A Comparative Study of the Criminal Liability of Law Enforcement Agencies in the Use of AI-Based Facial Recognition Systems in the Legal Systems of the United States and the European Union

Hediye Afroozi
ORCID: https://orcid.org/0009-0005-7963-2960

Haydeh Shirzadrajavoni
ORCID: https://orcid.org/0009-0000-6140-6432

Amirreza Mahmoudi
ORCID: https://orcid.org/0000-0001-8997-5071

Abstract: The rapid advancement of artificial intelligence, particularly facial recognition systems, has profoundly transformed traditional mechanisms of crime detection and evidentiary assessment within criminal justice systems. These systems, which rely on biometric data processing and complex machine-learning algorithms, ostensibly enhance the efficiency, accuracy, and speed of policing and judicial decision-making. Nevertheless, due to their probabilistic, opaque, and sometimes biased nature, they may generate erroneous identifications that directly threaten fundamental rights, including due process, privacy, and the presumption of innocence. This raises a central question: when a wrongful arrest, prosecution, or conviction is caused by an algorithmic error, which actor within the criminal justice system bears criminal liability—the police officer, investigative authority, judicial decision-maker, or even the system's designers and developers? Adopting a comparative methodology, this study examines the approaches of the United States and the European Union to the problem of algorithmic error and criminal accountability. The findings indicate that the United States continues to adhere to the classical principle of individual criminal responsibility, whereby technological tools serve merely as auxiliary inputs, and human decision-makers remain solely accountable. U.S. courts generally regard algorithmic outputs as probabilistic indicators rather than conclusive evidence. In contrast, the European Union—through its risk-based Artificial Intelligence Act (AI Act)—imposes stringent obligations of algorithmic transparency, documentation, human oversight, and regulated deployment of high-risk systems such as facial recognition, alongside a distributed model of accountability across the technological supply chain. In Iran, despite the absence of explicit statutory provisions regarding AI-generated evidence, general principles embedded in the Islamic Penal Code—such as the personal nature of criminal responsibility (Article 140), evidentiary standards, and the rules of causation—provide implicit foundations for assigning liability to law-enforcement actors. Based on comparative insights and the unique challenges posed by high-risk AI systems, this article proposes a "chain liability model," according to which criminal responsibility is allocated across designers, developers, supervisory bodies, law-enforcement officials, and judicial authorities. This model mitigates institutional responsibility-avoidance, reinforces criminal justice safeguards, and ensures a balanced integration of technological efficiency with the protection of citizens' rights.

Keywords: Criminal liability, facial recognition systems, algorithmic error, law enforcement agencies, comparative criminal law

مطالعه تطبیقی مسئولیت کیفری نهادهای مجری قانون در استفاده از سامانه‌های تشخیص چهره مبتنی بر هوش مصنوعی در نظام‌های حقوقی ایالات متحده و اتحادیه اروپا

هدیه افروزی

ORCID: https://orcid.org/0009-0005-7963-2960

هایده شیرزادراجعونی

ORCID: https://orcid.org/0009-0000-6140-6432

امیررضا محمودی

ORCID: https://orcid.org/0000-0001-8997-5071

چکیده: پیشرفت شتابان هوش مصنوعی و به‌ویژه سامانه‌های تشخیص چهره طی سال‌های اخیر، ساختار سنتی کشف جرم و تولید ادله کیفری را دستخوش تحول بنیادین کرده است. این سامانه‌ها که بر تحلیل داده‌های بیومتریک و الگوریتم‌های پیچیده یادگیری ماشین متکی‌اند، در ظاهر با افزایش سرعت، دقت و کارآمدی فرآیندهای پلیسی و قضایی همراه هستند، اما در عمل به دلیل ماهیت احتمالاتی، غیرقابل‌تبیین و گاه سوگیرانه خود می‌توانند منشأ خطاهای جدی و نقض حقوق بنیادین افراد شوند. ازاین‌رو، پرسش کلیدی این است که در صورت بروز بازداشت یا محکومیت نادرست ناشی از خطای الگوریتمی، مسئولیت کیفری متوجه کدام نهاد یا مقام خواهد بود: مأمور پلیس، ضابطان دادگستری، قاضی صادرکننده تصمیم، یا حتی طراح و توسعه‌دهنده سامانه؟ این پژوهش با اتخاذ رویکردی تطبیقی میان نظام‌های حقوقی ایالات متحده و اتحادیه اروپا نشان می‌دهد که آمریکا همچنان به اصل فردی بودن مسئولیت کیفری و پاسخگویی تصمیم‌گیرنده انسانی پایبند است و خروجی الگوریتم تنها نقش «قرینه کمکی» دارد. در مقابل، اتحادیه اروپا با اتخاذ رویکرد مبتنی بر ریسک در قانون هوش مصنوعی(AI Act) ، سازوکاری پیشرفته‌تر مبتنی بر تقسیم مسئولیت در زنجیره فناوری، الزام به شفافیت الگوریتمی، نظارت سخت‌گیرانه و محدودیت جدی در کاربردهای پرخطر ـ از جمله تشخیص چهره ـ ارائه کرده است. در ایران، اگرچه قوانین کیفری موجود مانند ماده ۱۴۰ قانون مجازات اسلامی و قواعد آیین دادرسی کیفری هنوز موضعی صریح در قبال ادله مبتنی بر هوش مصنوعی ندارند، اما اصولی چون شخصی بودن مسئولیت کیفری، معیارهای اثباتی و قواعد تسبیب می‌توانند مبنایی برای تحلیل مسئولیت نهادهای مجری قانون در مواجهه با خطاهای الگوریتمی فراهم سازند. در نهایت، با توجه به ویژگی‌های خاص سامانه‌های پرریسک، پژوهش حاضر مدل «مسئولیت زنجیره‌ای» را پیشنهاد می‌کند؛ مدلی که بر مبنای آن، مسئولیت کیفری به‌صورت مرحله‌ای میان طراحان، توسعه‌دهندگان، نهادهای ناظر، کاربران نهایی و مقامات قضایی توزیع می‌شود. این الگو می‌تواند ضمن حفظ کارآمدی فناوری، از بروز مسئولیت‌گریزی نهادی جلوگیری کرده و زمینه لازم برای تضمین عدالت کیفری و صیانت از حقوق شهروندان را فراهم آورد.

کلیدواژه‌ها :مسئولیت کیفری، سامانه‌های تشخیص چهره، خطای الگوریتمی، نهادهای مجری قانون، حقوق کیفری تطبیقی

مقدمه

تحولات سریع فناوری‌های هوش مصنوعی در دهه اخیر، ساختار سنتی فرآیندهای انتظامی و قضایی را دگرگون ساخته است. در میان این فناوری‌ها، سامانه‌های تشخیص چهره جایگاهی ویژه دارند؛ ابزاری که به نهادهای مجری قانون ـ از پلیس و ضابطان دادگستری تا دستگاه قضایی ـ امکان می‌دهد در کوتاه‌ترین زمان ممکن به شناسایی مظنونان یا کنترل افراد در اماکن عمومی اقدام کنند. جذابیت اصلی این سامانه‌ها در وعده افزایش سرعت، کاهش خطای انسانی و ارتقای کارآمدی فرآیند کشف جرم نهفته است. با این حال، همین فناوری به دلیل ماهیت احتمالاتی و غیرشفاف خود، می‌تواند به نقض آزادی‌های فردی، تعرض به حریم خصوصی و حتی بازداشت‌های نادرست منجر شود.

مسئله محوری در این میان، خطاپذیری ذاتی الگوریتم‌های یادگیری ماشین است. خروجی سامانه‌های تشخیص چهره همواره احتمالاتی است و هیچ‌گاه قطعیت ندارد. پدیده‌ای موسوم به «جعبه سیاه الگوریتمی» ـ یعنی ناتوانی در توضیح منطق دقیق تصمیم‌گیری سیستم ـ و همچنین سوگیری‌های داده‌ای، دقت این سامانه‌ها را در شناسایی برخی گروه‌ها (مانند زنان یا افراد دارای رنگ پوست تیره) کاهش می‌دهد. پیامد چنین خطاهایی نه‌تنها خدشه به حیثیت و آزادی افراد است، بلکه می‌تواند اعتبار کل فرآیند دادرسی را زیر سؤال ببرد.

در این شرایط، پرسش بنیادین پژوهش حاضر چنین است :وقتی خطای الگوریتمی به بازداشت یا محکومیت نادرست منجر شود، مسئولیت کیفری بر عهده کدام نهاد است؟ پلیس، ضابطان دادگستری یا قضات؟ آیا مأمور یا قاضی می‌تواند تصمیم خود را به الگوریتم منتسب کند و از پاسخگویی شانه خالی نماید، یا باید مسئولیت میان طراحان، توسعه‌دهندگان، نهادهای ناظر و مجریان قانون به‌صورت زنجیره‌ای تقسیم شود؟

بررسی تطبیقی نشان می‌دهد که نظام‌های حقوقی مختلف راهبردهای متفاوتی برگزیده‌اند. در ایالات متحده، اصل فردی بودن مسئولیت کیفری همچنان بر تصمیم‌گیرندگان انسانی حاکم است، هرچند برخی ایالت‌ها محدودیت‌های جدی برای استفاده از فناوری تشخیص چهره وضع کرده‌اند. در مقابل، اتحادیه اروپا با رویکرد مبتنی بر ریسک در پیش‌نویس قانون هوش مصنوعی[1]، تقسیم مسئولیت در زنجیره فناوری و الزام به شفافیت الگوریتمی را پذیرفته است. اما در ایران، قوانین موجود مانند ماده ۱۴۰ قانون مجازات اسلامی (اصل شخصی بودن مسئولیت کیفری) و مقررات آیین دادرسی کیفری، هنوز صراحتی درباره سامانه‌های هوش مصنوعی ندارند و رویه قضایی نیز سکوت اختیار کرده است. این خلأ موجب سردرگمی نهادهای مجری قانون و افزایش خطر سوءاستفاده یا خطاهای جبران‌ناپذیر شده است.

از این رو، پژوهش حاضر با تمرکز بر مسئولیت کیفری نهادهای مجری قانون در استفاده از سامانه‌های تشخیص چهره، می‌کوشد ضمن بررسی ابعاد فنی و حقوقی این فناوری، خلأهای موجود در حقوق ایران را آشکار ساخته و با اتکا به مطالعات تطبیقی،

[1] AI Act

چارچوبی برای توزیع مسئولیت ارائه دهد. هدف اصلی، یافتن پاسخی متوازن است؛ پاسخی که از یک سو ضرورت‌های امنیتی و کارآمدی فرآیند کشف جرم را نادیده نگیرد و از سوی دیگر، اصول بنیادین عدالت کیفری و حقوق شهروندان را تضمین کند.

مرور پیشینه

الف) مباحث نظری مسئولیت کیفری در هوش مصنوعی

در ادبیات کیفری، یکی از پرسش‌های اصلی آن است که آیا می‌توان مسئولیت کیفری را مستقیماً به سامانه‌های هوش مصنوعی نسبت داد یا خیر. جعفری (۱۳۹۶) با تکیه بر اصول کلاسیک حقوق کیفری، بر شرط عقل، بلوغ و اختیار تأکید کرده و شخصیت کیفری برای سامانه‌های غیرانسانی را مردود می‌داند. یوسفی (۱۴۰۲، ۱۴۰۴) با رویکرد تطبیقی سه مدل مشهور ـ مباشر، واسطه‌ای و زنجیره‌ای ـ را بررسی کرده و مدل زنجیره‌ای را واقع‌بینانه‌ترین پاسخ به خطاهای فناورانه معرفی کرده است. در سطح بین‌المللی نیز Raposo (2024) با تمرکز بر خطاهای تشخیص چهره و Nelson & Simek (2020) با طرح مفهوم «جعبه سیاه الگوریتمی» هشدار داده‌اند که عدم شفافیت می‌تواند به نقض حق دفاع منجر شود. ضعف مشترک این آثار آن است که نقش نهادهای مجری قانون به‌عنوان استفاده‌کنندگان اصلی این سامانه‌ها کمتر در کانون بحث قرار گرفته است.

ب) ادله فناورانه و نظام کیفری ایران

بخش مهمی از پژوهش‌های داخلی بر ارزش اثباتی داده‌های فناورانه در دادرسی کیفری ایران متمرکز بوده است. کوشا و باقری (۱۴۰۳) نشان داده‌اند که فقدان ضوابط روشن در آیین دادرسی کیفری می‌تواند اصل برائت و حق دفاع متهم را تضعیف کند. قوامی‌پور و محمودی (۱۴۰۴) نیز با تحلیل تطبیقی پیشنهاد کرده‌اند که ایران باید از مدل‌های مسئولیت ترکیبی و قواعد مسئولیت مدنی برای تنظیم ادله مبتنی بر هوش مصنوعی بهره گیرد. یافته‌های خارجی همچون Qandeel (2024) نیز تأیید می‌کند که بدون تضمین شفافیت الگوریتمی، خروجی سامانه‌های AI صرفاً «قرینه» محسوب می‌شوند. نقد مشترک این دسته آثار، تمرکز بیش از حد بر «اعتبار دلیل» و غفلت از مسئولیت کیفری اشخاص دخیل (پلیس، ضابطان و قضات) است.

ج) مسئولیت کیفری نهادهای مجری قانون

تنها در برخی پژوهش‌ها به‌طور مستقیم به نقش نهادهای مجری قانون پرداخته شده است. فتحی، بختیاری و فخاری (۱۴۰۳) مسئولیت کیفری پلیس و ضابطان را در بهره‌گیری از سامانه‌های هوش مصنوعی بررسی کرده و هشدار داده‌اند که نبود سیاست جنایی تقنینی می‌تواند زمینه‌ساز مسئولیت‌گریزی مأموران شود. انصاریان‌فر، شهبازی و حسینی (۱۴۰۲) نیز بر همین نکته تأکید کرده‌اند که سکوت مقررات، مانع پاسخگویی مأموران اجرایی است. در مطالعات تطبیقی نیز Raposo (2024) در آمریکا و Qandeel (2024) در اروپا نشان داده‌اند که به‌رغم تفاوت‌های بنیادین، هر دو نظام بر ضرورت پاسخگویی نهادهای اجرایی تأکید دارند: در آمریکا با محوریت مسئولیت فردی مأمور و در اروپا با الگوی تقسیم مسئولیت و الزام به شفافیت ساختاری.

برآیند این مرور نشان می‌دهد که گرچه مبانی نظری مسئولیت کیفری در هوش مصنوعی و ارزش اثباتی ادله فناورانه مورد توجه قرار گرفته، اما جایگاه نهادهای مجری قانون ـ به‌عنوان تصمیم‌گیرندگان نهایی در استفاده از سامانه‌های تشخیص چهره ـ کمتر به‌طور مستقل بررسی شده است. شکاف اصلی در حقوق ایران نیز نبود چارچوب روشن برای تعیین مسئولیت کیفری پلیس، ضابطان دادگستری و قضات است؛ خلأیی که این پژوهش در پی پر کردن آن است.

الف) تأثیر هوش مصنوعی در فرآیند کشف و اثبات جرم در دادرسی کیفری

فناوری تشخیص چهره به‌عنوان یکی از مهم‌ترین کاربردهای هوش مصنوعی، اگرچه پیشرفت‌های چشمگیری در شناسایی و احراز هویت افراد داشته است، اما همچنان با چالش‌های اساسی در حوزه دقت، شفافیت و قابلیت اعتماد مواجه است. این سامانه‌ها اساساً بر مبنای استخراج قالب‌های ریاضی از داده‌های بیومتریک و مقایسه آن‌ها با پایگاه‌های موجود عمل می‌کنند. با وجود این، پیچیدگی الگوریتم‌ها و ماهیت احتمالاتی نتایج، زمینه بروز خطاهای شناسایی را فراهم می‌سازد؛ خطاهایی که می‌توانند تبعات سنگینی در حوزه حقوق کیفری ایجاد کنند .

یکی از عوامل اصلی بروز خطا آن است که خروجی سامانه‌های تشخیص چهره هیچ‌گاه قطعیت ندارد و صرفاً نشانگر درصدی از احتمال تطبیق است. به همین دلیل تعیین «آستانه اطمینان» برای پذیرش یا رد نتایج، اهمیت اساسی پیدا می‌کند. انتخاب آستانه پایین می‌تواند به بازداشت بی‌مورد افراد بی‌گناه منتهی شود، و در مقابل، آستانه بیش از حد بالا ممکن است مانع کشف سریع مجرمان گردد. بنابراین تنظیم دقیق این معیار فنی، به‌طور مستقیم با تضمین امنیت قضایی و حقوقی افراد مرتبط است .

مشکل دیگر، عدم شفافیت فرآیند تصمیم‌گیری الگوریتم‌هاست؛ پدیده‌ای که از آن با عنوان «جعبه سیاه الگوریتمی» یاد می‌شود. در چنین شرایطی امکان نظارت قضایی، بازبینی و اصلاح خطاها یا رفع تبعیض‌های احتمالی بسیار محدود است. افزون بر این، سوگیری الگوریتمی ناشی از داده‌های آموزشی نامتوازن یا پیش‌فرض‌های ذهنی طراحان، دقت سامانه‌ها را در شناسایی گروه‌های خاص مانند زنان یا افراد دارای رنگ پوست تیره کاهش می‌دهد؛ امری که مصداق تبعیض و مغایر با اصول حقوق بشر است .

خطای ناشی از شناسایی اشتباه صرفاً خسارات مادی به همراه ندارد، بلکه می‌تواند موجب صدمات حیثیتی و معنوی نیز گردد؛ امری که در بسیاری از نظام‌های حقوقی مبنای مسئولیت و جبران قرار می‌گیرد. در حقوق اتحادیه اروپا، قواعد مسئولیت محصول توسعه‌دهندگان و تولیدکنندگان را مکلف به پاسخگویی می‌داند. همچنین کاربران نهایی ـ از جمله نهادهای مجری قانون ـ موظف‌اند پیش از اتکای کیفری به داده‌های احتمالاتی، قابلیت اعتماد آن‌ها را بررسی کنند. در غیر این صورت، در صورت وقوع آسیب، مسئولیت کیفری و انضباطی متوجه آنان خواهد بود .

برای کاهش خطا و پیشگیری از پیامدهای کیفری نامطلوب، اتخاذ تدابیر چندوجهی ضروری است؛ از جمله ارتقای کیفیت داده‌های آموزشی، پایش مستمر عملکرد الگوریتم‌ها، و طراحی سامانه‌ها بر مبنای عدالت‌محوری. افزون بر این باید توجه داشت که دقت سامانه‌ها به محیط استفاده وابسته است: در محیط‌های کنترل‌شده مانند فرودگاه‌ها، کارایی بالاتر است، در حالی که در محیط‌های عمومی مانند تصاویر دوربین‌های مداربسته شهری، میزان خطا افزایش می‌یابد. این وضعیت نشان می‌دهد که استفاده منصفانه و ایمن از فناوری تشخیص چهره، نیازمند مداخله قانونگذار و تدوین مقررات الزام‌آور است(Raposo et al., 2024: 1857–1869) .

ب) مبانی مسئولیت کیفری در استفاده از سامانه‌های هوش مصنوعی در فرآیند کیفری

مسئولیت کیفری در هر نظام حقوقی بر پایه سه عنصر فعل مادی، عنصر روانی و قابلیت انتساب به شخص استوار است. در حقوق جزای بین‌الملل نیز همین سه‌گانه، بنیان نظری تعیین حدود مسئولیت محسوب می‌شود (افروزی، شیرزاد راجعونی و محمودی، ۱٤۰٤: ۱۲–۲۰).

۱ .اصل فردی بودن مسئولیت کیفری و چالش سامانه‌های غیرانسانی

در حقوق کیفری سنتی، اصل فردی بودن مسئولیت کیفری از اصول بنیادین است. تنها انسان، آن هم با تحقق شرایط عقل، بلوغ، اختیار و سوءنیت قابل مؤاخذه است. ابزارهای فناورانه صرفاً «وسیله» محسوب می‌شوند و فاقد اهلیت کیفری هستند. نکته مهم آن است که مسئولیت کیفری زنجیره‌ای به معنای شراکت کیفری موضوع مواد ۱۲۶ و ۱۲۷ ق.م.ا نیست. در شراکت، چند نفر با قصد واحد و رفتار مجرمانه مشترک، در تحقق رکن مادی دخالت می‌کنند. اما در مسئولیت زنجیره‌ای، نقش‌ها ماهیتاً غیرهم‌زمان، ناهمگون و گاه غیرمباشرند (مانند برنامه‌نویس یا نهاد ناظر). بنابراین اشخاص دخیل در زنجیره فناوری لزوماً شریک در جرم نیستند، بلکه هر یک در حوزه تقصیر یا قصورِ مرتبط با نقش حرفه‌ای خود مسئول‌اند. تنها در مواردی که قصد مجرمانه مشترک و همکاری هم‌زمان میان بازیگران وجود داشته باشد، امکان انطباق با مقررات مشارکت یا معاونت فراهم است.

اما ظهور سامانه‌های هوش مصنوعی با قابلیت تصمیم‌گیری خودکار، این منطق کلاسیک را با چالش مواجه ساخته است. برای نمونه، اگر یک سامانه تشخیص چهره مبتنی بر یادگیری عمیق، فردی بی‌گناه را به‌اشتباه مظنون معرفی کند، مسئولیت کیفری این خطا بر عهده چه کسی خواهد بود؟ کاربر نهایی، طراح الگوریتم یا نهاد سفارش‌دهنده؟ در نظام‌های حقوقی آلمان و ایالات متحده، اصل شخصی بودن مسئولیت کیفری همچنان مانع از شناسایی مستقیم شخصیت کیفری برای سامانه‌هاست. با این حال، برای پاسخ به پیچیدگی‌های جدید، سه رویکرد نوین مطرح شده است: مدل مباشر (شخصیت مستقل سامانه)، مدل واسطه‌ای (سامانه به‌عنوان ابزار صرف)، و مدل ترکیبی یا زنجیره‌ای که مسئولیت را میان طراح، کاربر و نهاد نظارتی تقسیم می‌کند. رویکرد اخیر به دلیل واقع‌گرایی، بیشترین توجه را به خود جلب کرده است (یوسفی، ۱٤۰٤: ۲–۳؛ قوامی‌پور و محمودی، ۱٤۰٤: ۱۰۱؛ کوشا و باقری، ۱٤۰۳: ۲٤٤).

۲ .رابطه میان خطای سیستمی و مسئولیت انسانی

در ادبیات کیفری نوین، برخی بر این باورند که سامانه‌های AI صرفاً ابزار تصمیم‌گیر انسانی هستند و مسئولیت به کاربر بازمی‌گردد. اما دیدگاهی دیگر معتقد است که در نظام‌های غیرشفاف و پیچیده، مسئولیت باید «تقسیم‌پذیر» میان طراحی، داده‌آموزی، پیکربندی و اجرا باشد (یوسفی، ۱٤۰۲: ٥). در ایران نیز به‌دلیل فقدان مقررات خاص، معمولاً مسئولیت به فردی که مستقیماً از سیستم استفاده کرده برمی‌گردد. اما باید توجه داشت که خطا گاه ناشی از الگوریتم یا داده‌های جانبدارانه است، نه کاربر نهایی (کوشا و باقری، ۱٤۰۳: ۲٤٥).

۳ .نقش تقصیر در انتساب مسئولیت کیفری

یکی از شاخصه‌های مهم مسئولیت کیفری، وجود تقصیر است. اگر کاربر یا طراح سامانه در استفاده، آموزش یا نگهداری مرتکب بی‌احتیاطی یا غفلت شود، مسئولیت کیفری متوجه او خواهد بود. برای مثال، بهره‌گیری از نسخه آزمایشی بدون اطمینان از صحت آن یا استفاده از داده‌های ناقص می‌تواند مصداق تقصیر باشد (قوامی‌پور و محمودی، ۱٤۰٤: ۱۰٥). در مقابل، اگر کاربر به‌طور متعارف عمل کرده ولی خطا ناشی از نقص طراحی باشد، انتساب عنصر روانی به او دشوار است (کوشا و باقری، ۱٤۰۳: ۲٤٦؛ چهره، ۲۰۲٥: ۷). در چنین شرایطی باید بررسی کرد که نهاد مجری قانون در مقام مباشر یا سبب عمل کرده است؛ زیرا تفکیک میان مباشرت و تسبیب در تعیین مسئولیت کیفری اهمیت بنیادین دارد (انصاریان‌فر، شهبازی و حسینی، ۱٤۰۲: ۲۲۲). در صورتی که مسئولیت زنجیره‌ای به‌عنوان یک ساختار

مسئولیت‌افزا در خطاهای الگوریتمی پذیرفته شود، پرسش مهم آن است که آیا قواعد عام تساوی اسباب مذکور در ماده ۵۳۳ قانون مجازات اسلامی نیز قابل اعمال است یا خیر. باید گفت که گرچه این ماده اصل را بر تساوی اسباب می‌گذارد، اما این حکم مربوط به وضعیتی است که اسباب در عرض یکدیگر و با درجه تأثیر برابر عمل کنند. حال آنکه در مسئولیت زنجیره‌ای، اسباب در طول یکدیگر قرار دارند و هر مرحله، نقش و سهم متفاوتی در ایجاد نتیجه دارد. بنابراین، قاعده تساوی اسباب به‌طور مطلق قابل اعمال نبوده و باید با ملاک ماده ٥٣٤ (تفاوت درجات تأثیر) و نظریه سلسله‌مراتب علیت ترکیب شود تا سهم هر بازیگر در زنجیره فناوری به‌صورت تفکیکی تعیین گردد.

٤ .تمایز خطای انسانی و خطای الگوریتمی

خطای انسانی معمولاً ناشی از سهو، غفلت یا سوءنیت است، اما خطای الگوریتمی محصول نقص ذاتی در محاسبات آماری و یادگیری ماشینی است؛ فرآیندهایی که غالباً برای انسان قابل بازسازی نیستند. این تفاوت ماهوی، نظریه‌های سنتی مبتنی بر تقصیر را ناکافی می‌سازد. از منظر حقوق کیفری ایران، اگر فرایند تصمیم‌گیری سامانه‌های هوش مصنوعی را متشکل از اسباب متعدد و طولی بدانیم، امکان تمسک به مواد ۵۳۵ و ٥٣٦ قانون مجازات اسلامی وجود دارد. مطابق این مواد، هرگاه اسباب در طول هم واقع شوند، مسئولیت بر عهده قوی‌ترین و نزدیک‌ترین سبب است؛ مگر آنکه سبب قبلی با تقصیر مؤثر عمل کرده باشد. در تحلیل سامانه‌های تشخیص چهره نیز می‌توان الگوریتم، داده آموزش، پیکربندی، و تصمیم مأمور را در قالب اسباب طولی تحلیل کرد و بر اساس معیار «سبب اقوی»، سهم مسؤولیت هر یک را تعیین نمود. با این حال، پیچیدگی فنی سامانه‌ها ایجاب می‌کند که این قواعد با مدل زنجیره‌ای ترکیب شود تا نقش هر عضو زنجیره به‌دقت سنجیده شود.

در حقوق کیفری باید پذیرفت که خطای الگوریتمی نیز می‌تواند مسئولیت‌آفرین باشد، حتی اگر تصمیم توسط مأمور انسانی اتخاذ شده باشد. بنابراین خروجی سامانه‌های AI تنها در حکم «قرینه» است و نمی‌تواند مبنای قطعیت قضایی تلقی شود. بر همین اساس، مسئولیت کیفری در این حوزه باید به‌صورت زنجیره‌ای میان طراحان، تولیدکنندگان و کاربران تقسیم شود (یوسفی، ١٤٠٢: ٥).

پ) نقد وضعیت حقوقی ایران در قبال سامانه‌های تشخیص چهره و مسؤولیت کیفری ناشی از خطای آن‌ها

١ .فقدان قواعد صریح و نظام‌مند

یکی از مهم‌ترین خلأهای موجود در حقوق کیفری ایران، فقدان مقررات شفاف درباره نحوه استفاده و ارزش اثباتی ابزارهای مبتنی بر هوش مصنوعی از جمله سامانه‌های تشخیص چهره است. نه قانون مجازات اسلامی و نه قانون آیین دادرسی کیفری، ضابطه مشخصی برای پذیرش یا رد این ادله پیش‌بینی نکرده‌اند. در نتیجه، دادگاه‌ها در مواجهه با داده‌های الگوریتمی با ابهام روبه‌رو هستند (قوامی‌پور و محمودی، ١٤٠٤: ١٠٧؛ کوشا و باقری، ١٤٠٣: ٢٤٧). در حقوق ایران همچنان اصل فردی بودن مسئولیت کیفری (ماده ١٤٠ ق.م.ا.) حاکم است و چون سامانه‌های AI فاقد اراده، قصد و بلوغ‌اند، نمی‌توان مسئولیت مستقیم بر آن‌ها بار کرد (انصاریان‌فر، شهبازی و حسینی، ١٤٠٢: ١٤٠). قابل‌تذکّر است که این قاعده اساساً در حوزه مسئولیت مدنی قرار دارد؛ به‌عبارت دیگر اصل فوق غالباً مبنای التزام به جبران خسارت مدنی است. با این حال، هنگامی که خطای الگوریتمی موجب نقض حقوق بنیادین یا ورود خسارت های جدّی

شود، همین مبانی مدنی می‌توانند به‌عنوان مبنای تفسیری و حمایتی برای وضع یا تقویت قواعد کیفری مورد استفاده قرار گیرند. بنابراین مسئولیت باید به بهره‌برداران یا طراحان نسبت داده شود. یکی از کاستی‌های بنیادین حقوق کیفری ایران آن است که برخلاف نظام‌های اروپایی، هیچ ضابطه‌ای برای چگونگی توزیع مسئولیت کیفری میان بازیگران مختلف در یک فرایند فناورانه پیش‌بینی نشده است. نه قانون مجازات اسلامی و نه آیین دادرسی کیفری، سازوکاری برای تعیین سهم تقصیر طراح، توسعه‌دهنده، نهاد ناظر و کاربر نهایی ارائه نمی‌کنند. این خلأ، عملاً موجب انتساب همه خطاها به مأمور اجرا می‌شود، در حالی که در ساختارهای پیچیده مبتنی بر هوش مصنوعی، خطا غالباً حاصل برهم‌کنش چند مرحله‌ای است. بنابراین پذیرش مدل زنجیره‌ای بدون تعیین معیارهای توزیع مسئولیت در حقوق ایران ناکافی بوده و نیازمند تقنین تکمیلی است.

با این حال، از آنجا که خطاهای الگوریتمی می‌توانند به نقض حقوق بنیادین افراد منجر شوند، برخی مبانی مطرح در مسئولیت مدنی – همچون لزوم پیشگیری از ضرر و الزام سازندگان و بهره‌برداران به رعایت استانداردهای ایمنی – می‌توانند در مقام تفسیر کیفری و تعیین حدود تکالیف اشخاص حقیقی و حقوقی مورد استفاده قرار گیرند؛ بدون آنکه ماهیت کیفری مسئولیت مخدوش شود.

۲ .تهدید حقوق بنیادین متهم

اتکای صرف بر خروجی سامانه‌های فاقد شفافیت می‌تواند حقوق بنیادین متهم را تهدید کند. اگر فردی صرفاً بر اساس نتیجه یک سامانه بازداشت شود، در حالی که امکان دسترسی به منطق الگوریتم یا داده‌های آموزشی وجود ندارد، حق دفاع مؤثر او سلب می‌شود. تأمین امنیت قضایی و جلوگیری از تضییع آزادی‌های اساسی متهم در نتیجه بازداشت یا محکومیت نادرست، مستلزم رعایت جدی اصولی چون تضمین برائت، حق سکوت، و حق داشتن وکیل در کلیه مراحل رسیدگی و اجرای قانون است و قصور در هر یک از این مراحل، ابزار حفظ و گسترش امنیت قضایی را تضعیف می‌سازد (وفادوست سبزوار و همکاران، ۱٤۰٤: ۲۱۰). این وضعیت با اصل برائت، حق دفاع و اصل شفافیت دادرسی تعارض دارد و حتی می‌تواند ماده ۳۵ قانون اساسی و ماده ۱۹۰ آیین دادرسی کیفری را نقض کند (قوامی‌پور و محمودی، ۱٤۰٤: ۱۰۹؛ Nelson & Simek, 2020: 17؛ چهره، ۲۰۲۵: ۹). فقدان نگاه تخصصی قضایی نسبت به ماهیت پیچیده فناوری‌ها ـ به‌ویژه سامانه‌های مبتنی بر هوش مصنوعی ـ می‌تواند موجب نادیده گرفتن ابعاد فنی خطای الگوریتمی شود؛ ازاین‌رو رسیدگی به این‌گونه پرونده‌ها توسط قضات متخصص و آگاه، برای حفظ حقوق بنیادین در دادرسی، ضرورتی انکارناپذیر است (اسماعیلی و همکاران، ۱٤۰۳: ۱۰).

۳ .ضرورت تدوین دستورالعمل‌ها و مقررات ویژه

برای رفع این خلأ، ضروری است که نهادهای تقنینی و قضایی دستورالعمل‌های خاصی تدوین کنند. در این مقطع لازم است تفکیک صریحی میان دو قلمرو صورت گیرد: جبران خسارت و جبران مادی/معنوی، موضوعِ مسئولیت مدنی است و بررسی تفصیلی آن از حیطه این پژوهش خارج است؛ اما تعیین حدود، شرایط و ضمانت‌اجراهای مسئولیت کیفری نهادهای تصمیم‌گیر در مواجهه با خطای الگوریتمی موضوع محوری این مطالعه است. این دستورالعمل‌ها باید شامل موارد زیر باشد:

- تعیین ارزش اثباتی و شرایط پذیرش خروجی سامانه‌های تشخیص چهره در دادگاه؛

- مشخص‌کردن مسئولیت کیفری طراحان، کاربران و مقامات در صورت بروز خطا؛
- الزام به مستندسازی فنی و شفاف‌سازی الگوریتم‌ها جهت بازبینی قضایی؛
- پیش‌بینی ضمانت‌اجرا برای استفاده نادرست یا خلاف ضابطه (کوشا و باقری، ۱٤۰۳: ۲٤۸؛ قوامی‌پور و محمودی، ۱٤۰٤: ۱۱۰).

٤ .چالش‌های حقوق بشری و حریم خصوصی

از منظر حقوق بشری، استفاده از سامانه‌های تشخیص چهره می‌تواند تهدیدی جدی علیه حریم خصوصی شهروندان باشد. در حالی که قوانین داخلی ایران عمدتاً به جنبه‌های جسمانی و خانوادگی حریم خصوصی توجه دارند، اسناد بین‌المللی ـ از جمله ماده ۱۲ اعلامیه جهانی حقوق بشر، ماده ۱۸ اعلامیه اسلامی حقوق بشر و کنوانسیون اروپایی حقوق بشر ـ حمایت گسترده‌تری از ابعاد مختلف این حق ارائه می‌دهند. همچنین کنوانسیون جرایم سایبری و پروتکل الحاقی آن چارچوب‌هایی برای صیانت از حریم خصوصی در فضای دیجیتال پیش‌بینی کرده‌اند. این اسناد می‌توانند الگویی برای تقویت نظام حقوق داخلی ایران در این حوزه باشند.

ت) بررسی تطبیقی: تجربه اروپا و آمریکا در مواجهه با خطاهای سامانه‌های تشخیص چهره

۱ .ایالات متحده آمریکا: محوریت مسئولیت فردی و محدودسازی‌های ایالتی

ایالات متحده یکی از نخستین کشورهایی بود که سامانه‌های تشخیص چهره را در حوزه‌های انتظامی و امنیتی به‌کار گرفت؛ از نظارت شهری گرفته تا کنترل مرزها. با این حال، پرسش اصلی این بود که در صورت بروز خطای الگوریتمی، مسئولیت کیفری متوجه چه کسی است. رویه غالب در نظام حقوقی آمریکا همچنان بر اصل پاسخگویی فردی استوار است؛ یعنی مأمور یا قاضی نمی‌تواند تصمیم خود را صرفاً به الگوریتم نسبت دهد.(Raposo, 2024: 213)

اما بروز خطاهای جدی ـ مانند بازداشت نادرست «رابرت ویلیامز» و «مایکل الیور» در دیترویت ـ موجب فشار اجتماعی و حقوقی شد. در نتیجه، برخی ایالت‌ها مانند سان‌فرانسیسکو و بوستون استفاده از فناوری تشخیص چهره را به‌کلی ممنوع یا محدود کردند (قوامی‌پور و محمودی، ۱٤۰٤: ۱۰٦). در سطح فدرال، قانون جامعی تصویب نشده است، اما دادگاه‌ها معمولاً خروجی الگوریتم‌ها را تنها به‌عنوان «قرینه» می‌پذیرند و نه «دلیل قطعی»؛ مگر آنکه تحت آزمایش‌های علمی معتبر تأیید شوند (کوشا و باقری، ۱٤۰۳: ۲٤٦). این رویکرد در عمل نوعی مسئولیت ترکیبی میان کاربر انسانی و توسعه‌دهنده ایجاد کرده است. برای نمونه، در ایالات متحده پرونده‌های معتبری همچون *Robert Williams* و *Michael Oliver* وجود دارد که در آن‌ها افراد به دلیل خطای سامانه‌های تشخیص چهره به‌اشتباه بازداشت شدند .(Garvie, 2020) این نمونه‌ها نشان می‌دهد که خطای الگوریتمی نه صرفاً احتمال، بلکه واقعیتی ملموس است که آثار کیفری بر زندگی افراد دارد. پرونده مشهور *State v. Loomis* (2016) در آمریکا نیز نشان داد که استفاده از الگوریتم COMPAS در تصمیم قضایی با چالش‌های اساسی از حیث شفافیت و حق دفاع همراه است (Angwin et al., 2016).این نمونه یکی از نخستین مصادیق جدی ورود بحث عدالت کیفری به حوزه هوش مصنوعی به شمار می‌آید.

۲ .اتحادیه اروپا: رویکرد محتاطانه و مبتنی بر ریسک

اتحادیه اروپا با تصویب پیش‌نویس قانون هوش مصنوعی[۲]، سامانه‌های تشخیص چهره را در زمره فناوری‌های پرریسک طبقه‌بندی کرده است. به موجب این سند:

- استفاده از این سامانه‌ها در فضاهای عمومی به‌طور کلی ممنوع است، مگر در شرایط استثنایی و با مجوز قضایی؛
- وجود ناظر انسانی در تمام مراحل الزامی است؛
- متهم حق دسترسی به ساختار فنی الگوریتم برای دفاع مؤثر دارد؛
- در صورت شناسایی اشتباه، جبران خسارت و حمایت حقوقی پیش‌بینی شده است (قوامی‌پور و محمودی، ۱٤۰٤: ۱۰۸).

در کشورهای عضو نیز رویه قضایی نسبت به داده‌های الگوریتمی با احتیاط عمل می‌کند. برای مثال، دادگاه‌های آلمان خروجی سامانه‌های AI را صرفاً در صورتی معتبر می‌دانند که قابلیت تبیین (explainability) داشته باشند و بار اثبات صحت آن نیز بر عهده مرجع استفاده‌کننده باشد.

۳ .درس‌های تطبیقی برای ایران

بررسی دو نظام نشان می‌دهد که هم در آمریکا و هم در اروپا، توازن میان کارآمدی فناوری و مسئولیت‌پذیری انسانی مورد توجه است. در آمریکا، تأکید اصلی بر مسئولیت فردی مأمور یا قاضی باقی مانده و فناوری صرفاً ابزار است. در مقابل، اروپا با رویکرد مبتنی بر ریسک و الزام به شفافیت ساختاری، تلاش کرده چارچوبی برای تقسیم مسئولیت در «زنجیره فناوری» ایجاد کند (Raposo, 2024: 220؛ یوسفی، ۱٤۰٤: ٦). در سطح بین‌المللی نیز اسنادی مانند کنوانسیون بوداپست در خصوص جرایم سایبری (۲۰۰۱) و منشور اخلاقی شورای اروپا درباره استفاده از هوش مصنوعی در نظام قضایی (۲۰۱۸) هرچند مستقیماً به مسئولیت کیفری نپرداخته‌اند، اما مبنای مهمی برای تأکید بر شفافیت و پاسخ‌گویی نهادهای مجری قانون محسوب می‌شوند (Council of Europe, 2018; Budapest Convention, 2001).

برای ایران، این تجربه‌ها نشان می‌دهد که سکوت تقنینی نمی‌تواند ادامه یابد. قانون‌گذار باید با الهام از مدل اروپا و در عین توجه به مبانی حقوقی داخلی، مقرراتی روشن برای:

- تعیین ارزش اثباتی ادله الگوریتمی،
- تقسیم مسئولیت میان پلیس، ضابطان، قضات و طراحان،
- و پیش‌بینی ضمانت‌اجرا برای نقض حقوق شهروندان تدوین کند (قوامی‌پور و محمودی، ۱٤۰٤: ۱۱۰؛ کوشا و باقری، ۱٤۰۳: ۲٤۸).

[2] AI Act

جدول تطبیقی مسئولیت کیفری در مواجهه با سامانه‌های هوش مصنوعی

نظام حقوقی	رویکرد اصلی	نکات کلیدی
ایران	شخص‌محوری (اصل فردی بودن مسئولیت کیفری)	• شرط عقل، بلوغ و اختیار برای مسئولیت کیفری (ق.م.ا. ماده ۱۴۰). • سامانه‌های هوش مصنوعی فاقد اراده و قصد محسوب می‌شوند. • تنها امکان انتساب غیرمستقیم (قاعده تسبیب، مسئولیت سازمانی یا تبعی) وجود دارد. انتساب مسئولیت کیفری مستقیم به هوش مصنوعی به دلیل فقدان اراده و قصد فاقد مبنای فلسفی و حقوقی است؛ بنابراین تنها امکان انتقال مسئولیت به طراح، تولیدکننده یا بهره‌بردار وجود دارد (زندی و رفیعی علوی، ۱۴۰۳: ۹۱–۹۲).
آمریکا	مسئولیت مدنی–محور	• تمرکز بر مسئولیت تولیدکننده، طراح یا اپراتور. • سامانه شخصیت کیفری مستقل ندارد. • دادگاه‌ها در پرونده‌هایی مثل State v. Loomis خروجی الگوریتم را فقط «قرینه» دانسته‌اند.
آلمان	تأکید بر اصل شخصی بودن مسئولیت کیفری	• پذیرش مسئولیت کیفری مستقیم برای سامانه منتفی است. • ایده «مسئولیت مشترک انسان و سامانه» توسط موسسات پژوهشی مثل(Max Planck) مطرح شده. • قوانین خاص در حوزه خودروهای خودران به‌روز شده‌اند.

اتحادیه اروپا	تنظیم‌گری آینده‌نگر و مبتنی بر ریسک (AI Act 2021–2024)	• طبقه‌بندی سامانه‌های هوش مصنوعی بر اساس سطح ریسک. • الزام شفافیت الگوریتمی، مستندسازی کامل و ممیزی قضایی. • بحث درباره «شخصیت الکترونیکی» در پارلمان اروپا (۲۰۱۷) ولی با مخالفت‌های جدی.

ث) جمع‌بندی تحلیلی و مدل پیشنهادی «مسئولیت زنجیره‌ای»

بررسی مبانی نظری، وضعیت ایران و تجربه تطبیقی آمریکا و اروپا نشان داد که هیچ‌یک از مدل‌های کلاسیک مسئولیت کیفری به‌تنهایی پاسخگوی چالش‌های ناشی از سامانه‌های تشخیص چهره نیستند .مدل مباشر (انتساب شخصیت کیفری به سامانه) از منظر اصول بنیادین حقوق کیفری غیرقابل پذیرش است؛ زیرا سامانه فاقد اراده و سوءنیت است (جعفری، ۱۳۹۶: ۹۷) .مدل واسطه‌ای (سامانه به‌عنوان ابزار صرف) نیز ناکافی است، چراکه خطاهای الگوریتمی غالباً از حوزه اختیار کاربر فراتر می‌رود (کوشا و باقری، ۱۴۰۳: ۲۴۶). از این رو، مدل ترکیبی یا زنجیره‌ای می‌تواند به‌عنوان راهکاری واقع‌بینانه مطرح شود (یوسفی، ۱۴۰۴: ۳).

۱ .تعریف و ماهیت مدل زنجیره‌ای

در این مدل، مسئولیت کیفری میان بازیگران مختلف زنجیره فناوری تقسیم می‌شود:

- **طراح و توسعه‌دهنده** در برابر نقص الگوریتم یا سوگیری داده‌ای؛
- **کاربر نهایی (پلیس یا ضابط)** در برابر استفاده نادرست یا بدون ملاحظات دادرسی؛
- **قاضی یا مقام قضایی** در برابر پذیرش بی‌ضابطه نتایج بدون بررسی ارزش اثباتی؛
- **نهاد ناظر یا حاکمیتی** در برابر قصور در تنظیم‌گری یا فقدان استانداردهای کنترلی(Raposo, 2024: 220؛ Qandeel, 2024: 97).

به این ترتیب، مسئولیت کیفری نه به یک شخص خاص، بلکه به مجموعه‌ای از کنشگران در زنجیره تصمیم‌گیری و اجرا نسبت داده می‌شود. در تحلیل این مدل، باید نسبت میان مسئولیت کیفری زنجیره‌ای و مسئولیت کیفری نیابتی نیز روشن شود. مسئولیت نیابتی در حقوق کیفری ایران عمدتاً در قالب مسئولیت شخص حقوقی و نظریه فعل غیر مطرح می‌شود و مبتنی بر انتقال یا انتساب رفتار زیان‌بار به نماینده یا زیرمجموعه است. اما در مسئولیت زنجیره‌ای، مبنای مسئولیت نه انتقال فعل، بلکه تقسیم منطقی و مرحله‌ای مسئولیت میان کنشگران متعدد در چرخه طراحی، توسعه، تصمیم‌گیری و اجراست. بنابراین، برخلاف مسئولیت نیابتی که رابطه عمودی و سلسله‌مراتبی دارد، مسئولیت زنجیره‌ای مبتنی بر رابطه افقی و مشارکتی است. با این حال، در مواردی که یکی از بازیگران

زنجیره در مقام نماینده یا قائم‌مقامِ نهاد دیگری فعالیت می‌کند، امکان تسری مسئولیت نیابتی در دل مسئولیت زنجیره‌ای وجود دارد؛ به‌ویژه نسبت به مقامات نظارتی و سازمان‌های بهره‌بردار سامانه‌های هوش مصنوعی.

۲ .ضمانت‌اجرا و کارکرد عملی

برای اجرای مؤثر این مدل در ایران، پیشنهاد می‌شود:

- **تقنین خاص**: تصویب مقررات ویژه در آیین دادرسی کیفری درباره ادله فناورانه؛
- **تعیین آستانه اطمینان** : برای پذیرش خروجی الگوریتم‌ها در دادگاه؛
- **پیش‌بینی مسئولیت کیفری و انضباطی**: برای مأموران و قضاتی که بدون ارزیابی کافی به سامانه استناد می‌کنند؛
- **الزام توسعه‌دهندگان داخلی**: به شفافیت و رفع سوگیری‌های داده‌ای؛
- **ایجاد نهاد ناظر مستقل**: برای ارزیابی عملکرد سامانه‌های پرریسک مانند تشخیص چهره (قوامی‌پور و محمودی، ۱٤۰٤: ۱۱۰؛ انصاریان‌فر، شهبازی و حسینی، ۱٤۰۲: ۲۲۲).

۳ .مزایا نسبت به سایر مدل‌ها

- برخلاف مدل مباشر، با مبانی حقوق کیفری سازگار است و شخصیت کیفری مستقل برای سامانه قائل نمی‌شود.
- برخلاف مدل واسطه‌ای، پیچیدگی‌های فنی و نقش توسعه‌دهندگان را نادیده نمی‌گیرد.
- با توزیع مسئولیت، مانع از «مسئولیت‌گریزی نهادی» می‌شود و عدالت کیفری را تقویت می‌کند (یوسفی، ۱٤۰۲: ٥؛ Raposo, 2024: 220)

بدین ترتیب، می‌توان نتیجه گرفت که مدل مسئولیت زنجیره‌ای بهترین پاسخ برای مواجهه با خطاهای ناشی از سامانه‌های تشخیص چهره در حقوق ایران است. این مدل با ترکیب عناصر فردی و نهادی، ضمن حفظ اصل شخصی بودن مسئولیت کیفری، نقش همه بازیگران در زنجیره فناوری را مورد توجه قرار می‌دهد. یکی از ویژگی‌های مهم مسئولیت زنجیره‌ای آن است که می‌تواند هم‌زمان بر اشخاص حقیقی (کاربران، مأموران، توسعه‌دهندگان) و اشخاص حقوقی (شرکت‌های تولیدکننده، نهادهای ناظر، سازمان‌های بهره‌بردار) بار شود. این هم‌پوشانی نه‌تنها با اصول حقوق کیفری ایران تعارضی ندارد، بلکه مطابق مواد ۱٤۳ و ۱٤٤ ق.م.ا، در جرایم ناشی از فناوری اطلاعات قابل اعمال است. در این ترکیب، شخص حقوقی به دلیل قصور ساختاری، ضعف نظارت، یا استفاده از سامانه معیوب مسئول است و شخص حقیقی به دلیل تصمیم یا تقصیر فردی؛ بنابراین نوعی مسئولیت جمعی یا هم‌افزایی(synergistic liability)شکل می‌گیرد که با ماهیت زنجیره‌ای فناوری‌های نوین هم‌خوان است. اجرای این مدل مستلزم اراده تقنینی، ایجاد نهادهای نظارتی مستقل و پذیرش رویکردی محتاطانه در ارزش‌گذاری ادله فناورانه است.

پیشنهادات

بررسی مبانی نظری، وضعیت حقوقی ایران و تجربه تطبیقی نظام‌های آمریکا و اتحادیه اروپا نشان داد که استفاده از سامانه‌های هوش مصنوعی به‌ویژه در حوزه تشخیص چهره، بدون چارچوب قانونی روشن، می‌تواند تهدیدی جدی برای حقوق بنیادین متهم و عدالت کیفری باشد. بر همین اساس، مجموعه‌ای از پیشنهادهای عملی برای قانون‌گذار و نهادهای قضایی ایران قابل ارائه است:

- **تقنین خاص در آیین دادرسی کیفری** :ضروری است مقررات ویژه‌ای در خصوص ارزش اثباتی داده‌های الگوریتمی تصویب شود. این مقررات باید شرایط پذیرش، حدود اعتبار و شیوه ارزیابی قضایی خروجی سامانه‌های AI را مشخص سازند.
- **تعیین مسئولیت زنجیره‌ای** :باید مسئولیت کیفری میان طراحان، توسعه‌دهندگان، کاربران نهایی (ضابطان و پلیس) و قضات تقسیم شود. چنین تقسیم‌بندی مانع از «مسئولیت‌گریزی نهادی» خواهد شد.
- **ایجاد نهاد ناظر مستقل** :تأسیس نهادی با صلاحیت تخصصی برای ارزیابی، ممیزی و صدور مجوز استفاده از سامانه‌های پرریسک مانند تشخیص چهره ضرورت دارد. این نهاد باید امکان نظارت بر شفافیت الگوریتم‌ها و رفع سوگیری‌های داده‌ای را فراهم کند.
- **پیش‌بینی ضمانت‌اجراهای کیفری و انضباطی** :مأموران و قضاتی که بدون ارزیابی کافی یا برخلاف ضوابط به داده‌های الگوریتمی استناد می‌کنند، باید مسئول شناخته شوند. این ضمانت‌اجراها می‌تواند از توبیخ اداری تا مسئولیت کیفری در صورت ورود خسارت جدی متغیر باشد.
- **تدوین دستورالعمل‌های فنی و آموزشی** :نهادهای قضایی و انتظامی باید دستورالعمل‌های روشن درباره چگونگی استفاده از سامانه‌های AI تدوین کنند و آموزش‌های لازم به کاربران نهایی ارائه شود.

نتیجه‌گیری

تحولات فناورانه در عرصه عدالت کیفری، ضرورت بازاندیشی در مبانی مسئولیت کیفری را آشکار ساخته است. مدل‌های سنتی یا صرفاً مباشرانه و یا صرفاً واسطه‌ای، توان پاسخگویی به پیچیدگی‌های ناشی از خطاهای الگوریتمی را ندارند. آنچه می‌تواند به‌عنوان راه‌حل واقع‌بینانه مطرح شود، **مدل مسئولیت زنجیره‌ای** است؛ مدلی که ضمن حفظ اصل شخصی بودن مسئولیت کیفری، نقش تمام بازیگران دخیل در چرخه طراحی، توسعه و بهره‌برداری را مورد توجه قرار می‌دهد.

اجرای این مدل در حقوق ایران مستلزم چند اقدام اساسی است: اصلاح مقررات آیین دادرسی کیفری، تدوین دستورالعمل‌های خاص برای ادله فناورانه، ایجاد نهاد ناظر مستقل، و الزام توسعه‌دهندگان داخلی به شفافیت و رفع سوگیری‌های داده‌ای. تنها در پرتو چنین اصلاحاتی است که می‌توان میان کارآمدی فناوری و حفظ حقوق بنیادین متهمان توازن برقرار کرد و نظام عدالت کیفری را در برابر چالش‌های ناشی از هوش مصنوعی مقاوم ساخت.

فهرست منابع:

الف)مقالات

۱. افروزی، ه.، شیرزادراجعونی، هـ & .،محمودی، م.ر. (۱٤۰٤). حقوق جزای بین‌الملل و تهدیدات جدید هوش مصنوعی: راهکارها و رویکردها. فصلنامه علمی فقه و حقوق نوین https://www.jaml.ir/article_728450.html .

۲. انصاریان‌فر، م.، شهبازی، م.ا & .،حسینی، س.م. (۱٤۰۲). بررسی انتساب مسئولیت کیفری سلبریتی از منظر حقوق جمهوری اسلامی ایران. ماهنامه علمی–تخصصی پایا شهر، (۸۰٤۰۰)، ۹۵–۲۲۲ https://payashahr.ir/wp-content/uploads/2024/06/بررسی-انتساب-مسئولیت-کیفری-سلبریتی-از-منظر-حقوق-جمهوری-اسلامی-ایران.pdf.

۳. اسماعیلی، م.، حبیب‌نژاد، س.ا & .،داودی، ح. (۱٤۰۳). آسیب شناسی دادرسی رسانه ای در نظام حقوقی ایران با نگاهی به مطالعات تطبیقی. فصلنامه تحقیق و توسعه در حقوق تطبیقی، ۱۷(۲۵)، ۹–۲۲. 10.22034/law.2024.2036740.1425

٤. بازوند، و & .،نورمحمدی، ح. (۱٤۰۰). مسئولیت کیفری در مفهوم انتزاعی و گستره حاکمیت آن بر رفتار شخص حقوقی (از تحلیل نظری تا واکنش قضایی). پژوهش‌های حقوقی، ۲۰(٤۷), ۵۵–۸۸ https://doi.org/10.48300/JLR.2021.140164 .

۵. جعفری، م. (۱۳۹٦). بازاندیشی در مفهوم مسئولیت کیفری فعل غیر. پژوهش حقوق کیفری، ٦(۲۰)، ۱۷۳–۲۰۰ . https://doi.org/10.22054/jclr.2017.12330.1216

٦. چهره، ا. (۲۰۲۵). هوش مصنوعی و حقوق کیفری: چالش‌های محاکمه منصفانه، جرایم جدید و مسئولیت هوش مصنوعی | LexTech .حقوق و فناوری . https://lextech.ir/ai-criminallaw

۷. زندی، م & .،رفیعی علوی، س.ا. (۱٤۰۳). مسئولیت کیفری در قبال سامانه‌های تشخیص چهره مبتنی بر هوش مصنوعی: مطالعه‌ای تطبیقی. فصلنامه فلسفه حقوق، ۳(۱)، ۹۰–۱٤۵ https://civilica.com/doc/2289244 .

۸. قوامی‌پور سرشکه، م & .،محمودی، ا. (۱٤۰٤). درآمدی بر چهارچوب‌های حقوقی مسئولیت کیفری برای سیستم‌های هوش مصنوعی. مجله حقوق فناوری‌های نوین، ۲(۲)، ۹۵–۱۱۲ https://mtlj.usc.ac.ir/article_212380.html .

۹. کوشا، ا & .،باقری، م. (۱٤۰۳). تأثیر به‌کارگیری هوش مصنوعی در جمع‌آوری ادله کیفری. ارائه‌شده در کنفرانس بین‌المللی علوم انسانی، مدیریت و مطالعات اجتماعی، تهران: مؤسسه افق روشن علم و دانش https://civilica.com/doc/1760242 .

۱۰. کوشا، ا & .،باقری، م. (۱٤۰۳). روش‌های رسیدگی و رویکردهای قانونی جرایم هوش مصنوعی علیه انسان. ارائه‌شده در کنفرانس بین‌المللی توسعه علوم انسانی و مطالعات اجتماعی، تهران: مؤسسه افق نو دانش https://civilica.com/doc/1760245 .

۱۱. فتحی، م.، بختیاری، ف & .،فخاری، م.س. (۱٤۰۳). تحلیل مسئولیت کیفری نهادهای مجری قانون در استفاده از سامانه‌های هوش مصنوعی. فصلنامه فلسفه حقوق، ۳(۱)، ۷۰–۹۸ https://mtlj.usc.ac.ir/article_212380.html .

۱۲. وفادوست سبزوار، م.، فتح‌آبادی، ح & .،شایگان‌فرد، م. (۱٤۰٤). واکاوی وظایف و اختیارات دادستان در حفظ و گسترش امنیت قضایی با رویکرد تطبیقی در حقوق ایران و فرانسه. فصلنامه تحقیق و توسعه در حقوق تطبیقی، ۱۸(۲۷)، ۲۰۹–۲۲۲ . 10.22034/law.2024.2037837.1437

۱۳. یوسفی، ع. (۱٤۰۲). بررسی مبانی، چالش‌ها و راهکارهای مسئولیت کیفری سامانه‌های هوش مصنوعی در حقوق ایران و تطبیق آن با نظام‌های اروپایی. ارائه‌شده در همایش ملی حقوق و فناوری نوین، تهران: دانشگاه علوم اسلامی رضوی https://civilica.com/doc/1774995 .

۱٤. یوسفی، ع. (۱٤۰٤). مسئولیت کیفری ناشی از عملکرد سامانه‌های هوش مصنوعی در حقوق ایران و نظام‌های تطبیقی. ارائه‌شده در چهارمین کنفرانس بین‌المللی دانش و فناوری حقوق و علوم انسانی ایران https://civilica.com/doc/2302984 .

References

1. Afroozi, H., Shirzadrajavoni, H., & Mahmoudi, M. R. (2025). International criminal law and new AI threats: Solutions and approaches. Scientific Quarterly of Jurisprudence and Modern Law. Retrieved from https://www.jaml.ir/article_728450.html (in Persian)
2. Ansarianfar, M., Shahbazi, M. A., & Hosseini, S. M. (2023). Examining the attribution of criminal liability to celebrities from the perspective of the law of the Islamic Republic of Iran. Paya Shahr Scientific–Specialized Monthly, (80400), 95–

222. Retrieved from https://payashahr.ir/wp-content/uploads/2024/06/-بررسي-انتساب-مسئوليت-كيفري-سلبريتي-از-منظر-حقوق-جمهوري-اسلامي-ايران.pdf (in Persian)
3. Bazvand, V., & Nourmohammadi, H. (2021). Criminal liability in abstract concept and its scope over corporate behavior (from theoretical analysis to judicial reaction). Legal Research, 20(47), 55–88. https://doi.org/10.48300/JLR.2021.140164 (in Persian)
4. Chehre, A. (2026). Artificial intelligence and criminal law: Challenges of fair trial, new crimes, and AI liability. LexTech | Law and Technology. Retrieved from https://lextech.ir/ai-criminallaw
5. Esmaeili, M., Habibnejad, S. A., & Davoodi, H. (2024). Pathology of media trial in the Iranian legal system: A comparative study. Quarterly Journal of Research and Development in Comparative Law, 17(25), 9–22. Retrieved from 10.22034/law.2024.2036740.1425 (in Persian)
6. Fathi, M., Bakhtiari, F., & Fakhari, M. S. (2024). Analysis of criminal liability of law enforcement agencies in the use of AI systems. Quarterly Journal of Philosophy of Law, 3(1), 70–98. Retrieved from https://mtlj.usc.ac.ir/article_212380.html (in Persian)
7. Ghavami-Pour Sarshke, M., & Mahmoudi, A. (2025). An overview of legal frameworks for criminal liability of artificial intelligence systems. Journal of New Technology Law, 2(2), 95–112. Retrieved from https://mtlj.usc.ac.ir/article_212380.html (in Persian)
8. Jafari, M. (2017). Rethinking the concept of criminal liability for another's act. Journal of Criminal Law Research, 6(20), 173–200. https://doi.org/10.22054/jclr.2017.12330.1216 (in Persian)
9. Kousha, A., & Bagheri, M. (2024). Impact of AI utilization in collecting criminal evidence. Presented at the International Conference on Humanities, Management, and Social Studies, Tehran, Iran. Retrieved from https://civilica.com/doc/1760242 (in Persian)
10. Kousha, A., & Bagheri, M. (2024). Legal approaches and prosecution methods for AI crimes against humans. Presented at the International Conference on Human Development and Social Studies, Tehran, Iran. Retrieved from https://civilica.com/doc/1760245 (in Persian)
11. Nelson, S. D., & Simek, J. W. (2020, August 26). The ethical and legal implications of black box artificial intelligence. Sensei Enterprises, Inc. Retrieved from https://senseient.com/wp-content/uploads/Black-Box-AI.pdf
12. Qandeel, M. (2024). Facial recognition technology: Regulations, rights and the rule of law. Frontiers in Big Data, 7, 1354659. https://doi.org/10.3389/fdata.2024.1354659
13. Raposo, V. L. (2024). The digital "To Kill a Mockingbird": Artificial intelligence biases in courts. California Western International Law Journal, 54(2), 459–488. https://scholarlycommons.law.cwsl.edu/cwilj/vol54/iss2/6
14. Raposo, V. L. (2024). When facial recognition does not 'recognise': Erroneous identifications and resulting liabilities. AI & Society, 39(6), 1857–1869. https://doi.org/10.1007/s00146-023-01634-z
15. Vafadoost Sabzevar, M., Fathabadi, H., & Shayganfard, M. (2025). Investigating the duties and powers of the prosecutor in maintaining and expanding judicial security: A comparative approach in Iran and France. Quarterly Journal of Research and Development in Comparative Law, 18(27), 209–222. Retrieved from 10.22034/law.2024.2037837.1437 (in Persian)
16. Yousefi, A. (2023). Examining the foundations, challenges, and solutions of criminal liability of AI systems in Iran and comparison with European legal systems. Presented at the National Conference on Law and New Technology, Tehran, Iran. Retrieved from https://civilica.com/doc/1774995 (in Persian)
17. Yousefi, A. (2025). Criminal liability arising from AI system performance in Iran and comparative legal systems. Presented at the 4th International Conference on Law, Science, and Human Technology, Iran. Retrieved from https://civilica.com/doc/2302984 (in Persian)
18. Zandi, M., & Rafiei Alavi, S. A. (2024). Criminal liability regarding AI-based facial recognition systems: A comparative study. Quarterly Journal of Philosophy of Law, 3(1), 90–145. Retrieved from https://civilica.com/doc/2289244 (in Persian)