانشگاه صنعتی شریف، تهران، ایران
۳. دانشجوی دکتری، دانشکده حقوق، دانشگاه شهید بهشتی، تهران، ایران
ایمیل نویسنده مسئول: s_shafiee@sbu.ac.ir

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

مقدمه

در سال‌های اخیر، بخش گسترده‌ای از مباحث حقوق کیفری و جرم‌شناختی به پیشگیری کنشی از جرم اختصاص یافته است، زیرا با افزایش پیچیدگی و شمار جرائم و هزینه‌های اجتماعی و اقتصادی مقابله با آنها، تردیدهای بسیاری درخصوص کارکرد مثبت تدابیر واکنشی پدید آمده است. ازاین‌رو، سیاست‌گذاران جنایی به بهره‌گیری از سازوکارهای پیشگیرانه توجه جدی نشان داده‌اند. پیشگیری موقعیت‌مدار[1] یکی از شاخه‌های پیشگیری از جرم است که از طریق مجموعه‌ای از اقدامات غیرکیفری و با تمرکز بر وضعیت‌های پیشاجنایی، در پی کاستن از فرصت‌های ارتکاب جرم از طریق افزایش خطر، دشوارسازی فرایند، کاهش منافع و کاهش عوامل تحریک و انگیزش ارتکاب جرم برمی‌آید.[2و 3]

این عرصه نیز امروزه تحت‌تأثیر هوش‌مصنوعی قرار گرفته و ناگزیر است برای حفظ کارایی خود از ظرفیت‌های این فناوری بهره برد. سامانه‌های نظارت تصویری هوش‌بنیان[4] که از دوربین‌های مداربسته[5] و الگوریتم‌های تحلیل تصویر[6] تشکیل شده‌اند، نمونهٔ مهمی از کاربست هوش‌مصنوعی در عرصهٔ پیشگیری موقعیت‌مدار از جرم است که امکان نظارت بر فضاهای عمومی را فراهم می‌گرداند.

در دهه اول قرن ۲۱ میلادی، الگوریتم‌های تحلیل تصویر مبتنی‌بر هوش‌مصنوعی، به‌تدریج به سامانه‌های نظارت تصویری راه یافتند و شیوهٔ کار آنها را تغییر دادند. با توسعه شاخه‌های یادگیری ماشین[7] و یادگیری عمیق[8]، الگوهای هوش مصنوعی[9] توانستند قواعد و روابط پنهان میان داده‌ها را کشف کنند و با یادگیری و اصلاح پیاپی، عملکرد خود را ارتقا بخشند. همچنین، شاخه بینایی کامپیوتر[10] نیز توسعه یافت و به بینایی‌شناختی[11] ارتقا پیدا کرد؛ سطحی از تحلیل که در آن، الگوریتم‌ها علاوه‌بر شناسایی ابژه‌ها، قادر به درک کنش‌های انسانی و تعاملات پیچیده میان اجزای تصویر شدند و توانستند با تکیه بر ظرفیت بالای خود برای تطبیق با محیط‌های غیرقابل پیش‌بینی، پویا و پیچیده، واکنش‌های هوشمندانه و متناسب ارائه دهند. این پیشرفت‌ها هوش‌مصنوعی را به بخش جدایی‌ناپذیر سامانه‌های نظارت تصویری تبدیل کرد، امکان اجرای پروژه‌های دشوارتر را فراهم آورد و سامانه‌ها را قادر به انجام وظیفه در شرایط پیچیدهٔ واقعی نمود.

در نظام‌های عدالت کیفری، سامانه‌های نظارت تصویری عموماً ماهیتی واکنشی داشته و با هدف دستگیری مجرمان مورد استفاده قرار می‌گیرند. در مقابل، گفتمان پیشگیرانه بر منصرف کردن مجرم از ارتکاب جرم در فرایند گذار از اندیشه به عمل، متمرکز است. در این چارچوب، سامانه‌های نظارت تصویری نه امکان فیزیکی ارتکاب جرم را از میان می‌برند و نه

---

1. Situational Crime Prevention

2. Clarke, R. V. "Situational Crime Prevention:Its Theoretical Basis and Practical Scope", *Crime and Justice: A Review of Research, University of Chicago Press*, Vol 4, 1983, p.225.

۳. نیازپور، امیرحسن، ***پیشگیری از جرم***، تهران: دادگستر، چاپ دوم، ۱۴۰۰، صص۱۸۶-۲۰۲.

4. AI-Based

5. Closed-Circuit Television (CCTV)

6. Video Analytics

7. Machine Learning

8. Deep Learning

۹. در این نوشتار، عبارت الگوی هوش مصنوعی معادل عبارت انگلیسی AI Model به‌کارگرفته شده است.

10. Computer Vision

11. Cognitive Vision

مانع وقوع مطلق آن می‌شوند، بلکه با بیدار کردن سازوکار ادراکی مجرم و تغییر برآورد او از میزان خطر و احتمال دستگیری، فرایند ارتکاب جرم را دشوار می‌کنند و این‌گونه از شمار جرائم می‌کاهند.[۱و۲]

برای دسترسی به این هدف، لازم است که با استفاده از دوربین‌های مشاهده‌پذیر و اعلام نظارت بر محدوده، اشخاص را از تحت‌نظارت بودن خود، آگاه کرد؛ البته، باید با برقراری تعادل میان اطلاع‌رسانی نظارت، عمومی‌سازی توانمندی‌های بازدارنده و امنیت عملیاتی سامانه‌ها، اثربخشی آنها را تضمین کرد.[۳]

سامانه‌های نظارت تصویری هوش بنیان، از ظرفیت‌های پیشگیرانه‌ای مانند تشخیص چهره، ردیابی افراد و اشیا، تحلیل رفتار و احساسات، تشخیص وضعیت‌های ناهنجار و مخاطره‌آمیز برخوردارند، اما استفاده از این سامانه‌ها توسط دولت‌ها، سازمان‌ها و حتی اشخاص حقیقی، با چالش‌هایی نیز همراه است که می‌تواند حقوق و آزادی‌های مدنی را به‌شدت تهدید کند و شهروندان را در معرض خطر نظارت فراگیر[۴] قرار دهد.

با گسترش استفاده از این سامانه‌ها[۵]، ضرورت وجود چارچوب‌های دقیق و روشن قانونی که چگونگی استفاده از هوش‌مصنوعی را مدیریت کند، بیش از پیش احساس شده و کشورها و نهادهای بین‌المللی جهت حفظ حقوق و آزادی‌های افراد و جوامع، ناگزیر از قاعده‌مندسازی این حوزه هستند. قوانین موجود عمدتاً به‌دلیل سرعت بالای پیشرفت فناوری و پیچیدگی آن، ابهامات برآمده از نو بودن مفاهیم، سرعت پایین قانونگذاری و ناآگاهی یا توجه نداشتن قانونگذاران نسبت به اهمیت موضوع، با کاستی‌های فراوانی روبه‌رو است. در این میان، اگرچه می‌توان به دستورالعمل‌های ارشادی ملی[۶] و بین‌المللی[۷] اشاره کرد، قانون هوش‌مصنوعی[۸] اتحادیه اروپا مصوب ۲۰۲۴ میلادی، نخستین سند جامع الزام‌آور در این عرصه است که به قاعده‌مندسازی شماری از ظرفیت‌های هوش‌مصنوعی و سامانه‌های نظارت تصویری هوش‌بنیان پرداخته است.

پرسش بنیادین آن است که سامانه‌های نظارت تصویری هوش‌بنیان در چارچوب پیشگیری موقعیت‌مدار از جرم، از چه ظرفیت‌هایی برخوردارند، با چه چالش‌هایی مواجه‌اند و وضعیت آنان در بستر نظام حقوقی چیست؟ این نوشتار با رویکردی

---

1. Ratcliffe, Jerry,"Video Surveillance of Public Places (Problem-Oriented Guides for Police.Response Guide Series.Guide No.4)", *U.S.Department of Justice Office of Community Oriented Policing Services*, Washington, DC: Center for Problem-Oriented Policing, 2006, p.13.

2. Welsh, B. C., and D. P. Farrington. "Surveillance for Crime Prevention in Public Space: Results and Policy Choices in Britain and America", *Criminology and Public Policy,* Vol 3, Issue 3, 2004, p.501.

3. Johnson, T. L., N. N. Johnson, V. Topalli, D. McCurdy, and A. Wallace, "Police Facial Recognition Applications and Violent Crime Control in U.S. Cities", *Cities*, Vol 155, 2024, p.12.

4. Mass Surveillance

۵. براساس آمارهای غیررسمی در سال۲۰۲۵، تعداد دوربین‌های نظارتی در سطح جهان حدود یک‌میلیارد عدد تخمین زده شده که سهم چین و آمریکا از این آمار، به‌ترتیب دویست‌میلیون و پنجاه‌میلیون دوربین برآورد شده است.https://www.fortunebusinessinsights.com/cctv-camera-market-107115

۶. سند ملی هوش‌مصنوعی ایران مصوب۱۴۰۳، اولین سند داخلی در این عرصه است که به بیان شماری‌از اولویت‌ها، اصول و اهداف کلی ازجمله ایجاد و توسعه زیرساخت‌های حقوقی، مالکیت فکری و پردازش داده جهت شتاب‌دهی به پیشرفت هوش‌مصنوعی و کاربردی‌سازی آن می‌پردازد.

۷. سازمان ملل متحد در مارس ۲۰۲۴، قطعنامه‌ای باعنوان Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development به‌تصویب رساند و نیز گزارشی با عنوان Governing AI for Humanity منتشر نمود. در سال۲۰۲۱ نیز سندی با عنوانUNESCO Recommendation on the Ethics of AI توسط این سازمان تهیه گردید.

8. Artificial Intelligence ACT (AI ACT), 2024.

توصیفی - تحلیلی، پس از تبیین نوآورانهٔ ظرفیت‌های پیشگیرانه سامانه‌ها در قالب چهاردسته جداگانه (بند اول)، به بررسی چالش‌های حقوقی و اجتماعی کاربست سامانه‌های مذکور می‌پردازد (بند دوم) و سپس، وضعیت حقوقی هر ظرفیت را با تمرکز بر قانون هوش‌مصنوعی۲۰۲۴ مطالعه می‌کند.

۱. ظرفیت‌های پیشگیرانه سامانه‌های نظارت تصویری هوش‌بنیان

سامانه‌های نظارت تصویری هوش‌بنیان، به‌عنوان ابزاری مهم برای پیشگیری موقعیت‌مدار از جرم، با رصد مداوم فضاهای عمومی می‌توانند به‌طور محسوس بر احتمال شناسایی، تعقیب و دستگیری بزهکاران بیفزایند و تصمیم آنان را برای ارتکاب جرم تحت تأثیر قرار دهند. به‌ویژه آنکه توسعهٔ پردازش بی‌درنگ[1] به‌معنای دریافت و تحلیل هم‌زمان داده‌های زنده در لحظهٔ وقوع، پیشگیری موقعیت‌مدار از جرم را وارد مسیر تازه‌ای کرد و فرصت‌های تازه‌ای در اختیار آن قرار داد. در ادامه، مهم‌ترینِ این ظرفیت‌ها ذیل چهار دستهٔ پایش موقعیت‌محور، هویت‌محور، فردمحور و جمعیت‌محور بررسی می‌شود.

۱. ۱. پایش موقعیت‌محور؛ ردیابی موضوع[2] و تشخیص اشیای رهاشده[3]

با پیشرفت پرشتاب یادگیری عمیق و شبکه‌های عصبی در عرصه بینایی کامپیوتر، ردیابیِ موضوع به یکی از ظرفیت‌هایی مهم و پیچیده سامانه‌های نظارت تصویری تبدیل شده است. در گذشته، الگوهای تک‌موضوعی[4] تنها قادر به ردیابی یک سوژهٔ مشخص بودند؛ اما به‌تدریج، الگوهای نویافتهٔ ردیابی چندموضوعی[5] امکان رهگیری تصویری چندین سوژه را به‌طور هم‌زمان فراهم آوردند. در الگوهای پیشرفته‌تر[6]، امکان شناسایی و تطبیق سوژه‌ها در تصاویری که هم‌زمان از دوربین‌هایی با زوایای گوناگون دریافت می‌شد، فراهم آمد و سطح تحلیل ارتقا یافت.[7] این ظرفیت‌ها به مجریان قانون اجازه می‌دهد که با تحلیل موقعیت، مسیر و نحوه حرکت اشخاص و اشیا و تحلیل روابط میان آنان، به پیش‌بینی وقوع جرم و اعمال تدابیر پیشگیرانه جهت ارتقای امنیت محدودهٔ تحت نظارت بپردازند.

البته این نظارت تصویری همچنان با چالش‌های متعددی از قبیل انسداد[8]، تغییر شکل هدف، تارشدگی، ازدحام شدید، تغییر نور و عدم تشخیص اشیای مشابه مواجه است.[9] محققان برای رفع این چالش‌ها، علاوه‌بر ارتقای نرم‌افزاری و سخت‌افزاری سامانه‌ها، شماری از روش‌های چندوجهی[10] که داده‌های تصویری را با سایر داده‌ها ازجمله متن، صدا، اشعه

---

1. Real-Time
2. Person/Object Tracking
3. Abandoned Object Detection
4. Single-Object Tracking Model (SOT)
5. Multi-Object Tracking Model (MOT)
6. Multi-View Multi-Human Association and Tracking Model(MvMHAT)
7. Feng, W., F. Wang, R. Han, Y. Gan, Z. Qian, J. Hou, and S. Wang, "Unveiling the Power of Self-Supervision for Multi-View Multi-Human Association and Tracking", *IEEE Transactions on Pattern Analysis and Machine Intelligence,* Vol 47, Issue 1, 2025, p.351.
8. Occlusion
9. Guan, Z., Z. Wang, G. Zhang, L. Li, M. Zhang, Z. Shi, and N. Jiang. "Multi-Object Tracking Review: Retrospective and Emerging Trend", *Artificial Intelligence Review,* Vol 58, Issue 235, 2025, p.3.
10. Cross-Modal MOT

مادون قرمز و... ترکیب می‌کند پیشنهاد کرده‌اند.[۱] برای مثال، با فراهم آوردن امکان دریافت و آنالیز داده‌های صوتی[۲] مانند فریاد، شلیک گلوله، شکستن شیشه یا انفجار، تشخیص منشأ صدا و تطبیق آن با سایر داده‌های تصویری، می‌توان با اطمینان بیشتری نسبت به مداخله زودهنگام اقدام کرد.

الگوریتم‌های ردیاب می‌توانند وارد شدن شخص به منطقه ممنوعه‌ای همچون نیروگاه هسته‌ای یا کارخانه صنعتی، عبور افراد از مسیرهای غیرمعمول و توقف‌های مشکوک را شناسایی و احتمال وقوع جرائمی مانند خرابکاری را ارزیابی کنند. ردیابی وسایل نقلیه و شناسایی تخلفات ترافیکی نیز کارکرد شناخته‌شدهٔ دیگری است که با کاهش بی‌نظمی، از وقوع رویدادهای پرمخاطره جلوگیری می‌کند. ترکیب الگوریتم‌های ردیابی گروه‌های آسیب‌پذیر مانند دوچرخه‌سواران، توان‌خواهان و عابران پیاده با چراغ‌های هوشمند راهنمایی و رانندگی نیز می‌تواند در کاهش تصادفات و جرائم رانندگی مؤثر باشد.

افزون‌بر این، از دههٔ گذشته متخصصان در پی توسعه الگوریتم‌هایی بودند که با ردیابی و تحلیل الگوی حرکتی و رفتاری افراد، به استخراج ارتباط میان آنان به‌عنوان اعضای یک گروه و شناسایی رفتارهای گروهی[۳] ازجمله پیوستن، جدا شدن، توقف جمعی یا هرگونه تعامل دیگری بپردازد.[۴] الگوهای پیشرفته‌تر این الگوریتم‌ها با تحلیل الگوی فردی در نسبت با دیگران، می‌کوشند ارتباط میان افراد را کشف کنند، آنان را گروه‌بندی نمایند، نوع فعالیت آنان را تشخیص دهند و حتی با تعیین میزان تأثیرگذاری افراد در گروه، افراد نامرتبط را تشخیص دهند و از تحلیل حذف نمایند.[۵] چنین ظرفیتی با کشف ارتباط پنهان میان اعضای یک گروه که ظاهراً مستقل حرکت می‌کنند یا پس از ورود به یک محدوده پراکنده می‌شوند، می‌تواند در پیشگیری از جرائم دسته‌جمعی ازجمله سرقت مسلحانه یا نزاع برنامه‌ریزی‌شده مؤثر واقع شود.

دیگر ظرفیت موقعیت‌محور سامانه‌های نظارت تصویری هوش‌بنیان شناسایی اشیای رهاشده در دو مرحله است: نخست، وجود و موقعیت شیء شناسایی می‌گردد و سپس، با تحلیل ویژگی‌های زمانی و مکانی، سطح خطر آن سنجیده می‌شود.[۶] با شناسایی زودهنگام اجسام مشکوکی مانند کیف، چمدان، بسته یا ماشینی که برای مدت غیرمعمول بدون مراقب رها شده و خارج کردن شیء یا تخلیه محل، می‌توان از جرائم فاجعه‌باری همچون حملات تروریستی، بمب‌گذاری و جاسوسی جلوگیری کرد. بااین‌حال، سنجش دقیق سطح خطر اشیای کوچک، به‌دلیل وقوع خطای مثبت‌کاذب[۷] یا منفی‌کاذب[۸]، همچنان چالش اصلی این حوزه به‌شمار می‌رود.

---

1. Ibid, pp.35-36.
2. Audio Analytics
3. Group Activity Recognition
4. Zaidenberg, S., B. Boulay, and F. Brémond, "A Generic Framework for Video Understanding Applied to Group Behavior Recognition", *IEEE Ninth International Conference on Advanced Video and Signal-Based Surveillance*, 2012, p.2.
5. Huang, J., L. Li, L. Qing, W. Tang, P. Wang, L. Guo, and Y. Peng, "Spatio-Temporal Interactive Reasoning Model for Multi-Group Activity Recognition", *Pattern Recognition,* Vol 159, 2025, 111104, pp.2-5.
6. Zhou, L., and J. Xu., "Enhanced Abandoned Object Detection through Adaptive Dual-Background Modeling and SAO-YOLO Integration", *Sensors,* Vol 24, Issue 20, 2024, p.2.
7. False Positive
8. False Negative

۲. ۱. پایش هویت‌محور؛ شناسایی چهره

برجسته‌ترین و حساس‌ترین ظرفیت‌های سامانه‌های نظارت تصویری هوش‌بنیان، در قالب فناوری‌های شناسایی چهره[۱] تبلور یافته و هدف آن، شناسایی هویت[۲] و احراز هویت[۳] اشخاص حقیقی است. این سامانه‌ها، با تحلیل داده‌های بایومتریک[۴]_ به‌معنای داده‌های شخصی و مربوط به ویژگی‌های منحصربه‌فرد فیزیولوژیکی یا رفتاری اشخاص از قبیل عنبیه چشم، فرم صورت، کف‌دست و الگوی‌حرکت و راه رفتن[۵]_، قادرند هویت سوژه را تشخیص دهند. چگونگی پردازش داده توسط این سامانه‌ها، به دو شیوهٔ بی‌درنگ و پسینی تقسیم می‌شود که قابلیت‌های متفاوتی دارند؛ دسته اول، بدون مشارکت فعال افراد، از راه دور و در لحظه، به مقایسه داده‌های بیومتریک فرد با سوابق موجود در یک پایگاه داده مرجع می‌پردازند و نتیجه را اعلام می‌کنند؛ اما دسته دوم، با تأخیر قابل‌توجهی هویت افراد را شناسایی می‌کنند.

نقش سامانه‌های شناسایی چهرهٔ پسینی در مرحله کشف جرم یا تحقیقات جنایی پررنگ‌تر است، اما سامانه‌ها بی‌درنگ، از ظرفیت‌های پیشگیرانه قابل‌توجهی برخوردارند؛ بدین‌گونه که از طریق افزایش سرعت و قطعیت نظام کیفری به پدیده‌های مجرمانه، ریسک جرم را بالا برده، براساس رویکرد بازدارندگی سزار بکاریا[۶]، می‌توانند بزهکاران احتمالی را از ارتکاب جرم منصرف نمایند.[۷] افزون‌بر این، با کاربست هدفمند این سامانه‌ها جهت شناسایی افراد معین_ مانند افراد خطرناک یا مجرمان سابقه‌دار_، می‌توان به‌موقع از حضور آنان در فضاهای حساس یا پرخطر جلوگیری کرد یا با تحت نظر داشتن آنان، از تکرار الگوی‌جرم جلوگیری به عمل آورد.

در فرایند شناسایی هویت، با تطبیق ویژگی‌های بایومتریک یک فرد ناشناس با ویژگی‌های بایومتریک افراد شناخته‌شده که در پایگاه داده موجود است، هویت سوژه شناسایی می‌گردد. برای این فرایند، سه مرحله ذکر شده است: در گام نخست، داده‌های لازم برای ایجاد پایگاه‌های داده و نیز، داده‌های مربوط به اشخاص تحت‌نظارت جمع‌آوری می‌گردد. سپس، این داده‌ها جهت استخراج ویژگی‌های بایومتریک پردازش می‌شود و الگوریتم، براساس میزان تطبیق ویژگی‌ها و شباهت‌های یافت‌شده، سیاهه‌ای از هویت‌های احتمالی به همراه درصد تطبیق آن را اعلام می‌نماید. در نهایت، نتایج حاصل‌شده جهت دستیابی به اهداف گوناگون_ ازجمله پیشگیری از جرم_، مورد بهره‌برداری قرار می‌گیرند.[۸] همچنین، برای رفع مشکلات تصویر در سامانه‌های پیشرفته، روش‌هایی همچون بازسازی چهره برای افزایش وضوح یا تکمیل جزئیات گمشده، دوربین‌های حرارتی و تصویرپردازی زیرپوستی[۹] برای ثبت الگوی رگ‌ها با کمک نور مادون قرمز وجود

---

1. Facial Recognition Technology (FRT)

2. Biometric Identification

۳. Biometric Verification: احراز هویت، فرایند تأیید یا رد ادعای فرد درخصوص داشتن هویتی خاص از طریق تطبیق داده‌های بایومتریک است و برای مثال، به محدودسازی دسترسی افراد به مکان‌های حساس یا سامانه‌های رایانه‌ای می‌پردازد. این ظرفیت به‌دلیل عدم کاربرد در فضای عمومی جامعه و کم‌خطرتر، موضوع بررسی این مقاله قرار نگرفته است.

4. Biometric Data

5. Gait Recognition

۶. بکاریا در رساله جرائم و مجازات‌ها، بازدارندگی را هدف اصلی کیفر می‌داند که از طریق کاهش سود جرم و افزایش خطر آن برای بزهکار، از ارتکاب جرم جلوگیری می‌کند. برای مطالعه بیشتر درخصوص اندیشه‌های بکاریا، نک به: پرادل، ژان، ***تاریخ اندیشه‌های کیفری***، ترجمه علی‌حسین نجفی ابرندآبادی، تهران: سمت، چاپ چهارم، ۱۳۸۸، صص۴۲-۶۰.

7. Johnson et al.,Op.Cit., pp.3-4.

8. Simmler, M., and G. Canova, "Facial Recognition Technology in Law Enforcement: Regulating Data Analysis of Another Kind", *Computer Law & Security Review,* Vol 56, 2025, p.3.

9. Subepidermal Imaging/Vein Matching

دارد که البته در محیط‌های شهری به‌ندرت استفاده می‌شود.[۱]

نتایج این الگوریتم‌ها ممکن است به‌دلیل ایرادات فنی، سوگیری، داده‌های کم و بی‌کیفیت و... به خطای مثبت کاذب و منفی کاذب دچار شود و شخص بی‌خطری را به‌عنوان مجرم احتمالی یا بالعکس، فرد خطرناک را بی‌خطر تلقی کند. همچنین باتوجه‌به اینکه فرایند شناسایی هویت، عموماً بدون رضایت یا حتی آگاهی افراد صورت می‌پذیرد، با انتقادات گسترده‌ای مواجه است. بنابراین، اثبات کارکرد پیشگیرانهٔ آنها نیازمند شواهد تجربی بیشتر و چارچوب‌های قانونی دقیق و شفاف است.

۳. ۱. پایش فردمحور؛ شناسایی رفتارها و احساس‌ها

در ذیل این چارچوب، دو ظرفیت پیشگیرانهٔ سامانه‌های نظارت تصویری، یعنی شناسایی رفتارهای عینی و شناسایی احساسات، مورد مطالعه قرار می‌گیرد. ظرفیت نخست، به تفکیک رفتارهای عادی و غیرعادی و شناسایی زودهنگام رفتارهای مشکوک[۲] و خشونت‌آمیز، پیش از وقوع جرم می‌پردازد. الگوریتم‌های یادگیری ماشین و یادگیری عمیق می‌توانند با تحلیل بی‌درنگ داده‌های تصویری، تشخیص الگوهای رفتاری غیرعادی و مرتبط با جرم مانند پرسه‌زنی، توقف طولانی، تغییر غیرعادی فواصل میان افراد، حرکات تهاجمی، فرار و پرتاب جسم و... و ترکیب آن با ظرفیت‌هایی همچون شناسایی اشیای خطرناک در صحنه، سطح خطر و احتمال وقوع جرم در آیندهٔ نزدیک را پیش‌بینی کنند و به نیروهای امنیتی هشدار دهند.[۳] برای مثال، سامانه می‌تواند حالت مستی یا استفاده از تلفن همراه حین رانندگی را به‌عنوان رفتار جرم‌زا شناسایی کند یا با پایش فاصله میان افراد و تشخیص سرعت غیرعادی نزدیک شدن یک عابر به کودکی که به‌تنهایی در خیابان حرکت می‌کند، احتمال وقوع سرقت یا کودک‌ربایی را اعلام نماید. البته، جداسازی نشانه‌های وقوع جرم از رفتارهای عادی_ مانند تفکیک فرار یا حمله از دویدن یک ورزشکار_، همچنان با چالش مواجه است.

یکی از نویافته‌ترین روش‌ها برای شناسایی نشانه‌های رفتاری وقوع جرم، تحلیل مسیر حرکت اسکلتی[۴] توسط هوش‌مصنوعی است که با بررسی مسیر حرکت مفصل‌ها و اسکلت افراد حاضر در تصویر در یک بازه زمانی، می‌کوشد رفتار غیرعادی را شناسایی کنند و با دسته‌بندی الگوهای حرکتی مجرمانه، ازجمله آزار جسمی، انواع سرقت، تیراندازی، نزاع و...، رفتار موردنظر را در نزدیک‌ترین طبقه قرار دهند.[۵] بااین‌حال، میزان موفقیت این الگوریتم‌ها در تفکیک انواع رفتار مجرمانه، به‌ویژه درمورد جرائم دارای الگوهای رفتاری مشابه مثل انواع سرقت‌ها، هنوز محدود و نیازمند توسعهٔ بیشتر است.

شناسایی احساسات[۶]، که ذیل مفهوم هوش‌مصنوعی عاطفی[۷] قرار می‌گیرد، ظرفیت فردمحور دیگری است که می‌کوشد

---

1. Johnson et al., Op.Cit., p.2.

2. Anomaly / Suspicious Behavior Detection

3. Ali, M. M., "Real-Time Video Anomaly Detection for Smart Surveillance", *IET Image Processing*, Vol 17, Issue 5, 2023, pp.1375-1376.

4. Skeletal Trajectory Analysis

5. Matei, A-D., E. Talavera, and M. Aghae, "Crime Scene Classification from Skeletal Trajectory Analysis in Surveillance Settings", *Engineering Applications of Artificial Intelligence*, Vol 141, 2025, pp.1-2.

6. Emotion Recognition

۷. Emotional AI: قلمرویی میان‌رشته‌ای شامل هوش‌مصنوعی، روان‌شناسی و علوم اعصاب است که با تحلیل نشانه‌های مختلف، ماشین را قادر به درک و تفسیر احساسات انسان و پاسخ‌دهی متناسب به او می‌گرداند.

با تحلیل وضعیت و تغییرات چهره افراد تاحدودی به احساسات و نیات درونی آنان پی ببرد. نهادهای پیشگیری از جرم پس از استخراج الگوهای احساسی و هیجانی و سنجش میزان همبستگی آنان با ارتکاب جرم براساس داده‌های تاریخی می‌توانند الگوریتم‌های شناسایی احساسات را به سامانه‌های نظارت‌تصویری اضافه کنند و بدین‌ترتیب، نسبت به پیش‌بینی و پیشگیری موقعیت‌مدار از وقوع جرم بپردازند.[1]

در سال‌های گذشته، الگوهای هوش مصنوعی عموماً به تشخیص احساسات طبق برچسب‌های کلی همچون شادی، غم، ترس و خشم می‌پرداختند و از توصیف پیچیدگی هیجانات انسانی ناتوان بودند. اما پژوهش‌های نوین، با اتکا بر رویکردی سمانتیک و با کشف رابطه معنایی بین واژگان توصیف‌کنندهٔ احساسات و نشانه‌های ظاهری آنها در چهره، الگویی آزمایشگاهی ترسیم کرده‌اند که قادر است تغییرات ظریف چهره را با مجموعه‌ای شامل ۱۳۵ واژه مرتبط با احساسات مثل عصبانیت، خشم، انزجار، بیزاری و... تطبیق دهد و نتایج دقیق‌تری استخراج کند.[2]

الگوهای شناسایی زودهنگام احساسات برای پیشگیری از جرم، با وجود جذابیت از منظر جرم‌شناسی و روان‌شناسی جنایی، بیش از سایر ظرفیت‌ها با مناقشه‌های علمی و اخلاقی مواجه است. پژوهش‌های تجربی در این حوزه بسیار معدود است و شواهد متقنی مبنی‌بر صحت عملکرد این الگوها وجود ندارد؛ بنابراین مشروعیت آنها به‌دلیل فقدان پشتوانه علمی کافی، به‌شدت مورد تردید است. افزون‌بر این، صرف وجود یک حالت هیجان‌مدارانه در فرد و همبستگی آن با ارتکاب جرم در آینده هرگز نمی‌تواند دلالت قطعی بر قصد و اراده ارتکاب جرم داشته باشد، عنصر معنوی آن را احراز کند و مبنای محدودسازی حقوق و آزادی‌های افراد قرار گیرد.[3]

۴. ۱. پایش جمعیت‌محور؛ شناسایی ناهنجاری جمعیت[4]

سامانه‌های نظارت تصویری هوش‌بنیان، با فراهم آوردن امکان پایش مستمر محیط و رفتارهای جمعی، از کارآمدترین ابزارها برای تحقق اهداف پیشگیرانه محسوب می‌شوند. این الگوریتم‌ها قادرند بدون نیاز به شناسایی هویت یا ردیابی فردی سوژه‌ها، به تحلیل الگوی رفتار جمعی بپردازند و براساس نشانه‌هایی همچون ایجاد ازدحام غیرمعمول، تغییر غیرعادی سرعت و جهت حرکت جمعیت و...، بروز ناهنجاری را شناسایی کنند.

با تشخیص زودهنگام ناهنجاری و مداخله فوری مانند کنترل ورودی‌ها و خروجی‌ها، مدیریت جریان جمعیت، اعزام نیروهای انتظامی و امدادی، می‌توان از تبدیل یک موقعیت ناهنجار به یک وضعیت بحرانی پیشگیری کرد. برای‌مثال، به‌کارگیری این سامانه‌ها در خیابان‌های اصلی، ایستگاه‌های مترو، بازارها و مراکز خرید، فرودگاه‌ها، رویدادهای بزرگ، تجمع‌ها و زندان‌ها، می‌تواند در پیشگیری موقعیت‌مدار از وقوع جرائمی همچون حملات تروریستی، سرقت، آزارهای جنسی و کودک‌ربایی، که عموماً در مکان‌های شلوغ و پرتردد ارتکاب می‌یابند، نقش اساسی ایفا نکماید.

الگوهای شناسایی ناهنجاری جمعیت عموماً بر الگوریتم‌های بینایی ماشین، یادگیری عمیق و شبکه‌های عصبی متکی‌اند.

---

[1]. Talaei Khoei, T., and A. Singh, "A Survey of Emotional Artificial Intelligence and crimes: Detection, Prediction, Challenges and Future Direction", *Journal of Computational Social Science,* Vol 7, 2024, p. 2363.

[2]. Chen, K., X. Yang, C. Fan, W. Zhang, and Y. Ding, "Semantic-Rich Facial Emotional Expression Recognition", *IEEE Transactions on Affective Computing,* Vol 13, Issue 4, 2022, pp.1906-1907.

[3]. Podoletz, L. "We Have to Talk about Emotional AI and Crime", *AI & Society,* Vol 38, Issue 3, 2023, p.1071.

[4]. Crowd Anomaly Detection

روش مبتنی‌بر رهگیری[1] مسیر حرکت افراد، یکی از این روش‌هاست که ضمن آن، سامانه با رصد پیوستهٔ مسیر حرکت هر سوژه، هرگونه الگوی نامعمول در سرعت، جهت یا میزان ازدحام را به‌عنوان ناهنجاری شناسایی و اعلام می‌کند. البته، بهره‌وری آن در محیط‌های بسیار شلوغ، به‌دلیل دشواری رهگیری مسیر حرکت افراد و هم‌پوشانی سوژه‌ها با مشکل مواجه است.[2]

الگوی دیگری[3] که اخیراً توسعه یافته، تحلیل میزان بی‌نظمی در حرکت جمعیت است و ضمن آن، مسیر حرکت افراد در طول زمان به شکل رشته‌هایی دنبال می‌شود که عموماً در حالت عادی، بدون برخورد و به‌طور موازی پیش می‌روند. درصورت بروز رفتاری غیرعادی، مانند دویدن، حرکت خلاف جهت یا هجوم ناگهانی جمعیت، این خطوط منظم به خطوطی درهم و مملو از نقاط تقاطع تبدیل می‌شوند. بدین‌ترتیب، الگوریتم با افزایش میزان نقاط تقاطع، که نشان‌دهندهٔ آشفتگی و تغییر الگوی حرکت است، وقوع ناهنجاری جمعی را شناسایی می‌کند و نسبت به پدید آمدن موقعیت مخاطره‌آمیز مانند فرار، نزاع یا وحشت‌زدگی هشدار می‌دهد.[4]

با وجود این، نظارت جمعی بر جامعه بدون اخذ رضایت افراد و بدون وجود شواهدی مبنی‌بر ارتکاب جرم ازسوی آنان با اصول بنیادین حقوق کیفری همچون اصل برائت، تناسب تدابیر پیشگیرانه و مداخله حداقلی در زندگی شهروندان در تعارض است و نبود چارچوب‌های حقوقی و اخلاقی روشن در این خصوص حقوق و آزادی‌های شهروندان را در سطح خرد و کلان در معرض خطر قرار می‌دهد.

۲. چالش‌های کاربست سامانه‌های نظارت تصویری هوش‌بنیان

سامانه‌های نظارت تصویری هوش‌بنیان، ظرفیت‌های فراوانی در پهنه پیشگیری موقعیت‌مدار از جرم فراهم می‌کنند، اما هم‌زمان با چالش‌ها و نقدهای جدی نیز روبه‌رو هستند. این سامانه‌ها ممکن است حقوق و آزادی‌های بنیادین را نقض کنند، چگونگی کنش افراد را تحت تأثیر قرار دهند، شکاف‌های اجتماعی را تشدید کنند یا ایدئولوژی‌های افراط‌گرایانه را ترویج نمایند.[5]

در ادامه، مهم‌ترین چالش‌های حقوقی و اجتماعی کاربست پیشگیرانه سامانه‌های مذکور ذیل پنج دستهٔ آزادی‌های بنیادین، حریم خصوصی و سوءاستفاده از داده‌های شخصی، اصل تناسب و نظارت فراگیر، اصل حاکمیت قانون و فرض برائت و مسئولیت نهادهای حاکمیتی و حق شهروندان بر اعتراض، بررسی می‌شود.

۱. ۲. نقض اصل حاکمیت قانون و فرض برائت

براساس اصل حاکمیت قانون[6]، به‌عنوان بنیان تمامی نظام‌های حقوقی مدرن، هرگونه سوءاستفاده از قدرت و نقض حقوق و آزادی‌های افراد ممنوع است و تمام اقدامات نهادهای حاکمیتی باید در چارچوب مشروع قانونی اعمال شوند. مهم‌ترین

---

1. Tracking-Based

2. Rezaee, Kh, S. Rezakhani, M. R. Khosravi, and M. K. Moghimi, "A Survey on Deep Learning-Based Real-Time Crowd Anomaly Detection for Secure Distributed Video Surveillance", *Personal and Ubiquitous Computing,* Vol 28, Issue 1, 2024, pp.138-139.

3. Cross-Trajectories

4. Akpulat, M., and M. Ekinci, "Anomaly Detection in Crowd Scenes via Cross Trajectories", *Applied Intelligence,* Vol 55, Issue 525, 2025, pp.3-6.

5. Haley, P., "The Impact of Biometric Surveillance on Reducing Violent Crime: Strategies for Apprehending Criminals While Protecting the Innocent", *Sensors,* Vol 25, Issue 10, 2025, p.7.

6. Rule of Law

قاعده درخصوص کاربست سامانه‌های نظارت تصویری هوش‌بنیان آن است که دولت‌ها هرگز نباید از آن به‌گونه‌ای استفاده کنند که به هر نحو، کرامت انسانی و حقوق بشر را در معرض خطر قرار دهد، آزادی‌های بنیادین را تضعیف کند یا حریم خصوصی افراد و جامعه را نقض نماید. در این راستا، ضروری است کاربردهای مجاز و ممنوع این سامانه‌ها، به‌طور دقیق در قوانین تعیین و محدودیت‌ها و استانداردهایی براساس معیارهای عینی ارائه شود تا از تسهیل نقض حقوق و آزادی‌های مردم توسط نهادهای قدرت جلوگیری شود. همچنین، تهیه کدهای رفتاری، دستورالعمل‌ها و آیین‌نامه‌های ارشادی، که اگرچه الزام قانونی در پی ندارند، چگونگی استفاده اخلاقی و ارزش‌مدارانه از سامانه‌های نظارتی را نهادینه می‌کنند، راهکاری تکمیلی اما مهم محسوب می‌شود.

رعایت اصلِ بنیادین برائت در عصر پیشگیری از جرم از طریق سامانه‌های نظارتی هوش‌بنیان، باتوجه‌به ماهیت پیشگیرانه این سامانه‌ها و فقدان عناصر تشکیل‌دهنده جرم در عالم واقع، از اهمیت دوچندانی برخوردار است و همواره در معرض خطر نقض قرار دارد. نبود ساختارهای قانونی محدودکننده، عدم شفافیت درخصوص اختیارات نهادهای ناظر، عدم آگاهی یا رضایت افراد تحت نظارت و با عادی‌سازی نظارت فراگیر بر مردم، فرض مجرمیت را جایگزین فرض برائت، و شهروندان را به مظنونین دائمی تبدیل می‌کند.

۲. ۲. نقض اصل تناسب و نظارت فراگیر

از مهم‌ترین چالش‌های ناشی از به‌کارگیری سامانه‌های نظارتی، خطر نقض اصل تناسب[1] در مواجهه با دو ارزش است: ازیک‌سو، ضرورت حفظ حریم خصوصی و آزادی‌های فردی و از سوی‌دیگر، میل نظام پیشگیری از جرم به نظارت بر جامعه با هدف صیانت از امنیت و منافع عمومی. هرگونه ناترازی در برقراری تعادل میان این دو، جامعه را در معرض خطر شکل‌گیری نظارت‌فراگیر و تسلط رویکردهای اقتدارگرایانه قرار می‌دهد.

رعایت اصل تناسب، نیازمند تحقق سه معیار است[2]: ۱. شایستگی و مناسب بودن[3]، این معیار ایجاب می‌کند سامانه نظارتی از قابلیت تحقق اهداف مشروع برخوردار باشد. استفاده از سامانه‌های نظارت تصویری در حوزه پیشگیری موقعیت‌مدار از جرم، تنها زمانی مجاز است که نوع نظارت، شدت آن و شیوه مداخله با اهداف پیشگیرانه همسو باشد و بتواند سازوکارهای ادراکی و انتخاب‌های عقلانی مجرمان احتمالی را تحت‌تأثیر قرار دهد. ۲. ضرورت[4]، این معیار که با اصل حداقلی بودن مداخله کیفری نیز مرتبط است، در پی آن است که از میان گزینه‌های موجود، کم‌خطرترین و کم‌مداخله‌ترین شیوه را انتخاب کند. برای مثال، با ممنوع‌سازی هرگونه نظارت همگانی و بدون محدودیت و مشروط نمودن اعمال نظارت به تعیین زمان، مکان، هدف، سوژه خاص و وجود توجیه قانونی، می‌توان از فراگیری بی‌حدوحصر سامانه‌های نظارتی و امنیتی شدن فضای جامعه جلوگیری کرد. ۳. اقتضا یا تناسب در مفهوم مضیق[5]، طبق این معیار، به‌کارگیری سامانه‌های نظارت‌تصویری، حتی در فرض رعایت شایستگی و ضرورت، هنگامی توجیه‌پذیر است که مزایای پیشگیرانه آن، بر آسیب‌ها و معایبش غلبه داشته باشد. برای‌مثال،اگر الگوریتم‌های تحلیل احساسات به تبعیض یا

---

1. The Principle of Proportionality

۲. اصفهانی، بابک و صابر نیاورانی، «اصل تناسب، ابزار تضمین وتعادل میان حق‌ها و آزادی‌های بنیادین و منافع عمومی»، *فصلنامه تحقیقات حقوقی*، دوره ۲۷، شماره ۴، ۱۴۰۳، ص ۲۱۵.

3. Suitability

4. Necessity

5. Proportiotnality in a Strict Sense

سوءاستفاده از قدرت منجر شوند، معیار اقتضا به ممنوعیت کامل آنها حکم می‌نکماید.

بنابراین، باتوجه‌به آنکه سامانه‌های نظارت تصویری هوش‌بیان، قدرت بی‌سابقه‌ای در اختیار دولت‌ها و نهادهای قدرت قرار می‌دهند و قابلیت بالایی برای تبدیل شدن به ابزار نظارت فراگیر بر شهروندان دارند، رعایت اصل تناسب در قانونگذاری، به‌کارگیری و نظارت بر این سامانه‌ها اهمیت بسیاری خواهد داشت؛ اصلی که قانون هوش‌مصنوعی ۲۰۲۴ در بند ۲۶ مقدمه خود به آن پرداخته و با اتخاذ رویکرد ریسک‌محور در پی محقق‌ساختن آن برآمده است.

۳. ۲. نقض آزادی‌های بنیادین

سامانه‌های نظارت تصویری هوش‌بنیان اگرچه در ذات خود تهدیدآمیز نیستند، کاربست غیرقانونی و بی‌ضابطهٔ آنها می‌تواند آزادی‌های بنیادین بشر و کرامت انسانی را با خطرات جدی مواجه سازد. نظام پیشگیری از جرم، باید همواره به این اصل پایبند باشد که سامانه‌های نظارت‌تصویری‌هوش‌بنیان،مثل هر فناوری دیگری، باید فقط در جهت خدمت به انسان‌ها به‌کار گرفته شوند. طبق اصل اخلاقی مشهور کانت، انسان همواره هدف است، نه وسیلهٔ رسیدن به هدف[۱]؛ اصلی که در عصر داده‌محوری و گسترش استفاده از هوش‌مصنوعی، بیش از هر زمان دیگری با تهدید مواجه است.

نظارت تصویری هوش‌بنیان، می‌تواند آزادی بیان و آزادی مشارکت در اجتماعات را، که طبق مواد ۱۹ و ۲۱ میثاق بین‌المللی مدنی سیاسی از آزادی‌های بنیادین به‌شمار می‌روند، نیز تحت‌تأثیر قرار دهد؛ بدین‌نحو که از طریق نظارت بر جامعه در همهٔ زمان‌ها و مکان‌ها، نوعی بازدارندگی مبتنی‌بر ارعاب ایجاد کند و مردم را از ابراز آزادانه دیدگاه‌ها یا مشارکت در اجتماعات مدنی مشروع، که ممکن است از طرف دولت‌ها ناهنجار تشخیص داده شود، منصرف سازد. استمرار چنین وضعیتی می‌تواند به تضعیف رویکردهای دمکراتیک و تقویت گرایش‌های اقتدارگرایانه بینجامد.

افزون‌بر این، استفاده نادرست یا سوگیرانه از داده‌ها و الگوریتم‌های هوش‌مصنوعی، می‌تواند به تولید نتایج تبعیض‌آمیز و نقض حق بر برابری و منع تبعیض منجر شود؛ چنان‌که بسیاری از پژوهش‌ها حکایت از نرخ بالای تبعیض در نتایج سامانه‌های شناسایی‌چهره، به‌ویژه براساس معیار نژاد و جنسیت، داشته و بیشترین تهدید را متوجه گروه زنان سیاه‌پوست دانسته‌اند.[۲] در سطح کلان نیز، تحلیل داده‌های رفتاری جمعی ممکن است به برچسب‌زنی گروهی و شکل‌گیری تبعیض ساختاری بینجامد؛ بدین‌معنا که در فقدان معیارهای فنی و حقوقی روشن، رفتارهای عادی در محلات فرودست اقتصادی، اقلیت‌نشین یا جوامع دارای الگوی فرهنگی متفاوت، می‌تواند براساس هنجارهای غالب یا پیش‌فرض‌های نهادی، به‌عنوان رفتار ناهنجار دسته‌بندی شود و آزادی‌های‌بنیادین فردی و جمعی را به‌طور ناموجهی نقض گرداند.[۳]

۴. ۲. نقض حریم خصوصی و سوء استفاده از داده‌های شخصی

یکی از چالش‌برانگیزترین مخاطرات به‌کارگیری سامانه‌های نظارت تصویری هوش‌بنیان، دسترسی گسترده به حجم

---

۱. کانت، ایمانوئل، ***نقد عقل عملی***، ترجمه انشاءالله رحمتی، تهران: نورالثقلین، چاپ چهارم، ۱۳۸۵، ص۱۴۶.

2. Serna, I., A. Morales, J. Fierrez, and N. Obradovich, "Sensitive Loss: Improving Accuracy and Fairness of Face Representations with Discrimination-aware Deep Learning", *Artificial Intelligence,* Vol 305, 2022, p.4.

۳. سند تحول و تعالی قوه قضائیه ۱۴۰۳، تدوین و پیگیری تصویب «لایحه حمایت از آزادی‌های مشروع» با احصای مصادیق آزادی‌های مشروع به‌صورت دقیق و شفاف و تعیین مجازات مناسب برای نقض آن را به‌عنوان راهکاری برای مقابله با نقض و محدودسازی سلیقه‌ای آزادی‌ها در دستور کار قوه قضائیه قرار داده است.

عظیمی از داده‌های فردی و جمعی است؛ ظرفیتی که نقض حریم خصوصی[۱] و سوءاستفاده از داده‌های شخصی را ممکن می‌گرداند. حتی الگوریتم‌هایی مانند الگوریتم‌های شناسایی ناهنجاری جمعیت، که عموماً بر ثبت و تحلیل داده‌های زمانی، مکانی و ظاهری افراد متکی‌اند و لزوماً داده‌های بایومتریک را استخراج نمی‌کنند، حریم خصوصی را در معرض تهدیدهای جدی قرار می‌دهند؛ زیرا داده‌هایی که برحسب آن بتوان افراد را ردیابی و شناسایی کرد، اگرچه داده بایومتریک نیست، همچنان در زمره داده‌های شخصی دسته‌بندی می‌شود.[۲]

رضایت و شفافیت، دو عنصر مهم در حفاظت از حریم خصوصی هستند. در اصول اخلاقی مربوط به محافظت از داده‌های شخصی، رضایت باید مشروط و پویا باشد؛ بدین معنا که هدف و حدود استفاده از آن مشخص شود و نیز، امکان بازپس‌گیری و لغو رضایت برای رضایت‌دهنده به رسمیت شناخته شود.[۳] همچنین، شماری از محققان نسبت به شرطی‌سازی رضایت توسط دولت‌ها یا نهادهای قدرتمند هشدار داده‌اند[۴]؛ به این معنا که نهاد نظارت‌کننده، ارائه خدمات عمومی یا دسترسی به امکانات اجتماعی را به رضایت افراد به پردازش داده‌های شخصی آنان مشروط نماید یا با معرفی یک فناوری به‌عنوان تنها راه پیشگیری از جرم براساس اطلاعات غیرواقعی، خودمختاری آگاهانه آنان را برای تصمیم‌گیری از میان ببرد. در این شرایط، رضایت فاقد وصف آزادانه است و ماهیتی تحمیلی و ابزاری برای مشروعیت‌بخشی صوری به استفاده از سامانه‌های نظارتی می‌یابد. فقدان رضایت یا اخذ صوری آن در مواردی که رضایت آزادانه و آگاهانه مبنای هرگونه پردازش است، مصداق قطعی سوءاستفاده و تعرض به حریم‌خصوصی به‌شمار می‌رود.

برای مقابله با این چالش‌ها، قانون‌گذاری دقیق و شفاف برای تعیین چارچوب‌های فنی و حقوقی حاکم بر سامانه‌های هوش‌بنیان و چگونگی پردازش داده ضروری است. حریم خصوصی با طراحی[۵]، چارچوبی حقوقی و فلسفی برای استفاده از فناوری است که حریم خصوصی را جزئی از معماری و ساختار فنی سامانه و نه جزئی بیرونی و پسینی می‌داند. در این رویکرد ملزومات رعایت حریم خصوصی باید در زمان طراحی هر فناوری و در خودِ فناوری تعبیه گردد و با کمینه‌سازی جمع‌آوری داده‌ها، شفاف‌سازی و توضیح‌پذیری فرایند، اخذ رضایت کاربران و... نقض حریم خصوصی را ناممکن یا دشوار می‌سازد.[۶] فناوری‌های ارتقادهنده حریم‌خ صوصی[۷]، یکی از ابزارهای اعمال این رویکرد است که با روش‌های نظیر ناشناس‌سازی، محو چهره و رمزنگاری، از ثبت داده‌های غیرمجاز و غیرضروری، افشای هویت افراد، نشت داده‌های شخصی و قرار گرفتن آن در اختیار افراد غیرصالح در حین فعالیت الگوهای هوش‌مصنوعی جلوگیری می‌کند.[۸]

---

۱. اهمیت بنیادین حق بر حریم خصوصی در اسناد بین‌المللی نظیر ماده ۱۲ اعلامیه جهانی حقوق بشر، ماده ۱۷ میثاق بین‌المللی حقوق مدنی سیاسی، ماده ۸ کنوانسیون اروپایی حقوق بشر و اصل ۲۵ قانون اساسی جمهوری اسلامی ایران به‌رسمیت شناخته شده است.

۲. ماده۴ قانون GDPR: «داده شخصی هرگونه اطلاعات مربوط به یک شخص حقیقیِ شناسایی‌شده یا قابل شناسایی است که می‌توان او را به‌طور مستقیم یا غیرمستقیم از طریق ارجاع به نام، شماره شناسایی، داده‌مکانی، شناسه‌الکترونیک، یا یک یا چند شناسه مربوط به هویت فیزیکی، فیزیولوژیکی، ژنتیکی، روانی، اقتصادی، فرهنگی یا اجتماعی شناسایی نمود».

3. The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems.Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems, First Edition, *IEEE*, 2019, p.112.

4. Fontes, C., E. Hohma, C. C. Corrigan, and C. Lütge, "AI-Powered Public Surveillance Systems: Why We (Might) Need Them and How We Want Them", *Technology in Society,* Vol 71, 2022, p.7.

5. Privacy by Design (PbD)

۶. این مفهوم در قانون GDPR باعنوان Data Protection by Design آمده است.

7. Privacy Enhancing Technology (PET)

8. Feretzakis, G., K. Papaspyridis, A. Gkoulalas-Divanis, and V. S. Verykios, "Privacy-Preserving Techniques in Generative AI and Large Language Models: A Narrative Review", *Information*, Vol 15, Issue 11, 2024, p.10.

در به‌کارگیری سامانه‌های نظارت‌تصویری، رعایت اصل شفافیت نیز نقش مهمی در حفاظت از حریم‌خصوصی دارد. ازاین‌رو، نه‌تنها لازم است نحوه کارکرد سامانه‌های نظارتی، تاحدی که به اهداف پیشگیرانه خللی وارد نکند، به اطلاع جامعه برسد، بلکه باید استفاده مخفیانه و غیرعلنی از آنها، جز در موارد استثنایی در چارچوب مجوز قانونی و تحت‌نظارت قضایی، ممنوع گردد و شهروندان از تحت‌نظارت بودن خود و حدود آن کاملاً آگاه شوند.

پذیرش اجتماعی سامانه‌های نظارت تصویری بیش‌از آنکه صرفاً تابع پیشرفت‌های فناورانه باشد، به کیفیت چارچوب‌های حقوقی، فنی و اخلاقی وابسته است. اگر این سامانه‌ها در بستری شفاف، پاسخ‌گو و قابل‌اعتماد به‌کار گرفته شوند و آثار واقعی و قابل‌سنجش آنان بر کاهش جرم و ارتقای امنیت عمومی اثبات گردد، اعلام رضایت آگاهانه و مختارانهٔ افراد نسبت به پردازش داده‌های آنان در حدود قانونی، امری محتمل و عقلانی خواهد بود. یافته‌های پژوهشی نیز نشان می‌دهد که اعتماد عمومی به دولت‌ها و نهادهای اجرای قانون، تعیین‌کننده‌ترین عامل موفقیت یا ناکامی اعمال نظارت تصویری است[1]؛ به‌گونه‌ای‌که حتی پیشرفته‌ترین سامانه‌های نظارتی، درصورت بی‌اعتمادی عمومی، نه‌تنها کارآمد نیستند، بلکه می‌توانند به مقاومت مدنی، کاهش همکاری اجتماعی و تضعیف سازوکارهای پیشگیرانه منجر شوند. نظارت‌تصویری هوش‌بنیان، فرایندی صرفاً فناورانه نیست، بلکه پدیده‌ای اجتماعی تکنیکی است که به نحوهٔ برخورد نهادهای نظارت‌کننده و برداشت مردم از نحوهٔ اعمال قدرت بستگی دارد. آیا مردم احساس می‌کنند که نظام پیشگیری از جرم، احترام و کرامت آنان را حفظ نموده و قابل‌اعتماد است یا خیر؟

۵. ۲. مسئولیت‌پذیری نهادی و لزوم نظارت انسانی[2]

با پذیرش اصول بنیادینی همچون حاکمیت قانون، برائت، تناسب، رعایت حریم خصوصی و آزادی‌های بنیادین، بار مسئولیت تماماً برعهده نهادهایی قرار می‌گیرد که در چرخه طراحی، توسعه، استقرار، بهره‌برداری و نظارت بر سامانه‌های نظارتی نقش دارند. بنابراین، حدود مسئولیت هریک از نهادها، ازجمله نهادهای انتظامی، قضایی، ناظر و بخش خصوص توسعه‌دهنده فناوری، باید به‌طور مستقل و شفاف، جهت جلوگیری از عدم‌پاسخ‌گویی و مسئولیت‌گریزی آنان تعیین گردد. همچنین، شماری‌از متخصصان عرصهٔ اخلاق و حقوق هوش‌مصنوعی، حضور، دخالت و نظارت انسان[3] در فرایند به‌کارگیری هوش‌مصنوعی‌های پرخطر و حساس را ضروری می‌دانند و از آن با عنوان «اصل انسان در چرخه»[4] یاد می‌کنند.[5] هرگونه تحلیل و تصمیم‌گیری توسط سامانه‌های نظارت‌تصویری که به هر نحو بر ابعاد حقوقی، اجتماعی، اقتصادی و... زندگی افراد تأثیر می‌گذارد، باید تحت نظارت یک یا چند عامل انسانی حقیقی قرار داشته باشد. عامل انسانی باید بر صحت فرایند و نتایج سامانه نظارت کند، اشتباهات آن را اصلاح یا حدف کند، از عملکرد سوگیرانه یا غیرقانونی سامانه جلوگیری کند و درصورت تقصیر در انجام وظیفه، مسئولیت قانونی آن را برعهده گیرد.

بر این مبنا، نظام حقوقی باید پیش از هرگونه استفاده از سامانه‌های نظارت تصویری هوش‌بنیان، مسئولیت هریک از

[1]. Choung, H., P. David, and T-W. Ling, "Acceptance of AI-Powered Facial Recognition Technology in Surveillance Scenarios:Role of Trust, Security, and Privacy Perceptions", *Technology in Society*, Vol 79, 2024, p.7.

[2]. Human Oversight

[3]. Human Oversight

[4]. Human-in-the-loop

[5]. Veltmeijer, E., and C. Gerritsen, "Legal and Ethical Implications of AI-based Crowd Analysis: The AI Act and Beyond", *AI Ethics,* Vol 5, Issue 3, 2025, p.3179.

عوامل نهادی یا انسانی را در زنجیرهٔ مسئولیت[1] مشخص کند تا بتوان درصورت بروز هرگونه خطا یا سوءاستفاده، شخص مسئول را ملزم‌به پاسخ‌گویی و جبران ضرر و زیان کرد.

۳. وضعیت حقوقی ظرفیت‌های سامانه‌های نظارت تصویری هوش‌بنیان

قانون هوش‌مصنوعی اتحادیه اروپا مصوب ۲۰۲۴، به‌عنوان نخستین مقررهٔ الزام‌آور در حوزهٔ هوش‌مصنوعی، نقطهٔ عطفی در تاریخ تنظیمگری این فناوری به‌شمار می‌رود و از ظرفیت فراوانی برای مدیریت خطرات و چالش‌ها در عصر هوش‌مصنوعی و حفاظت از حقوق و آزادی‌های‌بنیادین برخوردار است. هدف اصلی این قانون طبق مقدمهٔ آن، بهبود کارکرد بازار داخلی ازطریق ایجاد چارچوب حقوقی واحد و هماهنگ در محدودهٔ اتحادیه‌اروپاست و هم‌زمان با حمایت از نوآوری و ترویج هوش‌مصنوعی انسان‌محور و قابل اعتماد، به پاسداشت ارزش‌های اتحادیه، ازجمله کرامت انسانی، دمکراسی و حاکمیت قانون، و همچنین تضمین سطح بالای سلامت، امنیت و حفاظت از حقوق و آزادی‌های بنیادین می‌پردازد.

این قانون، با رویکردی مبتنی‌بر ریسک، سامانه‌های هوش‌مصنوعی را در چهار سطح تقسیم‌بندی می‌کند: ۱. هوش‌مصنوعی با خطر غیرقابل قبول[2] که استفاده از آن ممنوع است، ۲. هوش‌مصنوعی پرخطر[3] که استفاده از آن مشروط به رعایت الزامات قانونی است، ۳. هوش‌مصنوعی با خطر محدود[4] که ملزم به رعایت تدابیر مربوط به شفافیت است، ۴. هوش‌مصنوعی کم‌خطر[5] که با محدودیت خاصی روبه‌رو نشده است.[6]

به‌موجب فصل دوم و سوم این قانون،سامانه‌های پرخطر باید مجموعه‌ای از الزامات فنی و سازمانی را رعایت کنند که اعمال آنها عمدتاً برعهده تأمین‌کنندگان، عرضه‌کنندگان و کاربران این سامانه‌هاست. این الزامات که شامل استقرار نظام مدیریت ریسک، کنترل کیفیت و نحوهٔ آموزش و استفاده از داده‌ها، ثبت مستندات فنی به‌روز، ثبت خودکار وقایع سامانه، رعایت اصل شفافیت، نظارت انسانی، برخورداری از دقت و استحکام و امنیت سایبری و... است، پیش‌نیاز ورود سامانه‌های هوش‌مصنوعی به اتحادیه‌اروپا و ادامهٔ حیاتشان در آن حوزه محسوب می‌شود.

قانون هوش‌مصنوعی ۲۰۲۴، اگرچه گام مهمی در مسیر نهادینه کردن رویکرد ریسک‌محور به هوش‌مصنوعی، کاهش چالش‌ها و حفاظت از حقوق و آزادی‌ها برداشته است، اما رویکردی بسیار کلی داشته و اعمال دقیق و واقع‌بینانهٔ آن نیازمند قانونگذاری‌های تفصیلی و جزئی‌تر است. افزون‌براین، این قانون از منظر سیاست‌جنایی پیشگیرانه با ناترازی‌هایی نیز مواجه است و میزان توجه آن به ظرفیت‌های گوناگون سامانه‌های هوش‌مصنوعی از انسجام و توازن کافی برخوردار نیست. برای‌مثال، باوجود وضع مقررات دقیق‌تری برای سامانه‌های شناسایی هویت بایومتریک، ظرفیت‌هایی همچون شناسایی رفتار، تحلیل ناهنجاری جمعیت و ردیابی سوژه، فاقد چارچوب اختصاصی‌اند. ازاین‌رو، برای پرهیز از تکرار

---

1. Accountability Chain
2. Unacceptable Risk AI Systems
3. High Risk AI Systems
4. Limited Risk AI Systems
5. Minimal Risk AI Systems
6. بر پایهٔ بندهای ۹ و ۱۰ مقدمه قانون‌هوش‌مصنوعی، مفاد این قانون باید در کنار سایر قوانین اتحادیه اروپا ازجمله قانون حفاظت از داده‌های شخصی (GDPR) ۲۰۱۶ تفسیر و اعمال گردد. باتوجه به عدم ارتباط مستقیم این قانون با وضعیت حقوقی استفاده از هوش‌مصنوعی، برای مطالعه بیشتر ر.ک به: انصاری، باقر، ***حقوق داده‌ها و هوش مصنوعی: مفاهیم و چالش‌ها***، تهران: شرکت سهامی انتشار، چاپ اول، ۱۴۰۰.

مباحث، بررسی وضعیت حقوقی شماری از ظرفیت‌ها به‌طور مجزا و شماری دیگر به‌نحو تجمیعی و با تکیه بر احکام کلی قانون صورت خواهد گرفت.

۱. ۳. وضعیت حقوقی پایش هویت‌محور

قانون هوش‌مصنوعی ۲۰۲۴، سامانه‌های شناسایی هویت بایومتریک را براساس زمان پردازش داده، به دو دستهٔ بی‌درنگ و پسینی تفکیک نموده و با اتخاذ رویکردی متمایز، به سامان‌دهی آنها پرداخته است.[۱] طبق این قانون، سامانه‌های شناسایی هویت بایومتریک بی‌درنگ[۲] که در فضاهای عمومی برای اجرای قانون[۳] استفاده می‌شوند، دارای خطر غیرقابل قبول بوده و استفاده از آنها به‌طور کلی ممنوع است (بند۱-h ماده ۵)؛ زیرا طبق بند۳۲ مقدمه قانون،این سامانه‌ها به‌دلیل ماهیت تهاجمی خود،به حقوق و آزادی‌های اشخاص تعرض نموده و احساس نظارت دائمی ایجاد می‌کنند. همچنین، در پردازش بی‌درنگ، فرصت محدودتری برای بررسی دقیق‌تر داده‌ها و اصلاح خطاها در اختیار کاربران قرار دارد و امکان بروز نتایج تبعیض‌آمیز و ناقض حقوق و آزادی‌های اشخاص به‌دلیل نارسایی‌های فنی افزایش خواهد یافت.

اما در ادامه ماده، این سامانه‌ها در سه مورد استثنایی زیر، پرخطر محسوب شده و به‌کارگیری آنان، مشروط به رعایت الزامات قانونی، مجاز خواهد بود (بند۱-h ماده ۵): ۱. برای جست‌وجوی بزه‌دیدگان جرائم خاص مذکور در این قانون، ۲. برای جلوگیری از یک تهدید خاص، جدی و قریب‌الوقوع نسبت به جان یا ایمنی فیزیکی افراد یا یک حمله تروریستی واقعی یا قابل پیش‌بینی، ۳. برای شناسایی مجرم یا مظنون به ارتکاب یکی از جرائم خاص مذکور در این قانون. چنان‌که ملاحظه می‌شود، کاربرد مجاز این سامانه‌ها برای پیشگیری از جرم صرفاً به مورد دوم محدود شده است.

البته این قانون، دامنهٔ استفاده از این سامانه‌ها در محدوده استثناهای فوق را مجدداً محدود کرده و به‌کارگیری آنان را صرفاً برای شناسایی هویت افراد هدف‌گذاری‌شده مجاز کرده است (بند۲ماده۵). همچنین، پیش از هرگونه اقدام، ارزیابی پیامدهای استفاده از این سامانه‌ها بر حقوق و آزادی‌های افراد و نیز سنجش میزان شدت، احتمال و مقیاس آسیب ناشی از عدم استفاده از آنها نیز الزامی است. به‌علاوه، اخذ مجوز موردی توسط مقام قضایی یا مقام صالح دیگر با رعایت ضرورت و تناسب، لازمهٔ کاربست آنها خواهد بود و نیز هیچ تصمیمی که اثر قانونی منفی بر یک شخص داشته باشد نباید صرفاً براساس خروجی این سامانه‌ها اتخاذ گردد (بند۳ ماده۵). افزون‌بر این،کشورهای عضو اتحادیه برای به‌کارگیری سامانه‌های شناسایی چهره در موارد مجاز استثنایی، ملزم به تهیهٔ قوانین تفصیلی داخلی خواهند بود (بند۵ ماده۵)؛ زیرا اگرچه قانون هوش‌مصنوعی به ارائه رهنمودها و قواعد کلی می‌پردازد، اما یک چارچوب حقوقی جامع، مستقل و جزئی نیست[4] و تدوین قواعد و تشریفات مربوط به آیین دادرسی داخلی از محدودهٔ صلاحیت اتحادیه اروپا و این قانون خارج است.[۵]

دسته دوم، یعنی سامانه‌های شناسایی هویت بایومتریک از راه دور پسینی[۶]، که عموماً در حوزه کشف جرم یا تحقیقات

---

۱. در این قانون به وضعیت سامانه‌های احراز هویت بایومتریک پرداخته نشده است.

2. Real-Time Remote Biometric Identification System

3. Law Enforcement

4. Simmler, M., and G. Canova, Op.Cit., p.10.

5. Ebers, M., V. R. S. Hoch, F. Rosenkranz, H. Ruschemeier, and B. Steinrötter, "The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society(RAILS)", *J — Multidisciplinary Scientific Journal* , Vol 4, Issue 4, 2021, p.590.

6. Post-Remote Biometric Identification

جنایی کاربرد دارند، در تمامی موارد پرخطر شناخته شده و درصورت رعایت الزامات قانونی منعی برای استفاده از آنها وجود ندارد. البته، استفاده از این سامانه‌ها نیز مستلزم اخذ مجوز از مقام صالح جهت تحقیق درباره فرد هدف‌گذاری شده دارای ارتباط مستقیم با جرم کیفری واقعی یا بالقوه است و هیچ تصمیمی که دارای اثر حقوقی نامطلوب بر فرد باشد، نباید صرفاً براساس نتایج ارائه شده توسط این سامانه‌ها اخذ گردد (بند۱۰ ماده ۲۹). شایان‌ذکر است که اگرچه این قانون به لزوم قانون‌گذاری داخلی جهت استفاده از سامانه‌های پیسینی اشاره نکرده، اما تضمین رعایت سایر شروط و الزامات تعیین‌شده همچنان در گرو آن خواهد بود.

در نهایت، قانون هوش‌مصنوعی هرگونه عرضه و استفاده از سامانه‌های هوش‌مصنوعی برای ایجاد یا گسترش پایگاه داده‌های تشخیص چهره به‌صورت بی‌هدف،چه از طریق دوربین‌های مداربسته و چه در بستر اینترنت، را ممنوع دانسته است (بند۱-e ماده ۵)؛ زیرا این اقدام نوعی پردازش دادهٔ شخصی تلقی می‌شود و مطابق مفاد قانون حفاظت از داده‌های شخصی ۲۰۱۶ غیرمجاز است.[1]

۳.۲. وضعیت حقوقی پایش فردمحور

قانون هوش‌مصنوعی، به‌طور مستقل به تعیین وضعیت حقوقی استفاده از هوش‌مصنوعی با هدف شناسایی رفتارها نپرداخته است. اما باتوجه‌به آنکه این ظرفیت عموماً با هدف پیش‌بینی وقوع جرم اعمال می‌شود، می‌توان از این منظر به تبیین چارچوب مجاز استفاده از آن پرداخت.

به‌موجب بند۱-d ماده ۵، هرگونه عرضه یا استفاده از هوش‌مصنوعی برای ارزیابی یا پیش‌بینی خطر ارتکاب جرم توسط اشخاص حقیقی که تنها بر پروفایل‌سازی[2] یا ارزیابی ویژگی‌ها و خصوصیات شخصیتی مبتنی باشد، ممنوع است؛ اما این ممنوعیت درمورد سیستم‌های هوش‌مصنوعی که برای حمایت از ارزیابی انسانی درخصوص دخالت یک فرد در یک فعالیت مجرمانه که بر حقایق عینی و قابل تأییدی که مستقیماً با یک عمل مجرمانه مرتبط است، اعمال نمی‌شود.

بدین‌ترتیب، این قانون، الگوریتم‌های پیش‌بینی جرم را فقط درصورتی مجاز به استفاده از رفتارهای شناسایی‌شده دانسته است که رفتارها عینی و مستقیماً مربوط به جرم باشند؛ اما پیش‌بینی جرم با استفاده از تحلیل یا استنتاج هوش‌مصنوعی بر مبنای رفتارهای غیرمستقیم ممنوع است؛ زیرا به پروفایل‌سازی و ارزیابی غیرمجاز ویژگی‌های شخصیتی منجر خواهد شد. همچنین، طبق بند۴۲ مقدمه این قانون، براساس اصل برائت، اشخاص حقیقی در اتحادیه اروپا باید همواره براساس رفتار واقعی خود قضاوت شوند، نه براساس رفتار پیش‌بینی‌شده توسط هوش‌مصنوعی که بر ظن معقول مبتنی‌بر حقایق عینی درخصوص درگیری در یک عمل مجرمانه متکی نیست. برای‌مثال، پیش‌بینی وقوع جرم ضرب و جرح براساس پردازش بی‌درنگ تصاویر فردی که چاقویی را از کیف خود درآورده و با حالت تهاجمی به‌سمت شخص دیگری می‌رود، باتوجه‌به وقوع رفتاری عینی و مستقیماً مربوط به جرم، مجاز است. اما اگر سامانه با تطبیق مسیر دو فرد که برای مدتی طولانی پشت‌سرهم حرکت می‌کردند استنتاج کند که یکی از افراد دیگری را تعقیب می‌کند، نمی‌توان این نتیجه را

---

[1]. در چارچوب مقررات داخلی، یکی از راهبردهای سند تحول و تعالی قوه قضائیه مصوب ۱۴۰۳ با عنوان بهره‌گیری از فناوری‌های نوین در فرایند کشف جرم و هوشمندسازی آن، تقویت توانایی شناسایی متهمان از طریق داده‌کاوی اطلاعات مجرمان را در دستور کار سازمان‌هایی از قبیل معاونت اجتماعی و پیشگیری از وقوع جرم قوه قضائیه قرار داده است. این کاربرد اگرچه با تأکید بر کشف جرم، و نه پیشگیری از آن، تدوین شده، اما از جهت ارتباط با موضوع نوشتار حاضر قابل‌توجه است؛ زیرا همچنان اصول و قواعد مشخصی برای اعمال چنین نظارتی بر افراد و جلوگیری از چالش‌های آن پیش‌بینی نشده است.

[2]. Profiling

مبنای پیش‌بینی قرار داد. بدین‌ترتیب، به‌نظر می‌رسد بسیاری از کارکردهای الگوریتم‌های شناسایی رفتار که ذیل بخش ۱. ۳. ذکر شد با ممنوعیت مواجه شود.

استفاده از سامانه‌های شناسایی و تحلیل احساسات نیز طبق بند۱-f ماده ۵ قانون هوش‌مصنوعی ۲۰۲۴ تنها در محیط‌های تحصیلی و شغلی غیرمجاز است؛ درحالی‌که عدم ممنوعیت استفاده از آنها در حوزه پیشگیری موقعیت‌مدار از جرم کاملاً ناموجه به‌نظر می‌رسد؛ زیرا به‌کارگیری همین الگوریتم‌ها در موقعیت‌های پیشگیرانه و امنیتی، می‌تواند خطر نقض کرامت انسانی، ایجاد تبعیض و مداخله ناقض حقوق و آزادی‌ها را به‌مراتب بیش از دو حوزه مذکور افزایش دهد. بااین‌حال، طبق بند۱-c ضمیمه سوم این قانون، کاربست این سامانه‌ها در سایر حوزه‌ها پرخطر محسوب شده و باید از الزامات مربوط به این دسته پیروی نمایند. افزون‌بر این، درصورتی‌که الگوریتم‌های شناسایی احساسات مشمول قواعد فوق درباره پیش‌بینی جرم قرار بگیرند، به‌کارگیری آنان نیز ممنوع خواهد بود. این رویکرد ناموجه، معیار دسته‌بندی سامانه‌های هوش‌مصنوعی را با ابهام و عدم انسجام مواجه می‌سازد.

۳. ۳. وضعیت حقوقی پایش موقعیت‌محور و جمعیت‌محور

قانون هوش‌مصنوعی ۲۰۲۴ مقررات مستقلی درباره استفاده از الگوریتم‌های ردیابی سوژه و اشیا و شناسایی ناهنجاری جمعیت پیش‌بینی نکرده است. بنابراین، مادام که این سامانه‌ها در زمرهٔ سامانه‌های دارای خطر غیرقابل قبول یا پرخطر قرار نگیرند، صرفاً ملزم به رعایت مفاد قانون حفاظت از داده‌های شخصی ۲۰۱۶ خواهند بود.

بااین‌حال، درصورتی‌که کارکرد این سامانه‌ها بر یکی از موارد مذکور در ماده ۵ یا ضمیمه سوم این قانون منطبق گردد، ممنوعیت‌ها و محدودیت‌های جدی بر آنها اعمال می‌شود. برای‌مثال، استفاده از سامانه‌های تحلیل رفتار جمعیت برای شناسایی هویت بایومتریک، تحلیل احساسات، پروفایل‌سازی و یا ایجاد و گسترش بی‌هدف پایگاه‌های دادهٔ تشخیص چهره، براساس مقرراتی که پیش‌تر ذکر شد، ممنوعیت یا محدودیت مواجه خواهد شد. همچنین، اگر هریک از الگوریتم‌های فوق بدون شناسایی هویت یا پیش‌بینی ارتکاب جرم توسط شخص خاص مورد استفاده قرار گیرند، قانون هوش‌مصنوعی مانعی برای به‌کارگیری آنها تعیین نکرده است؛ اما چنانچه این سامانه‌ها توسط نهادهای اجرای قانون و بر مبنای تحلیل داده‌های فردی، مانند تغییر سرعت و جهت حرکت، برای پیش‌بینی ارتکاب جرم اشخاص حقیقی به‌کار گرفته شوند، طبق بند۶-d ضمیمه سوم این قانون پرخطر محسوب شده و مشمول محدودیت‌های سخت‌گیرانه خواهند شد.

نتیجه‌گیری

سامانه‌های نظارت تصویری هوش‌بنیان، اگرچه به‌تنهایی از وقوع جرائم در سطح جامعه پیشگیری نمی‌کنند، جایگاه مهمی را در سبد تدابیر پیشگیری موقعیت‌مدار به خود اختصاص داده‌اند. براساس یافته‌های این پژوهش، بهره‌گیری مسئولانه و کارآمد از ظرفیت‌های پیشگیرانه این سامانه‌ها هنگامی ممکن است که با سیاست‌گذاری ارزش‌مدار و انسان‌محور همراه شود و از طریق جلب اعتماد عمومی و مشارکت سازندهٔ شهروندان در راستای تأمین امنیت به‌نحو مشروع اعمال گردد؛ درغیراین‌صورت به کاهش اعتماد اجتماعی و شکست اهداف پیشگیرانه منجر خواهد شد. ازاین‌رو، نظام حقوقی موظف است چارچوبی دقیق و شفاف برای نحوهٔ جمع‌آوری، پردازش و نگهداری داده‌ها، رعایت حریم خصوصی، صیانت از آزادی‌های بنیادین، پیاده‌سازی استانداردهای فنی و تعیین مسئولیت نهادها و ناظران انسانی ارائه کند؛ چنان‌که قانون

هوش‌مصنوعی ۲۰۲۴ گامی مهم و شایسته در مسیر دستیابی به آن برداشته است.البته، استمرار و ارتقای کارآمدی و مشروعیت این قانون، مشروط به تکمیل و اصلاح کاستی‌های مذکور در این نوشتار و توجه به سایر انتقاداتی است که نیازمند پژوهش‌های دیگر خواهد بود.

در نظام حقوقی ایران، باوجود گسترش نظارت تصویری در سال‌های اخیر توسط نهادهایی همچون پلیس[1] و تصریح بند اول ماده ۵ سند ملی هوش‌مصنوعی۱۴۰۳ به لزوم تدوین نظام حکمرانی داده، لوایح قانونی لازم به‌منظور ایجاد زیرساخت‌های حقوقی مورد نیاز برای مواجهه با مخاطرات هوش‌مصنوعی و تدوین استانداردهای مربوط به سامانه‌های هوش‌مصنوعی، هنوز هیچ مقرره تخصصی در این حوزه تهیه نشده و وظیفهٔ مدیریت چالش‌ها تنها بر عهدهٔ چند مادهٔ قانونی معدود و غیرتخصصی قرار گرفته است. قانونگذار اگرچه کنترل صوتی و تصویری خلاف قانون در محیط کار، اماکن عمومی و فروشگاه‌ها (ماده ۴۱ منشور حقوق شهروندی)، دسترسی غیرمجاز به داده‌های حفاظت شده (ماده ۱ قانون جرائم رایانه‌ای مصوب ۱۳۸۸)، انتشار غیرمجاز داده‌های شخصی (تبصره ماده ۲۱ قانون انتشار و دسترسی آزاد به اطلاعات مصوب ۱۳۸۷) و ذخیره، پردازش و توزیع داده پیام‌های شخصی (ماده ۵۸ قانون تجارت الکترونیک مصوب ۱۳۸۲) را جرم‌انگاری نموده، اما حدود حریم‌خصوصی و مصادیق دسترسی غیرمجاز همچنان مبهم است.[2]به‌علاوه، این مواد کلی و محدود، توان مواجهه با ابعاد، چالش‌ها و سرعت پیشرفت حوزهٔ پیچیدهٔ هوش‌مصنوعی را نداشته و در سامان‌دهی ظرفیت‌های آن، به‌ویژه هنگامی‌که توسط نهادهای قدرت به‌کار گرفته‌شود، ناکارآمدند. تداوم این خلأ قانونی، به عدم‌آگاهی مردم از حقوق خود، فقدان محدودیت‌های لازم برای نهادهای حاکمیتی، رواج تفسیرهای سلیقه‌ای و موسع و بروز بحران‌های حقوقی، اجتماعی و اخلاقی خواهد انجامید. همچنین، مطالعات مشخصی برای پایش وضعیت نظارت تصویری هوش‌بنیان در ایران یافت نشد که پیشنهاد می‌شود با توجه به اهمیت آن، مدنظر پژوهشگران قرار گیرد.

براین‌اساس، تدوین و تصویب قانون جامع هوش‌مصنوعی ضرورتی غیرقابل انکار تلقی می‌شود؛ قانونی که نه‌تنها باید محدودهٔ مجاز و الزامات استفاده از فناوری هوش‌مصنوعی را در حوزه‌های حساسی همچون پیشگیری موقعیت‌مدار از جرم و تحقیقات جنایی مشخص کند، بلکه باید تکالیف و مسئولیت‌های تمامی اشخاص حقیقی و حقوقی را نیز تعیین نماید. همچنین پیشنهاد می‌شود چارچوب ملی ارزیابی ریسک فناوری‌های هوش‌مصنوعی طراحی شود تا پیش از استقرار هر سامانهٔ هوش‌بنیان، ریسک‌های فنی، حقوقی، اخلاقی و امنیتی آن سنجیده شده و درصورت کسب امتیاز لازم، مجوز بهره‌برداری صادر گردد. چنین سازوکاری بنیان لازم برای استفادهٔ مسئولانه و کرامت‌محور از هوش‌مصنوعی را فراهم خواهد آورد.

نظارت بر این پهنهٔ پیچیده، پویا و تخصصی نیازمند یک نهاد ملی مستقل و متشکل از متخصصان هوش‌مصنوعی، حقوق‌دانان و سیاستگذاران حوزه فناوری است. اهمیت استقلال این نهاد زمانی آشکارتر می‌گردد که از قاعده‌مندسازی و نظارت بر نحوهٔ استفادهٔ نهادهای حاکمیتی از سامانه‌های نظارتی هوش‌بنیان سخن به میان می‌آید؛ زیرا یک نهاد مستقل از اختیارات بیشتر و ارادهٔ راسخ‌تری برای جلوگیری از تجاوز از مرزهای قانونی، تفسیرهای سلیقه‌ای یا سوءاستفاده از این ابزار توسط حاکمیت‌ها و نهادهای صاحب قدرت همچون پلیس، برخوردار است. ازاین‌رو، پیشنهاد می‌شود سازمان ملی

---

[1]. طبق بند (خ) ماده ۱۰۳ قانون برنامه پنج‌ساله هفتم پیشرفت جمهوری اسلامی ایران (۱۴۰۳ـ ۱۴۰۷)، دسترسی به سامانه‌های نظارتی (کنترلی) و مراقبتی هوشمند کلیه معابر اصلی، میادین و بزرگ‌راه‌ها در مراکز استان‌ها، کلان شهرها، جاده‌های اصلی و آزادراه‌ها که توسط شهرداری‌ها و وزارت راه و شهرسازی، نصب، نگهداری و به‌روزرسانی می‌شود نیز، به‌صورت برخط در اختیار فرماندهی انتظامی قرار می‌گیرد.

[2]. قناد، فاطمه و الهام شریف، «مطالعه اجمالی حمایت از داده‌های شخصی در نظام حقوقی ایران و سند مقررات عمومی حفاظت از داده‌های اتحادیه اروپا»، *دوفصلنامه حقوق فناوری‌های نوین*، دوره ۲، شماره ۴، ۱۴۰۰، ص ۱۸.

نظارت بر هوش‌مصنوعی با استقلال حقوقی و اداری تأسیس شود و مسئولیت تهیه پیش‌نویس مقررات، نظارت بر اجرای قانون و انجام ممیّزی‌های دوره‌ای را برعهده گیرد. یادآوری می‌شود که هم‌اکنون، هیچگونه نظارت بیرونی بر نحوهٔ استفادهٔ نهادهای دولتی و انتظامی از سامانه‌های نظارت‌تصویری در ایران وجود ندارد.

ازسوی‌دیگر، به رسمیت شناختن حقوق شهروندان در مواجهه با فناوری‌های هوش‌مصنوعی از الزامات بنیادین در بستر حکمرانی داده‌محور و هوش‌بنیان است. ازاین‌رو، لازم است دسترسی افراد به سوابق پردازش الگوریتم‌ها در مواقعی که تصمیم سامانه بر حقوق و آزادی‌های آنان اثر می‌گذارد، حق اعتراض به نتایج پردازش‌ها و الزام نهادها به پاسخ‌گویی و شفاف‌سازی نیز تصویب و تضمین شود. تحقق این امر از طریق ایجاد مرکز رسیدگی به شکایات الگوریتمی که زیرنظر سازمان مستقل مذکور، با مشارکت نهادهایی همچون قوه قضائیه، امکان‌پذیر خواهد بود.

در نهایت، با توجه به ماهیت فراملی، بی‌مرز و پویای هوش‌مصنوعی، ایجاد هماهنگی‌های فنی و حقوقی در سطح بین‌المللی ضرورت دارد.[1] عدم‌انطباق مقررات داخلی با استانداردهای جهانی، می‌تواند کشور را در معرض انزوای حقوقی، اقتصادی و فناورانه قرار دهد. البته، رعایت این نکته به‌معنای بی‌توجهی به ارزش‌های فرهنگی جامعه نیست، بلکه مؤید رویکردی تلفیقی است که علاوه‌بر معرفی ارزش‌های اخلاقی و فرهنگی جامعهٔ ایران در سطح بین‌المللی، بر بهره‌گیری از ظرفیت‌های مثبت و تجربیات موفق دیگر جوامع با هدف ارتقای وضعیت حکمرانی در حوزهٔ فناوری و همسویی با جامعهٔ جهانی، تأکید می‌کند.

منابع

کتاب

۱. انصاری، باقر، ***حقوق داده‌ها و هوش مصنوعی: مفاهیم و چالش‌ها***، تهران: شرکت سهامی انتشار، چاپ اول، ۱۴۰۰.

۲. پرادل، ژان، ***تاریخ اندیشه‌های کیفری***، ترجمه علی‌حسین نجفی ابرندآبادی، تهران: سمت، چاپ چهارم، ۱۳۸۸.

۳. کانت، ایمانوئل، ***نقد عقل عملی***، ترجمه انشاءالله رحمتی، تهران: نورالثقلین، ۱۳۸۵.

۴. نیازپور، امیرحسن، ***پیشگیری از جرم***، تهران: دادگستر، چاپ دوم، ۱۴۰۲.

مقاله

۵. اصفهانی، بابک و صابر نیاورانی، «اصل تناسب، ابزار تضمین و تعادل میان حق‌ها و آزادی‌های بنیادین و منافع عمومی»، *فصلنامه تحقیقات حقوقی*، دوره ۲۷، شماره ۴، ۱۴۰۳، صص ۲۰۷-۲۲۴. https://doi.org/10.48308/jlr.2022.220751.1852

۶. قناد، فاطمه و الهام شریف، «مطالعه اجمالی حمایت از داده‌های شخصی در نظام حقوقی ایران و سند مقررات عمومی حفاظت از داده‌های اتحادیه اروپا»، *دوفصلنامه حقوق فناوری‌های نوین*، دوره ۲، شماره ۴، ۱۴۰۰، صص۱-۲۲. https://doi.org/10.22133/clj.2021.244608.1020

[1]. قانون هوش‌مصنوعی۲۰۲۴، نمونه‌ای مهم برای ایجاد رویکردی واحد و هماهنگ در سطح منطقه به‌شمار می‌رود. «پیمان جهانی دیجیتال»(Global Digital Compact) مصوب۲۰۲۴ نیز، چارچوب پیشنهادی سازمان ملل متحد برای تقویت همکاری جهانی در زمینه فناوری‌های دیجیتال ازجمله هوش‌مصنوعی است. در این راستا، شورای عالی فضای مجازی ایران در سال ۱۴۰۱، تشکیل کارگروه تخصصی و تقسیم کار جهت مشارکت در روند شکل‌گیری پیمان جهانی دیجیتال سازمان ملل متحد را تصویب نمود؛ اگرچه به‌نظر می‌رسد تاکنون ارادهٔ جدی مبنی‌بر اجرای مفاد آن وجود نداشته است. همچنین، در سطح جهانی پیشنهادهایی برای تأسیس آژانس بین‌المللی هوش‌مصنوعی (IAIA) با الگوبرداری از آژانس بین‌المللی انرژی اتمی (IAEI) ارائه شده است.

References

Books

1. Ansari, Bagher, *Data Rights and Artificial Intelligence: Concepts and Challenges*, Tehran: Sahami Enteshar Company, First Edition, 2021. (In Persian)
2. Kant, Immanuel, *Critique of Practical Reason,* Translated by: InshaAllah Rahmati, Tehran: Nour al-Thaqalain, 2006. (In Persian)
3. Niazpour, Amir Hassan, *Crime Prevention,* Tehran, Dadgostar, Second Edition, 2023. (In Persian)
4. Pradel, Jean, *History of Penal Doctrines,* Translated by: Ali Hossein Najafi Abrand-Abadi, Tehran: Samt, Fourth Edition, 2009. (In Persian)

Articles

5. Akpulat, M., and M. Ekinci, "Anomaly Detection in Crowd Scenes via Cross Trajectories", *Applied Intelligence*, Vol 55, Issue 525, 2025, pp.1-16. https://doi.org/10.1007/s10489-025-06338-z /
6. Ali, M. M., "Real-Time Video Anomaly Detection for Smart Surveillance", IET Image Processing, Vol 17, Issue 5, 2023, pp.1375-1388.https://doi.org/10.1049/ipr2.12720/
7. Chen, K., X. Yang, C. Fan, W. Zhang, and Y. Ding, "Semantic-Rich Facial Emotional Expression Recognition", *IEEE Transactions on Affective Computing*, Vol 13, Issue 4, 2022, pp.1906-1916. https://doi.org/10.1109/TAFFC.2022.3201290/
8. Choung, H., P. David, and T-W. Ling. "Acceptance of AI-Powered Facial Recognition Technology in Surveillance Scenarios:Role of Trust, Security, and Privacy Perceptions", *Technology in Society,* Vol 79, 2024, pp.1-11.https://doi.org/10.1016/j.techsoc.2024.102721/
9. Clarke, R. V., "Situational Crime Prevention: Its Theoretical Basis and Practical Scope", *Crime and Justice: A Review of Research*, *University of Chicago Press*, Vol 4, 1983, pp.225–256. https://doi.org/10.1086/449090
10. Ebers, M., V. R. S. Hoch, F. Rosenkranz, H. Ruschemeier, and B. Steinrötter. "The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society(RAILS)", *J — Multidisciplinary Scientific Journal,* Vol 4, Issue 4, 2021, pp.589-603. https://doi.org/10.3390/j4040043/
11. Esfahani, Babak and Saber Niavarani, "The Principle of Proportionality; A Tool to Guarantee and Balance the Fundamental Rights and Freedoms and Public Interests", *Legal Research Quarterly*, Volume 27, Issue 4, 2024, pp.207-224. (In Persian) https://doi.org/10.48308/jlr.2022.220751.1852/
12. Feng, W., F. Wang, R. Han, Y. Gan, Z. Qian, J. Hou, and S. Wang, "Unveiling the Power of Self-Supervision for Multi-View Multi-Human Association and Tracking", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol 47, Issue 1, 2025, pp.351-368. https://doi.org/10.1109/TPAMI.2024.3463966/
13. Feretzakis, G., K. Papaspyridis, A. Gkoulalas-Divanis, and V. S. Verykios, "Privacy-Preserving Techniques in Generative AI and Large Language Models: A Narrative Review", *Information*, Vol 15, Issue 11, 2024, pp.1-25. https://doi.org/10.3390/info15110697/
14. Fontes, C., E. Hohma, C. C. Corrigan, and C. Lütge, "AI-Powered Public Surveillance Systems: Why We (Might) Need Them and How We Want Them", *Technology in Society*, Vol 71, 2022, pp.1-12. https://doi.org/10.1016/j.techsoc.2022.102137 /
15. Ghanad, Fatemeh and Elham Sharif, "Comprehensive Study of Personal Data Protection in Iran's Legal System and European General Data Protection Regulations", *Modern Technologies Law Quarterly,* Volumw 2, Issue 4, 2021, pp.1-22. (In Persian) https://doi.org/10.22133/clj.2021.244608.1020/

16. Guan, Z., Z. Wang, G. Zhang, L. Li, M. Zhang, Z. Shi, and N. Jiang. "Multi-Object Tracking Review: Retrospective and Emerging Trend", *Artificial Intelligence Review*, Vol 58, Issue 235, 2025, pp.1-46. https://doi.org/10.1007/s10462-025-11212-y/
17. Haley, P. "The Impact of Biometric Surveillance on Reducing Violent Crime: Strategies for Apprehending Criminals While Protecting the Innocent", *Sensors*, Vol 25, Issue 10, 2025, pp.1-21. https://doi.org/10.3390/s25103160 /
18. Huang, J., L. Li, L. Qing, W. Tang, P. Wang, L. Guo, and Y. Peng. "Spatio-Temporal Interactive Reasoning Model for Multi-Group Activity Recognition", *Pattern Recognition*, Vol 159, 2025, pp.1-14. https://doi.org/10.1016/j.patcog.2024.111104/
19. Johnson, T. L., N. N. Johnson, V. Topalli, D. McCurdy, and A. Wallace. "Police Facial Recognition Applications and Violent Crime Control in U.S. Cities", *Cities,* Vol 155, 2024, pp.1-14. https://doi.org/10.1016/j.cities.2024.105472 /
20. Matei, A-D., E. Talavera, and M. Aghae."Crime Scene Classification from Skeletal Trajectory Analysis in Surveillance Settings", *Engineering Applications of Artificial Intelligence*, Vol 141, 2025, pp.1-14. https://doi.org/10.1016/j.engappai.2024.109800
21. Podoletz, L. "We Have to Talk about Emotional AI and Crime", *AI & Society*, Vol 38, Issue 3, 2023, pp.1067–1082. https://doi.org/10.1007/s00146-022-01435-w/
22. Rezaee, Kh, S. Rezakhani, M. R. Khosravi, and M. K. Moghimi. "A Survey on Deep Learning-Based Real-Time Crowd Anomaly Detection for Secure Distributed Video Surveillance", *Personal and Ubiquitous Computing,* Vol 28, Issue 1, 2024, pp.135–151.https://doi.org/10.1007/s00779-021-01586-5/
23. Serna, I., A. Morales, J. Fierrez, and N. Obradovich. "Sensitive Loss: Improving Accuracy and Fairness of Face Representations with Discrimination-aware Deep Learning", *Artificial Intelligence,* Vol 305, 2022, pp.1-15.https://doi.org/10.1016/j.artint.2022.103682/
24. Simmler, M., and G. Canova. "Facial Recognition Technology in Law Enforcement: Regulating Data Analysis of Another Kind", *Computer Law & Security Review*, Vol 56, 2025, pp.1-10. https://doi.org/10.1016/j.clsr.2024.106092/
25. Talaei Khoei, T., and A. Singh. "A Survey of Emotional Artificial Intelligence and Crimes: Detection, Prediction, Challenges and Future Direction", *Journal of Computational Social Science,* Vol 7, 2024, pp.2359–2402. https://doi.org/10.1007/s42001-024-00313-3/
26. Veltmeijer, E., and C. Gerritsen. "Legal and Ethical Implications of AI-based Crowd Analysis: The AI Act and Beyond", *AI Ethics*, Vol 5, Issue 3, 2025, pp.3173–3183. https://doi.org/10.1007/s43681-024-00644-x/
27. Welsh, B. C., and D. P. Farrington. "Surveillance for Crime Prevention in Public Space: Results and Policy Choices in Britain and America", *Criminology and Public Policy*, Vol 3, Issue 3, 2004, pp.497–526. https://doi.org/10.1111/j.1745-9133.2004.tb00054.x/
28. Zaidenberg, S., B. Boulay, and F. Brémond. "A Generic Framework for Video Understanding Applied to Group Behavior Recognition", *IEEE Ninth International Conference on Advanced Video and Signal-Based Surveillance*, 2012, pp.1-7. https://doi.org/10.1109/AVSS.2012.1/
29. Zhou, L., and J. Xu. "Enhanced Abandoned Object Detection through Adaptive Dual-Background Modeling and SAO-YOLO Integration", *Sensors*, Vol 24, Issue 20, 2024, pp.1-20. https://doi.org/10.3390/s24206572

Reports

30. Ratcliffe, Jerry, "Video Surveillance of Public Places (Problem-Oriented Guides for Police. Response Guide Series. Guide No. 4)", *U.S.Department of Justice Office of Community Oriented Policing Services*, Washington, DC: Center for Problem-Oriented Policing, 2006. https://popcenter.asu.edu/sites/g/files/litvpz3631/files/video_surveillance.pdf
31. The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems. Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems,

First Edition. *IEEE*, 2019.https://standards.ieee.org/content/ieee-standards/en/industry-connections/ec/autonomous-systems.html/

Website

32. "CCTV Camera Market Size, Global Report 2022-2029", Fortune Business Insights, 2025, Accessed 02 December 2025. https://www.fortunebusinessinsights.com/cctv-camera-market-107115/