Comparative Studies in Jurisprudence, Law, and Politics

Criminal Liability in the Age of Artificial Intelligence and Cybercrime: A Comparative Analysis of the Foundations of Imami and Maliki Jurisprudence

1. Lida Samadiyan: Department of Criminal Law and Criminology, Ka.C., Islamic Azad University, Karaj, Iran
2. Sadegh Moradi*: Department of Jurisprudence and Law, CT.C., Islamic Azad University, Tehran, Iran. Email: Sad.moradi@iauctb.ac.ir (Corresponding Author)
3. Amir Samavati Pirouz: Department of Criminal and criminology, Ka.C., Islamic Azad University, Karaj, Iran

ABSTRACT

The rapid advancements in artificial intelligence technologies and the expansion of cybercrime have placed criminal liability within a complex and multidimensional domain. Today, many offenses are committed in digital environments through the use of intelligent systems, which has created serious challenges in identifying the human agent, determining criminal intent, and assessing the extent of human involvement in the commission of crimes. In light of these fundamental transformations, the need to reconsider the traditional foundations of criminal liability and to analyze their capacity to address emerging offenses has become increasingly evident. The aim of this study is to conduct a comparative examination of the foundations of criminal liability in Imami (Jaʿfari) jurisprudence and Maliki jurisprudence and to analyze the capacity of these two jurisprudential systems to confront the challenges posed by the age of artificial intelligence and cybercrime. The research method adopted in this article is descriptive–analytical and is based on the study of jurisprudential and legal sources. The findings indicate that Imami jurisprudence, through its acceptance of indirect liability, flexibility in the analysis of intent and the instrumental means of committing crimes, and the possibility of analogical inference from comparable cases, possesses greater capacity to respond to intelligent and cyber offenses. This capacity facilitates the development of legal frameworks compatible with emerging technologies. In contrast, Maliki jurisprudence, due to certain limitations regarding the inclusion of offenses arising from automated systems and its emphasis on direct perpetration and explicit intent, faces shortcomings in addressing digital crimes. The final conclusion of this research emphasizes the necessity of utilizing the capacities of comparative jurisprudence to reconsider criminal liability and to formulate regulations compatible with the digital and artificial intelligence era, demonstrating that the adaptation of traditional principles to modern technologies can provide an effective solution for filling legal and jurisprudential gaps in combating cybercrime.

Keywords: *Criminal liability, Artificial intelligence, Cybercrime, Imami jurisprudence, Maliki jurisprudence, Adaptation of jurisprudence to technology.*

How to cite: Samadiyan, L., Moradi, S., & Samavati Pirouz, A. (2026). Criminal Liability in the Age of Artificial Intelligence and Cybercrime: A Comparative Analysis of the Foundations of Imami and Maliki Jurisprudence. *Comparative Studies in Jurisprudence, Law, and Politics*, *8*(3), 1-20.

Submit Date: 23 September 2025
Revise Date: 03 February 2026
Accept Date: 10 February 2026
Initial Publish Date: 06 April 2026
Final Publish Date: 23 July 2026

پژوهش‌های تطبیقی فقه، حقوق و سیاست

مسئولیت کیفری در عصر هوش مصنوعی و جرائم سایبری؛ با تحلیل تطبیقی مبانی فقه امامیه و مالکی

۱. لیدا صمدیان: گروه حقوق کیفری و جرم شناسی، واحد کرج، دانشگاه آزاد اسلامی، کرج، ایران
۲. صادق مرادی*: گروه فقه و حقوق، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران. پست الکترونیک: Sad.moradi@iauctb.ac.ir (نویسنده مسئول)
۳. امیر سماواتی پیروز: گروه جزا و جرم شناسی، دانشگاه شهید بهشتی، واحد کرج ، دانشگاه آزاد اسلامی، کرج، ایران

چکیده

تحولات سریع فناوری هوش مصنوعی و گسترش جرائم سایبری، مسئولیت کیفری را وارد قلمرویی پیچیده و چندوجهی کرده است. امروزه بسیاری از جرائم در فضای دیجیتال و با بهره‌گیری از سیستم‌های هوشمند ارتکاب می‌یابند و این موضوع، تشخیص عامل انسانی، تعیین قصد مجرمانه و میزان دخالت انسان در ارتکاب جرم را با چالش‌های جدی مواجه ساخته است. با توجه به این تغییرات بنیادین، ضرورت بازنگری در مبانی سنتی مسئولیت کیفری و تحلیل قابلیت‌های آنها در پاسخگویی به جرائم نوظهور بیش از پیش احساس می‌شود. هدف این تحقیق، بررسی تطبیقی مبانی مسئولیت کیفری در فقه امامیه و فقه مالکی و تحلیل ظرفیت این دو نظام فقهی برای مواجهه با چالش‌های عصر هوش مصنوعی و جرائم سایبری است. روش تحقیق این مقاله، توصیفی–تحلیلی و مبتنی بر مطالعه منابع فقهی و حقوقی است. یافته‌های تحقیق نشان می‌دهد که فقه امامیه با پذیرش مسئولیت غیرمستقیم، انعطاف در تحلیل قصد و ابزار ارتکاب جرم و امکان استنباط از موارد مشابه، توانایی بیشتری برای پاسخگویی به جرائم سایبری و هوشمند دارد. این ظرفیت، امکان توسعه چارچوب‌های قانونی متناسب با فناوری‌های نوین را فراهم می‌آورد. در مقابل، فقه مالکی با محدودیت‌هایی در شمول جرائم ناشی از سامانه‌های خودکار و تمرکز بر مباشرت و قصد صریح، در مواجهه با جرائم دیجیتال دارای کاستی‌هایی است. نتیجه‌گیری نهایی این تحقیق بر لزوم بهره‌گیری از ظرفیت‌های فقه تطبیقی برای بازنگری در مسئولیت کیفری و تدوین مقررات سازگار با عصر دیجیتال و هوش مصنوعی تأکید دارد و نشان می‌دهد که تطبیق اصول سنتی با فناوری‌های نوین می‌تواند راهکار مؤثری برای پر کردن خلأهای قانونی و فقهی در مقابله با جرائم سایبری باشد.

واژگان کلیدی: *مسئولیت کیفری، هوش مصنوعی، جرائم سایبری، فقه امامیه، فقه مالکی، تطبیق فقه با فناوری.*

نحوه استناددهی: صمدیان، لیدا.، مرادی، صادق.، و سماواتی پیروز، امیر. (۱۴۰۵). مسئولیت کیفری در عصر هوش مصنوعی و جرائم سایبری؛ با تحلیل تطبیقی مبانی فقه امامیه و مالکی. *پژوهش‌های تطبیقی فقه، حقوق و سیاست*، ۸(۳)، ۲۰-۱.

تاریخ ارسال: ۱ مهر ۱۴۰۴
تاریخ بازنگری: ۱۴ بهمن ۱۴۰۴
تاریخ پذیرش: ۲۱ بهمن ۱۴۰۴
تاریخ چاپ اولیه: ۱۷ فروردین ۱۴۰۵
تاریخ چاپ نهایی: ۱ مرداد ۱۴۰۵

مقدمه

در دهه‌های اخیر، تحولات فناورانه با سرعتی بی‌سابقه، ساختار جوامع انسانی و روابط اجتماعی و اقتصادی را متحول کرده است. ظهور فناوری‌های نوین مانند هوش مصنوعی، اینترنت اشیاء، یادگیری ماشین و سیستم‌های خودکار، نه تنها امکان بهره‌وری و دسترسی به داده‌ها را افزایش داده‌اند، بلکه قلمرو فعالیت‌های انسانی را فراتر از محدوده‌های فیزیکی سنتی برده و به فضای مجازی و سامانه‌های دیجیتال منتقل کرده‌اند. در چنین بستری، جرائم کیفری نیز از شکل کلاسیک و سنتی خود که عمدتاً مبتنی بر اعمال فیزیکی و حضور مستقیم مجرم بود، فاصله گرفته و به شکل‌های پیچیده و نوظهور دیجیتال تبدیل شده‌اند. نفوذ به شبکه‌های رایانه‌ای، حملات سایبری، جعل دیجیتال، جرائم مالی هوشمند و حتی اقدامات خودکار در محیط‌های سایبری نمونه‌هایی از این چالش‌ها هستند که نیازمند بازنگری در مفاهیم و مبانی سنتی مسئولیت کیفری است.

با گسترش این پدیده‌ها، یکی از مسائل بنیادین حقوق کیفری، تعیین محدوده مسئولیت بازیگران انسانی و غیرانسانی در ارتکاب جرم است. سیستم‌های هوشمند و الگوریتم‌های خودکار، به گونه‌ای عمل می‌کنند که آثار و نتایج آنها می‌تواند مشابه اقدامات انسانی باشد، ولی فاقد اراده و قصد انسانی هستند. این مسئله، مبانی سنتی مسئولیت کیفری را به چالش می‌کشد، زیرا حقوق کیفری کلاسیک عمدتاً بر اساس عناصر قصد، فعل و رابطه علیت میان عامل و نتیجه شکل گرفته است. در این زمینه، ضرورت بررسی و بازتعریف معیارهای مسئولیت کیفری در برخورد با فناوری‌های هوشمند، به یک نیاز علمی و عملی تبدیل شده است(میری،۱۴۰۴: ۲۳).

فقه اسلامی، به ویژه فقه امامیه و فقه مالکی، طی قرون متمادی با ارائه اصولی دقیق در باب قصد، فعل، مسئولیت و آثار حقوقی اعمال، چارچوبی نظری برای تحلیل رفتار انسانی و تعیین مجازات فراهم کرده است. این اصول فقهی، با وجود ریشه‌های سنتی، قابلیت تطبیق و تعمیم به مسائل نوین حقوقی را دارند و می‌توانند به عنوان پایه‌ای برای بررسی مسئولیت کیفری در فضای سایبری و جرائم هوش مصنوعی مورد استفاده قرار گیرند. تحلیل تطبیقی میان دو مکتب فقهی، علاوه بر شناسایی نقاط قوت و محدودیت‌های هر یک، امکان ارائه راهکارهای نوآورانه و متناسب با فناوری‌های جدید را فراهم می‌آورد.

با وجود اهمیت موضوع، پژوهش‌های علمی و تطبیقی در این حوزه هنوز محدود و ناقص هستند و اغلب به صورت پراکنده به بررسی جرائم سایبری پرداخته‌اند بدون آنکه چارچوب نظری و فقهی مسئولیت کیفری در مواجهه با هوش مصنوعی به طور نظام‌مند تحلیل شود. از این رو، این مقاله با رویکردی تطبیقی و تحلیلی، تلاش می‌کند تا ضمن بررسی اصول فقه امامیه و فقه مالکی، توانمندی و محدودیت هر یک در مواجهه با جرائم سایبری و هوش مصنوعی را ارزیابی کند و پیشنهادهایی برای توسعه چارچوب حقوقی مناسب ارائه دهد. این تحقیق با هدف پاسخ به این پرسش اساسی انجام شده است که چگونه می‌توان با استفاده از اصول فقهی سنتی، چارچوبی قابل اتکا برای تعیین مسئولیت کیفری در فضای مجازی و سامانه‌های هوشمند تدوین کرد؟

تعریف مسئولیت کیفری

«مسئولیت» در لغت عبارتنداز آنچه انسان عهده دار و مسئول آن باشد و «مسئول» به معنای پرسیده شده و خواسته شده است (Amid, 1984).

«کیفر» در لغت به معنای مکافات بدی، جزا و پاداش، عقوبت، عقاب و مجازات قانونی است (دهخدا، ۱۳۸۸: ۱۸۳۳).

«مسئولیت کیفری» مسئولیت مرتکب جرمی از جرائم مصرح در قانون را گویند و شخص مسئول به یکی از مجازات‌های مقرر در قانون خواهد رسید. متضرر از جرم غالباً اجتماع است، برخلاف مسئولیت مدنی که متضرر از عمل مسئول، افراد می‌باشند (Jafari Langroudi, 2023). برخی دیگر از حقوقدانان در تعریف مسئولیت کیفری بیان داشته‌اند: به طورکلی برای مسئولیت دو مفهوم وجود دارد: مسئولیت بالقوه و مسئولیت بالفعل. مسئولیت بالقوه، مجرد است (ذهنی صرف است) و مسئولیت بالفعل، واقعی است. مراد از مفهوم اول صلاحیت و اهلیت شخص است، چراکه فرد باید متحمل پیامد کار خود باشد. مسئولیت به این معنا، صفت و یا حالتی است که با او ملازمه دارد، اعم از اینکه فعلی مسئولیت آور از او صادر شود یا خیر. مراد از مفهوم دوم، تحمل شخص نسبت به پیامدهایی است که حقیقت از وی صادر شده است و مسئولیت به این معنا مجرد صفت یا حالت قائم به شخص نیست، بلکه علاوه بر آن، جزا را هم در پی دارد. به لزوم حکم عقلی، مفهوم دوم دربردارنده مفهوم اول است و یا مفهوم اول مفروض گرفته می‌شود؛ زیرا که اعمال پیامدهای انجام کاری به شخص متصور است و یا مفهوم اول مفروض گرفته می‌شود؛ زیرا که اعمال پیامدهای انجام کاری به شخص متصور. به طور کلی باید گفت الزام شخص به پاسخگویی در برابر تعرض به دیگران، خواه به جهت حمایت از حقوق فردی صورت گیرد و خواه به منظور دفاع از جامعه، تحت عنوان «مسئولیت کیفری» یا «مسئولیت جزایی» مطرح می‌شود. با این وجود، در هیچ یک از قوانین جزایی چه در گذشته و چه در حال حاضر، ماهیت حقوقی و تعریف مسئولیت کیفری به طور مشخص بیان نشده است. به هر حال مسئولیت کیفری نوعی الزام شخصی به پاسخگویی آثار و نتایج نامطلوب پدیده جزایی یا جرم است (Mirsaeidi, 2019).

در واقع مسئولیت کیفری پلی است میان جرم و مجرم. یعنی عملی که جرم تلقی می‌شود باید به نحوی به یک شخص منتسب شود، این شخص همان مجرم است. از دیدگاه حقوق کیفری، ارتکاب جرم یا هر نوع تخطی از قوانین و مقررات جزایی به تنهایی و به خودی خود موجب مسئولیت کیفری نیست، بلکه برای این که مرتکب جرم را از نظر اخلاقی و اجتماعی مسئول و قابل سرزنش و مجازات بدانیم، لازم است که شرایطی با هم جمع شوند که عبارتند از:

اول: وقوع رفتار مجرمانه که از میل و اراده آگاهانه مرتکب آن نشات گرفته باشد و نحوه پندار، کردار و جریان تصمیم گیری او را مشخص کند.

دوم: عمل مجرمانه‌ای که با اندیشه، قصد و میل مرتکب، به صورت عینی تحقق یافته است باید حاکی از قصد مجرمانه مرتکب یا ناشی از خبط و خطای او باشد.

سوم: برای این که مرتکب جرم را مسئول بشناسیم، علاوه بر اراده ارتکاب جرم و قصد مجرمانه، باید بین جرم انجام یافته و فاعل آن، قابلیت انتساب موجود باشد (Mirsaeidi, 2019).

به طور کلی، هرکسی که با علم و اطلاع دست به ارتکاب جرم میزند، لزوماً مسئول شناخته نمی‌شود، بلکه علاوه بر تحقق اراده ارتکاب جرم و انجام جرم، باید دارای شرایط و خصوصیات فردی متعارفی باشد تا بتوان وقوع جرم را به او نسبت داد. در نتیجه، وقتی انسان از نظر کیفری مسئول شناخته می‌شود که مسبب و علت حادثه‌ای باشد؛ یعنی بتوان آن حادثه را به او نسبت داد و منسوب نمود. پس مسئولیت کیفری، محصول نسبت دادن و قابلیت انتساب است. مقصود از قابلیت انتساب آن است که بر مقامات قضایی معلوم گردد که فاعل جرم، از نظر رشد جسمی، عقلی و نیروی اراده و اختیار، دارای چنان شرایطی می‌باشد که می‌توان رابطه علیت بین جرم انجام یافته و مجرم برقرار کرد. در

حقیقت مسئولیت کیفری از نتایج مستقیم انتساب جرم به مجرم احراز می‌شود و از این جهت به طور مختصر می‌توان گفت مسئولیت کیفری قابلیت انتساب و نسبت دادن و اسناد عمل مجرمانه است.

با توجه به تعاریف مختلفی که پیرامون مسئولیت کیفری از سوی حقوقدانان ارائه شده، می‌توان آنها را به یکی از سه تعریف ذیل ارجاع نمود:

۱-مسئولیت کیفری عبارت است از قابلیت یا اهلیت شخص برای تحمل تبعات جزایی رفتار مجرمانه خود؛

۲-مسئولیت کیفری آن است که تبعات جزایی رفتار مجرمانه شخص بر او الزام یا تحمیل گردد.

۳-التزام یا مجبور بودن شخص نسبت به تحمل تبعات جزایی رفتار خود، مسئولیت کیفری نامیده می‌شود (Mirsaeidi, 2019).

حال حاضر بر اساس قوانین ایران و حقوق اسلام، نمی‌توان هوش مصنوعی را دارای مسئولیت کیفری دانست و مجازات کرد، زیرا آنها نه توانایی عمل مجرمانه را دارند عدم وجود عمد در فعل و عدم وجود اراده) و نه می‌توانند تصور و یا ایده مجازات را درک نمایند (عدم وجود قصد مجرمانه). با این حال، در آینده ممکن است ربات‌ها آن قدر شبیه به انسان شوند که همانند ما، قادر به "احساس" مجازات کیفری بشوند زمانی که این مرحله فرا رسید مجازات کردن ربات‌ها ممکن است منطقی به نظر برسد. براساس مبانی مسئولیت کیفری در ایران، اپراتورهای هوش مصنوعی یا به عبارتی برنامه نویسان، ممکن است در صورتی که یک هوش به دلیل بد عمل کردن قابل پیش بینی، مرتکب جرم شوند. در این صورت مسئولیت کیفری میتواند بر اپراتورها مطابق با قواعد عام مسئولیت کیفری سنتی اعمال شود، حتی اگر سهل انگاری آنها تنها یک قصور یا کوتاهی برای واکنش نشان دادن صحیح در خصوص گزارش‌های مربوط جرایم خطرناک بوده باشد. اما پیش بینی و کنترل رفتار هوش مصنوعی، ممکن است برای اپراتورهای انسانی بسیار دشوار شود که در نتیجه ممکن است لازم باشد تا الزامات مسئولیت کیفری در مورد سهل انگاری را مطرح سازیم، تا مبادا خطر مجازات مانع از توسعه و استفاده بیشتر از این فناوری شود.

ویژگی‌های جرائم سایبری

۱-غیرمادی بودن: ارتکاب جرم بدون تماس فیزیکی

یکی از بارزترین و تمایزدهنده‌ترین ویژگی‌های جرائم سایبری، غیرمادی بودن آن‌هاست. برخلاف جرائم سنتی که معمولاً با اعمال فیزیکی، تماس مستقیم با قربانی یا استفاده از ابزار مادی همراه است، جرائم سایبری عمدتاً در بستر دیجیتال و فضای مجازی رخ می‌دهند. این ویژگی باعث می‌شود که ماهیت جرم به‌طور کامل از تماس فیزیکی جدا شود و مرتکب بتواند بدون حضور فیزیکی و صرفاً از طریق ابزارهای دیجیتال، خسارت قابل توجهی به فرد، سازمان یا حتی دولت وارد کند. به عبارت دیگر، در جرائم سایبری، ابزار اصلی ارتکاب جرم همان فناوری‌های اطلاعاتی و ارتباطی هستند و فیزیکی بودن عمل به هیچ وجه الزامی نیست (Paridar, 2025).

عدم تماس فیزیکی، آثار متعددی بر نظام قضایی و کیفری دارد. از یک سو، شناسایی مرتکب و جمع‌آوری شواهد فیزیکی پیچیده می‌شود و از سوی دیگر، تعریف دقیق جرم و تعیین حدود مسئولیت حقوقی دشوارتر خواهد شد. برای مثال، در جرائم فیشینگ یا هک بانک‌ها، عامل می‌تواند در کشوری کاملاً متفاوت از قربانی حضور داشته باشد، بدون آنکه حتی یک بار با قربانی روبرو شود یا فیزیکاً در محل حضور یابد. این امر، جنبه بین‌المللی بودن جرائم سایبری را نیز تقویت می‌کند و نیاز به همکاری‌های فراملیتی بین دولت‌ها را بیش از پیش آشکار می‌سازد. علاوه بر این، غیرمادی بودن جرم باعث ایجاد پیچیدگی در تحلیل آثار و پیامدهای آن می‌شود. خسارات می‌توانند اقتصادی، روانی، اجتماعی یا حتی سیاسی باشند، بدون آنکه هیچ گونه آثار فیزیکی قابل مشاهده‌ای برجای بگذارند. برای مثال، انتشار اطلاعات شخصی کاربران در

شبکه‌های اجتماعی ممکن است به تخریب اعتبار، تهدید امنیت شخصی و حتی مشکلات شغلی یا خانوادگی منجر شود، در حالی که هیچ تماس فیزیکی میان مرتکب و قربانی رخ نداده است (Soufi & Saleh-Nejad, 2023).

از منظر حقوق کیفری، غیرمادی بودن جرائم سایبری نیازمند توسعه قواعد و رویه‌های قضایی جدید است. قوانین سنتی که بر شواهد فیزیکی و حضور مرتکب مبتنی هستند، قادر به پاسخگویی به این نوع جرائم نیستند. به همین دلیل، بسیاری از کشورها در حال بازنگری و توسعه قوانین دیجیتال و سایبری هستند تا بتوانند به شکل موثری مسئولیت افراد را در فضای غیرمادی شناسایی و تعقیب کنند. همچنین، این ویژگی جرائم سایبری، اهمیت علم دیجیتال و تحلیل داده‌ها در فرآیندهای تحقیقاتی و قضایی را افزایش داده است.

۲-گستردگی و سرعت: خسارت قابل توجه در زمان کوتاه

ویژگی دیگر جرائم سایبری، توانایی آن‌ها در ایجاد خسارت گسترده و سریع است. برخلاف جرائم سنتی که اغلب محدود به زمان، مکان و تعداد قربانیان هستند، جرائم سایبری می‌توانند در کوتاه‌ترین زمان ممکن، دامنه وسیعی از قربانیان و نهادها را تحت تأثیر قرار دهند. به بیان دیگر، یک حمله سایبری می‌تواند همزمان بر هزاران نفر، شرکت یا سازمان در مناطق جغرافیایی مختلف اثر بگذارد، بدون آنکه مرتکب نیازی به حضور فیزیکی داشته باشد. سرعت انتشار آثار جرائم سایبری به واسطه فناوری‌های دیجیتال و شبکه‌های اینترنتی افزایش می‌یابد. برای مثال، انتشار بدافزارها یا ویروس‌های رایانه‌ای می‌تواند در عرض چند دقیقه هزاران سیستم را آلوده کند و خسارات اقتصادی و عملیاتی قابل توجهی ایجاد کند. این ویژگی باعث می‌شود که واکنش فوری و اقدامات پیشگیرانه برای مهار آسیب‌ها اهمیت حیاتی پیدا کند، زیرا تأخیر حتی چند ساعت در پاسخگویی می‌تواند خسارات را به شدت افزایش دهد (Miri, 2025).

گستردگی و سرعت جرائم سایبری همچنین باعث پیچیدگی در تعیین میزان خسارت و نحوه جبران آن می‌شود. خسارات اقتصادی می‌توانند از دست رفتن سرمایه، اختلال در عملیات تجاری، کاهش اعتماد مشتریان و حتی افت ارزش بازار سهام ناشی شوند. خسارات غیرمادی مانند افشای اطلاعات شخصی یا اسناد محرمانه نیز می‌توانند تبعات قانونی و اجتماعی گسترده‌ای ایجاد کنند که جبران آن دشوار است. این ویژگی‌ها همچنین چالش‌های جدیدی برای سیاست‌گذاران و مقامات قضایی ایجاد کرده است. نیاز به تدوین پروتکل‌های واکنش سریع، ایجاد سیستم‌های مانیتورینگ و تحلیل داده‌ها و طراحی مقررات منع گسترش بدافزارها و حملات سایبری، از جمله الزامات مهم در مقابله با این نوع جرائم است (Vahbi, 2023).

گستردگی و سرعت جرائم سایبری، بر اهمیت همکاری‌های بین‌المللی و ایجاد سازوکارهای هماهنگ برای مقابله با تهدیدات دیجیتال تأکید می‌کند.

۳-ابهام مسئولیت: دشواری تعیین عامل انسانی و قصد

یکی از پیچیده‌ترین مسائل در حوزه جرائم سایبری، ابهام مسئولیت است. این ابهام ناشی از دشواری تعیین عامل انسانی و قصد مرتکب است. در بسیاری از جرائم سایبری، عملیات به صورت خودکار توسط برنامه‌ها، ربات‌ها یا هوش مصنوعی انجام می‌شود و تشخیص اینکه آیا عامل انسانی به صورت مستقیم در ارتکاب جرم دخیل بوده، بسیار دشوار است. برای مثال، حمله‌ای که توسط بدافزار یا ربات ایجاد شده است، ممکن است به اشتباه از سوی قربانی به یک فرد خاص نسبت داده شود، در حالی که عامل انسانی در پشت پرده ناشناخته باقی می‌ماند. ابهام مسئولیت همچنین در زمینه تعیین قصد مرتکب نمود پیدا می‌کند. در جرائم سنتی، شواهد فیزیکی، شهادت شهود و سایر مدارک می‌توانند قصد و نیت مرتکب را روشن کنند. اما در فضای سایبری، شواهد اغلب دیجیتال، پراکنده و به راحتی دستکاری‌پذیر هستند. بنابراین، تشخیص

اینکه آیا رفتار عامل با قصد سوء و آگاهی کامل انجام شده یا صرفاً ناشی از بی‌احتیاطی یا سوءاستفاده از آسیب‌پذیری‌های سیستم بوده، چالش بزرگی است (Mouraj & Akhtari, 2024).

ابهام مسئولیت، اثر مستقیم بر روندهای قضایی و قانونی دارد. قوانین سنتی که بر اصل قصد و عمل فیزیکی مبتنی هستند، ممکن است در مواجهه با جرائم سایبری ناکارآمد باشند. برای مثال، تعیین مسئولیت در مورد حملات گسترده سایبری که با استفاده از شبکه‌های پیچیده‌ای از سیستم‌ها انجام شده‌اند، نیازمند تحلیل‌های تخصصی فنی و حقوقی است. این امر باعث شده تا مفهوم «مسئولیت قانونی دیجیتال» و «مسئولیت نهادهای واسطه» مورد توجه قرار گیرد و قوانین جدیدی برای روشن کردن حدود مسئولیت تدوین شود. ابهام مسئولیت در جرائم سایبری باعث می‌شود که رویکرد پیشگیرانه و توسعه استانداردهای امنیتی و پروتکل‌های کنترل دسترسی اهمیت بیشتری پیدا کنند. از یک سو، تشخیص دقیق عامل جرم نیازمند فناوری‌های پیشرفته تحلیل داده و ردگیری دیجیتال است و از سوی دیگر، قوانین باید به گونه‌ای طراحی شوند که بدون شواهد فیزیکی محکم، نتایج قانونی عادلانه‌ای حاصل شود. این ترکیب، پیچیدگی ویژه‌ای به نظام حقوقی و قضایی تحمیل می‌کند که تنها با تعامل میان حقوق، فناوری و امنیت سایبری قابل مدیریت است (Paridar, 2025).

چالش‌های حقوقی و فقهی در مواجهه با هوش مصنوعی و فناوری‌های نوین

۱-ارتکاب جرم توسط سیستم‌های خودکار

در عصر معاصر، فناوری‌های هوش مصنوعی و سیستم‌های خودکار توانسته‌اند مرزهای سنتی مسئولیت و کنش انسانی را به طرز چشمگیری تغییر دهند. این سیستم‌ها قادرند بر اساس داده‌های ورودی، تحلیل‌های آماری و الگوریتم‌های پیشرفته، تصمیماتی اتخاذ کنند که تأثیر مستقیم بر زندگی انسان‌ها و امنیت جامعه دارند. این وضعیت موجب شکل‌گیری پرسش‌های بنیادین درباره مسئولیت کیفری و مسئولیت مدنی شده است، زیرا چارچوب‌های سنتی حقوقی و فقهی که بر اساس اراده و اختیار انسانی طراحی شده‌اند، به طور کامل قابلیت پوشش عملکرد مستقل ماشین‌ها را ندارند. از دیدگاه حقوق کیفری، مسئولیت تنها متوجه شخصی است که با قصد و آگاهی عمل می‌کند، اما وقتی یک سیستم خودکار تصمیمی می‌گیرد که منجر به صدمه جانی، مالی یا اخلاقی می‌شود، سوال اساسی این است که آیا می‌توان ماشین را به عنوان عامل جرم مورد مؤاخذه قرار داد یا خیر و اگر نه، مسئولیت چگونه بین طراح، توسعه‌دهنده، کاربر و مدیر سیستم تقسیم می‌شود (Keyvanpour et al., 2019).

از منظر فقه اسلامی، مسئولیت کیفری و مؤاخذه تنها بر انسان عاقل و مختار قابل اعمال است. اصولی مانند "العقل یقتضی المسؤولیة" و "لا یعذّر الجاهل" نشان می‌دهند که تنها کسی که دارای درک، شعور و توانایی تشخیص بین حق و باطل باشد، می‌تواند مورد مؤاخذه قرار گیرد. در مقابل، ماشین‌ها و سیستم‌های خودکار فاقد اراده، شعور و اختیار هستند؛ بنابراین نمی‌توان مستقیماً آن‌ها را مسئول جرم دانست. با این حال، این سیستم‌ها قابلیت انجام اعمالی را دارند که نتیجه آن‌ها منجر به ضرر و آسیب می‌شود و این امر چارچوب‌های فقهی سنتی را به چالش می‌کشد. در پاسخ به این مسئله، برخی فقه معاصر تلاش کرده‌اند با استفاده از اصول کلی فقه مانند "سدّ الذرائع" و "ضرر یزال"، مسئولیت عمل ناشی از فناوری‌های هوشمند را از طریق واسطه‌های انسانی تعریف کنند، به گونه‌ای که کنترل و نظارت انسان بر سیستم به معیار اصلی مسئولیت تبدیل شود (Mirshekarloo et al., 2025).

یک جنبه بسیار مهم دیگر، پیش‌بینی و جلوگیری از ارتکاب جرم توسط سیستم‌های خودکار است. سیستم‌های هوشمند، به ویژه آن‌هایی که مبتنی بر یادگیری ماشین هستند، قابلیت تکامل و بهبود عملکرد خود را دارند، که این ویژگی می‌تواند بدون دخالت مستقیم انسان به نتایج

غیرمنتظره و آسیب‌زا منجر شود. این امر ضرورت ایجاد چارچوب‌های پیشگیرانه و کنترلی را افزایش می‌دهد، به‌گونه‌ای که نه تنها پس از وقوع جرم، بلکه پیش از وقوع آن، از اعمال خطرناک جلوگیری شود. در فقه اسلامی، این موضوع با اصل "المفسدة تقدم علی المصلحة" قابل تطبیق است، به این معنا که جلوگیری از ضرر باید مقدم بر بهره‌برداری و توسعه فناوری باشد. بنابراین، هم حقوق کیفری و هم فقه اسلامی، بر ضرورت ایجاد سیستم‌های نظارتی، معیارهای ایمنی و مکانیزم‌های پیشگیرانه برای فناوری‌های خودکار تأکید می‌کنند (Zandi & Rafiei Alavi, 2024).

علاوه بر مسائل کیفری، پیامدهای اخلاقی و اجتماعی ناشی از تصمیمات سیستم‌های خودکار نیز قابل توجه است. تصمیماتی که الگوریتم‌ها اتخاذ می‌کنند می‌تواند شامل تبعیض‌های ناعادلانه، نقض حقوق شهروندی یا تأثیر منفی بر اقتصاد و محیط زیست باشد. بنابراین، لازم است چارچوب‌های حقوقی و فقهی با رویکردی جامع و چندلایه، نه تنها مسئولیت مستقیم بلکه مسئولیت ناشی از تأثیرات غیرمستقیم این سیستم‌ها را نیز در نظر بگیرند. ایجاد چنین چارچوبی نیازمند تعامل میان علوم حقوق، فقه، اخلاق فناوری، مهندسی سیستم‌ها و جامعه‌شناسی است تا بتوان به یک مدل مسئولیت جامع و قابل اجرا دست یافت.

۲-مسئولیت مدیران و طراحان هوش مصنوعی

یکی از پیچیده‌ترین مسائل حقوقی و فقهی مرتبط با هوش مصنوعی، مسئله مسئولیت مدیران، طراحان و توسعه‌دهندگان این فناوری‌ها است. حتی اگر سیستم‌های خودکار توانایی تصمیم‌گیری مستقل داشته باشند، مسئولیت نهایی برای طراحی، توسعه، راه‌اندازی و نظارت بر عملکرد آن‌ها به انسان‌ها بازمی‌گردد. این موضوع از دیدگاه حقوق مدنی تحت عناوینی مانند قصور حرفه‌ای، سهل‌انگاری یا مسئولیت ناشی از غفلت بررسی می‌شود و در حقوق کیفری نیز تحت عنوان مسئولیت ناشی از تسهیل جرم یا کوتاهی در کنترل اعمال سیستم مطرح است. این مسئله در حوزه‌هایی مانند خودروهای خودران، روبات‌های پزشکی، سیستم‌های معاملاتی الگوریتمی و سامانه‌های امنیتی اهمیت ویژه‌ای پیدا می‌کند، زیرا عملکرد نادرست یا خطای سیستم می‌تواند پیامدهای گسترده و جبران‌ناپذیری داشته باشد (Hosseini, 2024).

در فقه اسلامی، مسئولیت طراحان و مدیران سیستم‌های هوش مصنوعی را می‌توان بر اساس اصل "التسبیب یوجب المسؤولیة" توضیح داد، به این معنا که هر کس با اقدام یا ترک اقدام خود سبب ضرر دیگری شود، مسئول شناخته می‌شود. این اصل می‌تواند شامل طراحان الگوریتم، مدیران پروژه‌های هوش مصنوعی و حتی نهادهای قانونی ناظر بر این سیستم‌ها شود. به عبارت دیگر، حتی اگر خود سیستم هیچ اراده‌ای ندارد، مسئولیت ناشی از اعمال انسان‌ها که آن سیستم را طراحی، کنترل یا بهره‌برداری می‌کنند، همچنان برقرار است. این امر باعث می‌شود که توجه ویژه به رعایت استانداردهای فنی، اخلاقی و قانونی در مرحله طراحی و پیاده‌سازی به یک الزام حیاتی تبدیل شود (Rostami Zabol, 2025).

از منظر حقوق تطبیقی، کشورهای مختلف با ایجاد چارچوب‌هایی مانند مسئولیت مبتنی بر کنترل و مسئولیت مبتنی بر خطر تلاش کرده‌اند مسئولیت طراحان و بهره‌برداران فناوری‌های هوشمند را روشن کنند. این چارچوب‌ها نه تنها شامل مسئولیت قانونی بلکه شامل الزامات بیمه، الزامات شفافیت و گزارش‌دهی و استانداردهای ایمنی فنی می‌شوند. به این ترتیب، یک مدیر یا توسعه‌دهنده سیستم هوش مصنوعی نمی‌تواند مسئولیت عملکرد سیستم را نادیده بگیرد، حتی اگر خود مستقیماً اقدامی انجام نداده باشد. فقه اسلامی نیز با بهره‌گیری از اصولی مانند پیشگیری از ضرر و رعایت عدالت، مسیر مشابهی برای تعیین مسئولیت انسانی در مقابل فناوری‌های نوین ارائه می‌دهد (Paridar, 2025).

علاوه بر جنبه حقوقی و فقهی، مسئولیت طراحان و مدیران با ابعاد اخلاقی و اجتماعی نیز گره خورده است. توسعه‌دهندگان باید پیش‌بینی کنند که تصمیمات سیستم‌های هوشمند ممکن است چه تأثیراتی بر حقوق شهروندان، عدالت اجتماعی و امنیت عمومی داشته باشد. بر این اساس، مسئولیت انسان در قبال فناوری‌های نوین تنها یک الزام قانونی نیست، بلکه یک وظیفه اخلاقی و دینی نیز محسوب می‌شود که رعایت آن برای حفاظت از جامعه و کاهش آسیب‌های ناشی از فناوری ضروری است.

۳-نیاز به قواعد تطبیقی فقهی برای شمول فناوری‌های نوین

ظهور فناوری‌های نوین و پیچیدگی‌های ناشی از هوش مصنوعی، روباتیک و سامانه‌های خودکار، نظام حقوقی و فقهی موجود را با محدودیت‌های جدی مواجه ساخته است. قواعد سنتی حقوقی و فقهی عمدتاً برای رفتار انسانی، کنش‌های اخلاقی و شرایط کلاسیک جامعه طراحی شده‌اند و نمی‌توانند به طور کامل پیچیدگی‌ها و پیامدهای تصمیمات مستقل سیستم‌های هوشمند را پوشش دهند. بنابراین، ایجاد قواعد تطبیقی فقهی برای شمول فناوری‌های نوین یک ضرورت اجتناب‌ناپذیر است. این قواعد باید توانایی پاسخگویی به مسائل نوین مانند مسئولیت سیستم‌های خودکار، پیامدهای اخلاقی تصمیمات الگوریتمی، تبعیض ناشی از داده‌های آماری و چالش‌های امنیتی و حریم خصوصی را داشته باشند (Mirshekarloo et al., 2025).

از منظر فقه اسلامی، ایجاد قواعد تطبیقی می‌تواند با تکیه بر اصول کلی مانند حفظ جان و مال، جلوگیری از ضرر، رعایت عدالت و مصالح عمومی صورت گیرد. اصولی مانند "لا ضرر و لا ضرار" و "سدّ الذرائع" قابلیت انعطاف‌پذیری لازم برای تطبیق با فناوری‌های نوین را دارند. برای مثال، اصل منع ضرر می‌تواند به عنوان مبنای وضع مقرراتی برای محدود کردن رفتارهای خطرناک سیستم‌های هوشمند و تعیین معیارهای ایمنی و نظارت بر طراحی الگوریتم‌ها به کار رود. این رویکرد باعث می‌شود فقه اسلامی بتواند با حفظ اصول بنیادین خود، پاسخگوی تحولات فناورانه و اجتماعی معاصر باشد (Vahabi Hashemabad & Nouri, 2025).

در سطح بین‌المللی نیز کشورهای پیشرو در زمینه فناوری، اقدام به تدوین قوانین خاص برای هوش مصنوعی، روباتیک و فناوری‌های پیشرفته کرده‌اند که بر شفافیت، پاسخگویی، امنیت و حقوق شهروندان تأکید دارند. این رویکرد می‌تواند به عنوان الگویی برای توسعه قواعد تطبیقی فقهی مورد استفاده قرار گیرد. همچنین، قواعد تطبیقی باید به گونه‌ای تدوین شوند که مسئولیت طراحان، مدیران و کاربران سیستم‌های هوشمند مشخص و قابل پیگیری باشد و چارچوبی برای پیشگیری و جبران خسارت فراهم کنند. تعامل مستمر میان فقه، حقوق، فناوری و اخلاق می‌تواند موجب شکل‌گیری یک نظام جامع و قابل اجرا برای شمول فناوری‌های نوین شود و اطمینان دهد که نوآوری با رعایت حقوق انسان‌ها و مصالح جامعه همسو باشد.

مسئولیت کیفری در فقه امامیه

۱-مبانی مسئولیت

مسئولیت کیفری در فقه امامیه بر پایه اصولی بنیادی و مستحکم استوار است که محور اصلی آن، اراده و علم فرد است. از نظر فقه شیعه، هیچ‌گونه مجازاتی بدون وجود قصد و اختیار فرد قابل اعمال نیست. این اصل، بر پایه آیات قرآن و روایات اهل بیت(ع) بنا شده است و به وضوح بیان می‌کند که انسان تنها زمانی مسئول اعمال خود است که قادر به تشخیص صحیح از ناصحیح باشد و عمل خود را بر اساس اراده و اختیار انجام دهد. به بیان دیگر، وجود قصد و علم، شرط اولیه و لازم برای مسئولیت کیفری است. در فقه امامیه، این مفهوم تحت عنوان

«قصد و اختیار» مورد بررسی قرار گرفته و اهمیت آن در تعیین میزان مجازات و نوع مسئولیت بسیار برجسته است (Rostami Zabol, 2025).

قصد و اختیار در فقه امامیه نه تنها به اراده فرد محدود نمی‌شود، بلکه شامل شناخت و درک عواقب عمل نیز هست. فرد باید بداند که عملی که انجام می‌دهد، موجب ضرر یا نقض حقوق دیگران می‌شود و بر اساس همین آگاهی، اقدام خود را انجام دهد. بدون این آگاهی و اراده آزاد، مسئولیت کیفری منتفی است. به همین دلیل، فقها تاکید دارند که کسی که به‌صورت ناخواسته یا نادانسته مرتکب جرمی می‌شود، مسئولیت کیفری ندارد، مگر در مواردی که ترک علم و بی‌توجهی او باعث وقوع جرم شده باشد. این رویکرد، زمینه‌ساز ایجاد مفهوم مسئولیت تعلیلی در فقه امامیه نیز شده است (Mohaqeq Damad, 2021).

در کنار اراده و قصد، فقه امامیه مفهوم «مسئولیت ابزار و واسطه» را مطرح می‌کند. به این معنا که استفاده از ابزار یا واسطه برای ارتکاب جرم، مسئولیت انسانی را از میان نمی‌برد. اگر چه ابزار می‌تواند عامل مستقیم در ارتکاب عمل مجرمانه باشد، ولی عامل انسانی همچنان مسئول عمل است (Shojai Langari, 2024).

این اصل اهمیت ویژه‌ای در زمینه جرائم سایبری دارد، زیرا در دنیای دیجیتال و هوش مصنوعی، سامانه‌ها و ربات‌ها به‌عنوان ابزار عمل می‌کنند، اما مسئولیت ناشی از عملکرد آن‌ها همچنان به گردن انسان است. در فقه امامیه، این موضوع به‌خوبی با اصول سنتی مسئولیت انسانی هماهنگ است و اجازه می‌دهد مسئولیت کیفری در برابر فناوری‌های نوین نیز اعمال شود.

به طور کلی، مبانی مسئولیت کیفری در فقه امامیه شامل ترکیبی از قصد و اختیار، مسئولیت ابزار و واسطه و مسئولیت تعلیلی است که زمینه را برای بررسی پیچیده‌ترین رفتارهای انسان و حتی اقدامات غیرمستقیم فراهم می‌کند. این اصول، به‌ویژه در فضای مجازی و جرائم سایبری، قابلیت انطباق بالایی دارند و می‌توانند به‌عنوان مبنایی برای تحلیل و تبیین مسئولیت کیفری در مواجهه با فناوری‌های هوشمند مورد استفاده قرار گیرند.

۲-کاربرد در جرائم سایبری

فقه امامیه با پذیرش مسئولیت غیرمستقیم، ظرفیت مناسبی برای انطباق با جرائم ناشی از فناوری‌های هوشمند و هوش مصنوعی دارد. در این رویکرد، فرد تنها زمانی مسئول نیست که هیچ دخالتی در عمل صورت نگرفته باشد، حتی اگر اقدام به‌صورت خودکار توسط سامانه‌های هوشمند انجام شده باشد. این مفهوم، در دنیای جرائم سایبری بسیار کاربردی است، زیرا بسیاری از عملیات دیجیتال و هک‌ها توسط الگوریتم‌ها و ربات‌ها انجام می‌شوند، اما مالک یا کاربر اصلی سیستم همچنان مسئول عواقب آن است. به‌عنوان مثال، مالک یک سامانه هک هوشمند که قابلیت اجرای حملات خودکار را دارد، حتی در صورتی که ربات بدون دخالت مستقیم او اقدام به نفوذ به سیستم‌های دیگر کند، مسئول شناخته می‌شود. فقه امامیه در این زمینه تأکید دارد که عدم دخالت مستقیم انسان، دلیل بر عدم مسئولیت نیست، زیرا عمل با اختیار و برنامه‌ریزی انسانی شکل گرفته و پیامدهای آن قابل پیش‌بینی است. این اصل، نوعی پاسخ عملی به چالش‌های حقوقی ناشی از هوش مصنوعی و فناوری‌های دیجیتال فراهم می‌کند (Paridar, 2025).

کاربرد فقه امامیه در جرائم سایبری تنها به مالکیت سامانه محدود نمی‌شود، بلکه شامل افرادی است که سیستم‌های هوشمند را مدیریت، برنامه‌ریزی و هدایت می‌کنند. مسئولیت کیفری در این حوزه شامل بررسی قصد، علم به پیامدها و کنترل انسانی است. حتی اگر عمل مجرمانه توسط الگوریتم‌ها انجام شود، فقدان نظارت یا سوءاستفاده از سیستم، مسئولیت کیفری ایجاد می‌کند. این رویکرد، امکان مقابله با تهدیدات

سایبری پیچیده را فراهم کرده و خلا قانونی ناشی از خودکار بودن جرائم را پر می‌کند. از سوی دیگر، فقه امامیه با پذیرش مسئولیت، قابلیت پوشش جرائم غیرمستقیم و پیامدهای غیرقابل پیش‌بینی را دارد. به این ترتیب، اگر عملکرد یک سامانه هوش مصنوعی باعث خسارت مالی یا نقض حقوق دیگران شود، عامل انسانی مسئول خواهد بود، حتی اگر قصد مستقیم ایجاد آن پیامدها را نداشته باشد. این اصل، تمایز فقه امامیه را با دیدگاه‌های محدودتر مسئولیت کیفری مشخص می‌کند و آن را به یک ابزار انعطاف‌پذیر برای تحلیل جرائم سایبری تبدیل می‌کند (Vahabi Hashemabad & Nouri, 2025).

کاربرد مبانی فقه امامیه در جرائم سایبری، با تأکید بر قصد، اختیار، مسئولیت ابزار و مسئولیت، امکان انطباق با پیچیده‌ترین رفتارهای دیجیتال و هوش مصنوعی را فراهم می‌آورد. این چارچوب، نه تنها قابلیت پیشگیری از جرائم را دارد، بلکه زمینه ایجاد سازوکارهای قانونی و قضایی متناسب با فناوری‌های نوین را نیز فراهم می‌کند و می‌تواند به‌عنوان یک مبنای نظری و عملی در نظام کیفری مدرن مورد استفاده قرار گیرد.

۳-نمونه‌های عملی

الف-جرائم مالی دیجیتال: جرائم مالی دیجیتال، یکی از بارزترین حوزه‌هایی است که مسئولیت کیفری فقه امامیه در آن قابل اعمال است. این جرائم شامل سرقت ارزهای دیجیتال، کلاهبرداری اینترنتی، جعل دیجیتال و سوءاستفاده از حساب‌های بانکی آنلاین می‌شوند. در فقه امامیه، فردی که با استفاده از سامانه‌های دیجیتال اقدام به سرقت یا کلاهبرداری می‌کند، مسئول عمل خود است، حتی اگر سیستم به‌صورت خودکار بخش‌هایی از فرایند را انجام دهد. این مسئولیت، بر اساس قصد و علم فرد و همچنین نقش وی در برنامه‌ریزی یا راه‌اندازی سامانه تعیین می‌شود (Vatankhah, 2025).

ب-حملات سایبری از طریق ربات‌ها و الگوریتم‌های هوشمند: حملات سایبری خودکار که توسط ربات‌ها و الگوریتم‌های هوشمند انجام می‌شوند، چالش مهمی در عرصه حقوق کیفری مدرن هستند. فقه امامیه با پذیرش مسئولیت تعلیلی، اجازه می‌دهد مالک یا برنامه‌ریز این سامانه‌ها مسئول شناخته شود، حتی اگر عمل مستقیماً توسط ربات انجام شده باشد. برای مثال، حمله‌ای که باعث اختلال در سامانه‌های بانکی یا شبکه‌های ارتباطی می‌شود، می‌تواند مسئولیت کیفری مالک یا توسعه‌دهنده ربات را در پی داشته باشد، زیرا پیامد عمل قابل پیش‌بینی بوده و کنترل آن از طریق ابزار انسانی امکان‌پذیر است.

ج-انتشار محتوای مجرمانه توسط سامانه‌های خودکار: یکی دیگر از نمونه‌های عملی، انتشار محتوای مجرمانه مانند اخبار جعلی، محتوای توهین‌آمیز یا فایل‌های غیرقانونی توسط سامانه‌های خودکار است. در این موارد، مسئولیت کیفری طبق فقه امامیه بر عهده فردی است که سامانه را راه‌اندازی کرده یا آن را مدیریت می‌کند. حتی اگر عمل خودکار سامانه بدون دخالت مستقیم انسان صورت گیرد، مالک یا مدیر سیستم به دلیل علم به پیامدهای احتمالی و عدم کنترل، مسئول شناخته می‌شود. این رویکرد، امکان پاسخ‌گویی به تهدیدات گسترده دیجیتال و پیشگیری از انتشار محتوای مجرمانه را فراهم می‌کند (Shojai Langari, 2024).

بنابراین، نمونه‌های عملی نشان می‌دهند که فقه امامیه با اصول مسئولیت کیفری شامل قصد و اختیار، مسئولیت ابزار و مسئولیت تعلیلی، توانایی انطباق با جرائم نوظهور سایبری را دارد. این چارچوب نظری، می‌تواند به شکل‌دهی سیاست‌های کیفری مدرن، تدوین قوانین مرتبط با هوش مصنوعی و سامانه‌های دیجیتال و آموزش قضات و حقوقدانان در زمینه مسئولیت کیفری فناوری‌های نوین کمک شایانی کند و تضمین‌کننده عدالت و پاسخ‌گویی قانونی در فضای دیجیتال باشد.

مسئولیت کیفری در فقه مالکی

۱-اصول بنیادین

الف-ارتباط مستقیم عمل و قصد: در فقه مالکی، یکی از اصول بنیادین مسئولیت کیفری، ارتباط مستقیم میان عمل و قصد مرتکب است. به این معنا که مسئولیت کیفری تنها متوجه کسی خواهد بود که شخصاً اقدام به انجام عمل مجرمانه کرده و قصد ارتکاب آن را داشته است. این اصل ریشه در آموزه‌های قرآنی و سنت پیامبر دارد که تأکید دارند «نیت» و «عمل» دو رکن اساسی برای تعیین گناه و مسئولیت هستند. در این چارچوب، عمل فیزیکی بدون قصد مجرمانه نمی‌تواند منجر به مسئولیت کیفری شود. برای مثال، اگر فردی به طور ناخواسته به دیگری آسیب برساند یا مرتکب خطای غیرعمد شود، مسئولیت کیفری بر او مترتب نخواهد بود، مگر اینکه بتوان قصد یا سوءنیت را ثابت کرد. همچنین، فقه مالکی در بررسی قصد، بین قصد عمدی و غیرعمدی تمایز قائل است. عمد به معنای ارتکاب آگاهانه عمل مجرمانه و همراه با دانش از حرام بودن آن است، در حالی که غیرعمد بیشتر به اعمال ناشی از سهو، خطا یا بی‌احتیاطی اطلاق می‌شود.

در نتیجه، مسئولیت کیفری تنها زمانی متوجه فرد خواهد بود که بین قصد و عمل پیوند منطقی و مستقیم برقرار شود. این ارتباط، معیار اصلی برای تمایز مسئولیت کیفری از مسئولیت مدنی یا اخلاقی در فقه مالکی است و موجب می‌شود سیستم کیفری بر عدالت و رعایت حق انسان‌ها استوار باشد.

علاوه بر این، فقه مالکی، تفاوت میان عمل شخصی و عمل توسط دیگران را نیز روشن می‌کند. اگر عملی توسط شخص ثالث یا فردی دیگر انجام شود، تنها در صورتی مسئولیت متوجه فرد خواهد شد که نقش فعال یا تسهیل‌کننده در ارتکاب عمل مجرمانه داشته باشد. این اصل در راستای جلوگیری از مسئولیت غیرمنصفانه و بی‌ارتباط با عمل واقعی وضع شده است و نشان‌دهنده محدودیت دامنه مسئولیت کیفری بر اساس ارتباط مستقیم عمل و قصد است (Ibn Qudamah al-Maqdisi, 1993).

ب-محدودیت در ابزار و واسطه‌ها: اصل دیگر در فقه مالکی، محدودیت مسئولیت در استفاده از ابزار و واسطه‌ها است. طبق این اصل، فرد تنها زمانی مسئول عمل ارتکابی است که خود آن عمل را انجام داده یا به‌طور مستقیم در تحقق آن دخالت داشته باشد. در صورتی که عمل مجرمانه توسط ابزار یا وسیله‌ای خودکار یا توسط شخص ثالث صورت گیرد، مسئولیت کیفری مرتکب اصلی محدود خواهد بود و در برخی موارد حتی به‌طور کامل از میان می‌رود. این محدودیت بر پایه عدالت فقهی و پیشگیری از مجازات‌های ناعادلانه استوار است و به‌ویژه در شرایطی که ابزارها و وسایل پیچیده یا خودکار دخیل باشند، اهمیت بیشتری پیدا می‌کند. به‌عنوان مثال، در فقه مالکی، اگر شخصی وسیله‌ای را در اختیار دیگری قرار دهد که به‌طور مستقیم به آسیب منجر شود، مسئولیت کیفری تنها زمانی متوجه او خواهد بود که قصد سوء استفاده یا دانش از نتایج آسیب‌زا وجود داشته باشد. در غیر این صورت، مسئولیت صرفاً اخلاقی یا مدنی مطرح می‌شود و از شمول کیفری خارج است. این محدودیت نشان می‌دهد که فقه مالکی بر مبنای عدالت فردی و ارتباط مستقیم با عمل تاکید دارد و از توسعه مسئولیت به واسطه‌ها و ابزارهای خودکار یا غیرمستقیم جلوگیری می‌کند (Vatankhah, 2025).

مفهوم محدودیت مسئولیت در ابزارها و واسطه‌ها، در مواجهه با فناوری‌های پیشرفته و سیستم‌های خودکار اهمیت بیشتری پیدا می‌کند، زیرا در چنین محیط‌هایی تشخیص عمل مستقیم از عمل غیرمستقیم و نقش واقعی انسان در وقوع جرم پیچیده‌تر می‌شود. این اصل فقهی، پایه و اساس بررسی چالش‌های مسئولیت کیفری در عصر فناوری‌های نوین و هوش مصنوعی را تشکیل می‌دهد.

۲-چالش‌ها در عصر هوش مصنوعی

الف-شمول محدود برای جرائم غیرمستقیم و خودکار: با ورود فناوری‌های نوین مانند هوش مصنوعی، اینترنت اشیاء و سیستم‌های خودکار، چارچوب‌های سنتی مسئولیت کیفری فقه مالکی با چالش‌های جدی مواجه شده‌اند. یکی از مهم‌ترین مسائل، شمول محدود مسئولیت برای جرائم غیرمستقیم و خودکار است. در بسیاری از جرائم سایبری و فناوری محور، عمل مجرمانه مستقیماً توسط انسان صورت نمی‌گیرد، بلکه توسط الگوریتم‌ها، ربات‌ها یا سیستم‌های خودکار انجام می‌شود. در این سناریو، پیوند مستقیم بین قصد و عمل که اساس مسئولیت کیفری در فقه مالکی است، به‌طور طبیعی تضعیف می‌شود. شخصی که سیستم خودکاری را راه‌اندازی می‌کند که به دیگران آسیب می‌رساند، ممکن است قصد مستقیم ارتکاب جرم را نداشته باشد، زیرا عمل واقعی توسط ماشین یا الگوریتم انجام می‌شود. بنابراین، چارچوب سنتی مسئولیت کیفری قادر به پوشش کامل چنین جرائمی نیست و خلأ قانونی و فقهی ایجاد می‌کند. این محدودیت، ضرورت بازنگری و توسعه اصول و قواعد فقهی برای انطباق با فناوری‌های مدرن را آشکار می‌سازد (Tahmasebi, 2006).

ب-دشواری اثبات قصد در ارتکاب جرائم سایبری: یکی دیگر از چالش‌های کلیدی در عصر دیجیتال، اثبات قصد در جرائم سایبری است. در فقه مالکی، قصد ارتکاب جرم یکی از ارکان اساسی مسئولیت کیفری است، اما در فضای مجازی، تشخیص قصد واقعی فرد دشوار می‌شود. بسیاری از جرائم سایبری شامل عملیات غیرمستقیم، ارسال خودکار داده‌ها یا حملات پیچیده هستند که امکان تعیین مستقیم قصد ارتکاب را محدود می‌کنند. برای مثال، هکری که از یک شبکه خودکار برای نفوذ استفاده می‌کند، ممکن است هدف نهایی مشخصی داشته باشد، اما عمل فیزیکی و مستقیم او توسط ابزارها و واسطه‌های دیجیتال انجام می‌شود. این وضعیت باعث می‌شود سیستم قضایی و فقهی بر اساس رویکرد سنتی با کمبود شواهد و پیچیدگی‌های اثبات نیت مواجه شود. در نتیجه، مسئولیت کیفری ممکن است محدود یا حتی غیرقابل اعمال شود، که این موضوع فشار بر قوانین و رویکردهای نوین قضایی برای انطباق با جرائم دیجیتال را افزایش می‌دهد (Azimi & Esmaeili, 2021).

ج-نیاز به توسعه قواعد برای انطباق با فناوری: با توجه به محدودیت‌ها و چالش‌های فوق، ضروری است که قواعد مسئولیت کیفری در فقه مالکی برای انطباق با فناوری‌های نوین توسعه یابند .این توسعه می‌تواند شامل تعریف دقیق‌تر مسئولیت برای اعمال غیرمستقیم، ایجاد معیارهای جدید برای تعیین قصد در جرائم خودکار و شمول برخی از جرائم سایبری تحت عنوان «مسئولیت تسهیل‌کننده» باشد.

در این مسیر، فقه مالکی می‌تواند با استفاده از اصول عمومی مانند عدالت، منع ضرر و رعایت حقوق دیگران، چارچوبی ارائه دهد که هم ماهیت سنتی مسئولیت کیفری را حفظ کند و هم با واقعیت‌های فناوری هماهنگ شود. بدون این اصلاحات، فقه مالکی در مواجهه با پیچیدگی‌های هوش مصنوعی و جرائم سایبری ناتوان از پاسخگویی کافی خواهد بود و این موضوع می‌تواند به شکاف میان عدالت فقهی و نیازهای جامعه مدرن منجر شود.

پیامدهای محدودیت‌ها

الف-کمبود پاسخ قانونی در برابر جرائم خودکار: یکی از مهم‌ترین پیامدهای محدودیت‌های موجود در فقه، کمبود پاسخ قانونی در برابر جرائم خودکار است. سیستم‌های خودکار و هوش مصنوعی می‌توانند بدون دخالت مستقیم انسان اعمال مجرمانه‌ای انجام دهند، مانند حملات سایبری، سرقت داده، یا انتشار محتواهای آسیب‌زا. در چارچوب سنتی فقه مالکی، که بر ارتباط مستقیم بین عمل و قصد تاکید دارد، چنین جرائمی ممکن است خارج از شمول مسئولیت کیفری قرار گیرند و قربانیان از حمایت قضایی لازم برخوردار نشوند. این کمبود می‌تواند منجر به افزایش جرائم خودکار و بهره‌برداری مجرمان از خلأ قانونی شود. همچنین، فقدان پاسخ قانونی مناسب، اعتماد عمومی به سیستم قضایی و

چارچوب فقهی را کاهش می‌دهد و ضرورت تدوین مقررات مکمل یا تفسیرهای نوین از اصول فقهی را تقویت می‌کند (Vatankhah, 2025).

ب-عدم توانایی کامل برای شمول مسئولیت مدیران سامانه‌ها: محدودیت دیگر، عدم توانایی کامل در شمول مسئولیت مدیران سامانه‌ها است. در بسیاری از سیستم‌های فناوری محور، افراد یا سازمان‌ها نقش نظارتی یا مدیریتی دارند، اما عمل مجرمانه به‌طور مستقیم توسط سیستم یا الگوریتم انجام می‌شود. در فقه مالکی، مسئولیت کیفری تنها زمانی متوجه این مدیران خواهد بود که نقش مستقیم و قصد مجرمانه آنها ثابت شود، که در عمل اثبات آن دشوار است. این وضعیت باعث می‌شود که برخی از مدیران سامانه‌ها از مسئولیت کیفری فرار کنند، حتی اگر اقدام یا غفلت آنها منجر به وقوع جرایم گسترده شود. پیامد این محدودیت، ایجاد فشار برای توسعه مفاهیم نوین مسئولیت، از جمله مسئولیت مبتنی بر «غفلت از نظارت» یا «تسهیل غیرمستقیم جرم»، است تا سیستم قضایی بتواند با پیچیدگی‌های عصر هوش مصنوعی و فناوری‌های پیشرفته همگام شود (Vahabi Hashemabad & Nouri, 2025).

چالش‌ها و محدودیت‌های فقه مالکی در حوزه مسئولیت کیفری، ضرورت تبیین و بازنگری اصول بنیادین را روشن می‌سازد و نشان می‌دهد که برای مقابله با جرائم دیجیتال و خودکار، باید چارچوب‌های سنتی با دیدگاه‌های نوین و منعطف تلفیق شوند. چنین رویکردی می‌تواند عدالت فقهی را حفظ کرده و پاسخگویی قانونی مناسبی در عصر فناوری‌های پیشرفته فراهم آورد.

تحلیل تطبیقی

۱. اشتراکات فقه امامیه و مالکی

یکی از مهم‌ترین مسائل در حوزه تطبیقی فقهی، شناسایی نقاط اشتراک و تقارب میان مکاتب فقهی مختلف است، زیرا این اشتراکات می‌توانند مبنایی برای تدوین چارچوب‌های حقوقی معاصر، به ویژه در زمینه جرائم نوظهور مانند جرائم سایبری و مسئولیت‌های ناشی از فناوری‌های نوین، باشند. از میان فقه امامیه و مالکی، دو محور اساسی در تقارب این دو مذهب قابل شناسایی است: اهمیت قصد و علم در تعیین مسئولیت و رعایت عدالت و انصاف در اعمال مجازات. این محورها نه تنها در متون فقهی مورد تأکید قرار گرفته‌اند، بلکه در توسعه نظام‌های کیفری مدرن نیز قابلیت انتقال و انطباق دارند.

نخست، محور اهمیت قصد و علم در تعیین مسئولیت یکی از ویژگی‌های برجسته هر دو مذهب است. در فقه امامیه، مسئله نیت و قصد در اعمال فرد از جایگاه محوری برخوردار است و بدون احراز قصد، تحقق مسئولیت کیفری امری غیرممکن تلقی می‌شود. این اصل از دیدگاه فقهی مبتنی بر قاعده «لا ضرر و لا ضرار» و اصل «العمده فی الجرم النیّه» است و بر این اساس، مسئولیت تنها زمانی تحقق می‌یابد که عمل با علم و قصد مرتکب انجام شده باشد. به طور مشابه، در فقه مالکی نیز نیت فرد از اهمیت بالایی برخوردار است و بسیاری از اعمال کیفری صرفاً زمانی قابل مجازات تلقی می‌شوند که قصد ارتکاب جرم محرز شود. این اشتراک فقهی نشان می‌دهد که هر دو مذهب گرایش به عدالت و تأمین حقوق افراد دارند و مسئولیت صرفاً بر اساس نتیجه اعمال، بدون در نظر گرفتن قصد، تعیین نمی‌شود.

دوم، محور رعایت عدالت و انصاف در اعمال مجازات نیز در هر دو مذهب برجسته است. در فقه امامیه، مجازات‌ها به گونه‌ای طراحی شده‌اند که نه تنها جنبه تنبیهی داشته باشند، بلکه متناسب با شدت و نوع جرم و وضعیت مجرم باشند. این نگاه مبتنی بر قاعده فقهی «المیزان فی الشرع العدل» است و در آن، حکم به تعادل میان حقوق فرد و جامعه تأکید می‌شود. در فقه مالکی نیز عدالت و انصاف در اعمال حدود و تعزیرات مورد توجه است، اگرچه روش‌ها و مصادیق کمی متفاوت است، اما اصل کلی این است که مجازات‌ها باید منصفانه، متناسب و با

هدف اصلاح و پیشگیری اعمال شوند. این وجه اشتراک نشان می‌دهد که هر دو مذهب در صدد تحقق عدالت و پیشگیری از ظلم و بی‌عدالتی در جامعه هستند، موضوعی که در عصر دیجیتال و جرائم سایبری اهمیت مضاعف می‌یابد، زیرا آثار اعمال مجرمانه می‌تواند گسترده و نامحسوس باشد.

همچنین، این اشتراکات فقهی نشان‌دهنده قابلیت ایجاد چارچوب‌های قانونی تلفیقی هستند که بتوانند در زمینه‌های نوین مسئولیت‌های دیجیتال و هوش مصنوعی مورد استفاده قرار گیرند. به عبارت دیگر، اگر چه فقه امامیه و مالکی دارای تفاوت‌های جزئی در روش استنباط و مصادیق احکام هستند، اما مبانی عدالت، تأکید بر قصد و رعایت انصاف، می‌توانند به عنوان زیربنای یک نظام کیفری مدرن، بویژه در زمینه مسئولیت مدیران سامانه‌ها، تحلیل داده‌های خودکار و جرائم سایبری، مورد بهره‌برداری قرار گیرند.

۲. تفاوت‌ها

در کنار اشتراکات، تحلیل تطبیقی فقه امامیه و مالکی نشان می‌دهد که تفاوت‌های بنیادینی نیز میان این دو مذهب وجود دارد که در زمینه تطبیق با جرائم سایبری اهمیت ویژه‌ای پیدا می‌کند. برای روشن‌تر شدن این تفاوت‌ها، مقایسه‌ای با محورهای مشخص انجام می‌شود: مسئولیت غیرمستقیم، مسئولیت ابزار خودکار، انعطاف در تحلیل قصد و تطبیق با جرائم سایبری.

الف–مسئولیت غیرمستقیم: در فقه امامیه، مسئولیت غیرمستقیم پذیرفته شده است. به عبارت دیگر، فرد ممکن است در صورتی که اعمال دیگری را تسهیل یا موجبات آن را فراهم کرده باشد، مسئول شناخته شود، حتی اگر عمل غیرمستقیم بوده و مجرم اصلی شخص دیگری باشد. این رویکرد انعطاف‌پذیری لازم برای مواجهه با جرائم پیچیده و شبکه‌ای، از جمله جرائم سایبری، را فراهم می‌کند، زیرا در دنیای دیجیتال، بسیاری از اقدامات به واسطه فناوری و ابزارهای خودکار انجام می‌شود و مرتکب اصلی ممکن است ناشناخته یا دور از صحنه عمل باشد. در مقابل، فقه مالکی در پذیرش مسئولیت غیرمستقیم محدودیت دارد و اغلب مسئولیت صرفاً متوجه فرد مباشر و فاعل مستقیم است. این امر در برخورد با جرائم سایبری که شامل زنجیره‌ای از اقدامات غیرمستقیم و وابسته به فناوری است، چالش‌برانگیز می‌شود و امکان پیگرد قانونی تمام افراد دخیل در یک عملیات سایبری را محدود می‌سازد.

ب–مسئولیت ابزار خودکار: فقه امامیه قابلیت انطباق مسئولیت با ابزار خودکار را دارد. از آنجا که این مذهب نسبت به مقاصد و آثار عمل و رابطه فرد با ابزارها انعطاف بیشتری دارد، می‌توان در چارچوب آن مسئولیت مدیران سامانه‌ها، طراحان الگوریتم‌ها و برنامه‌نویسان را در جرائم سایبری تحلیل کرد. در مقابل، فقه مالکی در این زمینه محدود است و پذیرش مسئولیت برای ابزارهای خودکار و واسطه‌ای چندان متداول نیست، که می‌تواند موجب ایجاد خلأ قانونی در برابر تهدیدات فناوری‌های هوشمند شود.

ج–انعطاف در تحلیل قصد: انعطاف فقه امامیه در تحلیل قصد، بسیار بالا است. این مذهب به پیچیدگی‌های نیت و انگیزه افراد و اثرات اقدامات غیرمستقیم توجه دارد و امکان استنباط مسئولیت حتی در شرایط پیچیده، مانند اقدامات مبتنی بر هوش مصنوعی، فراهم است. در مقابل، فقه مالکی انعطاف کمتری دارد و تحلیل قصد معمولاً محدود به اقدامات مستقیم و ساده است. این محدودیت می‌تواند مانع از استنباط مسئولیت در موارد نوین، مانند حملات سایبری پیچیده، شود.

د–=تطبیق با جرائم سایبری: نتیجه نهایی این تفاوت‌ها در تطبیق با جرائم سایبری مشاهده می‌شود. فقه امامیه با تأکید بر قصد، مسئولیت غیرمستقیم و ابزارهای خودکار، مناسب برای چارچوب‌های قانونی مرتبط با فناوری و هوش مصنوعی است. اما فقه مالکی، با محدودیت‌های

خود، تطبیق با جرائم سایبری را دشوار و چالش‌برانگیز می‌سازد، به ویژه در مورد جرائم شبکه‌ای، نفوذهای دیجیتال و مسئولیت مدیران سامانه‌ها.

نتیجه‌گیری

ظهور فناوری‌های هوش مصنوعی و گسترش جرائم سایبری، تحول بنیادینی را در عرصه حقوق کیفری ایجاد کرده است؛ چرا که بسیاری از قواعد سنتی مسئولیت کیفری، که بر اعمال فیزیکی و قصد مستقیم متکی بودند، اکنون در مواجهه با پیچیدگی‌های فضای دیجیتال و سامانه‌های هوشمند ناکافی به نظر می‌رسند. هوش مصنوعی، با قابلیت تصمیم‌گیری مستقل و انجام اعمال بدون دخالت مستقیم انسان، پرسش‌های نوینی درباره عنصر مادی جرم، قصد و تقصیر ایجاد کرده و چارچوب‌های سنتی مسئولیت کیفری را به چالش کشیده است. در این زمینه، فقه امامیه با انعطاف در تحلیل قصد و پذیرش مسئولیت غیرمستقیم، توانایی پاسخگویی نسبی به این چالش‌ها را دارد و می‌تواند بر اساس اصولی مانند «لا ضرر» و «المسؤولیۀ عن الفعل» به تحلیل جرائم مبتنی بر فناوری‌های نوین بپردازد. در مقابل، فقه مالکی با تکیه بر قواعد سنتی‌تر و تمرکز بر مسئولیت مستقیم و اعمال فیزیکی، نیازمند بازنگری و توسعه قواعد برای شمول فناوری‌های نوین و جرائم سایبری است تا بتواند نقش مؤثری در تنظیم مسئولیت کیفری در عصر دیجیتال ایفا کند. این ضرورت، ایجاد نظام حقوقی تطبیقی را بیش از پیش ضروری می‌سازد؛ سیستمی که تلفیقی از اصول فقهی، قواعد سنتی و نیازهای روز جامعه دیجیتال باشد و بتواند همزمان عدالت کیفری و پاسخگویی به پیچیدگی‌های فناوری را تضمین کند. در این راستا، تحلیل تطبیقی میان فقه امامیه و فقه مالکی می‌تواند به شناسایی نقاط قوت و ضعف هر رویکرد و ارائه راهکارهای عملی برای تنظیم مسئولیت کیفری در جرائم هوش مصنوعی کمک کند. افزون بر این، توسعه چارچوب‌های قانونی که شامل تعاریف روشن از عامل هوشمند، سطح مسئولیت انسانی و معیارهای تشخیص قصد و تقصیر در فضای مجازی باشد، از اهمیت ویژه‌ای برخوردار است. همچنین، بهره‌گیری از ابزارهای فناوری اطلاعات و امنیت سایبری در راستای پیشگیری و کشف جرائم، به همراه ایجاد مقررات انطباقی و منعطف، امکان تطبیق سریع‌تر حقوق با نوآوری‌های فناورانه را فراهم می‌سازد. توجه به تجربیات بین‌المللی، از جمله مقررات اتحادیه اروپا و اصول حاکم بر مسئولیت در فضای سایبری، می‌تواند به طراحی نظامی کارآمد و جامع کمک کند که هم اخلاق و حقوق را رعایت کرده و هم پاسخگوی پیچیدگی‌های فنی باشد. بدین ترتیب، تلفیق اصول فقهی با دانش حقوق تطبیقی و فناوری اطلاعات، مسیر مؤثری برای ایجاد عدالت کیفری در عصر هوش مصنوعی و مدیریت جرائم سایبری ارائه می‌دهد و نشان می‌دهد که حقوق سنتی، اگر با تحلیل تطبیقی و به‌روزرسانی سازگار شود، می‌تواند پاسخگوی نیازهای نوین جامعه دیجیتال باشد.

با توجه به اشتراکات و تفاوت‌های تحلیل شده، می‌توان برخی پیشنهاداتی سایبری ارائه کرد:

-پذیرش مسئولیت تعلیلی و غیرمستقیم است. این امر با مبانی فقه امامیه هم‌خوانی دارد و می‌تواند شامل مواردی شود که فرد مستقلاً عمل مجرمانه‌ای انجام نداده، اما با فراهم کردن ابزار یا داده، باعث تحقق جرم شده است. این انعطاف‌پذیری، تطبیق با جرائم سایبری و شبکه‌ای را تسهیل می‌کند و به نظام کیفری امکان می‌دهد تا با پیچیدگی‌های فناوری نوین همگام شود.

-تدوین مقررات تلفیقی فقهی-حقوقی است. چنین مقرراتی باید عناصر فقه امامیه، به ویژه تأکید بر قصد، عدالت و مسئولیت غیرمستقیم را با چارچوب‌های حقوقی مدرن ترکیب کند. هدف این است که یک نظام قانونی جامع، انعطاف‌پذیر و قابل اجرا در زمینه هوش مصنوعی، داده‌های خودکار و جرائم سایبری ایجاد شود. این تلفیق می‌تواند اطمینان ایجاد کند که هم حقوق فرد حفظ می‌شود و هم جامعه در برابر تهدیدات فناوری‌های نوظهور محافظت می‌گردد.

تعارض منافع

در انجام مطالعه حاضر، هیچ‌گونه تضاد منافعی وجود ندارد.

مشارکت نویسندگان

در نگارش این مقاله تمامی نویسندگان نقش یکسانی ایفا کردند.

حامی مالی

این پژوهش حامی مالی نداشته است.

EXTENDED SUMMARY

The rapid evolution of artificial intelligence technologies and the expansion of cybercrime have fundamentally transformed the landscape of criminal liability, moving it from a predominantly physical and territorially bounded framework into a complex, transnational, and digitally mediated domain. Traditional criminal law was historically constructed upon tangible acts, direct human agency, and identifiable causal chains between conduct and harm; however, in the contemporary digital environment, many offenses are perpetrated through automated systems, machine-learning algorithms, and networked infrastructures that obscure the immediacy of human intervention. This transformation raises profound doctrinal questions concerning attribution, culpability, and the relationship between intent and outcome. Classical elements of criminal liability—actus reus, mens rea, and causal nexus—are strained when the harmful act is executed by an intelligent system lacking consciousness or moral agency. The article situates these developments within a comparative jurisprudential inquiry, examining whether the foundational principles of Imami (Jaʿfari) and Maliki jurisprudence possess sufficient conceptual elasticity to address crimes committed through artificial intelligence and cyber platforms. By revisiting core notions of responsibility, intention, and attribution in Islamic jurisprudence, and integrating contemporary legal reflections on criminal responsibility (Amid, 1984; Jafari Langroudi, 2023; Mirsaeidi, 2019), the study frames the central problem as one of doctrinal adaptation: how can traditional jurisprudential systems, grounded in human intentionality, respond to technologically mediated harms without undermining their normative coherence?

A critical dimension of the inquiry concerns the structural characteristics of cybercrime itself, which differentiate it sharply from conventional criminal conduct. Cyber offenses are typically immaterial in execution, borderless in scope, rapid in dissemination, and often automated in operation. The absence of physical contact between perpetrator and victim complicates evidentiary processes and blurs territorial jurisdiction, while the scalability of digital attacks allows a single actor—or even a self-propagating program—to inflict widespread damage within moments. Moreover, attribution becomes exceedingly difficult when malicious code is deployed through distributed networks or when algorithmic processes evolve beyond the immediate oversight of their creators. These features produce what the article terms “ambiguity of responsibility,” particularly in distinguishing between direct intent, negligent facilitation, and unintended algorithmic outcomes. The jurisprudential challenge is therefore twofold: first, to identify the human agent behind technologically mediated harm; and second, to determine whether the classical requirement of explicit intent can be satisfied in contexts where harm arises indirectly or through complex causal chains. The study draws upon contemporary analyses of cybercrime and digital harm to demonstrate the magnitude of these challenges (Miri, 2025; Mouraj & Akhtari, 2024; Paridar, 2025; Soufi & Saleh-Nejad, 2023; Vahbi, 2023), arguing that any viable theory of criminal liability in the age of artificial intelligence must

incorporate mechanisms for addressing non-physical conduct, distributed causation, and technologically mediated agency.

Within this transformed environment, the article first examines the doctrinal foundations of criminal liability in Imami jurisprudence. Central to this framework is the principle that liability is predicated upon knowledge (ʿilm), intent (qaṣd), and voluntary agency (ikhtiyār). No punishment may be imposed absent conscious and deliberate conduct, yet Imami jurisprudence also recognizes forms of indirect responsibility (tasabbub) whereby an individual who causes harm through an intermediary—whether human or instrumental—may still be held accountable. This recognition of mediated causation provides significant conceptual resources for addressing harms generated by artificial intelligence systems. The doctrine that the use of tools does not negate human responsibility enables the attribution of liability to programmers, operators, or system managers whose actions foreseeably generate harmful outcomes, even if the immediate act is performed by an automated process (Mohaqeq Damad, 2021; Rostami Zabol, 2025; Shojai Langari, 2024). Furthermore, contemporary jurisprudential reflections emphasize preventive principles such as the removal of harm and the prioritization of public interest, allowing for regulatory oversight of high-risk technologies (Mirshekarloo et al., 2025; Zandi & Rafiei Alavi, 2024). In the cybercrime context, this translates into a willingness to treat algorithmic systems as instruments whose misuse or negligent configuration can ground criminal responsibility. Applications include digital financial crimes, automated cyberattacks, and the dissemination of unlawful content through self-operating platforms, where liability may attach to those who design, deploy, or fail to control such systems (Paridar, 2025; Vahabi Hashemabad & Nouri, 2025; Vatankhah, 2025). The article thus concludes that Imami jurisprudence possesses notable adaptability in confronting technologically mediated offenses.

In contrast, the analysis of Maliki jurisprudence reveals a more restrictive orientation toward criminal liability, particularly regarding indirect and automated harms. Maliki doctrine places strong emphasis on the direct connection between act and intent, requiring clear proof that the accused personally committed the prohibited conduct with explicit criminal purpose. While this framework ensures rigorous protection against unjust attribution, it limits the extension of liability to cases involving complex technological intermediaries. Responsibility through tools or third parties is recognized only where a direct and intentional causal link can be established, thereby constraining the scope of liability in automated contexts (Ibn Qudamah al-Maqdisi, 1993; Vatankhah, 2025). In the age of artificial intelligence, where harm may arise from self-learning algorithms or distributed digital infrastructures, this insistence on direct perpetration complicates prosecution and may leave certain technologically mediated harms insufficiently addressed. The difficulty of proving intent in cyber operations further exacerbates the problem, particularly where the accused's role is limited to system development or oversight rather than direct execution of the harmful act (Azimi & Esmaeili, 2021; Tahmasebi, 2006). Although Maliki jurisprudence upholds justice and proportionality as core principles, its narrower conception of indirect liability may generate doctrinal gaps in responding to cybercrime and automated wrongdoing.

The comparative dimension of the study synthesizes these doctrinal divergences to assess their implications for contemporary criminal law. Both Imami and Maliki jurisprudence share foundational commitments to intention, moral agency, and equitable punishment, yet they diverge significantly in their treatment of mediated causation and responsibility through instruments. Imami jurisprudence's acceptance of indirect liability and its analytical flexibility in assessing intention allow it to accommodate technologically complex scenarios more readily. By contrast,

Maliki jurisprudence's focus on direct action and explicit intent, while safeguarding against overcriminalization, limits its capacity to address distributed or automated harms. In practical terms, this divergence affects the ability to prosecute system designers, operators, and digital intermediaries whose involvement in cybercrime is indirect but causally significant. The article suggests that a jurisprudential synthesis—preserving the ethical rigor of Maliki doctrine while incorporating the causal elasticity of Imami principles—could provide a more comprehensive framework for regulating artificial intelligence and cyber offenses. Such a synthesis would clarify standards of attribution, expand the recognition of negligent facilitation, and articulate clearer criteria for responsibility in algorithmically mediated environments (Paridar, 2025; Vahabi Hashemabad & Nouri, 2025).

In conclusion, the study demonstrates that the transformation of criminal activity through artificial intelligence and cyber technologies necessitates a corresponding evolution in jurisprudential analysis. While both Imami and Maliki traditions ground liability in intention and moral agency, only Imami jurisprudence, with its developed doctrine of indirect responsibility and its openness to causal mediation, currently offers a more adaptable framework for addressing intelligent and cyber offenses. Nevertheless, the preservation of justice, proportionality, and doctrinal integrity requires that any adaptation remain faithful to core principles rather than adopting purely technological determinism. The future of criminal liability in the digital era thus lies not in abandoning classical jurisprudential foundations, but in reinterpreting and harmonizing them with contemporary technological realities to ensure accountability, fairness, and effective regulation in an increasingly automated world.

References

Amid, H. (1984). *Persian Dictionary*. Amirkabir Publishing.

Azimi, M. H., & Esmaeili, S. (2021). Identifying artificial intelligence components in Iranian databases. *Journal of Knowledge Studies*, *14*(54), 94-107.

Hosseini, S. M. (2024). Analysis of the civil liability of AI designers and developers. 2nd International Conference on Law, Management, Educational Sciences, Psychology, and Educational Planning Management, Tehran.

Ibn Qudamah al-Maqdisi, A. (1993). *Al-Mughni*. Bayt al-Afkar al-Dawliyyah.

Jafari Langroudi, M. J. (2023). *Terminology of Law*. Ganj-e-Danesh.

Keyvanpour, M. R., Javideh, M., & Pourebrahimi, M. R. (2019). Computer analysis of crime utilizing AI and data mining methods in proactive crime detection. *Karagah (Detective) Journal*, *2*(7).

Miri, S. (2025). *Application of Artificial Intelligence in Criminal Policy and Criminal Procedure*. Manzoumeh Kherad Pajouhan.

Mirsaeidi, M. (2019). *Criminal Liability: Scope and Elements*. Mizan Publishing.

Mirshekarloo, K., Yasin, & Ghiyasi, J. (2025). Attributing liability to Artificial Intelligence with emphasis on the causal relationship in cybercrimes. *Judicial Precedent*, *1*(1).

Mohaqeq Damad, S. M. (2021). *Rules of Jurisprudence: Criminal Section*. Islamic Sciences Publication Center.

Mouraj, Z., & Akhtari, S. (2024). Examining the role of AI technologies in facilitating economic crimes: A criminological perspective. 3rd International Congress on Advocacy, Law, and Humanities, Hamedan.

Paridar, A. (2025). *Criminalization of crimes committed using Artificial Intelligence* Islamic Azad University, Shahrekord Branch].

Rostami Zabol, B. (2025). Criminal liability arising from the actions of autonomous Artificial Intelligence in the Iranian criminal legal system: Challenges and legislative necessities. 14th International and National Conference on Management, Accounting, and Law Studies, Tehran.

Shojai Langari, S. Y. (2024). The impact of Artificial Intelligence and data mining on crime prevention: Opportunities and challenges. *Qazanameh Quarterly*, *6*(2).

Soufi, S., & Saleh-Nejad, S. (2023). The impact of Artificial Intelligence on the commission of cybercrimes. *Journal of Law Studies*, *11*(55).

Tahmasebi, M. R. (2006). Fundamental approaches in Artificial Intelligence. *Wisdom and Philosophy*, *2*(2), 25-48.

Vahabi Hashemabad, M., & Nouri, S. (2025). Jurisprudential approaches to emerging issues: A comparative study on Islamic jurisprudence and new technologies. 11th International Congress of Interdisciplinary Research in Islamic Humanities, Jurisprudence, Law, and Psychology, Tehran.

Vahbi, Z. (2023). AI crimes: An interdisciplinary analysis; Threats and predictable solutions. *Legal Civilization Quarterly*, *6*(18).

Vatankhah, P. (2025). The role of Artificial Intelligence in civil procedure: Challenges and opportunities. Seminar of the Judiciary Lawyers Center, Isfahan.

Zandi, M., & Rafiei Alavi, S. E. (2024). Feasibility of criminal liability in Artificial Intelligence based on its philosophical foundations. *Philosophy of Law*, *3*(1).