

A Comparative Analysis of the Status and Legal Requirements of Using Artificial Intelligence in Criminal Investigations, with Emphasis on the Iranian Criminal Justice System

1. Salameh Abolhasani*: Department of Criminal Law and Criminology, NT.C., Islamic Azad University, Tehran, Iran. Email: salameabolhasani@iau.ac.ir (Corresponding Author)
2. Mahboobeh Sharifi Roodbali: Department of Criminal Law and Criminology, NT.C., Islamic Azad University, Tehran, Iran
3. Morteza Azimi: Department of Criminal Law and Criminology, NT.C., Islamic Azad University, Tehran, Iran
4. Mehdi Baravandi: Department of Criminal Law and Criminology, NT.C., Islamic Azad University, Tehran, Iran

ABSTRACT

In the contemporary world, the integration of emerging technologies into law-enforcement and judicial processes has fundamentally transformed the traditional paradigm of criminal investigation. Accordingly, the present study aims to analyze the status and legal requirements governing the use of artificial intelligence in criminal investigations, with particular emphasis on the Iranian criminal justice system. The significance and necessity of this study arise from the fact that, despite enhancing the efficiency of processing and analyzing large volumes of criminal data, intelligent decision-support systems have created serious and far-reaching challenges to the protection of defendants' fundamental rights and the principles of a fair trial. These developments have made it increasingly necessary to reconsider the rules governing algorithmic accountability and judicial security. The principal research question is how the legal requirements and legislative challenges associated with the use of artificial intelligence tools in criminal investigation procedures can be explained and appropriately balanced within the Iranian legal system. The findings indicate that the absence of an explicit legal framework constitutes the principal obstacle to ensuring algorithmic transparency and accountability in the administration of smart justice. It is therefore necessary to revise the traditional rules governing evidence and to adopt specific regulations for managing the risks arising from automated analyses, thereby establishing an appropriate balance between the discovery of truth and the protection of human dignity. This study employs a descriptive-analytical research method based on library research and the examination of domestic and international legal instruments.

Keywords: *Artificial Intelligence, Criminal Investigations, Smart Justice, Fair Trial, Digital Evidence.*

How to cite: Abolhasani, S., Sharifi Roodbali, M., Azimi, M., & Baravandi, M. (2027). A Comparative Analysis of the Status and Legal Requirements of Using Artificial Intelligence in Criminal Investigations, with Emphasis on the Iranian Criminal Justice System. *Comparative Studies in Jurisprudence, Law, and Politics*, 9(1), 1-14.

© 2027 the authors. This is an open access article under the terms of the Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

Submit Date: 28 March 2026

Revise Date: 29 July 2026

Accept Date: 05 August 2026

Initial Publish Date: 21 September 2026

Final Publish Date: 21 April 2027



بررسی تطبیقی جایگاه و الزامات حقوقی استفاده از هوش مصنوعی در تحقیقات جنایی با تأکید بر نظام کیفری ایران

۱. سلامه ابوالحسنی*: گروه حقوق جزا و جرم‌شناسی، واحد تهران شمال، دانشگاه آزاد اسلامی، تهران، ایران.

پست الکترونیک: salameabolhasani@iau.ac.ir (نویسنده مسئول)

۲. محبوبه شریفی رودبالی: گروه حقوق کیفری و جرم‌شناسی، واحد تهران شمال، دانشگاه آزاد اسلامی، تهران، ایران

۳. مرتضی عظیمی: گروه حقوق کیفری و جرم‌شناسی، واحد تهران شمال، دانشگاه آزاد اسلامی، تهران، ایران

۴. مهدی براوندی: گروه حقوق کیفری و جرم‌شناسی، واحد تهران شمال، دانشگاه آزاد اسلامی، تهران، ایران

چکیده

در جهان معاصر، ادغام فناوری‌های نوظهور در فرآیندهای انتظامی و قضایی، پارادایم سنتی کشف جرم را با تحولی بنیادین مواجه ساخته است که پژوهش حاضر با هدف تحلیل جایگاه و الزامات حقوقی استفاده از هوش مصنوعی در تحقیقات جنایی، با تأکید بر نظام کیفری ایران، به این موضوع می‌پردازد. اهمیت و ضرورت این مطالعه از آن‌جا ناشی می‌شود که سیستم‌های تصمیم‌یار هوشمند با وجود افزایش کارآمدی در تحلیل داده‌های حجیم جنایی، چالش‌های جدی و دامنه‌داری را برای تضمین حقوق بنیادین متهمان و اصول دادرسی عادلانه ایجاد کرده‌اند و لزوم بازخوانی ضوابط حاکم بر مسئولیت الگوریتم‌ها و امنیت قضایی را بیش از پیش نمایان ساخته‌اند. پرسش اصلی این است که الزامات حقوقی و چالش‌های تقنینی به‌کارگیری ابزارهای هوش مصنوعی در فرآیند تحقیقات جنایی در نظام حقوقی ایران چگونه قابلیت تبیین و توازن‌یابی دارند. بر پایه بررسی‌های صورت‌گرفته، یافته‌ها نشان می‌دهد که فقدان چارچوب قانونی صریح، مانع اصلی در تضمین شفافیت الگوریتم‌ها و مسئولیت‌پذیری در اجرای عدالت هوشمند است و ضرورت دارد تا با بازنگری در قواعد سنتی ادله اثبات دعوا و تدوین مقررات اختصاصی برای مدیریت ریسک‌های ناشی از تحلیل‌های خودکار، تعادلی میان کشف حقیقت و حفظ کرامت انسانی برقرار گردد. روش تحقیق حاضر توصیفی-تحلیلی با بهره‌گیری از مطالعات کتابخانه‌ای و اسناد حقوقی بین‌المللی و داخلی است.

واژگان کلیدی: هوش مصنوعی، تحقیقات جنایی، عدالت هوشمند، دادرسی عادلانه، ادله دیجیتال.

نحوه استناددهی: ابوالحسنی، سلامه، شریفی رودبالی، محبوبه، عظیمی، مرتضی، و براوندی، مهدی. (۱۴۰۶). بررسی تطبیقی جایگاه و الزامات حقوقی استفاده از هوش مصنوعی در تحقیقات جنایی با تأکید بر نظام کیفری ایران. *پژوهش‌های تطبیقی فقه، حقوق و سیاست*، ۹(۱)، ۱-۱۴.

© ۱۴۰۶ تمامی حقوق انتشار این مقاله متعلق به نویسنده است. انتشار این مقاله به‌صورت دسترسی آزاد مطابق با گواهی (CC BY-NC 4.0) صورت گرفته است.

تاریخ ارسال: ۸ فروردین ۱۴۰۵

تاریخ بازنگری: ۷ مرداد ۱۴۰۵

تاریخ پذیرش: ۱۴ مرداد ۱۴۰۵

تاریخ چاپ اولیه: ۳۰ شهریور ۱۴۰۵

تاریخ چاپ نهایی: ۱ اردیبهشت ۱۴۰۶

مقدمه

در نظام‌های حقوقی معاصر، نظر غالب بر این استوار است که به‌کارگیری هوش مصنوعی در تحقیقات جنایی، با هدف بهینه‌سازی سرعت و دقت در فرآیند کشف حقیقت، امری اجتناب‌ناپذیر و در خدمت تحقق عدالت کیفری است و طرفداران این دیدگاه، با تأکید بر قدرت تحلیل داده‌های کلان توسط الگوریتم‌ها، معتقدند که جایگزینی یا تقویت قضاوت انسانی با سیستم‌های هوشمند، خطاهای شناختی را کاهش داده و امنیت عمومی را ارتقا می‌بخشد. با این حال، رویکرد این مقاله متفاوت از این نگاه ابزاری صرف بوده و بر این مبنا استوار است که هوش مصنوعی در دادرسی کیفری نباید به مثابه جعبه‌ای سیاه نگریسته شود که تصمیماتش واجد اعتبار ذاتی است؛ بلکه این ابزارها باید همواره ذیل اصول آمره دادرسی عادلانه، اصل شفافیت و حق دفاع متهم ارزیابی شوند تا از تبدیل شدن عدالت پیش‌دستانه به ابزاری برای نقض حقوق شهروندی جلوگیری به عمل آید. نوآوری اصلی این پژوهش در این است که، برخلاف مطالعات موجود که عمدتاً بر جنبه‌های فنی یا کلیات اخلاقی متمرکز هستند، به صورت تخصصی و درون‌ساختاری، چالش‌های انطباق منطق الگوریتمیک را با مفاهیم کلاسیک ادله اثبات دعوا در حقوق کیفری ایران واکاوی می‌کند و با نقد خالاهای تقنینی، الگویی برای مسئولیت‌پذیری پلتفرم‌های ارائه‌دهنده خدمات هوش مصنوعی در تحقیقات جنایی ارائه می‌دهد. این مطالعه، با عبور از نگاه‌های تقدیس‌گرایانه یا هراس‌افکنانه نسبت به فناوری، به دنبال برقراری یک تعادل حقوقی میان ضرورت‌های انتظامی و صیانت از حریم خصوصی و کرامت انسانی است و تلاش دارد تا در بستری از واقع‌گرایی حقوقی، راهکارهایی برای گذار از دادرسی‌های سنتی به سمت یک حکمرانی دیجیتال مسئولیت‌پذیر در نظام کیفری ایران ترسیم نماید، به نحوی که استفاده از هوش مصنوعی، به جای تهدید امنیت قضایی، ضامن عدالت مبتنی بر شواهد و تضمین‌کننده رویه‌های شفاف دادرسی باشد. این پژوهش، ضمن شناسایی چالش‌های ساختاری در سیستم قضایی ایران، راهبردهایی برای اصلاح زیرساخت‌های نظارتی پیشنهاد می‌کند که در نهایت، منجر به ایجاد یک سیستم عدالت کیفری هوشمند، اما مقید به قواعد بنیادین حقوق بشر می‌گردد.

مفاهیم بنیادین و مبانی نظری به‌کارگیری هوش مصنوعی در کشف جرم

تبیین ماهیت فنی و کارکردهای چندگانه هوش مصنوعی در فرآیندهای جنایی، پیش‌شرط فهم تحولاتی است که الگوریتم‌های پیشرفته، با پردازش داده‌های کلان و شناسایی الگوهای پیچیده مجرمانه، در توانمندی‌های اکتشافی ایجاد کرده‌اند؛ فرآیندی که در پیوند با جایگاه حقوقی ادله دیجیتال و سیستم‌های تصمیم‌یار در حقوق کیفری مدرن، مفاهیم سنتی شواهد و مدارک را دگرگون ساخته و نظام‌های حقوقی را با چالش‌های نوینی در نحوه پذیرش و ارزیابی استنادات دیجیتال مواجه کرده است.

تبیین ماهیت و کارکردهای هوش مصنوعی در فرآیندهای جنایی

کاربرد هوش مصنوعی و یادگیری ماشین در نظام عدالت کیفری، از جمله مهم‌ترین و درعین حال مناقشه‌برانگیزترین چالش‌های علمی و حقوقی عصر حاضر به شمار می‌رود (Ashabi et al., 2025). این در حالی است که هوش مصنوعی در نظام عدالت کیفری، با بهره‌گیری از الگوریتم‌های یادگیری ماشین و تحلیل کلان‌داده‌ها، نقش تعیین‌کننده‌ای در پیش‌بینی رفتارهای مجرمانه، شناسایی الگوهای ارتکاب جرم و بهینه‌سازی فرآیندهای تحقیقاتی ایفا می‌کند؛ این فناوری نه تنها در مرحله کشف جرم، از طریق سیستم‌های هوشمند پایش تصویری و تحلیل داده‌های دیجیتال، به کار گرفته می‌شود، بلکه در مراحل دادرسی نیز، به عنوان ابزاری برای ارزیابی ریسک تکرار جرم توسط متهمان، جهت کمک به قضات در تصمیم‌گیری برای صدور قرارهای تأمین کیفری یا تعیین مجازات، اهمیت روزافزونی یافته است.

باین‌حال، استفاده از این سیستم‌ها با چالش‌های بنیادین حقوقی، از قبیل ابهام در شفافیت الگوریتمی، احتمال سوگیری‌های نژادی یا طبقاتی نهفته در داده‌های آموزشی و چالش‌های مربوط به اصل تساوی سلاح‌ها و حق دفاع متهم، مواجه است؛ چراکه استناد به نتایج «جعبه سیاه» هوش مصنوعی، بدون امکان ارزیابی دقیق نحوه دستیابی به آن نتایج، می‌تواند مخاطرات جدی برای رعایت موازین دادرسی منصفانه به همراه داشته باشد. در همین راستا، پرونده قضایی ایالت ویسکانسین علیه اریک لومیس (۲۰۱۶) در ایالات متحده، یکی از برجسته‌ترین نمونه‌های تحلیل‌شده در این زمینه است (Aljinovic, 2024) که در آن، استفاده از ابزار ارزیابی ریسک «کومپس» [COMPAS] برای تعیین مجازات متهم مورد چالش قرار گرفت؛ لومیس استدلال کرد که تکیه دادگاه بر یک الگوریتم اختصاصی و غیرشفاف، حق او برای فرآیند قانونی عادلانه را نقض کرده است؛ زیرا امکان بررسی و به چالش کشیدن مبنای محاسباتی این سیستم برای وی فراهم نبود. اگرچه دیوان عالی ویسکانسین در نهایت، استفاده از این ابزار را با شروط خاصی مجاز دانست، اما این پرونده به نقطه عطفی در ادبیات حقوقی پیرامون ضرورت پاسخ‌گویی، شفافیت و نظارت انسانی بر فناوری‌های هوش مصنوعی در حوزه عدالت کیفری تبدیل شد که جزئیات و تحلیل‌های حقوقی مرتبط با آن در دسترس می‌باشد.

جایگاه ادله دیجیتال و سیستم‌های تصمیم‌یار در حقوق کیفری مدرن

یکی از مباحث مهم و حساس در نظام‌های حقوقی، ادله و نحوه استناد و پذیرش آن جهت اثبات یا رد دعوی خصوصی و جزایی است، به‌نحوی که می‌توان گفت بدون دلیل، هیچ دعوایی سرانجام ندارد؛ پس اسناد و مدارک ناشی از کارکردهای فناوری اطلاعات را نیز باید در همان فضا و به‌صورت الکترونیکی جست‌وجو کرد (Heydarinejad, 2017). در این میان، جایگاه ادله دیجیتال و سیستم‌های تصمیم‌یار در حقوق کیفری مدرن، به‌طور فزاینده‌ای از یک ابزار کمکی فراتر رفته و به یکی از عناصر مؤثر در فرآیند کشف جرم، تحلیل شواهد، ارزیابی خطر و تصمیم‌سازی قضایی تبدیل شده است. ادله دیجیتال شامل داده‌های استخراج‌شده از تلفن‌های همراه، رایانه‌ها، دوربین‌های نظارتی، سامانه‌های موقعیت‌یاب، شبکه‌های اجتماعی و سایر آثار الکترونیکی است که در بسیاری از پرونده‌های کیفری، نقش تعیین‌کننده‌ای در اثبات یا رد اتهام دارند. در کنار آن، سیستم‌های تصمیم‌یار مبتنی بر هوش مصنوعی، با تحلیل حجم گسترده‌ای از داده‌های جنایی، الگوهای رفتاری و سوابق کیفری، می‌توانند به ضابطان و مقامات قضایی در شناسایی مظنونان، پیش‌بینی احتمال تکرار جرم، اولویت‌بندی تحقیقات و ارزیابی ریسک کمک کنند. با وجود این، حقوق کیفری مدرن استفاده از چنین ابزارهایی را تنها در صورتی مشروع می‌داند که اصل شفافیت، قابلیت راستی‌آزمایی، امکان اعتراض متهم و نظارت انسانی بر تصمیمات الگوریتمی تضمین شود؛ زیرا تصمیم‌های مبتنی بر الگوریتم نباید جایگزین قضاوت مستقل مقام قضایی شوند.

یکی از نمونه‌های جدید و قابل‌توجه در زمینه ارزیابی اعتبار ادله دیجیتال و سامانه‌های هوش مصنوعی، پرونده‌های مرتبط با ابزار Cybercheck در ایالت اوهایو آمریکا است که در سال‌های ۲۰۲۴ و ۲۰۲۵، با انتقادهای گسترده قضایی و علمی مواجه شد (Feathers, 2024). این سامانه، با بهره‌گیری از الگوریتم‌های هوش مصنوعی و تحلیل داده‌های متن‌باز، مدعی تعیین موقعیت مکانی مظنونان با درصد بالایی از اطمینان بود و گزارش‌های آن در چند پرونده قتل، به‌عنوان مستند تحقیقات مورد استفاده قرار گرفت. باین‌حال، پس از بررسی‌های کارشناسی مشخص شد که الگوریتم Cybercheck فاقد شفافیت کافی بوده، امکان راستی‌آزمایی مستقل نتایج آن وجود ندارد و حتی در برخی پرونده‌ها، داده‌های نادرست یا تاریخ‌های اشتباه مبنای تحلیل قرار گرفته است. در نتیجه، دادستان‌های چند حوزه قضایی استفاده از این گزارش‌ها را کنار گذاشتند و برخی دادگاه‌ها نیز اعتبار آن را مورد تردید قرار دادند.

این پرونده نشان می‌دهد که در حقوق کیفری مدرن، ادله دیجیتال، هرچند می‌تواند سرعت و دقت تحقیقات جنایی را افزایش دهد، اما تا زمانی که منشأ داده‌ها، نحوه عملکرد الگوریتم، میزان خطا و امکان ارزیابی مستقل آن برای طرفین دعوا روشن نباشد، نمی‌تواند جایگزین ادله سنتی یا مبنای انحصاری تصمیمات قضایی قرار گیرد. تجربه Cybercheck بیانگر آن است که اصل دادرسی عادلانه اقتضا می‌کند متهم و وکیل وی بتوانند روش تولید ادله دیجیتال را مورد اعتراض و ارزیابی قرار دهند؛ زیرا اتکای صرف به خروجی سامانه‌های هوشمند، بدون قابلیت توضیح‌پذیری، خطر محکومیت‌های نادرست و نقض حقوق دفاعی را افزایش می‌دهد. این رویکرد با گرایش جدید ادبیات حقوقی نیز همسو است که بر ضرورت «دقت رویه‌ای»، قابلیت ممیزی الگوریتم‌ها و حفظ زنجیره اعتبار ادله دیجیتال در تحقیقات کیفری تأکید می‌کند.

ظرفیت‌ها و چالش‌های حقوقی استفاده از هوش مصنوعی در تحقیقات جنایی ایران

انطباق ابزارهای هوشمند با اصول بنیادین دادرسی عادلانه و حقوق شهروندی، نیازمند واکاوی چالش‌های تقابلی میان کارآمدی پلیسی و حریم خصوصی متهمان در فضای حقوقی است که در امتداد آن، با شناسایی خلأهای قانونی و نارسایی‌های زیرساختی در نظام کیفری ایران، مشخص می‌شود چگونه فقدان مقررات صریح برای مدیریت سیستم‌های خودکار، امنیت قضایی را در فرآیندهای تحقیقات مقدماتی با مخاطرات جدی روبه‌رو ساخته و توازن میان کشف حقیقت و صیانت از حقوق دفاعی را مخدوش کرده است.

انطباق ابزارهای هوشمند با اصول دادرسی عادلانه و حقوق شهروندی

نظام حقوقی ایران در مواجهه با ابزارهای هوشمند در تحقیقات جنایی، با چالش جدی فقدان نص صریح در آیین دادرسی کیفری مواجه است؛ چراکه اصول بنیادین دادرسی عادلانه مندرج در قانون اساسی و قانون آیین دادرسی کیفری، برای تعاملات سنتی میان ضابط و متهم تدوین شده‌اند و ظرفیت‌های فعلی قوانین، به دلیل عدم پیش‌بینی ماهیت الگوریتمیک ادله، برای صیانت از حقوق شهروندی در برابر تحلیل‌های خودکار هوش مصنوعی بسیار محدود است. این نارسایی، اصل برائت و حق دفاع متهم را در وضعیتی مخاطره‌آمیز قرار می‌دهد؛ زیرا هنگامی که یک سیستم تصمیم‌یار جنایی، بر پایه داده‌کاوی، گزارشی از احتمال ارتکاب جرم توسط فردی ارائه می‌دهد، به دلیل نبود شفافیت در کدهای برنامه‌نویسی یا همان ماهیت «جعبه سیاه» الگوریتم‌ها، متهم عملاً قادر به چالش کشیدن مبنای اتهام نبوده و حق رویارویی با ادله علیه خود، که در ماده ۳۵۱ قانون آیین دادرسی کیفری بر آن تأکید شده است، عملاً به حاشیه رانده می‌شود.

به عنوان مثال، اگر پلیس برای شناسایی هویت سارقان یا پیش‌بینی نقاط جرم‌خیز، از نرم‌افزارهای تشخیص چهره یا تحلیل رفتاری استفاده کند و بر پایه خطای الگوریتمی، شهروندی بی‌گناه را تحت پیگرد قرار دهد، قوانین جاری در زمینه مسئولیت مدنی دولت و نحوه جبران خسارت، فاقد زیرساخت لازم برای انتساب تقصیر به شرکت سازنده یا نهاد بهره‌بردار هستند و در نتیجه، شهروند در این خلأ قانونی نمی‌تواند علیه تصمیمات خودکار اتخاذشده، دادرسی متناسب و عادلانه‌ای را در دادگاه‌های کیفری به سرانجام برساند.

اگرچه ماده ۶۵ قانون آیین دادرسی کیفری، ضابطان را مکلف به رعایت حقوق شهروندی کرده است، اما تفسیر این تکلیف در فضای حکمرانی دیجیتال، نیازمند تدوین مقرراتی است که «حق بر توضیح» و «حق بر بازبینی انسانی» را در قبال خروجی‌های هوش مصنوعی تضمین کند؛ در غیر این صورت، ظرفیت فعلی قوانین ایران تنها در حد نظارت‌های صوری باقی مانده و توان مقابله با سوءاستفاده‌های احتمالی از فناوری در کشف جرم را نخواهد داشت، مگر آنکه با نگاهی به اصل ۱۵۸ قانون اساسی و ضرورت‌های دادرسی الکترونیک، بستری برای ایجاد نظام مسئولیت‌پذیر الگوریتمیک فراهم گردد که در آن، ماشین تنها به عنوان دستیار قاضی و نه قاضی نهایی، در چارچوب معیارهای دادرسی منصفانه عمل نماید.

تحلیل خلأهای قانونی و زیرساخت‌های نظارتی در نظام کیفری ایران

در نظام کیفری ایران، استفاده از هوش مصنوعی در تحقیقات جنایی، با وجود توسعه تدریجی سامانه‌های هوشمند در پلیس، پزشکی قانونی و قوه قضائیه، همچنان فاقد چارچوب قانونی اختصاصی و منسجم است. قانون آیین دادرسی کیفری، قانون جرایم رایانه‌ای و سایر مقررات موجود، اگرچه امکان بهره‌گیری از ادله الکترونیکی را فراهم کرده‌اند، اما درباره مشروعیت تصمیم‌های الگوریتمی، حدود استفاده از سامانه‌های پیش‌بینی جرم، مسئولیت ناشی از خطاهای هوش مصنوعی، معیارهای اعتبارسنجی خروجی الگوریتم‌ها و حقوق متهم در برابر تصمیم‌های خودکار سکوت کرده‌اند. این خلأ تقنینی می‌تواند موجب تضعیف اصل قانونی بودن دادرسی، حق دفاع، اصل برائت و شفافیت فرآیند تحقیقات شود؛ زیرا مشخص نیست در صورت وقوع خطا یا تبعیض الگوریتمی، مسئولیت متوجه توسعه‌دهنده سامانه، مقام قضایی، ضابط دادگستری یا نهاد بهره‌بردار خواهد بود.

از منظر نظارتی نیز، ایران فاقد نهاد مستقلی برای ارزیابی و ممیزی سامانه‌های هوش مصنوعی مورد استفاده در نظام عدالت کیفری است. در بسیاری از موارد، معیارهای فنی الگوریتم‌ها، میزان دقت، نرخ خطا، نحوه آموزش مدل‌های هوش مصنوعی و احتمال بروز سوگیری نسبت به گروه‌های مختلف اجتماعی، برای قضات، وکلا و حتی کاربران سازمانی شفاف نیست (Homiry, 2026). نبود سازوکارهای الزام‌آور برای انجام ارزیابی اثرات حقوق بنیادین [Fundamental Rights Impact Assessment]، ثبت و مستندسازی تصمیم‌های الگوریتمی و امکان اعتراض مؤثر به نتایج تولیدشده توسط هوش مصنوعی، می‌تواند اعتماد عمومی به عدالت کیفری را کاهش داده و زمینه بروز اختلافات قضایی درباره اعتبار ادله مبتنی بر هوش مصنوعی را فراهم کند.

در مقابل، اتحادیه اروپا طی سال‌های اخیر، چارچوب نسبتاً جامعی برای حکمرانی هوش مصنوعی ایجاد کرده است. مهم‌ترین نمونه، مقررات EU Artificial Intelligence Act است (Neuwirth, 2023) که بسیاری از کاربردهای هوش مصنوعی در حوزه اجرای قانون و عدالت کیفری را در زمره «سامانه‌های پرخطر» قرار داده است. این مقررات، توسعه‌دهندگان و بهره‌برداران را مکلف می‌کند پیش از استفاده از سامانه، ارزیابی ریسک، مستندسازی فنی، تضمین کیفیت داده‌های آموزشی، نظارت انسانی مؤثر، ثبت عملکرد سیستم، مدیریت سوگیری و امکان حسابرسی مستقل را فراهم کنند. همچنین، در کنار این مقررات، الزامات حفاظت از داده‌ها در چارچوب General Data Protection Regulation و دستورالعمل اجرای قانون (Law Enforcement Directive) نیز محدودیت‌های مهمی بر پردازش خودکار اطلاعات کیفری اعمال کرده‌اند.

نمونه عملی این رویکرد را می‌توان در رأی (Schufa Holding (Scoring) مشاهده کرد که دیوان دادگستری اتحادیه اروپا در سال ۲۰۲۳ صادر کرد (Paun, 2024). اگرچه موضوع پرونده مستقیماً تحقیقات جنایی نبود، اما دادگاه اعلام کرد تصمیم‌هایی که به‌طور اساسی بر افراد اثر می‌گذارند، نباید صرفاً بر پایه ارزیابی خودکار الگوریتمی اتخاذ شوند و اشخاص باید از حق اطلاع، امکان اعتراض و مداخله انسانی برخوردار باشند (Martinovic, 2025). این رأی به یکی از مهم‌ترین مبانی حقوقی اروپا در محدودسازی تصمیم‌گیری کاملاً خودکار تبدیل شده و آثار آن در حوزه‌های انتظامی و قضایی نیز مورد استناد قرار گرفته است؛ زیرا بر ضرورت شفافیت، پاسخ‌گویی و کنترل انسانی در استفاده از هوش مصنوعی تأکید دارد.

الگوگیری از تجربه اتحادیه اروپا می‌تواند مسیر اصلاح حقوق کیفری ایران را تسهیل کند. تدوین قانون اختصاصی درباره کاربرد هوش مصنوعی در تحقیقات جنایی، الزام به ارزیابی اثرات حقوق بنیادین پیش از استقرار سامانه‌های هوشمند، ایجاد نهاد مستقل برای ممیزی

الگوریتم‌ها، پیش‌بینی حق دسترسی متهم به مبانی تصمیم‌های الگوریتمی، تعیین مسئولیت مدنی و کیفری ناشی از خطاهای هوش مصنوعی و ممنوعیت اتکای انحصاری به تصمیم‌های خودکار در مراحل حساس تحقیقات، از جمله اقداماتی است که می‌تواند ضمن بهره‌گیری از مزایای فناوری، اصول دادرسی عادلانه، امنیت قضایی و حقوق بنیادین شهروندان را نیز تضمین کند. این اصلاحات، علاوه بر افزایش اعتماد عمومی به نظام عدالت کیفری، زمینه استفاده مسئولانه و قانونمند از فناوری‌های هوش مصنوعی را در فرآیند کشف جرم و تعقیب کیفری فراهم خواهد ساخت.

تحلیل تطبیقی و واکاوی امنیت قضایی در تعامل با هوش مصنوعی

ارزیابی انتقادی ضوابط حاکم بر مسئولیت مدنی و کیفری الگوریتم‌های جنایی در مواجهه با خطاهای احتمالی سیستم، گامی ضروری برای روشن‌سازی چالش‌های انتساب تقصیر و پاسخ‌گویی حقوقی در فضای سایبری است که در پرتو مدل‌های آینده‌نگرانه برای ارتقای اعتماد عمومی در عدالت کیفری هوشمند، چارچوبی را بر پایه شفافیت الگوریتمیک و نظارت قضایی مؤثر ترسیم می‌کند تا تعامل مسئولانه میان فناوری و نظام عدالت کیفری، فراتر از نگاه‌های ابزاری، تضمین‌کننده امنیت قضایی در مواجهه با تحولات دیجیتال باشد.

ارزیابی انتقادی ضوابط حاکم بر مسئولیت مدنی و کیفری الگوریتم‌های جنایی

با توجه به پیشرفت‌های چشمگیر در حوزه سیستم‌های هوش مصنوعی و تأثیرات گسترده آن‌ها در جنبه‌های مختلف زندگی، به نظر می‌رسد شناسایی شخصیت حقوقی برای این سامانه‌ها ضرورتی اجتناب‌ناپذیر باشد (Bagheri, 2025). بررسی نظام مسئولیت در حقوق ایران در مواجهه با خطاهای هوش مصنوعی جنایی، با چالش ناشی از عدم وجود شخصیتی حقوقی یا کیفی برای الگوریتم‌ها روبه‌روست؛ چراکه در قوانین موجود، به‌ویژه قانون مجازات اسلامی، مسئولیت کیفری تنها متوجه اشخاص حقیقی و یا اشخاص حقوقی شناخته‌شده، مطابق ماده ۱۴۳ قانون مجازات اسلامی، است و الگوریتم‌های هوشمند، به دلیل فقدان اراده و شعور حقوقی، قابلیت انطباق با این مفاهیم را ندارند؛ وضعیتی که انتساب تقصیر در جنایات ارتكابی توسط سیستم‌های خودکار را با بن‌بست تقنینی مواجه کرده است.

از منظر مسئولیت مدنی، اگرچه قانون مسئولیت مدنی ایران در مواد ۱ تا ۵، خسارات ناشی از تقصیر را قابل جبران می‌داند، اما در خصوص هوش مصنوعی، شناسایی عنصر «تقصیر» در لایه‌های پنهان کدگذاری یک سیستم تصمیم‌یار بسیار دشوار است؛ برای مثال، اگر یک الگوریتم تحلیل جرم، به‌طور اشتباه فردی را به‌عنوان مظنون اصلی شناسایی کرده و این گزارش منجر به بازداشت غیرقانونی و ورود خسارت به وی شود، معلوم نیست آیا تقصیر متوجه شرکت سازنده نرم‌افزار است، یا ضابط قضایی بهره‌بردار، یا حتی خود دیتاستی که داده‌های سوگیرانه به سیستم خورانده است. در تحلیل این مصادیق، تکیه بر قواعد سنتی مسئولیت، مانند «قاعده لاضرر» یا مسئولیت ناشی از «تسبیب»، به دلیل پیچیدگی زنجیره علت و معلولی در سیستم‌های هوشمند ناکارآمد است؛ چراکه سیستم‌های تصمیم‌یار جنایی اغلب در محیط‌های ابری و توسط پیمانکاران خصوصی توسعه می‌یابند که این امر، تمایز میان مسئولیت دولت و مسئولیت پیمانکار فنی را در دادگاه‌های کیفری به شدت مبهم می‌سازد.

به‌عنوان نمونه، اگر در پرونده‌ای سیستم پیش‌بینی جرم، با سوگیری نژادی یا قومیتی، منجر به هدف‌گیری گروهی خاص شود، قوانین فعلی ما در رابطه با جرایم ناشی از سوگیری سیستماتیک، هیچ سازوکار جبران خسارتی برای قربانیان تبعیض الگوریتمیک پیش‌بینی نکرده‌اند. برای برون‌رفت از این وضعیت، نظام حقوقی ایران ناچار است که به سمت «مسئولیت مبتنی بر ریسک» یا همان مسئولیت محض برای نهادهای بهره‌بردار حرکت کند، به‌طوری‌که صرف به‌کارگیری این ابزارها در تحقیقات جنایی، بدون نیاز به اثبات تقصیر، موجب مسئولیت مدنی برای

دولت باشد تا حداقل بخشی از حقوق زیان‌دیدگان تأمین شود. در نهایت، ضرورت دارد که با اصلاح قانون آیین دادرسی کیفری، مسئولیت ناشی از خروجی‌های هوش مصنوعی به‌عنوان یک عنوان مجرمانه یا مدنی مستقل تعریف شود تا در پرونده‌های آینده، قاضی مجبور به تمسک به قواعد مبهم سنتی نباشد و بتواند با تعیین تکلیف دقیق جایگاه توسعه‌دهنده، ضابط و قاضی در قبال خطاهای ماشینی، امنیت قضایی را در فرآیندهای هوشمند تضمین نماید.

از منظر تطبیقی، بسیاری از نظام‌های حقوقی پیشرفته تلاش کرده‌اند با وضع قواعد اختصاصی، مسئولیت استفاده از هوش مصنوعی را شفاف‌تر سازند. برای مثال، در اتحادیه اروپا، مقررات **EU AI Act** استفاده از سامانه‌های هوش مصنوعی در حوزه اجرای قانون را در زمره کاربردهای پرخطر قرار داده است (Kusche, 2024) و برای آن‌ها الزامات سخت‌گیرانه‌ای، مانند ارزیابی ریسک، ثبت کامل عملکرد سامانه، نظارت انسانی مستمر، تضمین کیفیت داده‌ها، مستندسازی تصمیم‌ها و امکان حسابرسی الگوریتمی، پیش‌بینی کرده است (Cantero Gamito & Marsden, 2024). همچنین، بهره‌بردار سامانه موظف است همواره امکان مداخله انسانی و توقف تصمیم خودکار را فراهم کند تا مسئولیت صرفاً به ماشین منتقل نشود. این رویکرد نشان می‌دهد که قانون‌گذار اروپایی، مسئولیت را متوجه اشخاص و نهادهای استفاده‌کننده از فناوری دانسته و نه خود فناوری. با توجه به این تحولات، نظام حقوقی ایران برای بهره‌گیری ایمن از هوش مصنوعی در تحقیقات جنایی، نیازمند اصلاحات اساسی است. تدوین قانون اختصاصی درباره هوش مصنوعی قضایی، تعیین مسئولیت مشترک میان تولیدکننده، توسعه‌دهنده، بهره‌بردار و مقام تصمیم‌گیر، الزام به شفافیت و قابلیت توضیح الگوریتم‌ها، ایجاد نظام ارزیابی و ممیزی مستقل، پیش‌بینی حق اعتراض نسبت به تصمیم‌های مبتنی بر هوش مصنوعی و تعیین سازوکار مؤثر جبران خسارت، از مهم‌ترین اقداماتی است که می‌تواند ضمن حفظ کارایی فناوری، از نقض حقوق بنیادین اشخاص جلوگیری کند. بدون چنین اصلاحاتی، توسعه سامانه‌های تصمیم‌یار در فرآیندهای جنایی ممکن است به‌جای افزایش عدالت، موجب گسترش مسئولیت‌های مبهم، کاهش پاسخ‌گویی و تضعیف اعتماد عمومی به نظام عدالت کیفری شود.

تحلیل آینده‌نگرانه و مدل‌های ارتقای اعتماد عمومی در عدالت کیفری هوشمند

تحول به‌سوی عدالت کیفری هوشمند تنها به توسعه فناوری وابسته نیست، بلکه بیش از هر چیز، نیازمند ایجاد اعتماد عمومی به تصمیم‌هایی است که با کمک سامانه‌های هوش مصنوعی اتخاذ می‌شوند. تجربه کشورهای پیشرو نشان می‌دهد که هرچه نقش الگوریتم‌ها در تحقیقات جنایی، تحلیل ادله دیجیتال، تشخیص هویت، بازسازی صحنه جرم و ارزیابی ریسک افزایش یافته است، قانون‌گذاران نیز هم‌زمان سازوکارهای نظارتی، الزامات شفافیت و تضمین‌های حقوق بشری را تقویت کرده‌اند. از این‌رو، آینده عدالت کیفری نه در جایگزینی قاضی یا ضابط با هوش مصنوعی، بلکه در ایجاد نظام «تصمیم‌یار انسانی» مبتنی بر نظارت مستمر، پاسخ‌گویی و قابلیت اعتراض نسبت به تصمیم‌های الگوریتمی تعریف می‌شود. گزارش‌های اخیر وزارت دادگستری آمریکا و نهادهای سیاست‌گذاری کیفری نیز بر این اصل تأکید دارند که هوش مصنوعی باید نقش کمکی داشته باشد و مسئولیت نهایی همواره بر عهده مقام انسانی باقی بماند.

در این خصوص، بسیاری از نظام‌های حقوقی سعی در انطباق خود با تحولات جهان داشته‌اند. تجربه ایالات متحده بیانگر آن است که استفاده از هوش مصنوعی در تحقیقات کیفری، به تدریج از مرحله آزمایشی به بهره‌برداری عملی رسیده است، اما هم‌زمان محدودیت‌های حقوقی آن نیز توسعه یافته است. وزارت دادگستری آمریکا فهرست کاربردهای هوش مصنوعی را در تحلیل اسناد، مدیریت پرونده‌ها، تحلیل تصاویر، پردازش داده‌های جنایی و تحقیقات دیجیتال منتشر کرده و بر اصل نظارت انسانی تأکید کرده است (Faqr, 2023). از سوی دیگر، در سال‌های اخیر برخی ایالت‌ها مقررات ویژه‌ای برای استفاده پلیس از ابزارهای هوش مصنوعی و تشخیص چهره وضع کرده‌اند تا از بازداشت‌های

اشتباه و تبعیض الگوریتمی جلوگیری شود. همچنین، آزمایش سامانه‌هایی مانند Longeye برای تحلیل میلیون‌ها سند و مکالمه در تحقیقات کیفری، همراه با الزام به قابلیت رهگیری تمام خروجی‌ها و امکان بررسی منشأ هر نتیجه، نمونه‌ای از تلاش برای ایجاد اعتماد از طریق قابلیت حسابرسی الگوریتم‌ها محسوب می‌شود (Justice, 2025).

در امارات متحده عربی نیز، سیاست «دولت هوشمند» موجب شده است هوش مصنوعی به‌طور گسترده وارد فرآیندهای انتظامی و قضایی شود. پلیس دبی از سامانه‌های تشخیص چهره، تحلیل تصاویر، بازسازی دیجیتال صحنه جرم [Digital Twin] و فناوری‌های مبتنی بر هوش مصنوعی برای تحلیل ادله استفاده می‌کند (Alaleeli, 2025). یکی از نمونه‌های قابل توجه، پرونده‌ای است که در آن بازسازی هوشمند صحنه جرم با فناوری Digital Twin نشان داد مرگی که در ابتدا خودکشی تلقی شده بود، در واقع ناشی از تصادف و فرار راننده بوده است و مسیر تحقیقات کیفری را به‌طور کامل تغییر داد. با وجود این پیشرفت‌ها، راهبرد رسمی امارات همچنان بر حفظ نظارت انسانی و مسئولیت نهایی دادستان و قاضی تأکید دارد و توسعه مقررات اختصاصی در این حوزه را دنبال می‌کند.

چین نیز از پیشرفته‌ترین کشورها در بهره‌گیری از هوش مصنوعی در عدالت کیفری به شمار می‌رود. دادگاه‌های هوشمند، سامانه‌های تحلیل پرونده، پیشنهاد آرای مشابه، مدیریت ادله دیجیتال و الگوریتم‌های کمک‌یار قضایی، طی سال‌های اخیر در بسیاری از استان‌ها مورد استفاده قرار گرفته‌اند (Shi, 2022). با این حال، مطالعات جدید نشان می‌دهد که حتی در چین نیز نگرانی درباره شفافیت الگوریتم‌ها، امکان سوگیری، کاهش استقلال قضات و محدود شدن اختیار قاضی همچنان ادامه دارد (Wang & Tian, 2022). به همین دلیل، دیوان عالی خلق چین دستورالعمل‌هایی برای استفاده از هوش مصنوعی در فرآیندهای قضایی صادر کرده و بر این نکته تأکید کرده است که قاضی باید نقش نهایی در ارزیابی ادله و صدور رأی را حفظ کند و الگوریتم صرفاً ابزار کمکی باشد.

تحلیل تطبیقی این تجربه‌ها نشان می‌دهد که اعتماد عمومی زمانی تقویت می‌شود که چند اصل به‌طور هم‌زمان رعایت شود: شفافیت عملکرد الگوریتم، قابلیت توضیح تصمیم‌ها، امکان اعتراض و بازبینی انسانی، حسابرسی مستقل سامانه‌های هوش مصنوعی، حفاظت از داده‌های شخصی، ارزیابی مستمر سوگیری‌های الگوریتمی و تعیین مسئولیت حقوقی روشن برای تولیدکنندگان و بهره‌برداران سامانه‌ها. هرچه این تضمین‌ها ضعیف‌تر باشد، احتمال بی‌اعتمادی عمومی، افزایش دعاوی ناشی از خطاهای الگوریتمی و تضعیف مشروعیت نظام عدالت کیفری بیشتر خواهد شد. تجربه برخی کشورها نیز نشان داده است که حتی پس از توسعه فناوری، در مواردی استفاده از ابزارهای مولد هوش مصنوعی برای تهیه اسناد قضایی یا گزارش‌های پلیسی، تا زمان تدوین استانداردهای لازم، متوقف یا محدود شده است تا دقت و صحت فرآیندهای کیفری حفظ شود.

در افق آینده، مناسب‌ترین مدل برای ایران، الگویی تلفیقی از «عدالت کیفری هوشمند با محوریت انسان» است؛ مدلی که در آن، هوش مصنوعی وظایفی مانند تحلیل ادله دیجیتال، کشف الگوهای جرائم، بازیابی اطلاعات، ترجمه اسناد، بازسازی صحنه جرم و مدیریت پرونده را انجام دهد، اما تصمیم‌های مؤثر بر آزادی، مسئولیت کیفری و حقوق بنیادین اشخاص، تنها با ارزیابی مستقل مقام قضایی اتخاذ شود. تحقق چنین مدلی مستلزم تصویب قانون جامع هوش مصنوعی، ایجاد نهاد ملی نظارت بر سامانه‌های هوشمند قضایی، تدوین استانداردهای اعتبارسنجی الگوریتم‌ها، آموزش تخصصی قضات و ضابطان، ممیزی دوره‌ای سامانه‌های مورد استفاده و پیش‌بینی حق دسترسی متهمان به اطلاعات مربوط به تصمیم‌های الگوریتمی است. تنها در چنین شرایطی می‌توان میان کارآمدی فناوری، امنیت عمومی، حفظ کرامت انسانی و اعتماد پایدار شهروندان به نظام عدالت کیفری تعادل برقرار کرد.

نتیجه‌گیری

در فرجام این پژوهش مشخص گردید که گذار از دادرسی کیفری سنتی به سوی استفاده از هوش مصنوعی در تحقیقات جنایی، ضرورتی اجتناب‌ناپذیر است که نظام حقوقی ایران باید با بهره‌گیری از ظرفیت‌های تطبیقی و درعین‌حال، با رعایت دقیق اصول آمره دادرسی عادلانه، به آن پاسخ دهد؛ چراکه هرگونه شتاب‌زدگی در استقرار این فناوری‌ها، بدون وجود بستر تقنینی منسجم، می‌تواند به تضعیف بنیادی حقوق شهروندی و مخدوش شدن اصل برائت منجر شود. یافته‌ها نشان می‌دهد که سیستم‌های تصمیم‌یار، با وجود توانایی‌های بی‌بدیل در تحلیل داده‌های حجیم و پیش‌بینی الگوهای مجرمانه، فاقد قوه تشخیص اخلاقی و درک روح عدالت قضایی هستند و بدین‌جهت، اعتماد مطلق به خروجی‌های این الگوریتم‌ها، بدون نظارت انسانی و قابلیت بازبینی قضایی، در تعارض آشکار با حق دفاع متهم و اصل شفافیت ادله قرار دارد. این مطالعه آشکار ساخت که در نظام کیفری ایران، میان کارکردهای هوشمندسازی و ساختار سنتی ادله اثبات دعوا، شکافی عمیق وجود دارد که نیازمند بازتعریف مفاهیمی همچون استنادپذیری ادله دیجیتال، مسئولیت مدنی ناشی از خطاهای الگوریتمیک و نحوه احراز صحت یافته‌های هوشمند است تا از این طریق، از تبدیل شدن تحقیقات جنایی به سیاهچاله‌ای از تصمیمات غیرشفاف الگوریتمیک جلوگیری شود. نوآوری حاصل از این تحلیل، لزوم جایگزینی رویکرد منفعلانه با استراتژی فعال نظارتی است که در آن، مسئولیت‌پذیری پلتفرم‌های ارائه‌دهنده خدمات هوش مصنوعی و شفافیت کدهای برنامه‌نویسی برای مراجع قضایی، به‌عنوان یک ضرورت فنی و قانونی، در متن قانون آیین دادرسی کیفری لحاظ گردد تا عدالت هوشمند، نه به‌عنوان ابزاری برای اقتدارگرایی تکنولوژیک، بلکه به‌مثابه بازویی برای صیانت از کرامت انسانی و تقویت امنیت قضایی بازخوانی شود. در نهایت، باید تأکید نمود که فناوری در خدمت عدالت است و نه جایگزین آن؛ لذا هرگونه سازوکار اجرایی در زمینه هوش مصنوعی باید در دل یک نظام نظارتی دموکراتیک و شفاف تعریف شود که تضمین‌کننده پاسخ‌گویی تمامی بازیگران، اعم از نهادهای انتظامی و تولیدکنندگان الگوریتم‌های جنایی، باشد؛ زیرا تنها در صورت تحقق این توازن است که امنیت قضایی در مواجهه با تحولات پرشتاب عصر دیجیتال، تداوم یافته و مشروعیت دادرسی کیفری در نظام حقوقی ایران محفوظ خواهد ماند و می‌توان اطمینان حاصل کرد که هوش مصنوعی، به‌جای تقلیل عدالت، به ارتقای آن در کشف حقیقت کمک خواهد کرد و زمینه‌ساز تحقق رویه‌هایی دقیق، سریع و درعین‌حال منطبق بر استانداردهای والای عدالت کیفری مدرن خواهد بود.

تعارض منافع

در انجام مطالعه حاضر، هیچ‌گونه تضاد منافع وجود ندارد.

مشارکت نویسندگان

در نگارش این مقاله تمامی نویسندگان نقش یکسانی ایفا کردند.

حامی مالی

این پژوهش حامی مالی نداشته است.

EXTENDED SUMMARY

The rapid integration of artificial intelligence into law-enforcement and judicial processes has fundamentally altered the traditional structure of criminal investigations and has created new possibilities for data analysis, crime detection, risk assessment, digital evidence processing, and judicial decision support. Contemporary criminal justice institutions increasingly employ machine-learning algorithms, facial-recognition systems, predictive-policing tools, automated document analysis, digital-forensics platforms, and algorithmic risk-assessment instruments to improve the

speed, consistency, and accuracy of investigative activities. Supporters of these technologies argue that artificial intelligence can reduce human cognitive error, identify complex patterns within large volumes of criminal data, assist investigators in prioritizing cases, and strengthen the evidentiary basis of prosecutorial and judicial decisions. Nevertheless, the incorporation of artificial intelligence into criminal proceedings cannot be evaluated solely from an instrumental or efficiency-oriented perspective. Algorithmic systems may operate as opaque “black boxes,” while their outputs can directly affect liberty, privacy, reputation, equality before the law, and the presumption of innocence. The use of such systems therefore raises serious questions concerning transparency, explainability, procedural fairness, human oversight, data protection, evidentiary reliability, and the ability of defendants to challenge the basis of automated conclusions. Existing scholarship has emphasized that the transformation of criminal justice through artificial intelligence requires a reconsideration of the philosophical and legal foundations of punishment, responsibility, and procedural legitimacy (Ashabi et al., 2025; Homiry, 2026). Accordingly, this study examines the legal status and requirements governing the use of artificial intelligence in criminal investigations, with particular emphasis on the Iranian criminal justice system. Its central question is how the benefits of intelligent investigative technologies can be reconciled with the mandatory principles of a fair trial, human dignity, the right to defense, and judicial security. The study adopts a descriptive-analytical and comparative method based on library research, domestic legal rules, international legal instruments, judicial experiences, and recent regulatory developments relating to artificial intelligence and criminal justice.

The conceptual foundation of the study rests on the distinction between artificial intelligence as an investigative assistant and artificial intelligence as an autonomous decision-maker. In criminal investigations, intelligent systems may perform multiple functions, including processing digital traces, analyzing mobile-phone and computer data, reviewing surveillance footage, identifying suspects, reconstructing crime scenes, predicting crime hotspots, detecting patterns of criminal behavior, and estimating the probability of recidivism. Digital criminal investigations are increasingly dependent on automated systems capable of collecting, classifying, correlating, and interpreting large quantities of electronic information that would be difficult for human investigators to process within a reasonable period (Faqr, 2023). At the same time, digital evidence derived from social networks, geolocation systems, electronic communications, cloud platforms, security cameras, and smart devices has become a central component of modern criminal proceedings. The legal validity of such evidence depends not only on its relevance but also on the reliability of the method through which it was obtained, preserved, analyzed, and presented. Iranian legal scholarship has already recognized the growing significance of electronic evidence, yet traditional evidentiary rules remain insufficiently adapted to automated forms of data interpretation (Heydarinejad, 2017). The difficulty becomes more pronounced when an algorithm does not merely organize evidence but generates an inferential conclusion, such as identifying a suspect, predicting dangerousness, or calculating the likelihood of reoffending. In such circumstances, the distinction between evidence and algorithmic opinion becomes blurred. The widely discussed use of the COMPAS risk-assessment instrument in the case of *State v. Loomis* illustrates the danger of relying on proprietary and nontransparent algorithms in sentencing and criminal decision-making. The defendant argued that his right to due process had been violated because he could not examine or challenge the computational basis of the risk score used against him. Although the court permitted limited use of the instrument, the case became an important reference point in debates concerning algorithmic bias, opacity, and judicial dependence on predictive systems (Aljinovic, 2024). It demonstrates that

artificial intelligence must remain subordinate to independent judicial evaluation and must never acquire presumptive evidentiary authority merely because of its technological complexity.

The findings of the study indicate that one of the most serious risks associated with artificial intelligence in criminal investigations is the possible erosion of fair-trial guarantees. Algorithmic systems may reproduce or intensify social, racial, ethnic, economic, and gender-based biases already embedded in historical datasets. If an artificial-intelligence model is trained on discriminatory policing records or inaccurate criminal databases, its outputs may systematically target particular communities and create a cycle in which past inequalities are converted into apparently objective predictions. Moreover, defendants may be unable to exercise an effective right of defense when the software architecture, training data, weighting criteria, or error rate of an algorithm remains confidential. The principle of equality of arms requires that the accused have a meaningful opportunity to examine and contest the evidence used by the prosecution. When an automated conclusion is treated as reliable without disclosure of its technical foundations, the defense is placed at a structural disadvantage. The controversy surrounding the Cybercheck system in criminal cases in the United States provides a significant example. The system was reportedly used to connect suspects to crime scenes through automated open-source intelligence analysis, yet subsequent scrutiny raised questions about the transparency, reproducibility, and accuracy of its conclusions (Feathers, 2024). Such experiences demonstrate that digital evidence generated or interpreted by artificial intelligence should not be accepted unless the origin of the data, the analytical process, the possibility of error, and the conditions of independent verification are clearly established. The legitimacy of algorithmic evidence therefore depends on procedural safeguards, including disclosure obligations, auditability, expert review, preservation of the digital chain of custody, judicial explanation, and the defendant's right to challenge both the data and the method of analysis. These requirements are closely connected to the broader concepts of algorithmic accountability and the right to an explanation. Without such safeguards, the use of artificial intelligence may transform criminal investigation from a truth-seeking process into a technologically mediated procedure in which invisible computational assumptions determine the course of prosecution.

In the Iranian criminal justice system, the principal legal problem is the absence of an explicit and coherent legislative framework governing the use of artificial intelligence in criminal investigations. The Constitution, the Code of Criminal Procedure, the Computer Crimes Act, and general rules concerning electronic evidence provide certain indirect protections, but they do not specifically regulate algorithmic decision-making, predictive policing, automated suspect identification, facial recognition, risk-assessment systems, or liability for artificial-intelligence errors. Existing rules were primarily designed for conventional interactions between investigators, prosecutors, judges, defendants, witnesses, and physical or documentary evidence. They do not adequately address the distinct characteristics of algorithmic systems, including opacity, autonomy, scalability, data dependency, and continuous machine learning. This legislative silence threatens the presumption of innocence, the right to defense, the legality of criminal procedure, and the transparency of preliminary investigations. It also creates uncertainty regarding responsibility when an artificial-intelligence system produces a false identification, discriminatory output, unlawful detention, or misleading evidentiary conclusion. Questions arise as to whether responsibility should be attributed to the software developer, the technology provider, the law-enforcement agency, the judicial officer, the operator, or the public institution that approved the system. The traditional structure of civil and criminal liability is difficult to apply because artificial intelligence lacks independent legal will, while the causal relationship between design, training data, deployment, and harmful output may be highly

complex. Although some scholars have proposed recognizing a form of legal personality for advanced intelligent systems, the more practical approach is to allocate responsibility among the natural and legal persons who develop, supply, supervise, and use the technology (Bagheri, 2025). For high-risk criminal-justice applications, a risk-based or strict-liability model may be necessary to ensure compensation without requiring the injured person to prove technical fault hidden within inaccessible code. Iran also lacks an independent institution capable of testing, certifying, auditing, and monitoring artificial-intelligence systems used by the police and judiciary. Consequently, legislative reform must be accompanied by institutional oversight, technical standards, documentation duties, and mandatory human review.

Comparative analysis shows that the European Union has developed one of the most advanced regulatory approaches to high-risk artificial-intelligence systems. The European framework treats many applications of artificial intelligence in law enforcement, border control, biometric identification, and the administration of justice as high-risk because of their potential impact on fundamental rights. The EU Artificial Intelligence Act is based on a risk-management model that requires technical documentation, data governance, accuracy testing, human oversight, record keeping, bias mitigation, post-market monitoring, and independent conformity assessment. It also prohibits or restricts certain practices considered incompatible with human dignity and democratic legal order (Neuwirth, 2023). The fundamental-rights orientation of this framework emphasizes that technological innovation cannot justify disproportionate interference with privacy, equality, procedural fairness, or personal autonomy (Kusche, 2024). Standards and co-regulatory mechanisms also play an important role in translating general legal duties into operational requirements for developers and users (Cantero Gamito & Marsden, 2024). The judgment of the Court of Justice of the European Union in the SCHUFA scoring case further illustrates the emerging legal resistance to decisions that significantly affect individuals and are based exclusively or predominantly on automated processing. The case strengthened the principles of transparency, access to information, human intervention, and the right to contest algorithmic assessments (Martinovic, 2025; Paun, 2024). Other jurisdictions have likewise emphasized the necessity of maintaining human authority over criminal-justice technologies. In the United States, artificial intelligence is increasingly used in document review, digital investigations, facial recognition, image analysis, and case management, but controversies concerning erroneous arrests and biased systems have encouraged stricter oversight and procedural limitations (Justice, 2025). The United Arab Emirates has expanded the use of facial recognition and intelligent security technologies, while formally maintaining the responsibility of prosecutors and judges for final decisions (Alaleeli, 2025). China has developed smart courts, sentencing-support systems, and automated case-management tools, yet concerns remain regarding judicial independence, algorithmic opacity, and the narrowing of judicial discretion (Shi, 2022; Wang & Tian, 2022). These comparative experiences support a human-centered model in which artificial intelligence assists but does not replace judicial reasoning.

In conclusion, the transition from traditional criminal investigation to artificial-intelligence-assisted investigation is both inevitable and legally sensitive. The study demonstrates that intelligent systems can significantly enhance the processing of digital evidence, identification of criminal patterns, management of complex cases, and efficiency of investigative institutions; however, these benefits cannot justify the weakening of fundamental procedural guarantees. Artificial intelligence lacks moral judgment, legal conscience, and the capacity to understand the substantive meaning of justice. Its outputs must therefore remain subject to independent human evaluation, judicial reasoning, and effective challenge by the defense. For Iran, the most appropriate model is a human-centered system

of intelligent criminal justice in which artificial intelligence performs supportive functions while all decisions affecting liberty, criminal responsibility, punishment, privacy, and fundamental rights remain under the authority of accountable human officials. Achieving this model requires the enactment of a comprehensive law on artificial intelligence in criminal justice, explicit rules on the admissibility and evidentiary value of algorithmic outputs, mandatory disclosure of relevant technical information, independent auditing of high-risk systems, continuous assessment of bias and error, protection of personal data, and recognition of the defendant's right to explanation and human review. The law should also establish a clear distribution of civil, administrative, and criminal responsibility among developers, suppliers, operators, judicial authorities, and law-enforcement institutions. Exclusive reliance on automated decisions in sensitive investigative and judicial stages should be prohibited. Judges, prosecutors, investigators, lawyers, and forensic experts must receive specialized training in algorithmic systems and digital evidence. Ultimately, technology should serve justice rather than replace it. Only through a transparent, accountable, rights-based, and democratically supervised framework can artificial intelligence contribute to the discovery of truth while preserving human dignity, public trust, judicial security, and the legitimacy of the Iranian criminal justice system.

References

- Alaleeli, S. (2025). *The Use of AI-Based Facial Recognition Technology in Security Information Management to Mitigate Minor Theft* Anglia Ruskin Research Online (ARRO)].
- Aljinovic, N. (2024). Artificial Intelligence in Judicial Decision-Making: Challenges of Bias and Lack of Transparency of Predictive Algorithms. *ORGANIZER*, 782.
- Ashabi, F., Hamidavi, A., & Mousizadeh Meykhosh, R. (2025). Artificial Intelligence and Rethinking Criminal Justice: A Retributivist and Utilitarian Analysis. *Research and Development in Criminal Law and Criminology*, 2(4).
- Bagheri, P. (2025). Legal Personality and Civil Liability of Artificial Intelligence: Legal Challenges and Solutions. *Private Law Research*, 13(51).
- Cantero Gamito, M., & Marsden, C. T. (2024). Artificial Intelligence Co-Regulation? The Role of Standards in the EU AI Act. *International Journal of Law and Information Technology*, 32(1), eaae011.
- Faqir, R. S. (2023). Digital Criminal Investigations in the Era of Artificial Intelligence: A Comprehensive Overview. *International Journal of Cyber Criminology*, 17(2), 77-94.
- Feathers, T. (2024). This AI Tool Helped Convict People of Murder. Then Someone Took a Closer Look. <https://www.wired.com/story/ai-tool-convicted-people-murder-cybercheck/>
- Heydarinejad, N. (2017). A Legal Examination of Electronic Evidence in the Current Legal System. *Qanunyar*, 3(3).
- Homiry, F. (2026). The Impact of Artificial Intelligence on Criminal Systems and Criminal Justice. *International Criminal Law*, 3(4), 97-108.
- Justice, I. O. C. (2025). Thinking About a Time-Based Topic: 21st-Century Criminal Justice to a Helps. (Vol. 5).
- Kusche, I. (2024). Possible Harms of Artificial Intelligence and the EU AI Act: Fundamental Rights and Risk. *Journal of Risk Research*, 1-14.
- Martinovic, A. (2025). *Automated Decision-Making and Algorithmic Management: Implications of the CJEU's SCHUFA (Scoring) Case for the EU Labour Law* 7th International Scientific Conference: Economics of Digital Transformation (EDT Conference 2024),
- Neuwirth, R. J. (2023). Prohibited Artificial Intelligence Practices in the Proposed EU Artificial Intelligence Act (AIA). *Computer Law & Security Review*, 48, 105798.
- Paun, R. D. (2024). Banking Scoring Versus Social Scoring: The Chinese Model in the Light of the Court of Justice of the European Union. *Journal of Law and Public Administration*, 10(19), 54-62.
- Shi, J. (2022). Artificial Intelligence, Algorithms and Sentencing in Chinese Criminal Justice: Problems and Solutions. *Criminal Law Forum*, 33, 121.
- Wang, N., & Tian, M. Y. (2022). Intelligent Justice: AI Implementations in China's Legal Systems. In *Artificial Intelligence and Its Discontents: Critiques from the Social Sciences and Humanities* (pp. 197-222). Springer International Publishing.