

Journal of Islamic Law Research

پژوهش‌نامه حقوق اسلامی

An Analysis of the Doctrine of Vicarious Liability as a Legal Basis for Responsibility Arising from Artificial Intelligence Outputs in Iranian Law, Inspired by Common Law Judicial Practice

Authors: Abbas Shiri | Mohammad Reza Barzegar

Stable URL: <https://doi.org/10.30497/law.2025.248106.3746>

تحلیل دکترین مسئولیت نیابتی به مثابه مبنای مسئولیت ناشی از هوش مصنوعی
در حقوق ایران، با الهام از رویه قضایی کامن لا

نویسندگان: عباس شیر | محمد رضا بارزگر

پیوند دائمی: <https://doi.org/10.30497/law.2025.248106.3746>

Copyright 2026 The Author(s).

Published by *Imam Sadiq University*, Tehran, Iran.

This work is fully Open Access under the Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) license, allowing non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited and not modified. *Islamic Law Research* strictly follows the ethical guidelines of the Committee on Publication Ethics (COPE), which all readers, authors, reviewers, and editors are expected to observe and uphold.



An Analysis of the Doctrine of Vicarious Liability as a Legal Basis for Responsibility Arising from Artificial Intelligence Outputs in Iranian Law, Inspired by Common Law Judicial Practice

Abbas Shiri • Associate Professor, Department of Criminal Law and Criminology, Faculty of Law and Political Sciences, University of Tehran, Tehran, Iran. (Corresponding Author)
ashiri@ut.ac.ir

Mohammad Reza Barzegar • PhD Student in Criminal Law and Criminology, Faculty of Law and Political Sciences, University of Tehran, Tehran, Iran.
mrbarzegar@ut.ac.ir

Abstract

Context & Objective: The most significant challenge which Artificial Intelligence (AI) poses for jurists is concerning the attribution of liability for the use of such systems and plugging the existing "liability gap." This research seeks to provide a solution to the issue of AI liability by harnessing the promise of the doctrine of vicarious liability. The primary aim of this research is to explain why this doctrine is being applied to deployers (principals) of intelligent systems. After explaining the application of the theory to AI, it discusses how possible it is to establish the substantive components of the doctrine despite the unique characteristics of AI.

Method & Approach: The paper adopts a doctrinal method and a descriptive-analytical approach, relying on library resources, including books, articles, and court cases. The economic, risk-based, operational, and control-based principles of the doctrine have been extracted. The principles are compared with analogous principles in Islamic law, such as the rule of "*man lahu al-ghunm fa'alayhi al-ghurm*" (he who enjoys the benefits of a thing must also bear its losses), and are applied to the case of an AI deployer. Subsequently, the existence of the substantive elements of vicarious liability – i.e., "the existence of a relationship" and "the connection of the wrongful act to that relationship" – is examined in the context of AI and its deployer. To establish a legal relationship between the AI system and the principal and link the wrongful act to that relationship, the "relationship akin to employment" test and the "close connection test" are proposed.



Findings: Analysis of the justifications of vicarious liability establishes its extension to deployers of AI as fully justified on the basis of: 1) The superior economic capacity of the principal to compensate for injuries and take on risk (deep pockets); 2) The legal-economic principle of risk creation by the party benefiting from it and the necessity of internalization of the costs its commercial venture causes; 3) The instrumental nature of AI and incorporation of its operation into the core business of the enterprise and value generation for it; and 4) Control by the principal over establishing or re-establishing objectives, training data, and monitoring of the intelligent system, as well as their ability to, in effect, "pull the plug." The article confirms that when an organization deploys an AI (for instance, a self-driving taxi) and harm is caused through the AI, the "relationship akin to employment" test, which has been adopted in common law, can effectively establish the legal relationship between the organization and the AI because the AI is "hired" for the fulfillment of the organization's objectives. In addition, the "close connection test" is able to determine the connection between the wrongful act of the system and its link with the company, since the harm resulting is usually the realization of an inherent risk connected with the very activity that is undertaken by the principal who has gained and profited by using the AI. By adopting such principles and such requirements, the responsibility is placed on the firm, whereas traditional rules of law are faced with challenges in attributing responsibility due to, for example, the autonomous action of AI, its black-box nature, and the complexity of the causal chain.

Conclusion: The study concludes that the doctrine of vicarious liability, through its flexible tests such as the "relationship akin to employment" and the "close connection" test, provides a coherent, justifiable, and practicable foundation for attributing liability to AI deployers and can effectively fill in the existing liability gap. By applying this doctrine to AI, the responsibility is on the one who controls and also benefits from the technology. The proposed model is aligned with acknowledged axioms of Islamic law, such as the axiom of "*man lahu al-ghunm fa'alayhi al-ghurm*" (he who enjoys the benefits of a thing must also bear its losses), and can be employed by the legislator for developing clear-cut rules in the field of artificial intelligence.

Keywords: Artificial Intelligence, Vicarious Liability, Close Connection Test, Cost Internalization.

تحلیل دکتربین مسئولیت نیابتی به مثابه مبانی مسئولیت ناشی از هوش مصنوعی در حقوق ایران، با الهام از رویه قضایی کامن لا

عباس شیرى • دانشیار، گروه حقوق جزا و جرم‌شناسی، دانشکده حقوق و علوم سیاسی، دانشگاه تهران، تهران، ایران.
ashiri@ut.ac.ir (نویسنده مسئول)
محمدرضا برزگر • دانشجوی دکتری حقوق جزا و جرم‌شناسی، دانشکده حقوق و علوم سیاسی، دانشگاه تهران، تهران، ایران.
mrbarzegar@ut.ac.ir

چکیده

هوش مصنوعی، نظام‌های حقوقی در سراسر جهان و از جمله نظام حقوقی ایران را با مسائل نوینی مواجه ساخته که شاید برجسته‌ترین آن، نحوه انتساب مسئولیت ناشی از خروجی‌های هوش مصنوعی و رفع «خلاء مسئولیت» ناشی از آن است. پژوهش حاضر با هدف ارائه یک چارچوب حقوقی کارآمد، به تحلیل ظرفیت دکتربین مسئولیت نیابتی برای پاسخگویی به این مسأله می‌پردازد. هدف اصلی، تبیین مبانی موجهه اعمال این دکتربین بر اشخاص به‌کارگیرنده سامانه‌های هوشمند، و امکان‌سنجی انطباق عناصر ماهوی آن با ویژگی‌های منحصر به فرد هوش مصنوعی خواهد بود. در این راستا، نوشتار حاضر با روش توصیفی تحلیلی، مبانی و عناصر این دکتربین را در پرتو ویژگی‌های هوش مصنوعی صورت‌بندی کرده و با اصول مشابه در حقوق ایران تطبیق می‌دهد. تحلیل مبانی مسئولیت نیابتی مؤید آن است که اصولی چون ظرفیت برتر اقتصادی اصیل جهت جبران خسارت بزه‌دیده و مدیریت ریسک، منطق حقوقی اقتصادی ایجاد ریسک توسط شرکت استفاده‌کننده و ضرورت درونی‌سازی هزینه‌ها، و همچنین ماهیت ابزاری و عملکرد ادغام‌شده هوش مصنوعی در فعالیت اصیل و کنترل راهبردی وی بر آن، توجیه‌پذیری اعمال مسئولیت نیابتی در این حوزه را مدلل می‌سازد. بر این اساس، عناصر دکتربین مذکور مورد بررسی قرار گرفته و استدلال می‌شود که معیار کامن‌لایی «رابطه شبیه به استخدام» به‌نحو مؤثری قادر به تبیین پیوند حقوقی میان شخص اصیل و سامانه هوشمند است، و معیار «ارتباط نزدیک» اتصال میان فعل مجرمانه ناشی از سیستم و رابطه مذکور را برقرار می‌سازد. نهایتاً، این نتیجه حاصل شده است که دکتربین مسئولیت نیابتی، چارچوبی منسجم، قابل دفاع و کارآمد برای انتساب مسئولیت به به‌کارگیرندگان هوش مصنوعی فراهم می‌آورد، و این چارچوب می‌تواند به مثابه مبنایی عملی برای قانون‌گذاری هوش مصنوعی در نظام حقوقی ایران و البته دیگر نظام‌های حقوقی که از این «خلاء مسئولیت» رنج می‌برند مورد توجه قرار گیرد؛ بر همین بنیاد، نگارندگان پیشنهادهایی نیز در خاتمه مقاله ارائه کرده‌اند.

واژگان کلیدی: هوش مصنوعی، مسئولیت نیابتی، معیار ارتباط نزدیک، درونی‌سازی هزینه‌ها.



مقدمه

هوش مصنوعی افق‌هایی را در عرصه‌های گوناگون حیات بشری گشوده و نویدبخش تحول در صنعت، بهداشت، حمل‌ونقل و فراتر از آن است. این تحولات سریع فناوری و تطورات الگوهای کسب‌وکار نوین با ویژگی‌هایی چون توسعه فناوری‌های تخریبگر، غیرملموس بودن، پویایی و تغییر دائمی فضا، تحقق حاکمیت قانون و اصول و قواعد حکمرانی به شکل مرسوم و سنتی آن را ناممکن کرده است. در چنین فضایی، نمی‌توان به قوانین سنتی اتکای چندانی کرد. در این میان، نظام‌های حکمرانی با استفاده از الگوها و سازوکارهای جدید تنظیم‌گری، در تلاش برای حداکثرسازی توسعه این فناوری‌ها و درعین‌حال، حفظ و تضمین حقوق شهروندان هستند (غمامی و هاشمی، ۱۴۰۴، ص. ۱) باین‌حال، این پیشرفت‌های فناورانه، مجموعه‌ای از مسائل حقوقی بی‌سابقه و بی‌پاسخ را نیز به همراه آورده‌اند^۱ که در کانون آن‌ها، مسئله «خلأ مسئولیت» در قبال آسیب‌های ناشی از عملکرد این سامانه‌ها قرار دارد.^۲ ویژگی‌هایی چون استقلال عملیاتی و ماهیت غیرقابل پیش‌بینی و غیرقابل توضیح، فرایند سنتی انتساب مسئولیت را با دشواری مواجه ساخته

۱. به‌طوری‌که حوزه‌های حقوقی متعددی مشخصاً در خصوص آن قانون‌گذاری کرده‌اند که ازجمله می‌توان به قانون هوش مصنوعی اتحادیه اروپا (EU AI Act) (نهایی‌شده در ۲۰۲۴)، مقررات مربوط به دیپ‌فیک (Deep Synthesis Provisions) (لازم‌الاجرا از ۲۰۲۳) در چین و قانون هوش مصنوعی و داده (AIDA) (پیشنهادشده در ۲۰۲۲) کانادا اشاره کرد. برای اطلاع جامع از قوانین کشورهای مختلف در خصوص هوش مصنوعی ر. ک به:

<https://www.aiprm.com/ai-laws-around-the-world/>

۲. بحث خلأ مسئولیت اولین بار در سال ۲۰۰۴، در یک مقاله مطرح شد و هم‌اکنون در سال ۲۰۲۵، این بحث آکادمیک ادامه دارد. آندرس ماتیاس - نویسنده - در آن مقاله (که بسیار پیش‌گامانه و جلوتر از زمانه خود بود) به الگوریتم‌هایی که دارای قابلیت یادگیری و خودمختاری هستند مانند شبکه‌های عصبی، الگوریتم‌های ژنتیک و معماری‌های عامل اشاره و استدلال کرد که رفتار این سیستم‌ها می‌تواند برای سازندگان یا اپراتورها غیرقابل پیش‌بینی شود و در نتیجه، تعیین مسئولیت برای اقدامات آن‌ها دشوار است. سه سال بعد، مقاله دیگری در این خصوص منتشر شد که استدلال‌ات مقاله قبلی را تقویت و تکمیل کرد. به این دو مقاله تاکنون بیش از هزار مرتبه استناد شده است. نویسنده این سطور درک خود از حقوق هوش مصنوعی را مدیون مقاله ماتیاس می‌داند.

Matthias, A. (2004). The responsibility gap: Ascribing responsibility for the actions of learning automata. *Ethics and information technology*, 6(3), p. 175-183.

Sparrow, R. (2007). Killer robots. *Journal of applied philosophy*, 24(1), 62-77.

است^۱ و منجر به نگرانی درباره تضمین حقوق بزه‌دیدگان و ایجاد بازدارندگی مؤثر شده است؛ زیرا تعیین مسئولیت برای درک علل وقایع نامطلوب، پیشگیری از تکرار آن‌ها و تنظیم انتظارات ما از فناوری ضروری است (Johnson, 2015, p. 713).

در چنین بستری، با توجه به آنکه سیاست‌های مرتبط با مسئولیت دارای تأثیرات اقتصادی و اجتماعی قابل توجهی هستند، انتخاب سازوکار (رژیم) مسئولیت مشخص و منسجم برای هوش مصنوعی اولیتی ضروری است (ذاکری‌نیا، ۱۴۰۲، ص. ۱۳۶). فقدان چنین سازوکاری می‌تواند منجر به افزایش ریسک‌های حقوقی و اقتصادی برای توسعه‌دهندگان و به‌کارگیرندگان و همچنین، ناکارآمدی معیارهای سنتی اعمال مسئولیت (همچون قابلیت پیش‌بینی و قصد مجرمانه) شود.^۲ در این صورت منتفعان هوش مصنوعی فاقد انگیزه‌های لازم برای به حداقل رساندن آسیب و خسارت، در اعمال دقت لازم قصور خواهند کرد یا حتی ممکن است عمداً باعث آسیب شوند؛ زیرا می‌توانند این کار را مبتنی بر خلأهای مسئولیت و بدون مجازات انجام دهند. بنابراین، نگرانی در مورد فقدان بازدارنده‌های^۳ رفتار مجرمانه است که ساختار انگیزشی مفید را از بین می‌برند (Königs, 2022, p. 5). در واکنش به این نیاز مبرم، رویکردهای مختلفی از پذیرش نوعی مسئولیت‌پذیری برای برخی سیستم‌های هوش مصنوعی^۴ تا تلاش برای یافتن راهکارهای عملی

۱. برای مطالعه در خصوص چیستی خلأ مسئولیت با توجه به پیشرفت‌های هوش مصنوعی ر. ک به:

Königs, P. (2022). Artificial intelligence and responsibility gaps: What is the problem?. *Ethics and Information Technology*, 24(3), 36.

۲. برای مطالعه مبسوط در خصوص اینکه چگونه پدیده هوش مصنوعی منجر به ناکارآمدی معیارهای سنتی مسئولیت (قصد-علیت) می‌شود، به اثر ارزشمند و تأثیرگذار زیر رجوع شود.

Bathae, Y. (2017). The artificial intelligence black box and the failure of intent and causation. *Harv. JL & Tech.*, 31.

3. Disincentives

۴. اولین بار بین سال‌های ۲۰۱۰ تا ۲۰۱۵، پروفیسور گابریل هالوی، نظریه مسئولیت کیفی مستقیم هوش مصنوعی را از طریق یک مقاله علمی و متعاقباً دو کتاب دیگر مطرح کرد. به‌رغم جذابیت ظاهری و خلاقانه بودن، این نظریه به دلیل فقدان رویکردهای عملیاتی و کاربردی برای حل مسائل موجود مورد نقد قرار گرفت و با وجود بررسی‌های جامع توسط نهادهای قانون‌گذاری ازجمله اتحادیه اروپا در روند تدوین مقررات هوش مصنوعی و سایر حوزه‌های قضایی، دیدگاه هالوی مبنای هیچ قانون‌گذاری‌ای واقع نشد؛ زیرا در حال حاضر امکان پیاده‌سازی آن وجود ندارد. برای مطالعه این نظر به منابع زیر مراجعه شود (پاورقی صفحه آتی).

جهت پر کردن خلأ موجود مطرح شده است. در میان این راهکارها، رجوع به دکترین انعطاف‌پذیر مسئولیت نیابتی^۱ که سابقه‌ای طولانی در نظام‌های حقوقی کامن‌لا و رومی-ژرمنی دارد، گزینه‌ای قابل تأمل به نظر می‌رسد. مسئولیت نیابتی به‌عنوان سازوکاری که تحت شرایط خاص، بار مسئولیت ناشی از فعل مجرمانه یک شخص (عامل) را بر شخص دیگری (اصیل^۲ یا مسئول نیابتی) که با او رابطه ویژه‌ای دارد (مانند کارفرما-کارمند والد-فرزند) تحمیل می‌کند - حتی بدون اثبات تقصیر یا عمد مستقیم اصیل - ظرفیت بالقوه‌ای برای فائق آمدن بر برخی موانع مسئولیت در عصر هوش مصنوعی دارد (Diamantis, 2023, p. 319).

البته اعمال مفاهیم مسئولیت بر هوش مصنوعی خالی از پیچیدگی نیست و مواردی همچون دشواری در احراز عنصر روانی (اعم از قصد یا تقصیر) و معضل توزیع مسئولیت در ساختارهای سازمانی پیچیده یا زنجیره‌های تأمین فناوری که از آن با عنوان «مشکل دست‌های زیاد»^۳ یاد می‌شود، در خصوص هوش مصنوعی تشدید می‌شود (Kerrigan, 2022, p. 149)، اما این پیچیدگی‌ها به‌جای آنکه مبنایی برای رد کامل امکان اعمال مسئولیت نیابتی باشند، ضرورت تحلیل دقیق و تطبیقی برای بررسی چگونگی انطباق این دکترین با ویژگی‌های منحصربه‌فرد هوش مصنوعی را آشکار می‌سازند؛ رویکردی که برخی اندیشمندان نیز با تأکید بر لزوم بسط و به‌روزرسانی چهارچوب‌های حقوقی موجود برای مواجهه با فناوری‌های نوین، بر آن صحه می‌گذارند (Johnson, 2015, p. 709).

از طرف دیگر، در نظام حقوقی ایران، چهارچوب کلی مسئولیت نیابتی در ماده ۱۴۲ قانون مجازات اسلامی تبیین شده است که شرایط آن را منوط به وجود مسئولیت قانونی یا ارتکاب تقصیر در قبال نتیجه می‌داند. درعین حال، صرف تلاش برای انطباق پدیده هوش مصنوعی با مقررات موجود که برای وضعیت‌های حقوقی متفاوتی تدوین شده‌اند، اساساً قادر به ارائه راهکاری

Hallevy, G. (2010). The criminal liability of artificial intelligence entities-from science fiction to legal social control. *Akron Intell. Prop. J.*, 4, 171.

Hallevy, G. (2013). *When robots kill: Artificial intelligence under criminal law*. UPNE.

Hallevy, G. (2015). *Liability for crimes involving artificial intelligence systems* (Vol. 257). New York, NY, USA: Springer International Publishing.

1. Vicarious Liability
2. Principal
3. Many Hands Problem

جامع و پایدار برای خلأ مسئولیت ناشی از هوش مصنوعی نیست و حتی می‌تواند غیرسازنده^۱ باشد و منابع پژوهشی را از وظیفه اولی یعنی بحث و تحلیل در خصوص ایجاد قواعد و مقررات اختصاصی برای هوش مصنوعی - همچون کشورهای پیشرو اروپایی - منحرف سازد. بدین جهت، پژوهش حاضر درصدد تحلیل انطباقی هوش مصنوعی با ماده ۱۴۲ نیست^۲. هدف اصلی این مقاله، ارائه و ارزیابی چهارچوب مفهومی و تحلیلی با الهام از دگرترین مسئولیت نیابتی (با تمرکز بر نظام کامن‌لا) و همچنین، تمهید مبانی نظری و ارائه ایده‌های عملی برای تدوین مقررات اختصاصی و کارآمد برای هوش مصنوعی در حقوق ایران است. این امر از آن جهت ضروری و کمک‌کننده می‌نماید که نظام تنظیم‌گری فناوری‌های جدید در ایران، ضعیف، غیرساختارمند، جزیره‌ای، نامنسجم و ناهماهنگ توصیف شده و نظام حقوقی ایران در حوزه هوش مصنوعی تاکنون رویکرد فعال و تنظیمی روشنی در پیش نگرفته و سیاست‌گذاری و حکمرانی در این حوزه معطل مانده است (غمامی و هاشمی، ۱۴۰۴، ص. ۱).

با توجه به مراتب مذکور، مقاله حاضر به تحلیل مبانی موجهه اعمال مسئولیت نیابتی بر اسیل در قبال عملکرد هوش مصنوعی می‌پردازد و چهارچوب مفهومی و تحلیلی عناصر دوگانه این مسئولیت - یعنی احراز رابطه حقوقی خاص (با تمرکز بر معیار «شبیه به استخدام»)^۳ و احراز ارتباط فعل مجرمانه با آن رابطه (با تمرکز بر معیار «ارتباط نزدیک»)^۴ - را صورت‌بندی و تشریح می‌کند. بدین منظور، ابتدا مبانی اقتصادی و مبتنی بر ریسک (۱) و سپس مبانی عملیاتی و کنترلی توجیه‌گر (۲) این مسئولیت که در رویه قضایی کامن‌لا مطرح شده‌اند، تحلیل می‌شود. در ادامه، عناصر مسئولیت نیابتی در پرتوی هوش مصنوعی (۳) مورد بررسی قرار می‌گیرد.

1. Counterproductive

۲. علاوه‌براین، باید توجه داشت که مسئولیت نیابتی در حقوق کیفری ایران در حد تصویب ماده ۱۴۲ باقی مانده است و هیچ‌گونه پشتوانه اجرایی در رویه قضایی ندارد. بنابراین، زمانی که اعمال آن بر جرائم و مجرم انسانی با اتهامات فراوانی مواجه است و این اتهامات منجر به بی‌استفاده ماندن ماده ۱۴۲ در نظام حقوقی ایران شده است، هر تلاشی برای تطبیق جرائم به‌کلی متفاوت هوش مصنوعی با آن محکوم به بی‌نتیجه بودن کارکردی است.

3. Akin to Employment

4. Close Connection

۱. مبانی اقتصادی و مبتنی بر ریسک در توجیه مسئولیت نیابتی هوش مصنوعی

در نظام‌های حقوقی مختلف، رویکردهای تنظیم‌گری فناوری‌های نوپدید به سمت ارزیابی و مدیریت ریسک حرکت می‌کنند. این رویکردها که گاه تحت عنوان «نظریه تنظیمی مبتنی بر ریسک» شناخته می‌شوند، به جای محدود کردن فناوری‌ها، بر شناسایی، ارزیابی و مدیریت ریسک‌های مرتبط با آن‌ها از طریق تدوین سیاست‌ها و مقررات مناسب تمرکز دارند (غمامی و هاشمی، ۱۴۰۴، ص. ۱۰). در همین راستا، تبیین قابلیت اعمال مسئولیت نیابتی بر جرائم ناشی از هوش مصنوعی نیز نیازمند تحلیل دقیق مبانی موجهه آن است. بخش نخست این تحلیل، بر ابعاد اقتصادی و ملاحظات ناظر بر تخصیص بهینه ریسک متمرکز است؛ ملاحظاتی که در رویه قضایی کاملاً نقش اساسی در توجیه این نوع مسئولیت ایفا می‌کنند. در این چهارچوب، دو محور اساسی مورد مذاقه قرار می‌گیرد. نخست، ظرفیت برتر اصیل در قیاس با عامل هوشمند جهت جبران خسارت و مدیریت تبعات مالی ریسک (۱.۱) و دوم، مبنای حقوقی-اقتصادی مسئولیت ناشی از ایجاد ریسک توسط شرکت و اصل درونی‌سازی هزینه‌های جرم (۱.۲). بررسی این دو محور، مبنایی برای درک چرایی انتساب مسئولیت به اصیل فراهم می‌آورد.

۱.۱. ظرفیت برتر اصیل در جبران خسارت و مدیریت ریسک‌های نوظهور

ملاحظات عمل‌گرایانه و اقتصادی به‌مثابه مبنایی برای توجیه مسئولیت نیابتی در رویه قضایی کاملاً به‌طور مکرر مورد تأکید قرار گرفته است. این رویکرد، مسئولیت را به نقطه‌ای در زنجیره فعالیت اقتصادی تخصیص می‌دهد که بیشترین ظرفیت را برای مدیریت و جبران خسارت‌های احتمالی دارا باشد. براین اساس، دو استدلال مطرح می‌شود. نخست، توانایی مالی و ساختاری برتر «اصیل» (به‌کارگیرنده) (۱.۱.۱) و دوم، چالش‌های ذاتی و موانع حقوقی در تخصیص شخصیت حقوقی به سامانه هوش مصنوعی که ضرورت تمرکز بر مسئولیت اصیل را تقویت می‌کند (۱.۱.۲).

۱.۱.۱. توانایی اصیل به‌مثابه بهترین اجتناب‌کننده هزینه

این واقعیت انکارناپذیر که اصیل که غالباً یک کارفرما، شرکت تجاری یا سازمان است، معمولاً در موقعیت به‌مراتب بهتری برای جبران آسیب وارده به اشخاص ثالث بزه‌دیده قرار دارد (ژوردن، ۱۳۹۴، ص. ۱۴۶)، یکی از عمل‌گرایانه‌ترین مبانی سیاستی توجیه‌گر دکترین مسئولیت نیابتی است که در رویه قضایی کاملاً مورد شناسایی و تأکید قرار گرفته است. دادگاه‌های کاملاً تصریح

کرده‌اند که هدف سیاستی زیربنایی مسئولیت نیابتی، حصول اطمینان از این موضوع است که مسئولیت نهایی تا حد امکان «منصفانه، عادلانه و معقول» بر عهده شخصی قرار گیرد که واجد وسیله جبران خسارت قربانی باشد (Various Claimants v. Catholic Child Welfare Society, 2012, para. 34).^۱ این توانمندی برتر اصیل، ریشه در عوامل متعددی دارد. سازمان‌ها و شرکت‌های تجاری از دارایی‌های ثابت، سرمایه در گردش، جریان‌های درآمدی مستمر و دسترسی به بازارهای سرمایه برخوردارند و این بنیه مالی که گاه در ادبیات حقوقی از آن با عنوان «جیب عمیق»^۲ کارفرما یاد می‌شود (Petrin & Witting, 2023, p. 291)، به آن‌ها امکان می‌دهد تا آسیب‌های مالی ناشی از فعالیت‌های خود یا کارکنانشان را حتی در مقیاس وسیع، جذب و جبران کنند.

نهادها و شرکت‌هایی که در خط مقدم تجاری‌سازی و بهره‌برداری از سامانه‌های هوشمند قرار دارند، اعم از غول‌های فناوری یا کسب‌وکارهای بهره‌بردار، همان بازیگرانی هستند که ضمن انتفاع از مزایای اقتصادی هوش مصنوعی، ریسک‌های مرتبط با آن را نیز به جامعه می‌آورند (Taplin, 2022, p. 6). این نهادها به واسطه ساختار سازمانی و منابع مالی خود، در بهترین موقعیت برای پیش‌بینی، مدیریت و درنهایت، پوشش مالی این ریسک‌ها قرار دارند. تحمیل مسئولیت نهایی بر دوش آن‌ها تضمین می‌کند که بزه‌دیدگان ناشی از هوش مصنوعی، از یک مسیر عملی و مؤثر برای احقاق حق برخوردار خواهند بود (Dremluiga et al, 2019, p. 111) و با یک عامل فاقد توانایی مالی یا زنجیره پیچیده علیت مواجه نخواهند شد. به بیان دیگر، این رویکرد موجب درونی‌سازی^۳ هزینه‌های ناشی از حوادث و خطاهای عملیاتی به‌عنوان جزئی از هزینه‌های متعارف آن فعالیت خاص در محاسبات اقتصادی شرکت می‌شود.

علاوه بر درونی‌سازی هزینه، رویکرد تحمیل مسئولیت بر اصیل، با دیگر معیارهای اقتصادی شناخت مسئولیت نیز همخوانی دارد. برای مثال، مبتنی بر «اصل ارزان‌ترین اجتناب‌کننده هزینه»^۴ شخصی باید مسئول شناخته شود که می‌تواند از خسارت با کمترین هزینه جلوگیری کند یا آن را

۱. از این پس: CCWS

2. Deep Pocket

3. Internalization

4. Best Cost Avoider

کاهش دهد؛ به شرطی که هزینه اجتناب یا کاهش خسارت کمتر از سود باشد. در مورد سیستم‌های هوش مصنوعی، غالباً این تولیدکننده یا به‌کارگیرنده اصلی است که در موقعیتی مناسب‌تر برای تعیین و بهبود ویژگی‌های ایمنی سیستم قرار دارد و به لحاظ اقتصادی می‌تواند ارزان‌ترین اجتناب‌کننده باشد (حکمت‌نیا و همکاران، ۱۳۹۸، ص. ۲۵۰). از منظر مبانی حقوق ایران نیز می‌توان مسئولیت شرکت در قبال زیان‌های ناشی از به‌کارگیری هوش مصنوعی را در راستای «اصل احترام» ارزیابی کرد. این اصل به‌عنوان مبانی فقهی با پشتوانه استدلالی قوی اقتضا دارد که حقوق اشخاص و جامعه محترم شمرده و هرگونه ضرر و زیان وارد جبران شود (حسینی و همکاران، ۱۴۰۳، ص. ۵۰). براین اساس، تحمیل مسئولیت بر «اصیل» (به‌کارگیرنده هوش مصنوعی) که از فناوری منتفع شده، ریسک‌های آن را ایجاد کرده است و توانایی مدیریت و پوشش این ریسک‌ها را دارد، علاوه بر عدالت و انصاف با جوهره «اصل احترام» در فقه نیز همسویی دارد و در راستای محترم شمردن حقوق بزه‌دیدگان است.

مآلاً قرار دادن مسئولیت بر عهده نهاد به‌کارگیرنده یا توسعه‌دهنده هوش مصنوعی به دلیل توانایی برتر آن در جبران خسارت و مدیریت ریسک (دیلیمی و دیگران، ۱۳۹۹، ص. ۷۱)، در انطباق کامل با معیار «منصفانه، عادلانه و معقول» بودن که توسط دیوان عالی در پرونده CCWS تبیین شد، قرار می‌گیرد. این رهیافت، منصفانه است؛ زیرا مسئولیت را بر دوش نهادی می‌نهد که از فناوری سود می‌برد و توانایی مدیریت ریسک آن را داراست؛ ضمن آنکه امکان جبران خسارت را برای بزه‌دیده فراهم می‌کند. عادلانه است؛ زیرا به تحقق عدالت جبرانی^۱ و عدالت توزیعی^{۲ و ۳} یاری می‌رساند و معقول و کارآمد است؛ زیرا راه‌حلی عملی برای مسئله خلأ مسئولیت ارائه می‌دهد و هم‌زمان، انگیزه‌های اقتصادی لازم برای سرمایه‌گذاری در ایمنی و کاهش ریسک را

1. Corrective Justice

2. Distributive Justice

۳. فعالیت‌های اقتصادی ذاتاً با ریسک همراه‌اند و عدالت توزیعی به این می‌پردازد که ریسک‌های ناشی از این فعالیت‌ها چگونه باید در جامعه توزیع شود. از طرف دیگر، مسئولیت نیابتی، ریسک مالی ناشی از خطای عامل در حین کار را به اصیل منتقل می‌کند و توجیه این انتقال ریسک، بر پایه ملاحظات اصل منفعت (Benefit Principle) و انصاف (Fairness) استوار است که در قلب عدالت توزیعی قرار دارد. برای مطالعه بیشتر به مهم‌ترین اثر در این حوزه یعنی منبع زیر رجوع شود. رالز، جان (۱۴۰۳). نظریه‌ای در باب عدالت (مرتضی نوری، مترجم). نشر مرکز (اثر اصلی در سال ۱۹۷۱ منتشر شده است).

ایجاد (Diamantis, 2023, p. 320) و بدین ترتیب، به هدف مهم بازدارندگی نیز به‌طور غیرمستقیم کمک می‌کند.

۱.۱.۲. شخصیت حقوقی هوش مصنوعی و ضرورت تمرکز بر مسئولیت اصیل

درحالی‌که تحلیل پیشین ظرفیت برتر «اصیل» (به‌کارگیرنده) در جبران خسارت را از منظر اقتصادی مدلل ساخت، رویکرد علمی اقتضای این را دارد که وضعیت حقوقی بازیگر دیگر این معادله یعنی سامانه هوشمند نیز بررسی شود. این بررسی به طرح این پرسش می‌انجامد که آیا اعطای شخصیت حقوقی به هوش مصنوعی می‌تواند راهکاری جایگزین و مطلوب برای تخصیص مسئولیت باشد؟ این ایده که در پی رخدادهایی نظیر اعطای شهروندی به ربات سوئیا و پیشنهادهای اولیه پارلمان اروپا برای ایجاد «شخصیت الکترونیک» مورد توجه قرار گرفت (Pagallo, 2018, pp. 3-4; Szentgali-Toth, 2021, p. 102)، به‌رغم جذابیت اولیه، به دلیل ناکارآمدی عملی و موانع مفهومی، درنهایت، مورد پذیرش نظام‌های حقوقی قرار نگرفت (Dremluiga et al, 2019, p. 108). حتی اقداماتی مانند اعطای شهروندی به سوئیا، بیش از آنکه مبتنی بر تحلیل حقوقی عمیق باشد، پرآمده از ملاحظات سیاسی و راهبردهای بازاریابی بود (Szentgáli-Tóth, 2021, p. 106).

مهم‌ترین مانع در این مسیر، بی‌اثر بودن تحمیل مسئولیت مستقیم بر عامل غیرانسانی است که فاقد دارایی و توانایی واقعی برای پاسخ‌گویی است. در نقطه مقابل، «اصیل» که غالباً یک شرکت تجاری یا سازمان است، توانایی جبران خسارت بزه‌دیده را دارد؛ وضعیتی که حتی در مقایسه با کارکنان انسانی نیز صادق است، زیرا آن‌ها نیز به‌ندرت از دارایی شخصی کافی برای جبران خسارات سنگین برخوردارند (Oliphant & Wagner, 2012, pp. 26-27) و این ناتوانی در مورد سامانه‌های هوش مصنوعی که ذاتاً فاقد هرگونه دارایی مستقل هستند، بارزتر است. افزون‌بر موانع عملی، اعطای شخصیت حقوقی به هوش مصنوعی با این پرسش اساسی روبه‌روست که چه منفعتی برای جامعه به همراه خواهد داشت؟ برای مثال، شناسایی شخصیت حقوقی برای شرکت‌ها، منافع اقتصادی واضحی مانند افزایش کارایی، شفافیت مالی و تسهیل پاسخ‌گویی را به دنبال داشته است (Dremluiga et al, 2019, p. 111) درحالی‌که چنین مزایای ملموسی برای اعطای شخصیت به هوش مصنوعی متصور نیست و شاید به همین دلیل هم تلاش‌های بین‌المللی در این زمینه با

مقاومت جدی مواجه شده است؛ چنان‌که هم اتحادیه اروپا و هم ایالات متحده، با این ایده مخالفتی صریح دارند (Dremluiga et al, 2019, p. 108) و نهادهای تخصصی مانند سازمان جهانی مالکیت فکری^۱ نیز اقداماتی را در جهت ممانعت از شناسایی حقوق مالکیت فکری برای هوش مصنوعی اتخاذ کرده‌اند^۲ (Chakrabarty & Baral, 2023, p. 3).

این مسئله در نظام حقوقی ایران و مبانی فقهی آن، به نحو بهتری درک می‌شود؛ چراکه هوش مصنوعی نه در قالب «شخص حقیقی» می‌گنجد؛ زیرا فاقد عناصر اساسی انسان بودن نظیر حیات، اراده و اهلیت است (ولی‌پور و اسماعیلی، ۱۴۰۰، صص. ۴-۵) و نه می‌توان آن را «شخص حقوقی» به شمار آورد. اشخاص حقوقی، هویتی اعتباری هستند که به اراده قانون‌گذار و افراد انسانی ایجاد می‌شوند درحالی‌که هوش مصنوعی فاقد چنین مبانی تأسیسی و ارادی است (ولی‌پور و اسماعیلی، ۱۴۰۰، صص. ۴-۵). درنتیجه، عدم امکان شناسایی هوش مصنوعی به‌عنوان شخص، هرگونه تلاش برای مسئول دانستن مستقیم آن را در حقوق ایران با مانع مواجه می‌سازد (حسینی و همکاران، ۱۴۰۳، ص. ۵۰).

بنابراین، می‌توان گفت ایده اعطای شخصیت حقوقی به هوش مصنوعی، راهکاری کارآمد و مطلوب برای رفع خلأ مسئولیت نیست و شاید تنها در آینده‌ای دور، پیشرفته‌ترین ربات‌های کاملاً خودمختار بتوانند کاندیدای کسب نوعی شخصیت حقوقی باشند، اما چنین چشم‌اندازی در حال حاضر موضوعیت ندارد (Szentgali-Toth, 2021, p. 113). براین اساس، منطقی‌ترین و عملی‌ترین راهکار، تمرکز بر مسئولیت‌پذیر ساختن اشخاص و نهادهای انسانی کنترل‌کننده این فناوری یعنی کاربران، مالکان و تولیدکنندگان آن است (Chakrabarty & Baral, 2023, p. 3). براین اساس، به‌جای خلق مفهومی حقوقی ساختگی و ناکارآمد، باید مسئولیت را به همان قانونی منتسب کرد که

1. WIPO

۲. در پرونده‌های قضایی بین‌المللی معروف به «دابوس» (DABUS)، تلاش شد تا یک سیستم هوش مصنوعی به‌عنوان مخترع دو اختراع ثبت شود، ولی نظام‌های حقوقی ازجمله در بریتانیا، ایالات متحده و دفتر ثبت اختراع اروپا (EPO)، با این استدلال که ماشین فاقد شخصیت حقوقی لازم برای این عنوان است، این درخواست را رد کردند. برای مطالعه به دو لینک زیر مراجعه شود. لینک دوم مربوط به دادگاه بریتانیا است.

<https://www.reuters.com/legal/litigation/us-appeals-court-says-artificial-intelligence-cant-be-patent-inventor-2022-08-05/>
<https://www.supremecourt.uk/cases/uksc-2021-0201>

از این فناوری منتفع شده، ریسک‌های آن را به جامعه تحمیل کرده است و در نهایت، کنترل راهبردی بر آن را در اختیار دارد.

۱.۲. فعالیت هوش مصنوعی به منابه بخش جدایی‌ناپذیر از فعالیت اصیل و لزوم درونی‌سازی هزینه‌های جرم

یکی از مبانی دوگانه‌ای که توجیه نظری تحمیل مسئولیت نیابتی بر اصیل را فراهم می‌آورد، حول دو محور شکل گرفته است. نخست، ادغام ماهوی و کارکردی فعالیت عامل در ساختار فعالیت اقتصادی اصیل و دوم، ایجاد یا تشدید ریسک توسط اصیل به واسطه همین فعالیت‌ها. بدین معنا که انتساب عمل زیان‌بار عامل به اصیل از منظر مسئولیت نیابتی، منوط به احراز این شرط است که عمل مذکور در جریان فعالیتی ارتکاب یافته باشد که بتوان آن را به‌عنوان جزئی لاینفک و ذاتی^۱ از مجموعه فعالیت‌های تجاری اصیل تلقی کرد. این اصل در چهارچوب روابط استخدامی سنتی، مصداق بارزی می‌یابد؛ زیرا وظایف محوله به مستخدم (کارگر یا کارمند)، ماهیتاً در راستای تحقق اهداف کارفرما تعریف شده است و عمل وی از منظر کارکردی، امتداد و تجلی فعالیت کارفرما محسوب می‌شود (دیلیمی و همکاران، ۱۳۹۹، ص. ۷۱؛ زوردن، ۱۳۹۴، ص. ۱۴۵).

استقرار و به‌کارگیری سامانه‌های هوش مصنوعی مصداق بارز منطق «ادغام در فعالیت تجاری»^۲ است؛ زیرا هوش مصنوعی در پارادایم کنونی به مؤلفه‌ای محوری در هسته عملیات تجاری مدرن مبدل شده است. سازمان‌ها، سامانه‌های هوشمند را نه برای امور حاشیه‌ای، بلکه دقیقاً به‌منظور اجرای وظایف مهم یا ارتقای کیفی فرایندهای ارزش‌آفرین خود به خدمت می‌گمارند^۳. تحلیل کلان‌داده‌ها جهت شخصی‌سازی پویا در استراتژی‌های بازاریابی شخصی‌سازی شده (Ebers & Gamito, 2021, p. 2)، اتوماسیون فرایندهای تولید به‌منظور افزایش بهره‌وری، ارائه خدمات مالی خودکار^۴ و استفاده از هوش مصنوعی در فرایندهای حساس مدیریتی

1. Integral

2. Integration into Business Activity

۳. برای مثال، می‌توان به استفاده پلیس از هوش مصنوعی یا استفاده دادگاه‌های آمریکایی از هوش مصنوعی اشاره کرد. برای مطالعه در خصوص چالش‌های استفاده پلیس از هوش مصنوعی به منبع زیر رجوع شود.

Berk, R. A. (2021). Artificial intelligence, predictive policing, and risk assessment for law enforcement. *Annual Review of Criminology*, 4(1), 209-237.

4. Robo-Advisors

و منابع انسانی، همگی مؤید این ادغام عمیق هستند. این سطح از یکپارچگی عملکردی به‌خصوص با در نظر گرفتن ریسک‌های ذاتی مترتب بر پردازش کلان‌داده‌ها نظیر نقض حریم خصوصی یا بروز تبعیضات الگوریتمی (Ebers & Gamito, 2021, p. 3)، نشان می‌دهد که فعل مجرمانه سامانه هوشمند در اثنای اجرای این وظایف، امری منفک از فعالیت کلی اصیل نبوده، بلکه به‌مثابه امتداد فناورانه آن قابل ارزیابی است.

این پیوند ذاتی میان فعالیت هوشمند و عملیات تجاری، مستقیماً به سنگ بنای دوم مسئولیت یعنی نظریه «خلق ریسک»^۱ پیوند می‌خورد. منطق حقوقی حکم می‌کند شخصی که برای کسب سود، فعالیت اقتصادی پرخطری را وارد جامعه می‌کند، باید مسئولیت تحقق آن خطرات را نیز بر عهده بگیرد (Brodie, 2010, p. 61). رویه قضایی نیز بر این منطق صحه گذارده است؛ چنان‌که در پرونده اسکاندیناویسکا^۲ و^۳ دادگاه تصریح کرد که تحمیل مسئولیت بر شخصی که «شرکت اقتصادی پرخطری را وارد جامعه می‌کند»، در زمان تجلی آن خطرات، امری عادلانه محسوب می‌شود و علاوه بر تأمین هدف جبران خسارت مؤثر، کارکرد بازدارندگی و ترغیب به اتخاذ تدابیر پیشگیرانه را نیز ایفا می‌کند (Giliker, 2022, p. 125). این استدلال به‌نحو انکارناپذیری بر به‌کارگیری سامانه‌های هوش مصنوعی قابل انطباق است. تصمیم یک بنگاه برای به‌کارگیری هوش مصنوعی به‌منزله ایجاد آگاهانه عدم قطعیت و ریسک است که از ویژگی‌های ماهوی این فناوری نشئت می‌گیرد (Nikolinakos, 2023, p. 699). پدیده جعبه سیاه به‌مثابه یکی از ویژگی‌های ذاتی هوش مصنوعی با ایجاد گسست در زنجیره علیت قابل پیش‌بینی، فهم چرایی تصمیم مخرب را حتی برای خالقان سیستم نیز ناممکن می‌سازد و مفهوم پیش‌بینی‌پذیری را به چالش می‌کشد (تخشید، ۱۴۰۰، ص. ۲۳۸) و منجر به ریسک‌هایی می‌شود که اعم از رفتارهای غیرقابل پیش‌بینی در شرایط نامتعارف، سوگیری‌های نظام‌مند ناشی از داده‌ها در استخدام هوشمند به‌وسیله هوش مصنوعی (Szapiro & Kacprzyk, 2022, p. 160) یا آسیب‌پذیری‌های امنیتی هستند. درنتیجه، اصیل با انتخاب استقرار این فناوری، این مجموعه از ریسک‌ها را آگاهانه به حوزه فعالیت خود و متعاقباً به جامعه تحمیل می‌کند.

1. Risk Creation

2. Skandinaviska

3. Skandinaviska Enskilda Banken AB v Asia Pacific Breweries (S) Pte Ltd, 2011.

براین اساس، تلاقی این دو مبنا استدلال حقوقی متقنی را صورت‌بندی می‌کند و آن اینکه، هنگامی که خسارتی از دل ریسک‌های ذاتی سیستمی هوشمند سر برمی‌آورد، مسئولیت نیابتی اصیل به دلیل ادغام ماهوی آن سیستم در فعالیت تجاری‌اش و هم به دلیل نقش آن به عنوان خالق آن ریسک، امری موجه است و تضمین می‌کند که هزینه‌های اجتماعی ناشی از این فناوری، بر عهده همان بازیگرانی قرار گیرد که از مزایای آن منتفع شده و به صورت هم‌زمان، توانایی و مسئولیت مدیریت ریسک‌های آن را به عنوان جزئی جدایی‌ناپذیر از فعالیت اقتصادی خود پذیرفته‌اند.

۲. مبانی عملیاتی و کنترلی در توجیه مسئولیت نیابتی هوش مصنوعی

فراتر از منطق اقتصادی تخصیص ریسک، معماری حقوقی مسئولیت نیابتی برای هوش مصنوعی بر دو بُعد مکمل و درهم‌تنیده تمرکز دارد که اقتدار حاکمیتی اصیل را آشکار می‌سازد. نخست، جایگاه کارکردی هوش مصنوعی به مثابه ابزاری که در خدمت اهداف و منافع غایی اصیل قرار دارد (۲.۱) و دوم، اثبات کنترل مؤثر اصیل بر چهارچوب کلان فعالیت سامانه حتی در صورت وجود خودمختاری عملیاتی (۲.۲). تبیین این دو مؤلفه، پیوند ناگسستنی میان اراده راهبردی اصیل و عملکرد عامل هوشمند را آشکار می‌سازد و مبنای حقوقی انتساب مسئولیت را مستحکم می‌کند.

۲.۱. تبعیت ابزاری هوش مصنوعی از اهداف اصیل

یکی از مبانی دکتترین مسئولیت نیابتی که در رویه قضایی نیز مورد توجه قرار گرفته^۱، بر این گزاره استوار است که فعل زیان‌بار باید در جریان فعالیتی ارتکاب یابد که عامل «از طرف»^۲ و در جهت «منافع» اصیل انجام می‌دهد. این اصل، مسئولیت را به ریسک‌های ذاتی و ملازم فعالیت اقتصادی سازمان‌یافته پیوند می‌زند. بدین معنا که اصیل باید پاسخ‌گوی آسیب‌هایی باشد که در مسیر تحقق اهداف سازمانش حادث می‌شوند؛ همچنان‌که این منطق به سهولت در روابط استخدامی سنتی قابل مشاهده است؛ فعالیت‌های کارمند، تجلی کارکردی بنگاه کارفرما در جهان خارج است و چنانچه

۱. ازجمله به‌طور ضمنی در تحلیل‌های پرونده CCWS.

2. on behalf of

در اثنای انجام دادن وظایف خود مرتکب خطایی شود، تبعات آن منطقاً بر عهده همان نهادی قرار می‌گیرد که از آن فعالیت منتفع شده و ریسک‌های آن را ایجاد کرده است (دیلمی و دیگران، ۱۳۹۹، ص. ۷۱).

این پیوند غایی میان فعل زیان‌بار و منافع اصیل به‌سادگی در خصوص هوش مصنوعی تحقق می‌یابد؛ زیرا یک سامانه هوشمند، فارغ از درجه خودمختاری عملیاتی‌اش^۱، ذاتاً ابزاری است که برای تحقق اهداف معین نهاد پشتیبان (اصیل) طراحی، آموزش داده و به کار گرفته می‌شود. بنابراین، کنش‌های آن حتی پیچیده‌ترین و غیرشفاف‌ترین آن‌ها، همواره در چهارچوب حاکمیتی و راهبردی همان اهداف قابل تفسیر است. هوش مصنوعی به نیابت از اصیل عمل می‌کند و خطاهای آن صرفاً یک «نقص فنی»^۲ یا رویداد پیش‌بینی‌ناپذیر نیست، بلکه اغلب، پیامد منطقی و درعین‌حال، ناخواسته بهینه‌سازی برای همان اهدافی است که برایش تعریف شده است. برای مثال، یک الگوریتم توصیه‌گر که برای بهینه‌سازی تعامل کاربر و درآمدزایی طراحی شده، ممکن است با ترویج افراط‌گرایی یا توزیع اطلاعات نادرست، به این هدف دست یابد (Soni et al, 2024, p. 99). یا یک خودروی خودران^۳ که هدف آن انتقال ایمن و کارآمد است (Krömker, 2022, p. 420)، ممکن است در سناریویی بغرنج با اتخاذ تصمیمی که پارامترهای ایمنی و کارایی را به شکلی نامطلوب موازنه می‌کند، موجب بروز صدمه جانی شود (برزگر و الهام، ۱۳۹۹، ص. ۲۰۸). در هر دو مورد، فعل زیان‌بار، فعلیت یافتن یکی از ریسک‌های ذاتی است که اصیل با تصمیم به استفاده از این ابزار فناورانه برای آن هدف خاص، آگاهانه آن را پذیرفته و در چرخه فعالیت خود ادغام کرده است.

در این تحلیل، خودمختاری عملیاتی هوش مصنوعی نافی این پیوند بنیادین نیست. تصمیمات سیستم هوشمند بدون مداخله آنی انسان اتخاذ می‌شوند، اما همچنان محصول مستقیم محدودیت‌ها، داده‌های آموزشی و اهداف کلانی هستند که توسط اصیل یا به سفارش اصیل، تعریف و مهندسی

1. Operational Autonomy

2. Technical Glitch

۳. بخش هشتم قانون ایالت نوادا خودروی خودران را چنین تعریف می‌کند که «وسیله نقلیه موتوری است که از هوش

مصنوعی، سنسورها و سیستم موقعیت‌یاب جهانی برای راندن خودش بدون مداخله اپراتور انسانی استفاده می‌کند» (Bill

8 AB511 Nevada Legislature, section 8).

شده‌اند (Szentgali-Toth, 2021, p. 104). در واقع، خودمختاری صرفاً به «چگونگی» اجرای وظیفه مربوط است حال آنکه «چرایی» و هدف نهایی آن همچنان در ید قدرت اصیل باقی می‌ماند. از این رو با عنایت به اینکه فعل مجرمانه هوش مصنوعی در مسیر تحقق منافع اصیل و به نیابت از او رخ می‌دهد، اعمال مسئولیت نیابتی بر وی، انطباق کامل با جوهره این دکتربین حقوقی دارد.

۲.۲. کنترل راهبردی و عملیاتی اصیل بر فعالیت سامانه هوشمند

معیار سنتی توجیه‌کننده مسئولیت نیابتی، مفهوم «کنترل»^۱ اصیل بر عامل در زمان ارتکاب فعل مجرمانه است. این معیار در مواجهه با سیستم‌های هوشمند با ویژگی‌های خاص آن از جمله پیچیدگی‌های فنی، دینامیسم تکاملی و سرعت تحولات (غمامی و هاشمی، ۱۴۰۴، صص. ۵-۶)، با چالش روبه‌رو می‌شود، اما این چالش با ارجاع به تحولات خود دکتربین حقوقی، پاسخی درخور می‌یابد. درک معیار کنترل در حقوق مدرن با توجه به تحولات بازار کار و پیچیدگی وظایف دستخوش تحول شده و رأی دیوان عالی در پرونده CCWS به مثابه یک نقطه عطف نظری، این گذار را صورت‌بندی کرده است (CCWS, 2012, para. 36). در این پارادایم نوین، «کنترل» دیگر به معنای توانایی دیکته کردن جزئیات اجرایی وظایف، آن گونه که در دوران «ارباب و خدمت‌کار»^۲ متصور بود، نیست، بلکه هسته کنترل در قدرت و اختیار راهبردی اصیل برای تعیین ماهیت و غایت فعالیت عامل یعنی تعریف وظایف، اهداف و قلمرو کلی عملکرد در راستای منافع بنگاه نهفته است و این گونه شرط مسئولیت از «مدیریت خرد روش» جدا می‌شود و به «حاکمیت کلان بر فعالیت» پیوند می‌خورد.

این بازتعریف مفهومی دارای منطق سیاستی قابل توجهی نیز است و آن اینکه، هنگامی که اصیل، عاملی را در ساختار سازمانی خود ادغام و فعالیت او را در جهت اهداف خود هدایت می‌کند، آن فعالیت را به بخشی از قلمرو مسئولیت خویش بدل می‌سازد. در این شرایط، حتی اگر کنترل کامل بر کنش‌های عامل در عمل ناممکن باشد، از منظر سیاست‌گذاری تحمیل مسئولیت نیابتی تضمین می‌کند که بنگاه‌ها با هزینه‌های کامل مورد انتظار ناشی از صدمات مواجه و در نتیجه،

1. Control

2. Master-Servant

از پذیرش ریسک‌های بیش از حد بازداشته شوند (Petrin & Witting, 2023, p. 291). حال پرسش اساسی این است که آیا مفهوم مدرن «کنترل بر فعالیت»، آن‌گونه که در رویه قضایی مسئولیت نیابتی و مشخصاً رأی CCWS تبیین شد، می‌تواند بر رابطه میان اصیل (به‌کارگیرنده یا توسعه‌دهنده) و سامانه‌های هوشمند نیز اعمال شود؟ پاسخ با در نظر گرفتن ابعاد چندگانه این رابطه، مثبت به نظر می‌رسد. این کنترل ممکن است متفاوت از نظارت مستقیم بر کارمند انسانی باشد، اما در لایه‌های مختلفی قابل شناسایی و از منظر حقوقی معنادار است. نخستین و شاید مهم‌ترین جنبه، کنترل بر تعریف هدف و وظیفه سامانه هوشمند است و در این راستا، این اصیل است که تصمیم می‌گیرد هوش مصنوعی برای چه مقصودی به کار گرفته شود، چه مشکلی را حل کند و در چه چهارچوبی فعالیت کند. این تعیین استراتژیک کارکرد و هدف، هسته اصلی کنترل اصیل بر فعالیت هوش مصنوعی را تشکیل می‌دهد و مسیر کلی عملکرد آن را مشخص می‌سازد. در کنار این، کنترل از طریق طراحی و پیکربندی اولیه نیز وجود دارد. اصیل، چه مستقیماً و چه با تعیین الزامات برای تیم توسعه، بر انتخاب الگوریتم‌ها، تعریف پارامترهای عملیاتی، تعیین محدودیت‌ها و قواعد رفتاری و پیاده‌سازی سازوکارهای ایمنی، نظارت و تأثیرگذاری قابل توجهی دارد و تصمیمات مراحل اولیه طراحی، شالوده و چهارچوب رفتار آتی سامانه را بنیان می‌نهد (Gero & Sudweeks, 2012, p. 136). سرانجام و شاید در مؤثرترین شکل کنترل، این سیطره به حوزه کنترل معرفت‌شناختی بر داده‌های آموزشی^۱ گسترش می‌یابد که در آن اصیل با انتخاب و مهندسی داده‌هایی که سیستم با آن‌ها جهان را می‌آموزد، به‌طور مستقیم جهان‌بینی و الگوهای تصمیم‌گیری آن را شکل می‌دهد (Azad & Nazari-Heris, 2024, p. 45). این لایه‌های کنترل، شبکه‌ای درهم‌تنیده از اقتدار را می‌سازند که از منظر حقوقی، بسیار معنادارتر از نظارت آنی و مستقیم است و مبنایی مستحکم برای انتساب مسئولیت نیابتی به اصیل فراهم می‌آورد.

این حاکمیت راهبردی اصیل از چهارچوب ایستا و اولیه طراحی فراتر می‌رود و در تمام چرخه حیات عملیاتی سامانه هوشمند در قالب نظارت مستمر، قابلیت به‌روزرسانی و بازآموزی^۲ سیستم

1. Control via Data

2. Control via Monitoring, Updating & Intervention

بر اساس بازخوردهای دریافتی به شکلی پویا استمرار می‌یابد (Charles Sr, 2025, pp. 214-215). مهم‌تر اینکه، این حاکمیت با توجه به اختیار نهایی اصیل برای مداخله، تحدید یا توقف کامل سامانه به اوج خود می‌رسد. این قدرت برای قطع کامل جریان و از کار انداختن سیستم (Cristiano et al, 2023, p. 173)، نافی هرگونه توهم استقلال مطلق و نبود کنترل است^۱. علاوه بر این، وابستگی وجودی سامانه به منابع محاسباتی، انرژی و مالی که کاملاً توسط اصیل تأمین و مدیریت می‌شود، لایه دیگری از این کنترل ساختاری و انکارناپذیر را به نمایش می‌گذارد. ممکن است در برابر این تحلیل، به خودمختاری عملیاتی^۲ و^۳ برخی سیستم‌های هوشمند استناد شود که به آن‌ها اجازه تصمیم‌گیری بدون دخالت آنی انسان را می‌دهد (Gatti, 2016, p. 142). این استدلال، اما خودمختاری عملیاتی در «روش» را با استقلال غایی در «هدف» یکسان می‌پندارد و از این منظر مغالطه می‌کند. همان‌گونه که در تفسیر مدرن مسئولیت نیابتی و رأی CCWS تبیین شد، کنترل حقوقی معنادار، ناظر بر هدایت کلان فعالیت است و نه لزوماً مدیریت خرد اجرای آن. بنابراین، خودمختاری هوش مصنوعی در نحوه رسیدن به هدف، ناقض کنترل اصیل بر تعیین خود هدف، چهارچوب عملکرد، محدودیت‌های عملیاتی و داده‌های ورودی نیست. این خودمختاری، خودمختاری محصور و هدایت‌شده‌ای است که در چهارچوب حاکمیتی عمل می‌کند که ابعاد آن از تعریف غایت تا مدیریت داده و نظارت پویا، کاملاً توسط اصیل مهندسی و مدیریت می‌شود.

این چهارچوب تحلیلی در انطباق کامل با «معیار قدرت و کنترل» که در ادبیات حقوقی مطرح است نیز قرار دارد؛ زیرا مطابق این معیار، مسئولیت باید بر عهده شخصی قرار گیرد که بیشترین

۱. تحلیلی که در اینجا ارائه شده است، دارای درون‌مایه‌های عمیق منطقی است و دقیقاً منطبق بر رویکردی عمل‌گرایانه است که با قانون‌گذاری کشورهای مختلف هم‌راستا است. برای مثال، ماده ۴ قانون هوش مصنوعی چین مصوب سال ۲۰۲۳ (Interim Measures for the Management of Generative AI Services) به‌صراحت ارائه‌دهنده سرویس را به‌عنوان نهاد مسئول محتوای تولیدشده با سیستم هوش مصنوعی‌اش معرفی می‌کند؛ همان‌طور که یک ناشر یا وب‌سایت مسئول محتوایی است که منتشر می‌کند. سایر مواد مانند مواد ۱۴ و ۱۵ نیز به اقدامات لازم در صورت کشف محتوای غیرقانونی و رسیدگی به شکایات کاربران می‌پردازند که مکمل این مسئولیت‌پذیری کلی است.

2. Functional Autonomy
3. Operational Autonomy

قدرت و کنترل را بر سیستم اعمال می‌کند (حکمت‌نیا و همکاران، ۱۳۹۸، صص. ۲۵۰-۲۵۱) و از آنجاکه اصل، همان‌طور که تشریح شد، از طریق مجموعه‌ای از کنترل‌های غایی، معماری شناختی، معرفت‌شناختی و نظارتی، حاکمیت مؤثری بر سامانه هوشمند دارد، انتساب مسئولیت به وی بر مبنای این معیار نیز کاملاً موجه است و در این راستا می‌توان اذعان داشت که قدرت تصمیم‌گیری در خصوص چرایی و چگونگی به‌کارگیری هوش مصنوعی و توانایی شکل‌دهی به چهارچوب عملکرد آن، مسئولیت متناظر را نیز به همراه دارد.

۳. تحلیل عناصر مسئولیت نیابتی در پرتوی هوش مصنوعی

بررسی‌های تطبیقی در نظام‌های حقوقی مختلف از جمله کشورهای عضو اتحادیه اروپا نشان می‌دهد که در جست‌وجوی مبنایی برای مسئولیت ناشی از هوش مصنوعی، اغلب چهارچوب‌های مسئولیت موجود از جمله مسئولیت ناشی از اشیاء، فعالیت‌های خطرناک، حیوانات و نیز مسئولیت نیابتی مورد توجه و تحلیل قرار می‌گیرند (ذاکری‌نیا، ۱۴۰۲، ص. ۱۴۳). نکته مهم اینکه فراتر از مبنای توجیهی، استقرار مسئولیت نیابتی منوط به احراز عناصر ماهوی دوگانه آن است. نخست، وجود رابطه حقوقی خاص میان اصیل و عامل مستقیم فعل مجرمانه و دوم، ارتکاب آن فعل «در جریان»^۱ یا به تعبیر فنی‌تر، در محدوده همان رابطه. در این قسمت برای بررسی این موضوع، ابتدا ظرفیت معیار انعطاف‌پذیر «شبیه به استخدام» (۳.۱) برای تبیین رابطه میان اصیل و عامل هوشمند ارزیابی و سپس معیار «ارتباط نزدیک» (۳.۲) به عنوان ضابطه سنجش پیوند میان فعل مجرمانه و آن رابطه معرفی و تشریح می‌شود.

۳.۱. عنصر رابطه از استخدام سنتی تا روابط «شبیه به استخدام» در عصر هوش مصنوعی

در طول عمر مسئولیت نیابتی در نظام کامن‌لا، پارادایم مسلط و تاریخی برای استقرار این نوع مسئولیت، همواره مبتنی بر رابطه کارفرمایی-کارگری^۲ بوده است. معیارهای نخستین جهت تشخیص و احراز این رابطه، در چهارچوب نظریه سنتی «ارباب و خدمت‌کار» صورت‌بندی شد که مبتنی بر عنصر کنترل مستقیم، جزئی و آمرانه ارباب بر شیوه اجرای تکالیف خدمت‌کار بود. مع هذا

1. In the Course of
2. Employer-Employee

با دگرگونی ساختاری در نظامات اقتصادی و اجتماعی از اواخر قرن ۱۷ به بعد و در پی انقلاب صنعتی، دگرگونی سنتی کنترل مستقیم کارآمدی عملیاتی خود را از دست داد و عدم انطباق ماهوی خود را با واقعیات حاکم بر بازار کار که متضمن ظهور نیروهای کار متخصص و برخوردار از استقلال عملکردی قابل توجه بود، آشکار ساخت (Giliker, 2022, p. 4). این تحولات منجر به پیدایش درک گسترده‌تر و انعطاف‌پذیرتری از رابطه استخدامی شد.

دگرگونی معاصر مسئولیت نیابتی با عبور از الزامات شکلی و صوری، دیگر بر احراز یک قرارداد استخدامی مدون یا قابلیت اعمال کنترل جزئی‌نگر بر روش‌های انجام کار استوار نیست (ژوردن، ۱۳۹۴، صص. ۱۴۸-۱۴۹). رویه قضایی در پرتوی رأی مهم دیوان عالی بریتانیا در پرونده CCWS، به سمت رویکرد ماهیت‌گرا و انعطاف‌پذیر حرکت کرده است. این رویکرد، قابلیت انتساب مسئولیت را در چهارچوب روابطی به رسمیت می‌شناسد که فاقد وصف حقوقی استخدام رسمی هستند، اما در جوهره خود، قرابت و شباهت قابل ملاحظه‌ای با آن دارند؛ روابطی که در ادبیات حقوقی تحت عنوان «شبیه به استخدام» مفهوم‌پردازی شده‌اند (Giliker, 2022, p. 128). دادگاه در رأی مذکور، با تحلیل پرونده فرعی GE (ناظر بر مسئولیت یک نهاد کلیسایی در قبال آزار جنسی ارتكابی توسط کشیش فاقد قرارداد استخدامی)^۱، تأکید کرد که برای احراز رابطه موجد مسئولیت، باید از عناوین ظاهری فراتر رفت و بر «ویژگی‌های حیاتی»^۲ آن رابطه تمرکز کرد (CCWS, 2012, para. 48) که مهم‌ترین آن، این است که آیا عامل از طرف اصیل منصوب شده تا به نیابت از او^۳ عمل کند یا خیر؟ این تحول مفهومی، پژوهش خود را در جدیدترین پیشنهادها حقوقی برای راهبری هوش مصنوعی نیز یافته است. تأکید پارلمان اروپا بر مسئولیت «پراتور» سیستم‌های پرخطر و عدم امکان فرار از مسئولیت با استناد به استقلال عملکرد سیستم (ذاکری‌نیا، ۱۴۰۲، ص. ۱۴۹)، نشان از هم‌گرایی جهانی به سمت شناسایی مسئول در جایگاه کنترل‌کننده و منتفع اصلی دارد.

این جابه‌جایی کانون مسئولیت از کاربر مستقیم به یک نهاد کنترل‌کننده در مواردی مانند

1. GE v The Trustees of the Portsmouth Roman Catholic Diocesan Trust [2012].

2. Crucial Features

3. on its behalf

خودروهای خودران، اهمیت بیشتری می‌یابد؛ زیرا در این سیستم‌ها، کاربر انسانی حتی در صورت حضور فیزیکی، غالباً در حکم مسافر تلقی و به دلیل عدم مشارکت فعال در کنترل وسیله، بحث تقصیر او منتفی می‌شود (مشهدی‌زاده و قلی‌نیا، ۱۴۰۱، صص. ۳۰۹-۳۱۰). این بازتعریف نقش‌ها که در آن سیستم خودران به «عامل» یا «ابزار» تحت کنترل راهبردی یک «اصیل» (سازنده یا ارائه‌دهنده خدمات مثلاً شرکت دارای تاکسی خودران) تبدیل می‌شود، زمینه را برای انطباق این رابطه با الگوی «شبیه به استخدام» به بهترین شکل فراهم می‌سازد. در تلاش برای توصیف این رابطه، ممکن است در نگاه نخست، نظریه کلاسیک نمایندگی به ذهن متبادر شود، اما این رویکرد با در نظر گرفتن استقلال عملکردی هوش مصنوعی، قابل پذیرش نیست؛ زیرا لازمه نمایندگی سنتی، انطباق کامل اراده نماینده با اراده و نفع اصیل است حال آنکه هوش مصنوعی پیشرفته ممکن است اهداف کلی (مانند بهینه‌سازی خود) را دنبال کند که لزوماً منطبق بر نفع مستقیم و آنی کاربر نیست (ولی‌پور و اسماعیلی، ۱۴۰۰، ص. ۵) و این استقلال نسبی در عملکرد، انطباق کامل با مفهوم سنتی نمایندگی را دشوار می‌سازد.

چهارچوب «رابطه شبیه به استخدام» که بر ماهیت و کارکرد تمرکز دارد، برای تحلیل رابطه اصیل و هوش مصنوعی از نظر حقوقی و منطقی مناسب و مدلل است؛ زیرا سیستم‌های هوش مصنوعی فراتر از صرف ابزار بودن، به گونه‌ای در عملیات نهادها ادغام می‌شوند که وظایف محوله را به نیابت و در جهت تحقق اهداف سازمانی اصیل به انجام می‌رسانند؛ خواه این وظیفه جایگزینی یک راننده انسانی باشد یا ایفای نقش مدیر گزینش یا حتی مشاور. این انتصاب کارکردی که از طریق طراحی، برنامه‌ریزی و استقرار سیستم صورت می‌گیرد، جوهره اصلی معیار «منسوب و مجاز شدن برای عمل از طرف اصیل» را که در رویه قضایی برای روابط شبیه به استخدام تبیین شده است، به‌طور کامل منعکس می‌کند و اولین شرط لازم برای استقرار مسئولیت نیابتی را فراهم می‌آورد.

در پرتوی این تحلیل، امتناع از شناسایی وضعیت «شبیه به استخدام» برای هوش مصنوعی صرفاً به دلیل ماهیت غیرانسانی آن، عقب‌گرد نظری محسوب می‌شود و می‌تواند منجر به ایجاد خلأ مسئولیت و تضعیف اهداف حقوقی که از جمله آن جبران خسارت و بازدارندگی است (شیری، ۱۳۹۶، صص. ۷۳-۷۴)، شود. افزون‌براین، انطباق رابطه اصیل و هوش مصنوعی با الگوی «شبیه به استخدام» از طریق تحلیل هم‌زمان دو مؤلفه «کنترل» و «انتفاع» که در کانون منطق حقوقی

مسئولیت نیابتی قرار دارند نیز قابل توجه است؛ همان‌طور که پیش‌تر تشریح شد (در قسمت‌های ۱.۲ و ۲.۲)، اصیل از طریق تعیین اهداف، پیکربندی معماری سیستم، مدیریت داده‌های آموزشی و تعریف محدودیت‌های عملیاتی، یک کنترل هنجاری و راهبردی بر رفتار سیستم اعمال می‌کند و از سوی دیگر، اصیل به‌طور مستقیم از کارایی، بهره‌وری و قابلیت‌های ناشی از به‌کارگیری همان سیستم منتفع می‌شود. این دوگانگی کنترل و انتفاع، حتی در تعاریف فنی نیز بازتاب یافته است. برای مثال، سازمان بین‌المللی استانداردسازی^۱، ربات را «مکانیسم فعال‌شده»^۲ و «قابل برنامه‌ریزی» توصیف می‌کند که برای «وظایف مورد نظر» به کار گرفته می‌شود (Simmler & Markwalder, 2019, p. 5). قید «فعال‌شده» به قدرت اصیل در ایجاد و استمرار فعالیت اشاره دارد و عبارت «قابل برنامه‌ریزی برای وظایف مورد نظر»، بیان‌کننده کنترل او بر غایت و کارکرد سیستم است و این هم‌زمانی کنترل بر منشأ ریسک و انتفاع از فعالیت، جوهره اصلی مسئولیت نیابتی را به‌طور کامل محقق می‌سازد. بنابراین، با اتکا به ویژگی‌های پیش‌گفته، می‌توان اولین شرط ماهوی برای استقرار مسئولیت نیابتی را احراز شده تلقی کرد.

۲.۳. عنصر ارتباط فعل مجرمانه هوش مصنوعی بر اساس معیار «ارتباط نزدیک»

پس از احراز وجود یک رابطه موجد مسئولیت، گام دوم در تحلیل مسئولیت نیابتی، ارزیابی پیوند میان فعل زیان‌بار عامل و آن رابطه است. این عنصر که به‌طور سنتی تحت عنوان ارتکاب فعل «در جریان» رابطه شناخته می‌شود، قلمرو مسئولیت اصیل را مشخص می‌کند و به دلیل پیچیدگی‌های تعاملات مدرن، همواره محل چالش‌های تفسیری بوده است (ژوردن، ۱۳۹۴، ص. ۱۵۱)؛ چنان‌که تبارشناسی این عنصر، یک جست‌وجوی طولانی برای گذار از معیارهای صلب و ناکارآمد به سمت ضابطه‌ای منعطف و کارآمد را نشان می‌دهد. در رویه قضایی، رویکردهای اولیه که مسئولیت را به دستور مستقیم اصیل برای ارتکاب فعل محدود می‌کردند، به سرعت جای خود را به معیار کلاسیک «سالموند»^۳ دادند. معیار سالموند^۴، مسئولیت را به افعال مجاز یا شیوه‌های غیرمجاز برای

1. ISO

2. Actuated Mechanism

3. Salmond

۴. «معیار سالموند» (Salmond Test) برای اولین بار توسط حقوق‌دانی به نام جان ویلیام سالموند (John William

Salmond) در کتاب زیر مطرح شد.

انجام دادن فعل مجاز محدود می‌کرد، اما در مواجهه با تخلفات عمدی کارکنان که ظاهراً خارج از چهارچوب وظایف شغلی بودند، با دشواری‌های جدی روبه‌رو بود و به نتایج غیرمنصفانه می‌انجامید (Giliker, 2022, pp. 9-11).

در مواجهه با این ناکارآمدی ضوابط سنتی، نظام‌های حقوقی کامن‌لا به تدریج به سوی پذیرش معیار انعطاف‌پذیر و سیاست‌محور برای احراز مسئولیت نیابتی حرکت کردند که تحت عنوان «آزمون ارتباط نزدیک»^۱ شناخته شد. دیوان عالی بریتانیا در رأی CCWS، این معیار را چنین تبیین می‌کند که آیا فعل زیان‌بار عامل «آن‌قدر با اعمالی که او مجاز به انجامشان بوده است، ارتباط نزدیک دارد که ممکن است آن فعل، به‌طور منصفانه و مناسب^۲ در جریان عادی آن رابطه تلقی شود؟» (Giliker, 2022, pp. 8-9, 126; Campbell & Lindsay, 2024, p. 191). براین اساس، تحلیل معاصر فراتر از جست‌وجوی مجوز صریح از سوی اصیل است و مبتنی بر شناسایی پیوند ماهوی و کیفی میان فعل زیان‌بار و ماهیت رابطه است؛ پیوندی که انتساب مسئولیت به اصیل را از منظر عدالت توزیعی و سیاست‌گذاری حقوقی موجه سازد و محاکم برای احراز آن، به بررسی عواملی چون فرصت^۳ ایجادشده توسط رابطه، ارتباط فعل با وظایف^۴ محوله و تحقق ریسک‌های ذاتی^۵ آن فعالیت می‌پردازند.

لازمه انطباق این ضابطه با حوزه عملکرد سامانه‌های هوشمند، اتخاذ رویکرد کارکردی است. بدین معنا که اصیل با تعریف اهداف غایی برای سیستم، خواه پیشینه‌سازی سود و کارایی، خواه بهینه‌سازی تعامل با کاربر، در واقع یک «محدوده ریسک»^۶ مشخص را ایجاد و مدیریت می‌کند (Barfield & Pagallo, 2018, p.399) و در این بستر، موجودیت و کارکرد عملیاتی سامانه هوشمند در خدمت نیل به همین اهداف از پیش مقررشده قرار دارد. در همین راستا، پرونده

Salmond, J. W. (1907). The law of torts. Stevens and Haynes.

1. Close Connection Test
2. Fairly and Properly
3. Opportunity
4. Connection to Duties
5. Inherent Risk
6. Field of Risk

کمبریج آنالیتیکا^۱ نمونه‌ای بارز از این پدیده است که نشان می‌دهد چگونه تعقیب یک هدف سازمانی ظاهراً مشروع (هدف‌گذاری تبلیغاتی) می‌تواند به‌طور مستقیم به نقض گسترده حقوق و آسیب‌های اجتماعی منجر شود. در این مثال، فعل زیان‌بار سیستم یک انحراف غیرمرتبط از فعالیت آن نیست، بلکه تحقق یکی از ریسک‌های ذاتی است که اصیل با تعریف آن هدف خاص، آن را ایجاد کرده است. چنین فعلی از «فرصت» ایجادشده با پلتفرم بهره می‌برد و با «وظیفه» اصلی آن یعنی بهینه‌سازی برای یک هدف معین، «ارتباطی تنگاتنگ» دارد. بنابراین، پیوند میان عملکرد زیان‌بار هوش مصنوعی و اهداف تعیین‌شده توسط اصیل، آنچنان عمیق و ماهوی است که انتساب مسئولیت به وی بر اساس معیار «ارتباط نزدیک»، هم ممکن و هم «منصفانه و مناسب» به نظر می‌رسد.

این انطباق معیار «ارتباط نزدیک» بر کنش‌های زیان‌بار هوش مصنوعی را می‌توان این‌گونه مستدل کرد که نفس تصمیم اصیل مبنی بر استقرار یک سامانه هوشمند برای انجام یک وظیفه، به‌خودی‌خود «فرصت» ایراد خسارت توسط آن سامانه را خلق می‌کند؛ فرصتی که بدون اقدام اصیل هرگز وجود نداشت. مهم‌تر آنکه، بسیاری از افعال زیان‌بار هوش مصنوعی تجلی مستقیم «ریسک‌های ذاتی» و نوعاً قابل پیش‌بینی هستند که با سپردن آن وظیفه خاص به عامل الگوریتمی ملازمه دارند. برای مثال، در مورد الگوریتم استخدام شرکت آمازون که به حذف سیستماتیک متقاضیان زن انجامید (Albert et al, 2022, p. 279)، فرصت تبعیض با تصمیم به خودکارسازی فرایند گزینش ایجاد شد و فعل زیان‌بار، تحقق ریسک ذاتی سوگیری در داده‌های آموزشی بود. انتساب این نتیجه به آمازون، حتی در غیاب قصد تبعیض، از آن‌رو «منصفانه و

۱. رسوایی شرکت کمبریج آنالیتیکا (Cambridge Analytica Scandal) مرتبط با حریم خصوصی داده‌ها، سوءاستفاده از اطلاعات شخصی در شبکه‌های اجتماعی و تأثیرگذاری بر روندهای سیاسی است که در سال ۲۰۱۸ علنی شد. برای مطالعه تفصیلی به کتاب زیر که توسط افشاگر اصلی ماجرای کمبریج آنالیتیکا نوشته شده و روایتی دست‌اول است، رجوع شود. نویسنده به‌عنوان مدیر تحقیقات سابق شرکت، در این کتاب به تفصیل توضیح می‌دهد که چگونه این شرکت از داده‌های فیس‌بوک برای ساخت سلاح‌های روانی و تأثیرگذاری بر انتخابات در سراسر جهان از جمله انتخابات ریاست‌جمهوری ۲۰۱۶ آمریکا و فراندوم برگزیت استفاده کرد.

Wylie, C. (2020). Mindf*ck: Cambridge Analytica. La trama para desestabilizar el mundo. Roca Editorial.

مناسب» است که آسیب مستقیماً از ریسک فعالیت انتفاعی و تصمیمات عملیاتی همان شرکت ناشی شده است.

این ارتباط تنگاتنگ، در عملکرد الگوریتم‌های توصیه‌گر محتوا که در پلتفرم‌های بزرگ به کار گرفته می‌شوند (Chakraborty, 2025, pp. 378-379) نیز نمایان می‌شود؛ با این توضیح که این الگوریتم‌ها وظیفه دارند تعامل کاربر را به نفع اهداف تجاری پلتفرم افزایش دهند و اگر در راستای انجام این وظیفه، محتوای افراطی یا کذب را ترویج کنند (Shin, 2024, p. 57)، این کنش انحراف از وظیفه نیست، بلکه محصول جانبی و منطقی بهینه‌سازی افراطی برای همان وظیفه است. این فعل زیان‌بار، نامطلوب، اما دارای پیوندی عمیق با وظیفه محوله و اهداف اصیل است و نمی‌توان آن را عملی کاملاً منفک از جریان عادی فعالیت پلتفرم دانست. بنابراین، با در نظر گرفتن این پیوند میان خلق فرصت توسط اصیل، تحقق ریسک‌های ذاتی ناشی از انتخاب فناوری توسط او و ارتباط تنگاتنگ فعل زیان‌بار با وظایف محوله، معیار «ارتباط نزدیک» قابلیت انطباق مؤثری با وضعیت هوش مصنوعی دارد. لذا اعمال دکترین مسئولیت نیابتی و تلقی این افعال به‌عنوان امری که «به‌طور منصفانه و مناسب» در جریان عادی رابطه با اصیل رخ داده، با منطق حقوقی این معیار سازگار است و دومین و آخرین عنصر لازم برای استقرار این مسئولیت را محقق می‌سازد.

نتیجه‌گیری

مقاله حاضر در پی ارائه و توجیه چهارچوبی منسجم برای انتساب مسئولیت ناشی از عملکرد سامانه‌های هوش مصنوعی در حقوق ایران بود. با در نظر گرفتن واقعیات موضوعی و تحلیل حقوقی امر، این نتیجه حاصل شد که ظرفیت‌های نظری و عملی دکترین مسئولیت نیابتی، آن را به راهکاری مناسب برای مسئول شناختن اشخاص به‌کارگیرنده (اصیل) هوش مصنوعی در نظام حقوقی ایران تبدیل می‌کند. تحلیل مبانی این رویکرد نشان داد که اصول بنیادین سیاست‌گذاری از جمله منطق اقتصادی «بهره‌مندی از منافع و درعین‌حال خلق ریسک»، ضرورت «درونی‌سازی هزینه‌ها» و توانایی برتر «اصیل» در مدیریت خسارات، توجیهی متقن برای مسئول دانستن نهاد به‌کارگیرنده فراهم می‌آورد و قابل توجه است که این مفاهیم قرابت مفهومی عمیقی با قواعدی چون «من له الغنم فعلیه الغرم» و «اصل احترام» در حقوق ایران نیز دارند. همچنین، صورت‌بندی تحلیلی و نظام‌مند از ارکان این نوع مسئولیت نشان داد که معیار «رابطه شبه‌استخدامی» با در نظر

گرفتن انتصاب کارکردی سامانه هوشمند توسط اصیل، کنترل وی بر اهداف و پارامترهای عملیاتی آن و انتفاع حاصل از به کارگیری آن، قابلیت انطباق با وضعیت هوش مصنوعی را دارد و احراز پیوند ذاتی میان فرصت‌ها و ریسک‌های مرتبط با هوش مصنوعی و وظایفی که اصیل به سامانه محول می‌کند، با در نظر گرفتن معیار «ارتباط نزدیک» میان خروجی مجرمانه سیستم و فعالیت‌های اصیل، امکان‌پذیر است. این چهارچوب با پر کردن خلأ مسئولیت، نظام حقوقی را در مواجهه با هوش مصنوعی کارآمد می‌سازد و با قرار دادن مسئولیت بر عهده گروهی که از ریسک منتفع شده‌اند و آن را کنترل می‌کنند، بازدارندگی را تقویت می‌کند و به ذی‌نفعان، انگیزه لازم برای توسعه و استفاده مسئولانه از این فناوری را می‌دهد. در نهایت، این پژوهش با توجه به نیاز نظام حقوقی ایران به ایجاد چهارچوب قانونی برای مسئولیت‌پذیری در حوزه فناوری‌های نوظهور، مبنایی تحلیلی و کاربردی در اختیار قانون‌گذار قرار می‌دهد. بر این اساس، پیشنهاد می‌شود سنگ بنای نظام مقرراتی ایران بر اصل مسئولیت اولیه منتفع یا «به کارگیرنده» استوار شود.

پیشنهاد برای قانون‌گذاری در ایران

۱. مسئولیت اولیه برای «به کارگیرنده»

پیشنهاد می‌شود قانون‌گذار، مسئولیت ناشی از سامانه‌های هوشمند را بر عهده شخص «به کارگیرنده» قرار دهد. این ایده با قاعده فقهی-حقوقی «من له الغنم فعلیه الغرم» و جوهره «اصل احترام» در فقه اسلامی همسوست و علاوه بر منصفانه بودن، بر این واقعیت مبتنی است که اصیل (شرکت یا سازمان) به دلیل برخورداری از منابع مالی بیشتر (جیب عمیق)، در بهترین موقعیت برای جبران خسارت زیان‌دیده قرار دارد. مسئولیت به کارگیرنده همچنین، کاملاً با منطق اقتصادی «ارزان‌ترین پیشگیری‌کننده از هزینه» مطابقت دارد؛ زیرا به کارگیرنده در بهترین و مقرون به صرفه‌ترین جایگاه برای مدیریت، کنترل و کاهش ریسک‌های سیستم قرار دارد.

۲. مقابله با خلأ مسئولیت با به کارگیری معیار «رابطه شبیه به استخدام»

جهت جلوگیری از ایجاد خلأهای مسئولیت، پیشنهاد می‌شود قانون‌گذار از چهارچوب‌های سنتی فراتر رود و با استفاده از چهارچوب انعطاف‌پذیر «رابطه شبه‌استخدامی»، مسئولیت را بر اساس ماهیت عملکردی رابطه تعریف کند. این معیار زمانی محقق می‌شود که سامانه هوشمند در فعالیت

اصلی بنگاه ادغام می‌شود و به نیابت از آن برای تحقق اهداف سازمانی عمل می‌کند. در این حالت، هوش مصنوعی به یک امتداد فناورانه از فعالیت اصیل تبدیل می‌شود مانند استفاده از آن به جای راننده، مسئول گزینش در استخدام یا حتی مشاور روان‌شناسی. پذیرفتن این «انتصاب کارکردی» که جوهره اصلی رویه قضایی مدرن است، مانع فرار شرکت‌ها از مسئولیت از طریق ساختارهای حقوقی سنتی می‌شود.

۳. به‌کارگیری معیار «ارتباط نزدیک» برای احراز رابطه استناد

به دلیل ماهیت «جعبه سیاه» هوش مصنوعی، یک خلأ مسئولیت از باب سخت بودن احراز رابطه استناد به وجود می‌آید. برای رفع این مشکل پیشنهاد می‌شود قانون‌گذار معیار مدرن «ارتباط نزدیک» را برای احراز پیوند میان عمل زیان‌بار هوش مصنوعی و فعالیت اصیل به کار گیرد. این معیار با بررسی این موضوع که آیا عمل زیان‌بار، تحقق یکی از ریسک‌های ذاتی و به‌نوعی ملازم با فعالیتی است که اصیل با سپردن آن وظیفه به هوش مصنوعی ایجاد کرده است، بر مشکل «جعبه سیاه» بودن الگوریتم‌ها فائق می‌آید. همان‌طور که در نمونه‌های عملی (مانند الگوریتم استخدامی آمازون یا الگوریتم‌های توصیه‌گر محتوا) مشاهده شد، این معیار به‌خوبی نشان می‌دهد که چگونه عملکرد زیان‌بار سیستم، ارتباطی تنگاتنگ با وظایف محوله و اهداف تجاری اصیل دارد.

۴. اتخاذ رویکرد نظارتی ریسک‌محور و تدوین استانداردهای فنی-حقوقی متناسب با ریسک‌ها

به‌منظور همگامی با روندهای حقوقی نوین جهانی پیشنهاد می‌شود که نظام نظارتی ایران مدل مؤثر «نظارت ریسک‌محور» را به‌عنوان مبنای سیاست‌گذاری خود اتخاذ کند. این روش امکان آن را فراهم می‌آورد که الزامات قانونی و سطح مسئولیت برای هر سیستم، بر اساس سطح ریسک به‌کارگیری آن تعیین شود. برای عملیاتی کردن این مدل، قانون‌گذار باید نهادهای نظارتی را موظف به تدوین استانداردهای فنی-حقوقی پویا کند. این استانداردها باید جنبه‌های فنی، ایمنی و اخلاقی (مانند کاهش سوگیری) را شامل شوند و همچنین، به حل «مشکل دست‌های زیاد» کمک کنند.

این مقاله - حسب اظهار نویسندگان - مستخرج است از رساله دکتری نویسنده دوم، که تحت عنوان «مبانی و قلمرو مسئولیت کیفری هوش مصنوعی؛ مطالعه تطبیقی با اسناد اروپایی» در دانشکده حقوق و علوم سیاسی دانشگاه تهران به تصویب رسیده است.

منابع

- ۱) برزگر، محمدرضا و الهام، غلامحسین (۱۳۹۹). مسئولیت کیفری کاربر خودروی خودران در قبال صدمات وارده توسط آن. فصلنامه پژوهش حقوق کیفری، ۸ (۳۰)، صص. ۲۰۱-۲۲۹.
- ۲) تخشید، زهرا (۱۴۰۰). مقدمه‌ای بر چالش‌های هوش مصنوعی در حوزه مسئولیت. حقوق خصوصی، ۱۸ (۱)، صص. ۲۲۷-۲۵۰. doi: 10.22059/jolt.2021.319529.1006965
- ۳) حسینی، الهام‌السادات، محمدیان امیری، مهدی و خیراللهی، محمدعلی (۱۴۰۳). بررسی فقهی مسئولیت در فناوری هوش مصنوعی. پژوهش‌های تطبیقی فقه، حقوق و سیاست، ۶ (۴)، صص. ۴۹-۶۶.
- ۴) حکمت‌نیا، محمود، محمدی، مرتضی و واثقی، محسن (۱۳۹۸). مسئولیت ناشی از تولید ربات‌های مبتنی بر هوش مصنوعی خودمختار. حقوق اسلامی، ۱۵ (۶۰)، صص. ۲۳۱-۲۵۵.
- ۵) دیلمی، احمد، زند لشنی، ناهید و جوادی، علی (۱۳۹۹). مبنای مسئولیت ناشی از فعل غیر در حقوق انگلستان و ایران. دوفصلنامه علمی دانش حقوق مدنی، ۹ (۲)، صص. ۶۷-۷۹. doi: 10.30473/clk.2021.49776.2660
- ۶) ذاکری‌نیا، حانیه (۱۴۰۲). ماهیت و مبنای مسئولیت ناشی از هوش مصنوعی در حقوق ایران و کشورهای اتحادیه اروپا. حقوق خصوصی، ۲۰ (۱)، صص. ۱۳۵-۱۵۲. doi: 10.22059/jolt.2023.356703.1007186
- ۷) ژوردن، پاتریس (۱۳۹۴). اصول مسئولیت (مجید ادیب، مترجم). چاپ ۴، تهران: میزان.
- ۸) شیرازی، عباس (۱۳۹۶). عدالت ترمیمی. چاپ ۱، تهران: میزان.
- ۹) غمامی، سیدمحمد مهدی و هاشمی، سیدحسین (۱۴۰۴). چالش‌های حقوقی نظام تنظیم‌گری فناوری‌های نوظهور مجازی در ایران. پژوهشنامه حقوق اسلامی، ۲۶ (۴)، صص. ۱۳۷۳-۱۴۰۸. doi: 10.30497/law.2025.247604.3690
- ۱۰) مهدی‌زاده، علیرضا و قلی‌نیا، رضا (۱۴۰۱). مسئولیت مدنی کاربر در به‌کارگیری سیستم هوش مصنوعی در خودرو. مجله پژوهش‌های حقوقی، ۲۱ (۵۰)، صص. ۳۰۵-۳۳۱. doi: 10.48300/jlr.2021.285755.1653
- ۱۱) ولی‌پور، علی و اسماعیلی، محسن (۱۴۰۰). امکان‌سنجی مسئولیت مدنی هوش مصنوعی عمومی ناشی از ایجاد ضرر در حقوق مدنی. فصلنامه اندیشه حقوقی معاصر، ۲ (۶)، صص. ۸-۱. doi: 10.22034/lth.2021.248596
- 12) Albert, M. V., Lin, L., Spector, M. J., & Dunn, L. S. (Eds.). (2022). Bridging human intelligence and artificial intelligence. Springer International Publishing. <https://doi.org/10.1007/978-3-030-84729-6>
- 13) Azad, S., & Nazari-Heris, M. (Eds.). (2024). Artificial intelligence in the operation and control of digitalized power systems. Springer Nature.

- 14) Barfield, W., & Pagallo, U. (Eds.). (2018). Research handbook on the law of artificial intelligence. Edward Elgar Publishing.
- 15) Brodie, D. (2010). Enterprise liability and the common law. Cambridge University Press.
- 16) Campbell, M., & Lindsay, B. (2024). Refining vicarious liability. *Edinburgh Law Review*, 28(2), 174-206.
- 17) Chakrabarty, I., & Baral, A. (2023). Artificial intelligence and personhood in the 21st century. *Indian Journal of Integrated Research in Law*, 3(1), 1-10.
- 18) Chakraborty, S. (Ed.). (2025). Ethical AI solutions for addressing social media influence and hate speech. IGI Global. <https://doi.org/10.4018/979-8-3693-9904-0>
- 19) Charles Sr., C. (2025). Security automation with Python: Practical Python solutions for automating and scaling security operations. Packt Publishing.
- 20) Cristiano, F., Broeders, D., Delerue, F., Douzet, F., & Géry, A. (2023). Artificial intelligence and international conflict in cyberspace. Taylor & Francis.
- 21) Diamantis, M. E. (2023). Vicarious liability for AI. *Indiana Law Journal*, 99(1), 317-334.
- 22) Dremluga, R., Kuznetsov, P., & Mamychyev, A. (2019). Criteria for recognition of AI as legal person. *Journal of Politics and Law*, 12(3), 105-112.
- 23) Ebers, M., & Gamito, M. C. (Eds.). (2021). Algorithmic governance and governance of algorithms. Springer.
- 24) Gatti, M. (2016). European External Action Service: Promoting coherence through autonomy and coordination (Vol. 11). Brill.
- 25) GE v The Trustees of the Portsmouth Roman Catholic Diocesan Trust, [2012] EWHC 1251 (QB).
- 26) Gero, J. S., & Sudweeks, F. (Eds.). (2012). Artificial intelligence in design '96. Springer Science & Business Media.
- 27) Giliker, P. (Ed.). (2022). Vicarious liability in the common law world. Hart Publishing.
- 28) Johnson, D. G. (2015). Technology with no human responsibility? *Journal of Business Ethics*, 127(4), 707-715.
- 29) Kerrigan, C. (Ed.). (2022). Artificial intelligence: Law and regulation. Edward Elgar Publishing.
- 30) Königs, P. (2022). Artificial intelligence and responsibility gaps: What is the problem? *Ethics and Information Technology*, 24(3), 36.
- 31) Krömker, H. (2022). HCI in mobility, transport, and automotive systems. Springer.
- 32) Nikolinakos, N. T. (2023). EU policy and legal framework for artificial intelligence, robotics and related technologies - The AI Act. Springer International Publishing AG.
- 33) Oliphant, K., & Wagner, G. (Eds.). (2012). Employers' liability and workers' compensation (Vol. 31). Walter de Gruyter.
- 34) Pagallo, U. (2018). Vital, Sophia, and Co.—The quest for the legal personhood of robots. *Information*, 9(9), 230. <https://doi.org/10.3390/info9090230>

- 35) Petrin, M., & Witting, C. (Eds.). (2023). Research handbook on corporate liability. Edward Elgar Publishing.
- 36) Shin, D. (2024). Artificial misinformation: Exploring human-algorithm interaction online. Springer Nature.
- 37) Simmler, M., & Markwalder, N. (2019). Guilty robots?—Rethinking the nature of culpability and legal personhood in an age of artificial intelligence. Criminal Law Forum, 30(1), 1-31.
- 38) Skandinaviska Enskilda Banken AB v Asia Pacific Breweries (S) Pte Ltd, [2011] SGCA 22.
- 39) Soni, H. K., Sharma, S., & Sinha, G. R. (Eds.). (2024). Text and social media analytics for fake news and hate speech detection. CRC Press.
- 40) Szapiro, T., & Kacprzyk, J. (Eds.). (2022). Collective decisions: Theory, algorithms and decision support systems. Springer.
- 41) Szentgali-Toth, B. (2021). The source of unexplored opportunities or an unpredictable risk factor? Could artificial intelligences be subject to the same laws as human beings? Public Governance, Administration and Finances Law Review, 6(2), 101-120.
- 42) Taplin, R. (2022). Artificial intelligence, intellectual property, cyber risk and robotics: A new digital age. Routledge.
- 43) Various Claimants v Catholic Child Welfare Society, [2012] UKSC 56.

References

- 1) Albert, M. V., Lin, L., Spector, M. J., & Dunn, L. S. (Eds.). (2022). Bridging human intelligence and artificial intelligence. Springer International Publishing. <https://doi.org/10.1007/978-3-030-84729-6>
- 2) Azad, S., & Nazari-Heris, M. (Eds.). (2024). Artificial intelligence in the operation and control of digitalized power systems. Springer Nature.
- 3) Barfield, W., & Pagallo, U. (Eds.). (2018). Research handbook on the law of artificial intelligence. Edward Elgar Publishing.
- 4) Barzegar, Mohammad Reza & Elham, Gholamhossein (1399 SH/2020). Mas'ūliyat-e Kayfari-ye Kārbar-e Khūdkār-e Khūdrān dar Qibāl-e Šadamāt-e Vāridah Tavassuṭ-e Ān [Criminal Liability of the Autonomous Vehicle User for Damages Caused by It]. Faslnameh Pazhuhesh-e Hoquq-e Keyfari [Criminal Law Research Quarterly], 8(30), pp. 201-229 [in Persian].
- 5) Brodie, D. (2010). Enterprise liability and the common law. Cambridge University Press.
- 6) Campbell, M., & Lindsay, B. (2024). Refining vicarious liability. *Edinburgh Law Review*, 28(2), 174-206.
- 7) Chakrabarty, I., & Baral, A. (2023). Artificial intelligence and personhood in the 21st century. *Indian Journal of Integrated Research in Law*, 3(1), 1-10.
- 8) Chakraborty, S. (Ed.). (2025). Ethical AI solutions for addressing social media influence and hate speech. IGI Global. <https://doi.org/10.4018/979-8-3693-9904-0>
- 9) Charles Sr., C. (2025). Security automation with Python: Practical Python solutions for automating and scaling security operations. Packt Publishing.
- 10) Cristiano, F., Broeders, D., Delerue, F., Douzet, F., & Géry, A. (2023). Artificial intelligence and international conflict in cyberspace. Taylor & Francis.
- 11) Deylami, Ahmad, Zand Lashni, Nahid & Javadiyeh, Ali (1399 SH/2020). Mabānī-ye Mas'ūliyat-e Nāshī az Fi'l-e Ghayr dar Ḥuqūq-e Ingilistān va Īrān [Fundamentals of Vicarious Liability in English and Iranian Law]. Doufaslnameh-ye Elmi-ye Danesh-e Hoquq-e Madani [Scientific Biannual Journal of Civil Law Knowledge], 9(2), pp. 67-79. doi: 10.30473/clk.2021.49776.2660 [in Persian].
- 12) Diamantis, M. E. (2023). Vicarious liability for AI. *Indiana Law Journal*, 99(1), 317-334.
- 13) Dremluga, R., Kuznetsov, P., & Mamychyev, A. (2019). Criteria for recognition of AI as legal person. *Journal of Politics and Law*, 12(3), 105-112.
- 14) Ebers, M., & Gamito, M. C. (Eds.). (2021). Algorithmic governance and governance of algorithms. Springer.
- 15) Gatti, M. (2016). European External Action Service: Promoting coherence through autonomy and coordination (Vol. 11). Brill.
- 16) GE v The Trustees of the Portsmouth Roman Catholic Diocesan Trust, [2012] EWHC 1251 (QB).
- 17) Gero, J. S., & Sudweeks, F. (Eds.). (2012). Artificial intelligence in design '96. Springer Science & Business Media.

- 18) Ghamami, Seyyed Mohammad Mehdi & Hashemi, Seyyed Hossein (1404 SH/2025). Chālīshhā-ye Ḥuqūqī-ye Nīzām-e Tanzīmgarī-ye Fannārīhā-ye Nawzuhūr-e Majāzī dar Īrān [Legal Challenges in the Regulatory Framework for Emerging Virtual Technologies in Iran]. Pazhuheshnameh Hoquq-e Eslami [Journal of Islamic Law Research], 26(4), pp. 1373-1408. doi: 10.30497/law.2025.247604.3690 [in Persian].
- 19) Giliker, P. (Ed.). (2022). Vicarious liability in the common law world. Hart Publishing.
- 20) Hekmatnia, Mahmoud, Mohammadi, Morteza & Vaseghi, Mohsen (1398 SH/2019). Mas'ūliyat-e Nāshī az Tawlīd-e Rubāthā-ye Mubtanī bar Hūsh-e Mašnū'ī-ye Khūddukhtār [Liability Arising from the Production of Autonomous AI-Based Robots]. Hoquq-e Eslami [Islamic Law], 15(60), pp. 231-255 [in Persian].
- 21) Hosseini, Elhamalsadat, Mohammadyan Amiri, Mehdi & Kheirollahi, Mohammad Ali (1403 SH/2024). Barrasī-ye Fiqhī-ye Mas'ūliyat dar Fannārī-ye Hūsh-e Mašnū'ī [Jurisprudential Review of Responsibility in Artificial Intelligence Technology]. Pazhuhesh-haye Tatbiqī-ye Feqh, Hoquq va Siasat [Comparative Research of Jurisprudence, Law and Politics], 6(4), pp. 49-66 [in Persian].
- 22) Johnson, D. G. (2015). Technology with no human responsibility? Journal of Business Ethics, 127(4), 707-715.
- 23) Jourdain, Patrice (1394 SH/2015). Uṣūl-e Mas'ūliyat [Principles of Liability] (M. Adib, Trans.) (4th ed.). Tehran: Mizan [in Persian].
- 24) Kerrigan, C. (Ed.). (2022). Artificial intelligence: Law and regulation. Edward Elgar Publishing.
- 25) Königs, P. (2022). Artificial intelligence and responsibility gaps: What is the problem? Ethics and Information Technology, 24(3), 36.
- 26) Krömker, H. (2022). HCI in mobility, transport, and automotive systems. Springer.
- 27) Mashhadizadeh, Alireza & Gholinia, Reza (1401 SH/2022). Mas'ūliyat-e Madanī-ye Kārbar dar Bih-kārgīrī-ye Sīstām-e Hūsh-e Mašnū'ī dar Khūdrū [User's Civil Liability in Employing Artificial Intelligence System in Cars]. Majalleh Pazhuhesh-haye Hoquqī [Law Research Journal], 21(50), pp. 305-331. doi: 10.48300/jlr.2021.285755.1653 [in Persian].
- 28) Nikolinakos, N. T. (2023). EU policy and legal framework for artificial intelligence, robotics and related technologies - The AI Act. Springer International Publishing AG.
- 29) Oliphant, K., & Wagner, G. (Eds.). (2012). Employers' liability and workers' compensation (Vol. 31). Walter de Gruyter.
- 30) Pagallo, U. (2018). Vital, Sophia, and Co. – The quest for the legal personhood of robots. Information, 9(9), 230. <https://doi.org/10.3390/info9090230>
- 31) Petrin, M., & Witting, C. (Eds.). (2023). Research handbook on corporate liability. Edward Elgar Publishing.
- 32) Shin, D. (2024). Artificial misinformation: Exploring human-algorithm

- interaction online. Springer Nature.
- 33) Shiri, Abbas (1396 SH/2017). 'Adālat-e Tarmīmī [Restorative Justice] (1st ed.). Tehran: Mizan [in Persian].
 - 34) Simmler, M., & Markwalder, N. (2019). Guilty robots?—Rethinking the nature of culpability and legal personhood in an age of artificial intelligence. *Criminal Law Forum*, 30(1), 1-31.
 - 35) Skandinaviska Enskilda Banken AB v Asia Pacific Breweries (S) Pte Ltd, [2011] SGCA 22.
 - 36) Soni, H. K., Sharma, S., & Sinha, G. R. (Eds.). (2024). Text and social media analytics for fake news and hate speech detection. CRC Press.
 - 37) Szapiro, T., & Kacprzyk, J. (Eds.). (2022). Collective decisions: Theory, algorithms and decision support systems. Springer.
 - 38) Szentgali-Toth, B. (2021). The source of unexplored opportunities or an unpredictable risk factor? Could artificial intelligences be subject to the same laws as human beings? *Public Governance, Administration and Finances Law Review*, 6(2), 101-120.
 - 39) Takhshid, Zahra (1400 SH/2021). Muqaddamah'ī bar Chālīshhā-ye Hūsh-e Mašnū'ī dar Hawzah-ye Mas'ūliyat [An Introduction to the Challenges of Artificial Intelligence in the Field of Liability]. *Hoquq-e Khosousi [Private Law]*, 18(1), pp. 227-250. doi: 10.22059/jolt.2021.319529.1006965 [in Persian].
 - 40) Taplin, R. (2022). Artificial intelligence, intellectual property, cyber risk and robotics: A new digital age. Routledge.
 - 41) Valipour, Ali & Esmaeili, Mohsen (1400 SH/2021). Imkānsanjī-ye Mas'ūliyat-e Madanī-ye Hūsh-e Mašnū'ī-ye 'Umūmī Nāshī az Ījād-e Żarar dar Huquq-e Madanī [Feasibility of Civil Liability of Artificial General Intelligence Arising from Causing Harm in Civil Law]. *Faslnameh Andisheh-ye Hoquqi-ye Moaser [Contemporary Legal Thought Quarterly]*, 2(6), pp. 1-8. doi: 10.22034/lth.2021.248596 [in Persian].
 - 42) Various Claimants v Catholic Child Welfare Society, [2012] UKSC 56.
 - 43) Zakerinia, Haniyeh (1402 SH/2023). Māhiyat va Mabnā-ye Mas'ūliyat-e Nāshī az Hūsh-e Mašnū'ī dar Huquq-e Īrān va Kishvarhā-ye Ittīhādiyah-ye Urūpā [Nature and Basis of Liability Arising from Artificial Intelligence in the Law of Iran and European Union Countries]. *Hoquq-e Khosousi [Private Law]*, 20(1), pp. 135-152. doi: 10.22059/jolt.2023.356703.1007186 [in Persian].