Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

Print ISSN: 2717-1469 | Online ISSN: 2717-1477

ISC | SID | NOORMAGS | MAGIRAN | Google Scholar

سال انتشار	۱۴۰۵	شماره انتشار		صفحات	۱-۱۸

مسئولیت کیفری ناشی از استفاده از ربات‌های گفت‌وگو در کلاهبرداری‌های اینترنتی

خانم سپیده هوشیار و آقای دکتر سید علیرضا میرحیدری لنگرودی

کارشناسی ارشد حقوق جزا وجرم شناسی، گروه حقوق، واحد بندرانزلی، دانشگاه آزاد اسلامی، بندرانزلی، ایران

استادیار، گروه حقوق، واحد لاهیجان، دانشگاه آزاد اسلامی، لاهیجان، ایران. (نویسنده مسئول)

چکیده

گسترش استفاده از ربات‌های گفت‌وگو مبتنی بر هوش مصنوعی، علاوه بر ایجاد فرصت‌های گسترده در حوزه ارتباطات دیجیتال، زمینه ظهور شیوه‌های نوین ارتکاب کلاهبرداری اینترنتی را نیز فراهم کرده است. مسئله اصلی پژوهش حاضر آن است که در جرائم ناشی از بهره‌گیری از ربات‌های گفت‌وگو، مسئولیت کیفری متوجه چه اشخاصی است و چگونه می‌توان رفتار مجرمانه را میان کاربران، توسعه‌دهندگان و ارائه‌دهندگان این فناوری‌ها منتسب کرد. هدف پژوهش، بررسی چالش‌های حقوق کیفری ناشی از استفاده مجرمانه از ربات‌های گفت‌وگو، تحلیل عناصر تشکیل‌دهنده جرم کلاهبرداری اینترنتی و ارائه الگویی مناسب برای تعیین حدود مسئولیت کیفری عوامل انسانی دخیل در فرآیند ارتکاب جرم است. روش تحقیق، توصیفی ـ تحلیلی بوده و با بهره‌گیری از منابع کتابخانه‌ای، مطالعات حقوقی داخلی و خارجی و بررسی دیدگاه‌های نوین در حوزه مسئولیت کیفری هوش مصنوعی انجام شده است. یافته‌های پژوهش نشان می‌دهد که در وضعیت کنونی، شناسایی مسئولیت کیفری مستقل برای ربات‌های گفت‌وگو با اصول سنتی حقوق کیفری سازگار نیست؛ زیرا این سامانه‌ها فاقد اراده، قصد مجرمانه و قابلیت سرزنش اخلاقی هستند. بنابراین، مسئولیت کیفری باید بر اساس میزان نقش، کنترل، آگاهی و امکان پیشگیری، میان کاربران، طراحان و عرضه‌کنندگان فناوری توزیع شود. همچنین، توسعه مقررات پیشگیرانه، الزامات نظارتی و معیارهای دقیق انتساب کیفری می‌تواند خلأهای موجود در مقابله با کلاهبرداری‌های مبتنی بر هوش مصنوعی را کاهش دهد.

واژگان کلیدی: ربات‌های گفت‌وگو، مسئولیت کیفری هوش مصنوعی، کلاهبرداری اینترنتی، انتساب کیفری دیجیتال

طبقه‌بندی : JEL فقه – حقوق – جزا و جرم شناسی – حقوق بین الملل – حقوق خصوصی

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

Print ISSN: 2717-1469 | Online ISSN: 2717-1477

ISC | SID | NOORMAGS | MAGIRAN | Google Scholar

Criminal liability arising from the use of chatbots in Internet fraud

Abstract

The expansion of the use of chatbots based on artificial intelligence, in addition to creating wide opportunities in the field of digital communication, has also provided the basis for the emergence of new methods of committing Internet fraud. The main issue of the current research is that in the crimes caused by the use of chatbots, which persons are criminally responsible and how can the criminal behavior be attributed among the users, developers and providers of these technologies. The aim of the research is to examine the challenges of criminal law caused by the criminal use of chatbots, to analyze the elements that constitute the crime of internet fraud and to provide a suitable model for determining the limits of criminal responsibility of human factors involved in the process of committing a crime. The research method is descriptive-analytical and it has been done by using library resources, domestic and foreign legal studies and examining new perspectives in the field of criminal responsibility of artificial intelligence. The findings of the research show that in the current situation, the identification of independent criminal responsibility for chatbots is not compatible with the traditional principles of criminal law; Because these systems lack will, criminal intent, and moral blameworthiness. Therefore, criminal responsibility should be distributed among users, designers and suppliers of technology based on the degree of role, control, awareness and possibility of prevention. Also, the development of preventive regulations, regulatory requirements and strict criteria for criminal attribution can reduce the existing gaps in dealing with AI-based fraud.

Keywords: Chatbots, Criminal responsibility of artificial intelligence, Internet fraud, Digital criminal assignment

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

Print ISSN: 2717-1469 | Online ISSN: 2717-1477

ISC | SID | NOORMAGS | MAGIRAN | Google Scholar

متن مقاله

تحولات شتابان فناوری‌های مبتنی بر هوش مصنوعی، به‌ویژه ظهور و توسعه ربات‌های گفت‌وگو، ساختار ارتباطات انسانی، فعالیت‌های تجاری و ارائه خدمات دیجیتال را دگرگون کرده است؛ با وجود مزایای گسترده این فناوری‌ها، قابلیت تولید محتوای متقاعدکننده، شبیه‌سازی تعامل انسانی، پاسخ‌گویی خودکار و پردازش حجم گسترده‌ای از اطلاعات، زمینه سوءاستفاده مجرمانه از آن‌ها را نیز فراهم ساخته است. یکی از مهم‌ترین حوزه‌های این سوءاستفاده، کلاهبرداری اینترنتی است که در آن مرتکبان می‌توانند با بهره‌گیری از ربات‌های گفت‌وگو، فرآیند فریب قربانیان را در مقیاسی گسترده‌تر و با پیچیدگی بیشتر نسبت به شیوه‌های سنتی انجام دهند. مسئله اساسی این پژوهش آن است که در جرائم ناشی از استفاده از ربات‌های گفت‌وگو، مسئولیت کیفری متوجه چه شخص یا اشخاصی است و آیا چارچوب‌های موجود حقوق کیفری توانایی پاسخ‌گویی به رفتارهایی را دارند که در آن‌ها میان مرتکب انسانی، سامانه هوشمند و نتیجه مجرمانه فاصله ایجاد شده است.اهمیت و ضرورت بررسی این موضوع از آن جهت است که اصول سنتی حقوق کیفری بر مفاهیمی مانند اراده آزاد، قصد مجرمانه، قابلیت انتساب رفتار و مسئولیت شخصی استوار هستند، در حالی که عملکرد ربات‌های گفت‌وگو گاه به‌گونه‌ای است که تعیین رابطه مستقیم میان رفتار انسانی و نتیجه زیان‌بار را دشوار می‌سازد. در چنین شرایطی، فقدان معیارهای روشن برای تعیین مسئولیت کاربران، توسعه‌دهندگان و ارائه‌دهندگان این فناوری می‌تواند موجب ایجاد خلأ کیفری یا برعکس، تحمیل مسئولیت نامتناسب به اشخاصی شود که نقش مستقیمی در وقوع جرم نداشته‌اند. احمدی (۱۳۹۷) در پژوهشی با عنوان «تحلیل اقتصادی و حقوقی جرایم سایبری» به بررسی ویژگی‌های جرائم سایبری، چالش‌های حقوقی ناشی از فناوری‌های نوین و ضرورت بازنگری در شیوه‌های مقابله با جرائم دیجیتال پرداخته و نشان داده است که ساختارهای سنتی حقوق کیفری در مواجهه با جرائم فناوری‌محور نیازمند بازتفسیر و توسعه هستند.در مطالعات خارجی نیز توجه ویژه‌ای به مسئله مسئولیت ناشی از عملکرد سامانه‌های هوش مصنوعی شده است. دیامانتیس[۱] (۲۰۲۴) در پژوهشی با عنوان «مسئولیت کیفری شرکت‌ها در قبال هوش مصنوعی» به بررسی مسئولیت کیفری اشخاص حقوقی در ارتباط با سامانه‌های هوش مصنوعی پرداخته و چالش‌های مربوط به انتساب رفتار مجرمانه به شرکت‌ها و عوامل انسانی مرتبط با فناوری‌های هوشمند را تحلیل کرده است. با وجود ارزش علمی این مطالعات، بیشتر پژوهش‌های موجود به‌صورت کلی به مسئولیت هوش مصنوعی پرداخته‌اند و کمتر پژوهشی به‌طور اختصاصی، فرآیند وقوع کلاهبرداری اینترنتی از طریق ربات‌های گفت‌وگو و نحوه توزیع مسئولیت میان بازیگران مختلف این فرآیند را مورد بررسی قرار داده است.

ویژگی متمایز پژوهش حاضر، تمرکز بر پیوند میان فناوری ربات‌های گفت‌وگو و جرم کلاهبرداری اینترنتی است؛ به این معنا که علاوه بر بررسی عناصر تشکیل‌دهنده جرم، مسئله انتساب کیفری در روابط میان کاربر انسانی، توسعه‌دهنده الگوریتم، ارائه‌دهنده خدمات و سامانه هوشمند تحلیل می‌شود. این پژوهش تلاش دارد با فاصله گرفتن از رویکرد صرفاً فناورانه، الگویی حقوقی برای تعیین مسئولیت ارائه دهد که با اصول بنیادین حقوق کیفری مانند اصل شخصی بودن مسئولیت، ضرورت احراز تقصیر و تناسب مسئولیت با نقش واقعی اشخاص هماهنگ باشد. به نظر می‌رسد با توجه به فقدان اراده مستقل و قصد مجرمانه در ربات‌های گفت‌وگو، این سامانه‌ها در وضعیت فعلی نمی‌توانند به‌عنوان مرتکب مستقل جرم شناخته شوند و مسئولیت کیفری باید بر اساس میزان آگاهی، کنترل، نقش مؤثر و امکان پیشگیری، میان اشخاص انسانی دخیل در طراحی، عرضه و استفاده از این فناوری توزیع شود.

۱. مفهوم‌شناسی ربات‌های گفت‌وگو و نقش آن‌ها در تحول کلاهبرداری‌های اینترنتی

ربات‌های گفت‌وگو به‌عنوان یکی از مهم‌ترین نمودهای توسعه فناوری

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

Print ISSN: 2717-1469 | Online ISSN: 2717-1477

ISC | SID | NOORMAGS | MAGIRAN | Google Scholar

هوش مصنوعی، سامانه‌هایی هستند که با استفاده از پردازش زبان طبیعی، الگوریتم‌های یادگیری ماشین و مدل‌های تحلیل داده، امکان برقراری ارتباط میان انسان و ماشین را به شکل تعاملی فراهم می‌سازند؛ این سامانه‌ها در مراحل اولیه توسعه، صرفاً قادر به ارائه پاسخ‌های محدود و مبتنی بر قواعد از پیش تعیین‌شده بودند، اما پیشرفت مدل‌های هوش مصنوعی موجب شده است که نسل جدید ربات‌های گفت‌وگو توانایی تحلیل مفاهیم زبانی، تشخیص الگوهای رفتاری کاربران، یادگیری از تعاملات پیشین و تولید پاسخ‌های جدید و متناسب با شرایط مکالمه را به دست آورند؛ در نتیجه، ماهیت این فناوری از یک ابزار ارتباطی ساده به یک سامانه هوشمند با قابلیت اثرگذاری بر تصمیم و رفتار انسان تغییر یافته است (رضایی، ۱۳۹۹، ۷۸).ویژگی اصلی ربات‌های گفت‌وگوی هوشمند، توانایی آن‌ها در شبیه‌سازی تعامل انسانی و ایجاد ارتباطی است که در بسیاری از موارد تشخیص آن از گفت‌وگوی واقعی دشوار می‌شود؛ این قابلیت ناشی از ترکیب فناوری‌های پیشرفته‌ای مانند یادگیری عمیق، تحلیل معنایی متن و تولید خودکار محتوا است که به سامانه اجازه می‌دهد پاسخ‌هایی متناسب با وضعیت روانی و اطلاعاتی مخاطب ارائه کند؛ از منظر حقوقی، همین ویژگی می‌تواند زمینه سوءاستفاده مجرمانه را فراهم سازد، زیرا مرتکبان جرائم سایبری قادر خواهند بود از ربات‌های گفت‌وگو برای ایجاد اعتماد کاذب، جعل هویت، ارسال پیام‌های فریبنده و هدایت قربانی به انجام اقدامات مالی زیان‌بار استفاده کنند؛ بنابراین، شناخت ماهیت این فناوری، پیش‌شرط تحلیل آثار کیفری ناشی از کاربرد مجرمانه آن محسوب می‌شود (سلطانی و کامکار، ۱۴۰۳، ص. ۵۳).در تحلیل حقوق کیفری، ربات‌های گفت‌وگو را نمی‌توان صرفاً یک ابزار فنی مشابه ابزارهای سنتی ارتکاب جرم دانست، زیرا میزان خودکارسازی، قابلیت یادگیری و توانایی تولید محتوای مستقل در این سامانه‌ها موجب شده است که فرآیند ارتکاب جرم میان چندین عامل انسانی و فنی توزیع شود؛ در نتیجه، در جرائمی مانند کلاهبرداری اینترنتی مبتنی بر ربات‌های گفت‌وگو، مسئله اصلی تنها اثبات وقوع رفتار مجرمانه نیست، بلکه تعیین رابطه میان عملکرد سامانه هوشمند و اراده اشخاص دخیل در طراحی، آموزش، عرضه یا استفاده از آن است؛ این وضعیت، ضرورت بازنگری در معیارهای سنتی انتساب کیفری و ارائه الگوهای جدید برای تعیین مسئولیت در جرائم ناشی از فناوری‌های هوشمند را آشکار می‌سازد (Hallevy, ۲۰۲۴, ۱۲).

تحول ربات‌های گفت‌وگو از سامانه‌های پاسخ‌گوی ساده به عامل‌های هوشمند، موجب تغییر اساسی در ساختار جرائم سایبری و به‌ویژه کلاهبرداری‌های اینترنتی شده است؛ در گذشته، بسیاری از عملیات‌های فریبکارانه در فضای مجازی نیازمند مداخله مستقیم و مستمر مرتکب بود، اما امروزه ربات‌های گفت‌وگو این امکان را فراهم کرده‌اند که فرآیند ارتباط با قربانیان به شکل خودکار، گسترده و هدفمند انجام شود؛ این سامانه‌ها می‌توانند با تحلیل اطلاعات موجود درباره کاربران، پیام‌هایی متناسب با ویژگی‌های شخصی، نیازهای مالی یا علایق آنان تولید کنند و از طریق ایجاد احساس اعتماد، احتمال موفقیت عملیات فریب را افزایش دهند؛ بنابراین، نقش ربات‌های گفت‌وگو در جرائم اینترنتی صرفاً به افزایش سرعت ارتکاب جرم محدود نمی‌شود، بلکه موجب تغییر ماهیت و پیچیدگی شیوه‌های مجرمانه نیز شده است (Zhang, ۲۰۲۵, ۸۱).یکی از مهم‌ترین کاربردهای مجرمانه ربات‌های گفت‌وگو در حوزه کلاهبرداری اینترنتی، استفاده از قابلیت آن‌ها برای اجرای حملات مهندسی اجتماعی است؛ در این شیوه، مرتکب تلاش می‌کند با تأثیرگذاری بر تصمیم و رفتار قربانی، وی را به افشای اطلاعات محرمانه، انتقال وجه یا انجام اقدامی که در حالت عادی انجام نمی‌داد، ترغیب کند؛ ربات‌های گفت‌وگو با قابلیت پاسخ‌گویی لحظه‌ای، حفظ استمرار مکالمه و ایجاد تعامل مشابه انسان، می‌توانند فرآیند فریب را تقویت کرده و تشخیص ماهیت غیرواقعی ارتباط را برای قربانی دشوار سازند؛ از این رو، استفاده از این فناوری سبب شده است که عنصر فریب در جرائم کلاهبرداری اینترنتی از شکل سنتی خارج شده و با بهره‌گیری از ظرفیت‌های هوش مصنوعی، به سطحی پیچیده‌تر و سازمان‌یافته‌تر ارتقا یابد (Delfino, ۲۰۲۴, ۴۲۵).گسترش استفاده از ربات‌های گفت‌وگو در ارتکاب جرائم مالی و سایبری، چالش‌های جدیدی را برای نظام عدالت کیفری ایجاد کرده است، زیرا در این نوع جرائم معمولاً چندین عامل در شکل‌گیری نتیجه مجرمانه نقش دارند و تشخیص مرز

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir
Print ISSN: 2717-1469 | Online ISSN: 2717-1477
ISC | SID | NOORMAGS | MAGIRAN | Google Scholar

میان عملکرد خودکار سامانه و تصمیم انسانی دشوار می‌شود؛ ممکن است کاربر مجرم از یک ربات گفت‌وگو به‌عنوان ابزار ارتکاب جرم استفاده کند، یا توسعه‌دهنده و ارائه‌دهنده سامانه به دلیل فقدان کنترل‌های لازم در پیشگیری از سوءاستفاده، در ایجاد زمینه وقوع جرم مؤثر باشد؛ بنابراین، تحول الگوی کلاهبرداری‌های اینترنتی تحت تأثیر ربات‌های گفت‌وگو، ضرورت بازتعریف مفاهیمی مانند رفتار مجرمانه، رابطه سببیت و انتساب کیفری را در حقوق فناوری‌های نوین مطرح ساخته است (Diamantis, ۲۰۲۴, ۸۰۳).

۲. تحلیل شیوه‌های ارتکاب کلاهبرداری اینترنتی با بهره‌گیری از ربات‌های گفت‌وگو مبتنی بر هوش مصنوعی

ربات‌های گفت‌وگو مبتنی بر هوش مصنوعی، الگوهای ارتکاب کلاهبرداری اینترنتی را از یک فرآیند محدود و وابسته به مداخله مستقیم انسان، به یک فرآیند خودکار، گسترده و هوشمند تبدیل کرده‌اند؛ در این شیوه، مرتکب جرم می‌تواند با استفاده از قابلیت‌های پردازش زبان طبیعی و تولید محتوای خودکار، ارتباط هم‌زمان با تعداد زیادی از کاربران برقرار کرده و پیام‌هایی متناسب با ویژگی‌های هر قربانی ایجاد کند؛ این قابلیت موجب شده است که روش‌های سنتی مانند ارسال پیام‌های یکسان و عمومی جای خود را به ارتباطات هدفمند و متقاعدکننده بدهند، به‌گونه‌ای که تشخیص ماهیت متقلبانه پیام برای کاربران دشوارتر شود (Zhang, ۲۰۲۵, ۸۲).یکی از رایج‌ترین شیوه‌های بهره‌برداری مجرمانه از ربات‌های گفت‌وگو، استفاده از آن‌ها در حملات فیشینگ و سرقت اطلاعات محرمانه کاربران است؛ در این روش، ربات با شبیه‌سازی ارتباط با بانک‌ها، شرکت‌های تجاری، ارائه‌دهندگان خدمات یا حتی افراد شناخته‌شده، تلاش می‌کند اعتماد مخاطب را جلب کرده و وی را به افشای اطلاعات شخصی یا انجام تراکنش مالی ترغیب کند؛ تفاوت مهم این نوع کلاهبرداری با روش‌های سنتی در آن است که ربات هوشمند می‌تواند براساس پاسخ‌های قربانی، مسیر مکالمه را تغییر داده و راهبرد فریب را تا دستیابی به هدف نهایی ادامه دهد؛ بنابراین، عنصر فریب در این جرائم از طریق یک تعامل پویا و هوشمند تحقق پیدا می‌کند (سلطانی و کامکار، ۱۴۰۳، ص. ۵۸).علاوه بر فیشینگ، ربات‌های گفت‌وگو در شکل‌گیری شیوه‌های جدیدی مانند جعل هویت دیجیتال، ایجاد اعتماد مصنوعی، تبلیغات گمراه‌کننده و ارائه خدمات یا محصولات جعلی نیز مورد استفاده قرار می‌گیرند؛ این سامانه‌ها به دلیل توانایی تولید پاسخ‌های طبیعی و حفظ تداوم مکالمه، می‌توانند قربانی را برای مدت طولانی در فرآیند فریب نگه دارند و زمینه تحقق ضرر مالی یا افشای اطلاعات را فراهم سازند؛ از منظر حقوق کیفری، گسترش این شیوه‌ها نشان می‌دهد که فناوری هوش مصنوعی نه‌تنها ابزار ارتکاب جرم را تغییر داده، بلکه کیفیت رفتار مجرمانه و دشواری‌های مربوط به کشف، اثبات و انتساب مسئولیت کیفری را نیز افزایش داده است (Delfino, ۲۰۲۴, ۴۳۶).

یکی از ویژگی‌های مهم کلاهبرداری‌های اینترنتی مبتنی بر ربات‌های گفت‌وگو، امکان شخصی‌سازی عملیات فریب و انطباق آن با ویژگی‌های هر قربانی است؛ در روش‌های سنتی کلاهبرداری، مرتکب معمولاً از الگوهای ثابت و پیام‌های مشابه برای جذب افراد استفاده می‌کرد، اما سامانه‌های هوشمند قادرند با تحلیل داده‌های رفتاری، علایق، سابقه تعاملات و اطلاعات منتشرشده در فضای دیجیتال، محتوایی متناسب با وضعیت هر فرد تولید کنند؛ این قابلیت باعث می‌شود که پیام‌های متقلبانه از حالت عمومی خارج شده و ظاهری کاملاً معتبر و متناسب با شرایط مخاطب پیدا کنند؛ به همین دلیل، ربات‌های گفت‌وگو به ابزاری مؤثر برای اجرای حملات پیچیده مهندسی اجتماعی تبدیل شده‌اند که شناسایی آن‌ها برای کاربران عادی دشوارتر است (Chen & Liu, ۲۰۲۶, ۴۱).در بسیاری از موارد، ربات‌های گفت‌وگو در کلاهبرداری‌های مالی نقش یک واسطه ارتباطی میان مرتکب و قربانی را ایفا می‌کنند و با ایجاد یک فرآیند ارتباطی مستمر، زمینه تحقق عناصر مادی و روانی جرم را فراهم می‌سازند؛ برای مثال، ربات می‌تواند با معرفی فرصت‌های سرمایه‌گذاری جعلی، ارائه پیشنهادهای تجاری غیرواقعی یا ایجاد ارتباط تحت عنوان پشتیبانی یک شرکت معتبر، قربانی را به انتقال وجه یا ارائه اطلاعات حساس ترغیب کند؛ در این وضعیت، پیچیدگی اصلی برای نظام عدالت کیفری آن است

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

Print ISSN: 2717-1469 | Online ISSN: 2717-1477

ISC | SID | NOORMAGS | MAGIRAN | Google Scholar

که رفتار مجرمانه نه در یک اقدام مستقیم انسانی، بلکه در تعامل میان کاربر، الگوریتم و سامانه ارتباطی تحقق می‌یابد و همین امر فرآیند شناسایی مرتکب واقعی را دشوار می‌کند.همچنین، استفاده از ربات‌های گفت‌وگو موجب افزایش قابلیت سازمان‌یافتگی جرائم کلاهبرداری اینترنتی شده است، زیرا گروه‌های مجرمانه می‌توانند بدون افزایش نیروی انسانی، عملیات‌های گسترده و مداوم را در فضای مجازی اجرا کنند؛ این وضعیت باعث شده است که مرز میان کلاهبرداری فردی و فعالیت‌های مجرمانه سازمان‌یافته در فضای دیجیتال کاهش یابد و ضرورت توجه به سازوکارهای جدید پیشگیری، نظارت و پاسخ کیفری بیش از گذشته احساس شود؛ بنابراین، ربات‌های گفت‌وگو نه‌تنها ابزار جدیدی برای ارتکاب کلاهبرداری هستند، بلکه عاملی مؤثر در تغییر ساختار جرم و ایجاد چالش‌های نوین در سیاست جنایی محسوب می‌شوند (Diamantis, ۲۰۲۴, ۷۹).

۳. بررسی عناصر تشکیل‌دهنده جرم کلاهبرداری اینترنتی در بستر استفاده از ربات‌های گفت‌وگو

در تحلیل جرم کلاهبرداری اینترنتی مبتنی بر ربات‌های گفت‌وگو، نخستین گام بررسی عناصر تشکیل‌دهنده جرم و میزان انطباق رفتارهای ناشی از استفاده از این فناوری با ارکان سنتی کلاهبرداری است؛ زیرا اگرچه فضای ارتکاب جرم و ابزار مورد استفاده تغییر یافته است، اما تحقق مسئولیت کیفری همچنان نیازمند احراز عناصر قانونی، مادی و معنوی جرم خواهد بود؛ در این میان، ربات گفت‌وگو به‌عنوان یک فناوری ارتباطی پیشرفته می‌تواند در تحقق رفتار متقلبانه نقش ایفا کند، اما وجود آن به‌تنهایی برای تحقق جرم کافی نیست و باید بررسی شود که آیا استفاده از این سامانه منجر به ایجاد فریب مؤثر، اغفال قربانی و ورود ضرر مالی شده است یا خیر؛ بنابراین، تحلیل عناصر جرم در این حوزه باید با توجه هم‌زمان به قواعد عمومی حقوق کیفری و ویژگی‌های خاص فناوری هوش مصنوعی انجام گیرد (احمدی، ۱۳۹۷، ۱۲۴).عنصر مادی کلاهبرداری اینترنتی مبتنی بر ربات‌های گفت‌وگو، شامل مجموعه‌ای از رفتارهای مثبت و فعال است که از طریق آن‌ها مرتکب با استفاده از قابلیت‌های سامانه هوشمند، شرایط فریب قربانی را ایجاد می‌کند؛ تولید پیام‌های جعلی، معرفی هویت غیرواقعی، ارائه اطلاعات نادرست، ایجاد اعتماد مصنوعی و هدایت قربانی به انتقال مال یا افشای اطلاعات محرمانه، از جمله مصادیق رفتارهایی است که می‌تواند در چارچوب عنصر مادی این جرم مورد بررسی قرار گیرد؛ ویژگی مهم این نوع جرائم آن است که رفتار مجرمانه ممکن است به‌صورت خودکار و بدون حضور مستقیم مرتکب در تمام مراحل انجام شود و همین امر، تشخیص نقش واقعی اشخاص دخیل در وقوع جرم را با دشواری مواجه می‌سازد (Hallevy, ۲۰۲۴, ۲۹).از منظر عنصر معنوی، تحقق کلاهبرداری اینترنتی نیازمند احراز قصد مجرمانه و آگاهی مرتکب نسبت به ماهیت فریبنده رفتار است؛ در جرائم مبتنی بر ربات‌های گفت‌وگو، این موضوع اهمیت بیشتری پیدا می‌کند، زیرا ممکن است میان طراح فناوری، ارائه‌دهنده خدمات، مالک سامانه و کاربر نهایی که از آن برای ارتکاب جرم استفاده می‌کند، تفاوت اساسی وجود داشته باشد؛ بنابراین، صرف استفاده از یک ابزار هوشمند یا وقوع خسارت مالی نمی‌تواند موجب انتساب کیفری شود، بلکه باید میزان علم، اراده و نقش مؤثر هر یک از اشخاص در فرآیند ارتکاب جرم مشخص شود تا مسئولیت کیفری بر اساس معیارهای پذیرفته‌شده حقوق کیفری تعیین گردد (Schultz, ۲۰۲۵, ۳۰۶).

عنصر قانونی در کلاهبرداری اینترنتی مبتنی بر ربات‌های گفت‌وگو، با چالش تطبیق مقررات سنتی کیفری بر رفتارهایی مواجه است که در بستر فناوری‌های نوین و با واسطه سامانه‌های هوشمند رخ می‌دهد؛ در حقوق کیفری، اصل قانونی بودن جرم و مجازات اقتضا دارد که رفتار مجرمانه دارای وصف قانونی مشخص باشد، اما ظهور ابزارهایی مانند ربات‌های گفت‌وگو موجب شده است برخی شیوه‌های جدید فریب و تحصیل مال، در قالب‌های سنتی به‌سادگی قابل تحلیل نباشند؛ ازاین‌رو، تفسیر موسع و روزآمد مقررات مربوط به جرائم رایانه‌ای و کلاهبرداری باید به نحوی صورت گیرد که ضمن حفظ اصول بنیادین حقوق کیفری، توانایی مقابله با روش‌های نوین ارتکاب جرم را نیز داشته باشد (رضایی، ۱۳۹۸، ص.

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir
Print ISSN: 2717-1469 | Online ISSN: 2717-1477
ISC | SID | NOORMAGS | MAGIRAN | Google Scholar

۹۶).در بررسی عنصر مادی، تفاوت مهم کلاهبرداری مبتنی بر ربات‌های گفت‌وگو با کلاهبرداری سنتی در نحوه تحقق رفتار فریبنده آشکار می‌شود؛ در این وضعیت، فریب ممکن است نه از طریق گفت‌وگوی مستقیم شخص مرتکب، بلکه از طریق پاسخ‌ها و محتوای تولیدشده توسط یک سامانه هوشمند تحقق یابد؛ بنابراین، بررسی نقش ربات در فرآیند ارتکاب جرم اهمیت ویژه‌ای دارد، زیرا باید مشخص شود که سامانه صرفاً وسیله‌ای برای اجرای اراده مجرم بوده یا به دلیل سطح بالای خودکارسازی، در شکل‌گیری رفتار مجرمانه نقش مؤثر داشته است؛ این مسئله، رابطه سببیت میان رفتار انسانی و نتیجه مجرمانه را به یکی از مهم‌ترین چالش‌های حقوق کیفری فناوری تبدیل کرده است (Delfino, ۲۰۲۴, ۴۴۲).در ارتباط با عنصر معنوی، مهم‌ترین مسئله تعیین حدود آگاهی و قصد اشخاصی است که در زنجیره عملکرد ربات‌های گفت‌وگو قرار دارند؛ ممکن است توسعه‌دهنده یک سامانه، از کاربردهای مجرمانه احتمالی آن آگاه نباشد، در حالی که کاربر نهایی با هدف فریب و تحصیل مال دیگری از همان فناوری استفاده کند؛ همچنین ممکن است ارائه‌دهنده خدمات به دلیل فقدان تدابیر کنترلی مناسب، زمینه سوءاستفاده از سامانه را فراهم کرده باشد؛ بنابراین، تعیین مسئولیت کیفری در این حوزه نیازمند تفکیک دقیق میان نقش‌ها، میزان کنترل، درجه تقصیر و ارتباط مستقیم هر شخص با وقوع جرم است تا از تحمیل مسئولیت بدون احراز عنصر روانی جلوگیری شود (Diamantis, ۲۰۲۴, ۸۱۲).

۴. چالش انتساب رفتار مجرمانه به کاربران، توسعه‌دهندگان و ارائه‌دهندگان ربات‌های گفت‌وگو

یکی از اساسی‌ترین چالش‌های حقوق کیفری در جرائم ناشی از استفاده از ربات‌های گفت‌وگو، تعیین شخص یا اشخاصی است که باید رفتار مجرمانه به آن‌ها منتسب شود؛ در الگوی سنتی مسئولیت کیفری، میان رفتار مرتکب و نتیجه مجرمانه معمولاً رابطه مستقیم‌تری وجود دارد، اما در محیط‌های مبتنی بر هوش مصنوعی، فرآیند ارتکاب جرم ممکن است حاصل تعامل چندین عامل انسانی و فنی باشد؛ به‌عنوان نمونه، کاربر نهایی ممکن است از ربات برای فریب قربانی استفاده کند، در حالی که توسعه‌دهنده، ارائه‌دهنده زیرساخت یا مالک پلتفرم نیز در ایجاد یا کنترل محیط ارتکاب جرم نقش داشته باشند؛ بنابراین، مسئله اصلی در این حوزه، یافتن معیار مناسب برای تعیین سهم هر یک از عوامل در تحقق رفتار مجرمانه و جلوگیری از گسترش بی‌ضابطه مسئولیت کیفری است (حسینی، ۱۳۹۹، ۶۷). کاربر انسانی که از ربات گفت‌وگو برای ارتکاب کلاهبرداری اینترنتی استفاده می‌کند، در بسیاری از موارد نزدیک‌ترین شخص به رفتار مجرمانه محسوب می‌شود، زیرا وی با قصد قبلی، سامانه را در جهت فریب قربانی، تحصیل مال یا دستیابی غیرقانونی به اطلاعات به کار گرفته است؛ در چنین شرایطی، ربات گفت‌وگو صرفاً نقش ابزار ارتکاب جرم را ایفا می‌کند و وجود فناوری هوشمند نمی‌تواند موجب سلب مسئولیت از شخصی شود که اراده مجرمانه خود را از طریق آن اجرا کرده است؛ با این حال، پیچیدگی زمانی ایجاد می‌شود که عملکرد سامانه فراتر از دستورات مستقیم کاربر باشد و بخشی از رفتار زیان‌بار ناشی از قابلیت‌های یادگیری و تصمیم‌گیری خودکار آن شکل گرفته باشد (Hallevy, ۲۰۲۴, ۳۴).

از سوی دیگر، توسعه‌دهندگان و ارائه‌دهندگان ربات‌های گفت‌وگو نیز ممکن است در شرایط خاص با مسئولیت کیفری یا دست‌کم مسئولیت ناشی از تقصیر مواجه شوند؛ این وضعیت زمانی مطرح می‌شود که اثبات شود طراح یا عرضه‌کننده فناوری، با علم به امکان استفاده مجرمانه از سامانه، اقدامات پیشگیرانه لازم را اتخاذ نکرده یا عمداً قابلیت‌هایی را ایجاد کرده است که ارتکاب جرم را تسهیل می‌کند؛ بنابراین، تحلیل مسئولیت این اشخاص باید بر پایه معیارهایی مانند میزان کنترل بر سامانه، آگاهی از خطرات، امکان پیشگیری و نقش مؤثر در وقوع جرم انجام شود و نمی‌توان صرف تولید یا ارائه فناوری را به‌تنهایی مبنای مسئولیت کیفری قرار داد (Diamantis, ۲۰۲۴, ۸۲۵).

در بررسی مسئولیت کیفری ناشی از عملکرد ربات‌های گفت‌وگو، یکی از مهم‌ترین مسائل، تعیین جایگاه حقوقی ارائه‌دهندگان پلتفرم‌ها و

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir
Print ISSN: 2717-1469 | Online ISSN: 2717-1477
ISC | SID | NOORMAGS | MAGIRAN | Google Scholar

شرکت‌هایی است که این فناوری را در اختیار کاربران قرار می‌دهند؛ زیرا برخلاف جرائم سنتی که معمولاً میان مرتکب و ابزار ارتکاب جرم رابطه ساده‌تری وجود دارد، در جرائم مبتنی بر هوش مصنوعی، ارائه‌دهنده فناوری ممکن است بدون دخالت مستقیم در عملیات مجرمانه، شرایطی را فراهم کند که امکان وقوع جرم افزایش یابد؛ ازاین‌رو، معیارهایی مانند وجود سازوکارهای نظارتی، هشدارهای استفاده، کنترل‌های ایمنی و میزان آگاهی از کاربردهای احتمالی مجرمانه سامانه، در تعیین حدود مسئولیت این اشخاص اهمیت پیدا می‌کند (Nerantzi & Sartor, ۲۰۲۵, ۱۱۸).مسئله دیگر در انتساب کیفری، وضعیت توسعه‌دهندگان الگوریتم‌ها و طراحان معماری ربات‌های گفت‌وگو است؛ در برخی موارد، ممکن است ضعف‌های طراحی، فقدان محدودیت‌های امنیتی یا عدم پیش‌بینی امکان سوءاستفاده از سامانه، زمینه ارتکاب جرم را فراهم کند؛ با وجود این، صرف وجود نقص فنی یا قابلیت سوءاستفاده نمی‌تواند به‌طور خودکار موجب مسئولیت کیفری توسعه‌دهنده شود، زیرا حقوق کیفری نیازمند احراز رابطه میان تقصیر شخص و نتیجه مجرمانه است؛ بنابراین، باید میان خطای فنی عادی، قصور قابل انتساب و مشارکت آگاهانه در تسهیل جرم تفکیک قائل شد تا مسئولیت کیفری بر پایه اصول شخصی بودن مجازات‌ها استوار باقی بماند (Parlangeli et al., ۲۰۲۴, ۱۷۲۲).علاوه بر این، مسئله انتساب در جرائم مبتنی بر ربات‌های گفت‌وگو زمانی پیچیده‌تر می‌شود که عملیات کلاهبرداری در بسترهای فرامرزی انجام گیرد؛ در این شرایط، ممکن است کاربر، سرور، شرکت ارائه‌دهنده فناوری و قربانی در کشورهای مختلف قرار داشته باشند و تعیین صلاحیت کیفری و دسترسی به ادله دیجیتال با دشواری مواجه شود؛ به همین دلیل، مقابله مؤثر با این نوع جرائم نیازمند توسعه همکاری‌های حقوقی بین‌المللی، ایجاد الزامات شفاف برای ارائه‌دهندگان خدمات هوش مصنوعی و طراحی معیارهای روشن برای تعیین مسئولیت اشخاص دخیل در چرخه تولید و بهره‌برداری از ربات‌های گفت‌وگو است (Chen & Liu, ۲۰۲۶, ۱۰۵).

۵. مسئولیت کیفری کاربر انسانی در بهره‌برداری مجرمانه از ربات‌های گفت‌وگو

در ساختار مسئولیت کیفری ناشی از کلاهبرداری‌های اینترنتی مبتنی بر ربات‌های گفت‌وگو، کاربر انسانی که از این فناوری برای تحقق اهداف مجرمانه استفاده می‌کند، اصلی‌ترین حلقه زنجیره ارتکاب جرم محسوب می‌شود؛ زیرا برخلاف خود سامانه هوشمند که فاقد اراده مستقل کیفری و قصد مجرمانه انسانی است، کاربر با آگاهی از قابلیت‌های فناوری و با هدف ایجاد فریب، تحصیل مال یا ورود ضرر به دیگری، ربات را در مسیر ارتکاب جرم به کار می‌گیرد؛ بنابراین، استفاده از هوش مصنوعی نمی‌تواند به‌عنوان عاملی برای زوال مسئولیت کیفری شخصی تلقی شود که اراده مجرمانه خود را از طریق یک ابزار دیجیتال اجرا کرده است؛ در این وضعیت، ربات گفت‌وگو صرفاً وسیله‌ای پیشرفته برای تحقق رفتار مجرمانه محسوب می‌شود (محمدی، ۱۳۹۹، ۴۲).

احراز مسئولیت کیفری کاربر در این حوزه، نیازمند بررسی دقیق رابطه میان رفتار انسانی و عملکرد سامانه هوشمند است؛ به این معنا که باید مشخص شود آیا کاربر صرفاً از یک ابزار ارتباطی مشروع استفاده کرده یا اینکه با تنظیم، هدایت یا بهره‌برداری هدفمند از ربات، فرآیند فریب را طراحی و اجرا کرده است؛ برای مثال، شخصی که دستورات لازم برای ایجاد پیام‌های جعلی، تقلید هویت یک نهاد معتبر یا ترغیب قربانی به انتقال وجه را به ربات ارائه می‌کند، در واقع از فناوری به‌عنوان امتداد اراده مجرمانه خود استفاده کرده است؛ از این منظر، معیار اصلی در تعیین مسئولیت، نه میزان استقلال فنی ربات، بلکه نقش ارادی و آگاهانه انسان در ایجاد نتیجه مجرمانه خواهد بود (Al-Jizani et al., ۲۰۲۵, ۴۲۱).با وجود این، در برخی موارد تعیین مسئولیت کاربر انسانی با دشواری‌هایی مواجه می‌شود، به‌ویژه زمانی که ربات‌های گفت‌وگو دارای قابلیت یادگیری و تولید پاسخ‌های پیش‌بینی‌نشده باشند؛ در چنین شرایطی ممکن است بخشی از رفتار نهایی سامانه خارج از دستور مستقیم کاربر شکل گیرد و این پرسش مطرح شود که آیا می‌توان تمام نتایج ایجادشده را به استفاده‌کننده نسبت داد یا خیر؛ پاسخ به این مسئله نیازمند بررسی میزان کنترل کاربر بر عملکرد سامانه، سطح آگاهی وی از قابلیت‌های ربات و

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir
Print ISSN: 2717-1469 | Online ISSN: 2717-1477
ISC | SID | NOORMAGS | MAGIRAN | Google Scholar

امکان پیش‌بینی نتیجه مجرمانه است، زیرا مسئولیت کیفری باید بر پایه وجود رابطه منطقی میان اراده انسانی و رفتار زیان‌بار استوار باشد (Schultz, ۲۰۲۵, ۳۰۵).

مسئولیت کیفری کاربر انسانی در استفاده مجرمانه از ربات‌های گفت‌وگو، بر پایه اصول عمومی حقوق کیفری و به‌ویژه اصل شخصی بودن مسئولیت کیفری قابل تحلیل است؛ بر اساس این اصل، تنها شخصی که با علم و اراده مرتکب رفتار مجرمانه شده یا در تحقق آن نقش مؤثر داشته است، باید پاسخ‌گو باشد؛ بنابراین، زمانی که فردی از یک ربات گفت‌وگو برای اجرای طرح کلاهبرداری اینترنتی استفاده می‌کند، وجود فناوری هوشمند تغییری در ماهیت مسئولیت وی ایجاد نمی‌کند، زیرا سامانه تنها ابزار ارتکاب جرم بوده و تصمیم نهایی برای استفاده از آن در مسیر غیرقانونی توسط انسان اتخاذ شده است؛ در نتیجه، بهره‌گیری از فناوری‌های نوین نمی‌تواند به‌عنوان دفاعی برای رهایی از مسئولیت کیفری مورد پذیرش قرار گیرد (کریمی و موسوی، ۱۳۹۹، ۲۶).

یکی از مسائل مهم در این زمینه، تفکیک میان استفاده مشروع و استفاده مجرمانه از ربات‌های گفت‌وگو است؛ زیرا بسیاری از این سامانه‌ها برای اهداف قانونی مانند پشتیبانی مشتریان، ارائه خدمات اطلاعاتی و تسهیل ارتباطات تجاری طراحی شده‌اند و صرف امکان سوءاستفاده از آن‌ها نمی‌تواند موجب مسئولیت کیفری همه کاربران شود؛ بنابراین، برای انتساب جرم به کاربر باید احراز شود که وی با آگاهی از قابلیت‌های سامانه و با هدف تحقق نتیجه مجرمانه، از آن بهره گرفته است؛ این موضوع اهمیت عنصر روانی جرم را در فضای هوش مصنوعی افزایش می‌دهد، زیرا بدون اثبات قصد یا علم کافی، انتساب کیفری با اصول بنیادین حقوق جزا سازگار نخواهد بود (Fajrin et al., ۲۰۲۶, ۲۱۴).همچنین، در مواردی که کاربر انسانی از ربات‌های گفت‌وگو به‌عنوان بخشی از یک عملیات سازمان‌یافته کلاهبرداری استفاده می‌کند، ممکن است مسئولیت وی از سطح استفاده‌کننده ساده فراتر رفته و در قالب مباشرت، معاونت یا مشارکت کیفری مورد بررسی قرار گیرد؛ برای مثال، شخصی که سامانه را برای تولید انبوه پیام‌های فریبنده طراحی کرده، دستورهای لازم را تنظیم نموده یا فرآیند ارتباط با قربانیان را مدیریت می‌کند، نقش فعال‌تری در تحقق جرم دارد؛ بنابراین، ارزیابی مسئولیت کیفری کاربر باید بر اساس میزان تسلط، نقش عملیاتی و ارتباط وی با نتیجه مجرمانه انجام شود و نمی‌توان همه موارد استفاده از ربات‌های گفت‌وگو را با یک معیار واحد تحلیل کرد (Murray, ۲۰۲۵, ۹۴).

۶. مسئولیت کیفری تولیدکنندگان، طراحان و عرضه‌کنندگان سامانه‌های گفت‌وگوی هوشمند

مسئولیت کیفری تولیدکنندگان، طراحان و عرضه‌کنندگان ربات‌های گفت‌وگو، یکی از پیچیده‌ترین مباحث در حوزه جرائم مبتنی بر هوش مصنوعی است؛ زیرا این اشخاص معمولاً به‌صورت مستقیم در فرآیند ارتکاب کلاهبرداری اینترنتی دخالت ندارند، اما ممکن است از طریق طراحی، توسعه یا عرضه سامانه‌ای که قابلیت استفاده مجرمانه دارد، زمینه وقوع جرم را فراهم کنند؛ در این چارچوب، پرسش اصلی آن است که آیا صرف ایجاد فناوری خطرناک یا قابل سوءاستفاده می‌تواند مبنای مسئولیت کیفری قرار گیرد یا اینکه تحقق مسئولیت نیازمند اثبات تقصیر، علم به احتمال سوءاستفاده و وجود رابطه مؤثر میان عملکرد تولیدکننده و نتیجه مجرمانه است؛ پاسخ به این پرسش، نیازمند فاصله گرفتن از نگاه مطلق به فناوری و توجه به نقش واقعی هر یک از عوامل انسانی دخیل در چرخه تولید و بهره‌برداری از سامانه است (حسینی، ۱۳۹۹، ۷۲).تولیدکنندگان ربات‌های گفت‌وگو در فرآیند طراحی، تصمیم‌های مهمی درباره معماری سامانه، سطح دسترسی‌ها، محدودیت‌های امنیتی و سازوکارهای کنترل محتوا اتخاذ می‌کنند؛ بنابراین، اگر ثابت شود که یک شرکت یا طراح با وجود آگاهی از خطرات احتمالی، هیچ‌گونه تدبیر منطقی برای جلوگیری از سوءاستفاده‌های آشکار اتخاذ نکرده یا عامدانه قابلیت‌هایی ایجاد کرده است که ارتکاب جرم را تسهیل می‌کند، بررسی مسئولیت وی امکان‌پذیر خواهد بود؛ البته این مسئولیت باید بر مبنای معیارهای دقیق تقصیر کیفری ارزیابی شود، زیرا توسعه فناوری به خودی خود نمی‌تواند جرم محسوب شود و توسعه‌دهندگان نباید صرفاً به دلیل امکان سوءاستفاده

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir
Print ISSN: 2717-1469 | Online ISSN: 2717-1477
ISC | SID | NOORMAGS | MAGIRAN | Google Scholar

دیگران از محصول خود، مسئول شناخته شوند (Nerantzi & Sartor, ۲۰۲۵, ۱۲۱).از سوی دیگر، ارائه‌دهندگان خدمات ربات‌های گفت‌وگو که زیرساخت لازم برای دسترسی کاربران به این فناوری را فراهم می‌کنند، ممکن است در صورت عدم رعایت الزامات نظارتی و امنیتی با پرسش‌های حقوقی مواجه شوند؛ برای مثال، فقدان سازوکارهای شناسایی سوءاستفاده، نبود سیستم‌های هشداردهنده یا بی‌توجهی به گزارش‌های مربوط به استفاده مجرمانه می‌تواند زمینه بررسی نقش این اشخاص در وقوع جرم را فراهم سازد؛ بنابراین، مسئولیت کیفری عرضه‌کنندگان باید بر پایه میزان کنترل آن‌ها بر سامانه، امکان پیشگیری از جرم و درجه آگاهی آنان نسبت به خطرات موجود تحلیل شود و میان خطای فنی، بی‌احتیاطی و مشارکت عمدی در جرم تفاوت قائل شد (رضایی، ۱۳۹۹، ۵۸).

در تعیین مسئولیت کیفری تولیدکنندگان و عرضه‌کنندگان ربات‌های گفت‌وگو، یکی از مسائل اساسی، تشخیص مرز میان مسئولیت ناشی از طراحی فناوری و مسئولیت ناشی از استفاده مجرمانه کاربران است؛ زیرا در اغلب موارد، یک فناوری واحد می‌تواند هم در مسیرهای قانونی و هم در فعالیت‌های غیرقانونی مورد استفاده قرار گیرد و صرف قابلیت سوءاستفاده نمی‌تواند مبنای انتساب جرم به سازنده آن باشد؛ بنابراین، معیار اصلی باید میزان پیش‌بینی‌پذیری خطر، سطح کنترل توسعه‌دهنده بر عملکرد سامانه و اقداماتی باشد که برای کاهش احتمال سوءاستفاده انجام شده است؛ این رویکرد از یک سو مانع ایجاد مسئولیت کیفری گسترده برای نوآوران فناوری می‌شود و از سوی دیگر، در برابر بی‌احتیاطی یا بی‌مبالاتی شدید در طراحی سامانه‌های پرخطر واکنش حقوقی مناسبی ایجاد می‌کند (Parlangeli et al., ۲۰۲۴, ۱۷۲۴).

یکی از چالش‌های مهم در این زمینه، تعیین مسئولیت در مواردی است که ربات گفت‌وگو پس از عرضه به بازار، از طریق یادگیری از داده‌های جدید یا تغییر تنظیمات توسط کاربران، رفتارهایی از خود نشان می‌دهد که در زمان طراحی اولیه قابل پیش‌بینی نبوده است؛ در چنین شرایطی، انتساب کیفری به توسعه‌دهنده نیازمند بررسی این موضوع است که آیا امکان کنترل، اصلاح یا محدودسازی رفتار سامانه وجود داشته و آیا شخص مسئول از خطرات احتمالی آگاهی داشته است یا خیر؛ به بیان دیگر، مسئولیت کیفری در این حوزه باید بر پایه وجود یک رابطه مشخص میان ترک وظیفه احتیاطی و وقوع نتیجه مجرمانه شکل گیرد، نه صرفاً بر مبنای تولید یک فناوری پیچیده (کریمی و موسوی، ۱۳۹۹، ۳۱).همچنین، در محیط فرامرزی اینترنت، مسئولیت کیفری ارائه‌دهندگان ربات‌های گفت‌وگو با مسائل مربوط به صلاحیت قضایی، دسترسی به اطلاعات و همکاری میان نظام‌های حقوقی مختلف پیوند می‌خورد؛ ممکن است شرکت ارائه‌دهنده فناوری در کشوری مستقر باشد، کاربر مجرم در کشور دیگری فعالیت کند و قربانی در منطقه‌ای متفاوت قرار داشته باشد؛ این پراکندگی جغرافیایی، شناسایی نقش عرضه‌کننده و اجرای ضمانت‌اجراهای کیفری را دشوار می‌سازد و ضرورت تدوین استانداردهای مشترک بین‌المللی برای تعیین تکالیف ارائه‌دهندگان سامانه‌های هوش مصنوعی را افزایش می‌دهد (Chen & Liu, ۲۰۲۶, ۱۰۴).

۷. امکان شناسایی مسئولیت کیفری مستقل برای هوش مصنوعی و ربات‌های گفت‌وگو

بحث درباره امکان شناسایی مسئولیت کیفری مستقل برای هوش مصنوعی و ربات‌های گفت‌وگو، از مهم‌ترین مباحث نظری در حقوق کیفری فناوری‌های نوین است؛ زیرا توسعه سامانه‌هایی که قادر به تحلیل داده، یادگیری، تولید محتوا و اتخاذ برخی تصمیم‌های خودکار هستند، این پرسش را مطرح کرده است که آیا می‌توان این فناوری‌ها را همانند اشخاص انسانی یا اشخاص حقوقی، دارای جایگاه مستقل در نظام مسئولیت کیفری دانست یا خیر؛ در پاسخ به این پرسش، دیدگاه غالب حقوقی بر این باور است که مسئولیت کیفری همچنان باید بر اراده، آگاهی و قابلیت انتساب رفتار به یک فاعل انسانی استوار باشد، زیرا هوش مصنوعی فاقد ویژگی‌های بنیادینی مانند قصد مجرمانه، درک اخلاقی و

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir
Print ISSN: 2717-1469 | Online ISSN: 2717-1477
ISC | SID | NOORMAGS | MAGIRAN | Google Scholar

اراده مستقل انسانی است؛ بنابراین، در شرایط فعلی، ربات‌های گفت‌وگو بیشتر به‌عنوان ابزار یا محیط ارتکاب جرم تحلیل می‌شوند تا مرتکب مستقل جرم (حسینی، ۱۳۹۹، ۸۱).

طرفداران پذیرش نوعی مسئولیت مستقل برای هوش مصنوعی معتقدند که افزایش استقلال عملکرد سامانه‌های هوشمند ممکن است الگوهای سنتی مسئولیت کیفری را ناکارآمد سازد؛ زیرا در برخی موارد، رفتار نهایی سیستم نه به‌طور کامل توسط برنامه‌نویس پیش‌بینی شده و نه می‌توان آن را صرفاً نتیجه دستور مستقیم کاربر دانست؛ از این منظر، ایجاد یک چارچوب مسئولیت ویژه برای سامانه‌های هوشمند می‌تواند خلأهای موجود در پاسخ‌گویی کیفری را کاهش دهد؛ با وجود این، پذیرش چنین دیدگاهی با موانع اساسی مواجه است، زیرا تحمیل مجازات کیفری بر یک سامانه فاقد آگاهی و تجربه ذهنی، با اهداف سنتی کیفر مانند اصلاح، بازدارندگی و سرزنش اخلاقی سازگاری محدودی دارد (Hallevy, ۲۰۲۴, ۱۸).از سوی دیگر، برخی نظریه‌های جدید پیشنهاد می‌کنند که به جای اعطای شخصیت کیفری مستقل به هوش مصنوعی، باید الگوهای جدیدی برای توزیع مسئولیت میان عوامل انسانی دخیل در چرخه تولید و استفاده از فناوری ایجاد شود؛ بر اساس این دیدگاه، تمرکز حقوق کیفری باید بر شناسایی اشخاصی باشد که امکان کنترل، پیشگیری یا مدیریت خطرات ناشی از سامانه را داشته‌اند؛ بنابراین، در جرائم کلاهبرداری مبتنی بر ربات‌های گفت‌وگو، مسئولیت اصلی همچنان متوجه کاربران مجرم، توسعه‌دهندگان یا ارائه‌دهندگانی خواهد بود که نقش مؤثر و قابل انتسابی در تحقق رفتار مجرمانه داشته‌اند (Schultz, ۲۰۲۵, ۳۰۳).

پذیرش مسئولیت کیفری مستقل برای ربات‌های گفت‌وگو با موانع مفهومی و عملی متعددی روبه‌رو است، زیرا نظام‌های کیفری موجود عمدتاً بر پایه وجود شخصی دارای اراده، آگاهی و قدرت انتخاب بنا شده‌اند؛ در حالی که هوش مصنوعی، حتی در پیشرفته‌ترین شکل خود، فاقد تجربه ذهنی، قصد مجرمانه و درک هنجاری از ممنوعیت‌های قانونی است؛ بنابراین، نسبت دادن مفاهیمی مانند سوءنیت، تقصیر یا قصد مجرمانه به یک سامانه الگوریتمی، نیازمند بازنگری عمیق در مبانی مسئولیت کیفری خواهد بود؛ از این رو، بسیاری از نظام‌های حقوقی ترجیح می‌دهند به جای شناسایی شخصیت کیفری مستقل برای هوش مصنوعی، مسئولیت را متوجه اشخاص انسانی مرتبط با طراحی، کنترل و استفاده از این فناوری کنند (رضایی، ۱۳۹۹، ۶۲).

با این حال، برخی دیدگاه‌های نوین حقوقی معتقدند که پیچیدگی روزافزون سامانه‌های هوشمند ممکن است در آینده نیازمند ایجاد یک مفهوم جدید از مسئولیت باشد که نه کاملاً مبتنی بر مسئولیت انسانی سنتی و نه مبتنی بر شخصیت کیفری کامل برای هوش مصنوعی باشد؛ بر اساس این دیدگاه، می‌توان نوعی نظام مسئولیت عملکردی ایجاد کرد که در آن، آثار حقوقی ناشی از رفتار سامانه بر اساس میزان استقلال، سطح خطر و قابلیت کنترل آن تعیین شود؛ چنین رویکردی تلاش می‌کند میان ضرورت پاسخ‌گویی حقوقی فناوری‌های پیشرفته و حفظ اصول اساسی حقوق کیفری تعادل ایجاد کند (Nerantzi & Sartor, ۲۰۲۵, ۱۲۶).در حوزه کلاهبرداری اینترنتی مبتنی بر ربات‌های گفت‌وگو، حتی در صورت افزایش استقلال عملکرد این سامانه‌ها، شناسایی مسئولیت کیفری مستقل برای خود ربات با دشواری‌های جدی مواجه است؛ زیرا جرم کلاهبرداری نیازمند وجود عناصر روانی مانند قصد فریب و هدف تحصیل مال نامشروع است که انتساب آن‌ها به یک سامانه غیرانسانی با چالش نظری روبه‌رو می‌شود؛ بنابراین، راهکار منطقی‌تر آن است که نظام کیفری با توسعه معیارهای انتساب، مسئولیت اشخاصی را که امکان کنترل، نظارت یا جلوگیری از رفتار مجرمانه سامانه را داشته‌اند، به‌صورت دقیق تعیین کند و هوش مصنوعی را در وضعیت فعلی به‌عنوان عامل خطرزا یا ابزار ارتکاب جرم مورد توجه قرار دهد (Al-Jizani et al., ۲۰۲۵, ۴۲۹).

۸. چالش‌های ادله اثبات جرم و کشف جرائم کلاهبرداری مبتنی بر ربات‌های گفت‌وگو

کشف و اثبات جرائم کلاهبرداری اینترنتی مبتنی بر ربات‌های گفت‌وگو، به دلیل ماهیت پیچیده و فنی این فناوری‌ها، با چالش‌های جدیدی در

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

Print ISSN: 2717-1469 | Online ISSN: 2717-1477

ISC | SID | NOORMAGS | MAGIRAN | Google Scholar

حوزه ادله کیفری مواجه شده است؛ در جرائم سنتی، معمولاً رابطه میان رفتار مرتکب و نتیجه مجرمانه از طریق آثار مادی و شواهد مستقیم قابل شناسایی است، اما در محیط‌های مبتنی بر هوش مصنوعی، بخش مهمی از فرآیند ارتکاب جرم در فضای دیجیتال، میان الگوریتم‌ها، داده‌ها و سامانه‌های خودکار رخ می‌دهد؛ ازاین‌رو، شناسایی منشأ پیام‌ها، تشخیص هویت واقعی استفاده‌کننده از ربات و اثبات اینکه محتوای تولیدشده ناشی از اراده مجرمانه یک شخص خاص بوده است، به یکی از مهم‌ترین مسائل اثباتی در این حوزه تبدیل شده است (احمدی، ۱۳۹۷، ۱۴۲). یکی از دشواری‌های اصلی در جمع‌آوری ادله، امکان تغییر، حذف یا پنهان‌سازی آثار دیجیتال ناشی از فعالیت ربات‌های گفت‌وگو است؛ مرتکبان می‌توانند با استفاده از حساب‌های ناشناس، سرورهای خارجی، ابزارهای تغییر هویت دیجیتال یا حذف سوابق ارتباطی، فرآیند تحقیقات کیفری را با مانع مواجه کنند؛ علاوه بر این، تشخیص اینکه یک پیام توسط انسان تولید شده یا توسط یک سامانه هوش مصنوعی ایجاد شده است، در بسیاری از موارد نیازمند استفاده از ابزارهای تخصصی کارشناسی دیجیتال است؛ بنابراین، ادله الکترونیکی در این جرائم باید علاوه بر قابلیت دسترسی، از شرایطی مانند اصالت، تمامیت و قابلیت انتساب نیز برخوردار باشد (Kilovaty, ۲۰۲۵, ۵۳۸).از سوی دیگر، استفاده از ربات‌های گفت‌وگو موجب شده است که مفهوم سنتی دلیل دیجیتال نیازمند بازنگری شود، زیرا در این جرائم، داده‌های ثبت‌شده در سامانه، گزارش‌های عملکرد الگوریتم، سوابق تعاملات و اطلاعات مربوط به نحوه آموزش یا تنظیم ربات می‌توانند در اثبات نقش اشخاص مختلف مؤثر باشند؛ در نتیجه، مقام تحقیق کیفری باید علاوه بر بررسی آثار نهایی جرم، فرآیند تولید و انتقال داده را نیز مورد تحلیل قرار دهد تا بتواند رابطه میان کاربر، سامانه هوشمند و نتیجه مجرمانه را مشخص کند؛ این امر ضرورت ارتقای دانش فنی مراجع قضایی و توسعه روش‌های نوین تحقیقات دیجیتال را افزایش می‌دهد (رضایی، ۱۳۹۹، ۷۴).

۹. چالش‌های ادله اثبات جرم و کشف جرائم کلاهبرداری مبتنی بر ربات‌های گفت‌وگو

یکی از مهم‌ترین مسائل در اثبات کلاهبرداری‌های مبتنی بر ربات‌های گفت‌وگو، تشخیص میزان اعتبار و قابلیت استناد به داده‌هایی است که توسط سامانه‌های هوشمند تولید یا پردازش شده‌اند؛ در این جرائم، ممکن است پیام‌ها، تصاویر، فایل‌های صوتی یا سایر محتواهای دیجیتال توسط یک ربات ایجاد شده باشد و همین موضوع، مسئله اصالت دلیل و امکان انتساب آن به شخص معین را با دشواری مواجه می‌کند؛ بنابراین، صرف مشاهده یک محتوای مجرمانه برای اثبات مسئولیت کیفری کافی نیست، بلکه باید مشخص شود چه کسی سامانه را فعال کرده، چه دستوری به آن داده، چه میزان کنترل بر عملکرد آن داشته و آیا میان رفتار وی و نتیجه زیان‌بار رابطه مستقیم وجود دارد (محمدی، ۱۳۹۹، ۴۸).در فرآیند تحقیقات کیفری، تحلیل داده‌های تولیدشده توسط ربات‌های گفت‌وگو نیازمند استفاده از روش‌های تخصصی مانند بررسی فراداده‌ها، تحلیل الگوهای ارتباطی، ردیابی مسیر انتقال اطلاعات و ارزیابی فنی عملکرد الگوریتم است؛ این موضوع سبب می‌شود نقش کارشناسان ادله دیجیتال در پرونده‌های مرتبط با هوش مصنوعی افزایش یابد، زیرا بسیاری از مفاهیم سنتی اثبات جرم برای درک سازوکار عملکرد سامانه‌های هوشمند کافی نیستند؛ همچنین، پیچیدگی فنی این فناوری‌ها ممکن است موجب شود مقام قضایی در ارزیابی دلیل دیجیتال با محدودیت مواجه شود و ضرورت استفاده از نظریه‌های کارشناسی تخصصی بیش از پیش احساس گردد (Parlangeli et al., ۲۰۲۴, ۱۷۲۶).علاوه بر مسائل فنی، چالش مهم دیگر مربوط به دسترسی قانونی به داده‌های ذخیره‌شده در سامانه‌های هوش مصنوعی و شرکت‌های ارائه‌دهنده خدمات ربات‌های گفت‌وگو است؛ بسیاری از این خدمات در بسترهای بین‌المللی فعالیت می‌کنند و اطلاعات مرتبط با مکالمات، تنظیمات سامانه یا سوابق استفاده ممکن است در خارج از قلمرو قضایی کشور محل وقوع جرم نگهداری شود؛ ازاین‌رو، تحقیقات کیفری در این حوزه نیازمند همکاری میان نهادهای قضایی، ارائه‌دهندگان خدمات دیجیتال و سازوکارهای بین‌المللی تبادل اطلاعات است تا امکان کشف حقیقت و انتساب صحیح مسئولیت

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir
Print ISSN: 2717-1469 | Online ISSN: 2717-1477
ISC | SID | NOORMAGS | MAGIRAN | Google Scholar

کیفری فراهم شود (Chen & Liu, ۲۰۲۶, ۱۰۶).

۱۰. بررسی تطبیقی رویکردهای حقوقی ایران و نظام‌های حقوقی منتخب در مقابله با کلاهبرداری‌های مبتنی بر هوش مصنوعی

نظام‌های حقوقی مختلف در مواجهه با کلاهبرداری‌های مبتنی بر ربات‌های گفت‌وگو، با یک چالش مشترک مواجه هستند و آن، تطبیق قواعد سنتی حقوق کیفری با ویژگی‌های نوظهور فناوری هوش مصنوعی است؛ در حقوق ایران، چارچوب مقابله با این جرائم عمدتاً بر مقررات عمومی کلاهبرداری و مقررات مرتبط با جرائم رایانه‌ای استوار است و مسئولیت کیفری معمولاً بر رفتار شخص انسانی متمرکز می‌شود؛ بنابراین، در شرایطی که ربات گفت‌وگو به‌عنوان ابزار ارتکاب جرم مورد استفاده قرار می‌گیرد، تمرکز اصلی بر شناسایی کاربر یا شخصی است که از سامانه برای تحقق عملیات متقلبانه بهره برده است؛ با وجود این، فقدان مقررات اختصاصی درباره نقش هوش مصنوعی در فرآیند ارتکاب جرم، می‌تواند موجب ایجاد خلأهایی در زمینه انتساب رفتار و تعیین حدود مسئولیت شود (رضایی، ۱۳۹۸، ۱۰۲).در مقابل، برخی نظام‌های حقوقی پیشرفته تلاش کرده‌اند با رویکردی پیشگیرانه‌تر، تکالیف مشخصی برای توسعه‌دهندگان و ارائه‌دهندگان سامانه‌های هوش مصنوعی ایجاد کنند؛ در این رویکرد، به جای انتظار برای وقوع جرم و اعمال ضمانت‌اجرای کیفری پس از آن، بر مدیریت خطر، شفافیت الگوریتمی و ایجاد سازوکارهای نظارتی تأکید می‌شود؛ هدف این رویکرد آن است که اشخاص کنترل‌کننده فناوری، پیش از تبدیل شدن سامانه به ابزار ارتکاب جرم، اقدامات لازم برای کاهش خطرات احتمالی را انجام دهند؛ این تفاوت رویکرد، نشان‌دهنده حرکت تدریجی حقوق فناوری از تمرکز صرف بر مجازات مرتکب به سمت تنظیم‌گری پیشگیرانه است (Nerantzi & Sartor, ۲۰۲۵, ۱۳۰).در نظام‌های حقوقی مبتنی بر کامن‌لا نیز، مسئله اصلی در جرائم هوش مصنوعی، یافتن شخصی است که بتوان رفتار مجرمانه را از نظر حقوقی به وی منتسب کرد؛ این نظام‌ها معمولاً از ایجاد مسئولیت کیفری مستقل برای هوش مصنوعی خودداری کرده و تلاش می‌کنند با استفاده از مفاهیمی مانند تقصیر، کنترل، وظیفه مراقبت و رابطه سببیت، مسئولیت اشخاص انسانی دخیل در چرخه فناوری را تعیین کنند؛ بر همین اساس، در کلاهبرداری‌های مبتنی بر ربات‌های گفت‌وگو نیز تمرکز بر بررسی نقش کاربر، توسعه‌دهنده و ارائه‌دهنده خدمات قرار دارد، نه شناسایی خود سامانه هوشمند به‌عنوان مرتکب جرم (Diamantis, ۲۰۲۴, ۸۱۸).

در مقایسه با نظام‌های حقوقی پیشرفته، حقوق ایران در زمینه تنظیم مسئولیت ناشی از جرائم مبتنی بر هوش مصنوعی هنوز در مرحله توسعه مفهومی قرار دارد؛ مقررات موجود مانند قانون جرائم رایانه‌ای و قواعد عمومی مسئولیت کیفری، ظرفیت‌هایی برای مقابله با سوءاستفاده از فناوری‌های نوین دارند، اما این مقررات عمدتاً برای جرائم رایانه‌ای متعارف طراحی شده‌اند و در مواجهه با سامانه‌هایی که قابلیت یادگیری، تولید محتوا و تعامل مستقل دارند، با محدودیت‌هایی مواجه می‌شوند؛ به همین دلیل، در پرونده‌های مرتبط با ربات‌های گفت‌وگو، قاضی ناگزیر است با تفسیر قواعد موجود، نقش هر یک از عوامل انسانی دخیل در ایجاد و بهره‌برداری از فناوری را تعیین کند (احمدی، ۱۳۹۷، ۱۵۶).در اتحادیه اروپا، رویکرد غالب به جای ایجاد مسئولیت کیفری مستقل برای هوش مصنوعی، بر تنظیم‌گری مبتنی بر ریسک و الزام بازیگران مختلف زنجیره فناوری به رعایت استانداردهای ایمنی و شفافیت استوار شده است؛ این رویکرد تلاش می‌کند با تعیین تکالیف برای توسعه‌دهندگان، عرضه‌کنندگان و استفاده‌کنندگان سامانه‌های هوشمند، احتمال وقوع خسارت و سوءاستفاده مجرمانه را کاهش دهد؛ در نتیجه، مسئولیت در این نظام‌ها بیشتر بر پایه میزان کنترل، قابلیت پیش‌بینی خطر و امکان اتخاذ تدابیر پیشگیرانه تحلیل می‌شود و نه صرفاً بر اساس وقوع نتیجه مجرمانه (Schultz, ۲۰۲۵, ۳۰۷).در ایالات متحده نیز، هرچند نظام حقوقی هنوز چارچوب واحدی برای مسئولیت کیفری هوش مصنوعی ارائه نکرده است، اما مطالعات حقوقی بر ضرورت بازنگری در مفاهیمی مانند مسئولیت شرکت‌ها، وظیفه نظارت و استانداردهای مراقبتی تأکید دارند؛ در این دیدگاه، شرکت‌ها و توسعه‌دهندگان فناوری ممکن است در صورت

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir
Print ISSN: 2717-1469 | Online ISSN: 2717-1477
ISC | SID | NOORMAGS | MAGIRAN | Google Scholar

بی‌توجهی به خطرات آشکار یا فقدان سازوکارهای کنترل مناسب، با پیامدهای حقوقی مواجه شوند، اما صرف توسعه یک ابزار هوشمند که بعداً توسط اشخاص ثالث مورد سوءاستفاده قرار گرفته است، برای ایجاد مسئولیت کیفری کافی تلقی نمی‌شود؛ این رویکرد می‌تواند برای نظام حقوقی ایران در طراحی الگوی مسئولیت متناسب با فناوری‌های هوشمند مورد توجه قرار گیرد (Nelson, ۲۰۲۵, ۱۴۲).

۱۱. نقش مقررات‌گذاری پیشگیرانه و الزامات نظارتی بر توسعه و استفاده از ربات‌های گفت‌وگو

گسترش استفاده از ربات‌های گفت‌وگو در حوزه‌های مختلف اجتماعی و اقتصادی، ضرورت ایجاد سازوکارهای پیشگیرانه برای کاهش خطرات ناشی از سوءاستفاده مجرمانه از این فناوری را افزایش داده است؛ زیرا واکنش صرف کیفری پس از وقوع جرم، در بسیاری از موارد نمی‌تواند خسارات ناشی از کلاهبرداری‌های گسترده دیجیتال را جبران کند؛ ازاین‌رو، سیاست جنایی نوین در حوزه هوش مصنوعی به سمت رویکردهای پیشگیرانه و تنظیم‌گرانه حرکت کرده است تا از طریق ایجاد الزامات فنی و حقوقی، امکان وقوع جرم از ابتدا کاهش یابد؛ در این چارچوب، شفافیت عملکرد سامانه‌ها، ثبت سوابق تعاملات، امکان شناسایی استفاده‌کنندگان و طراحی سازوکارهای کنترل محتوا، از مهم‌ترین ابزارهای پیشگیری از سوءاستفاده از ربات‌های گفت‌وگو محسوب می‌شوند (رضایی، ۱۳۹۹، ۸۵).

یکی از مهم‌ترین الزامات نظارتی، ایجاد تکالیف مشخص برای توسعه‌دهندگان و ارائه‌دهندگان ربات‌های گفت‌وگو است؛ این تکالیف می‌تواند شامل ارزیابی خطر پیش از عرضه سامانه، طراحی قابلیت‌های محدودکننده برای جلوگیری از تولید محتوای مجرمانه، اطلاع‌رسانی درباره ماهیت هوش مصنوعی ارتباط‌گیرنده و ایجاد سازوکار گزارش‌دهی سوءاستفاده‌ها باشد؛ چنین رویکردی موجب می‌شود مسئولیت اجتماعی و حقوقی توسعه‌دهندگان افزایش یافته و از تبدیل فناوری‌های هوشمند به ابزار ارتکاب جرم جلوگیری شود؛ البته این الزامات باید به گونه‌ای طراحی شوند که ضمن تأمین امنیت عمومی، مانع نوآوری و توسعه فناوری نیز نشوند (Zhang, ۲۰۲۵, ۸۴).همچنین، استفاده از استانداردهای فنی و حقوقی برای کنترل عملکرد ربات‌های گفت‌وگو می‌تواند نقش مهمی در پیشگیری از کلاهبرداری‌های اینترنتی داشته باشد؛ استانداردهایی مانند ثبت قابل بررسی فعالیت‌های سامانه، امکان حسابرسی الگوریتمی و ایجاد سازوکارهای تشخیص رفتارهای غیرعادی، می‌توانند فرآیند کشف سوءاستفاده و پاسخ سریع به تهدیدات را تسهیل کنند؛ بنابراین، تنظیم‌گری مؤثر در این حوزه باید ترکیبی از قواعد حقوقی، تدابیر فنی و نظارت مستمر باشد تا میان توسعه فناوری هوش مصنوعی و کاهش خطرات کیفری ناشی از آن تعادل ایجاد شود (Panattoni, ۲۰۲۵, ۹۶).

مقررات‌گذاری پیشگیرانه در حوزه ربات‌های گفت‌وگو، نیازمند ایجاد تعادل میان حمایت از امنیت عمومی و حفظ آزادی توسعه فناوری است؛ زیرا وضع مقررات بیش از حد محدودکننده ممکن است موجب کاهش نوآوری و جلوگیری از بهره‌برداری‌های مشروع از هوش مصنوعی شود، در حالی که فقدان نظارت کافی نیز می‌تواند زمینه گسترش جرائمی مانند کلاهبرداری اینترنتی، جعل هویت دیجیتال و فریب سازمان‌یافته کاربران را فراهم کند؛ بنابراین، سیاست‌گذار باید به جای ممنوعیت کلی فناوری، بر مدیریت خطر و تعیین مسئولیت بازیگران اصلی زنجیره تولید، عرضه و استفاده از سامانه‌های هوشمند تمرکز کند (کریمی و موسوی، ۱۳۹۹، ۳۵).یکی از راهکارهای مهم در این زمینه، الزام ارائه‌دهندگان ربات‌های گفت‌وگو به رعایت اصول شفافیت و قابلیت توضیح‌پذیری عملکرد سامانه است؛ کاربران باید بدانند که در حال تعامل با یک سامانه هوش مصنوعی هستند و نه یک شخص واقعی، زیرا پنهان کردن ماهیت غیرانسانی ارتباط می‌تواند زمینه ایجاد اعتماد کاذب و تحقق فریب را فراهم سازد؛ همچنین، توسعه‌دهندگان باید امکان بررسی سوابق عملکرد سامانه و شناسایی مسیر تولید محتوا را فراهم کنند تا در صورت وقوع جرم، فرآیند تحقیقات کیفری با دشواری کمتری مواجه شود (Nerantzi & Sartor, ۲۰۲۵, ۱۳۴).علاوه بر الزامات مربوط به شفافیت، ایجاد سازوکارهای مسئولیت‌پذیری برای تمامی عوامل دخیل در چرخه حیات ربات‌های

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir
Print ISSN: 2717-1469 | Online ISSN: 2717-1477
ISC | SID | NOORMAGS | MAGIRAN | Google Scholar

گفت‌وگو، از طراحی تا بهره‌برداری، اهمیت ویژه‌ای دارد؛ این سازوکارها باید مشخص کنند که در صورت وقوع کلاهبرداری اینترنتی، هر یک از کاربران، توسعه‌دهندگان و ارائه‌دهندگان خدمات چه وظایفی داشته و در چه شرایطی ممکن است با مسئولیت حقوقی یا کیفری مواجه شوند؛ چنین رویکردی موجب می‌شود فناوری هوش مصنوعی در چارچوبی کنترل‌شده توسعه یابد و در عین بهره‌مندی از مزایای آن، خطر تبدیل شدن ربات‌های گفت‌وگو به ابزار ارتکاب جرم کاهش یابد (Al-Jizani et al., ۲۰۲۵, ۴۳۶).

۱۲. ارائه الگوی پیشنهادی برای تعیین مسئولیت کیفری ناشی از کلاهبرداری‌های اینترنتی مبتنی بر ربات‌های گفت‌وگو

تعیین مسئولیت کیفری در کلاهبرداری‌های اینترنتی مبتنی بر ربات‌های گفت‌وگو، نیازمند ارائه الگویی است که بتواند میان اصول سنتی حقوق کیفری و ویژگی‌های خاص فناوری‌های هوشمند هماهنگی ایجاد کند؛ زیرا الگوهای موجود که عمدتاً بر رفتار مستقیم انسان و رابطه ساده میان مرتکب و نتیجه مجرمانه استوار هستند، در برابر جرائمی که در آن‌ها چندین عامل انسانی و فنی دخالت دارند، کارایی کامل ندارند؛ بر این اساس، الگوی پیشنهادی باید به جای تمرکز صرف بر خود فناوری، بر زنجیره نقش‌آفرینی اشخاص مرتبط با سامانه تمرکز کند و مسئولیت را بر اساس میزان کنترل، آگاهی، نقش مؤثر و امکان پیشگیری هر شخص تعیین نماید؛ چنین رویکردی ضمن حفظ اصل شخصی بودن مسئولیت کیفری، امکان پاسخ‌گویی مؤثر به جرائم نوظهور را فراهم می‌سازد (محمدی، ۱۳۹۹، ۵۱).در این الگو، نخستین سطح مسئولیت متوجه کاربری است که با هدف ارتکاب جرم از ربات گفت‌وگو استفاده می‌کند؛ زیرا در این حالت، سامانه هوشمند صرفاً وسیله اجرای اراده مجرمانه انسان محسوب می‌شود و عناصر قصد، آگاهی و تصمیم‌گیری مجرمانه به شخص استفاده‌کننده بازمی‌گردد؛ بنابراین، در مواردی که کاربر دستورات مشخص برای فریب، جعل هویت یا تحصیل مال غیرقانونی به سامانه ارائه می‌کند، مسئولیت کیفری وی باید بر اساس قواعد عمومی مباشرت یا معاونت در جرم مورد بررسی قرار گیرد؛ این رویکرد مانع از آن می‌شود که پیچیدگی فناوری به ابزاری برای فرار مرتکبان واقعی از پاسخ‌گویی کیفری تبدیل شود (Fajrin et al., ۲۰۲۶, ۲۱۸).سطح دوم این الگو به مسئولیت توسعه‌دهندگان و ارائه‌دهندگان سامانه اختصاص دارد؛ در این مرحله، ملاک مسئولیت نباید صرف تولید یا عرضه فناوری باشد، بلکه باید بر اساس معیارهایی مانند آگاهی از خطرات، امکان کنترل سامانه، رعایت استانداردهای ایمنی و میزان تقصیر در جلوگیری از سوءاستفاده تعیین شود؛ به عبارت دیگر، اگر ارائه‌دهنده یک ربات گفت‌وگو با وجود اطلاع از کاربردهای مجرمانه احتمالی، هیچ اقدام مؤثری برای کاهش خطر انجام ندهد، امکان بررسی مسئولیت وی فراهم خواهد بود؛ این مدل می‌تواند تعادلی میان حمایت از نوآوری فناوری و ضرورت پیشگیری از جرائم سایبری ایجاد کند (Diamantis, ۲۰۲۴, ۸۲۹).

در الگوی پیشنهادی مسئولیت کیفری، باید نظامی چندلایه طراحی شود که در آن نقش هر یک از عوامل انسانی دخیل در چرخه عملکرد ربات‌های گفت‌وگو به‌صورت مستقل ارزیابی شود؛ زیرا در جرائم مبتنی بر هوش مصنوعی، تعیین یک مسئول واحد در همه موارد امکان‌پذیر نیست و ممکن است رفتار مجرمانه حاصل تعامل میان کاربر، توسعه‌دهنده، ارائه‌دهنده خدمات و حتی نهادهای نظارتی باشد؛ بنابراین، معیارهایی مانند میزان اختیار، سطح آگاهی، قابلیت پیش‌بینی خطر، امکان جلوگیری از وقوع جرم و میزان تأثیرگذاری در نتیجه نهایی باید به‌عنوان شاخص‌های اصلی انتساب کیفری مورد توجه قرار گیرند؛ این رویکرد، امکان اعمال مسئولیت متناسب با نقش واقعی هر شخص را فراهم می‌کند و از ایجاد مسئولیت مطلق و غیرعادلانه جلوگیری خواهد کرد (رضایی، ۱۳۹۹، ۹۱).درسطح تقنینی، پیشنهاد می‌شود قانون‌گذار برای جرائم ناشی از استفاده مجرمانه از ربات‌های گفت‌وگو، علاوه بر تکیه بر مقررات عمومی کلاهبرداری و جرائم رایانه‌ای، قواعد اختصاصی درباره تکالیف و مسئولیت بازیگران حوزه هوش مصنوعی وضع کند؛ این قواعد می‌تواند شامل الزام به ثبت سوابق عملکرد سامانه، ایجاد امکان شناسایی کاربران، پیش‌بینی سازوکارهای جلوگیری از تولید محتوای مجرمانه و تعیین ضمانت‌اجرا برای

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

Print ISSN: 2717-1469 | Online ISSN: 2717-1477

ISC | SID | NOORMAGS | MAGIRAN | Google Scholar

عدم رعایت الزامات ایمنی باشد؛ چنین رویکردی موجب می‌شود نظام کیفری از حالت واکنشی صرف خارج شده و به سمت پیشگیری فعال از جرائم فناوری‌محور حرکت کند (Murray, ۲۰۲۵, ۱۰۱).در نهایت، الگوی مناسب برای مسئولیت کیفری ربات‌های گفت‌وگو باید بر مبنای اصل «مسئولیت انسانی هدایت‌شده با فناوری» استوار باشد؛ به این معنا که هوش مصنوعی و ربات‌های گفت‌وگو در وضعیت کنونی به‌عنوان مرتکب مستقل جرم شناخته نشوند، بلکه مسئولیت بر اشخاصی تحمیل شود که امکان ایجاد، کنترل، نظارت یا جلوگیری از رفتار مجرمانه را داشته‌اند؛ چنین الگویی ضمن سازگاری با اصول بنیادین حقوق کیفری، قابلیت انطباق بیشتری با تحولات آینده فناوری خواهد داشت و می‌تواند چارچوب مناسبی برای مقابله با کلاهبرداری‌های اینترنتی مبتنی بر سامانه‌های هوشمند فراهم سازد (Jaff et al., ۲۰۲۶, ۲۵۶۱).

نتیجه‌گیری

گسترش ربات‌های گفت‌وگو مبتنی بر هوش مصنوعی، اگرچه موجب تسهیل ارتباطات دیجیتال و افزایش کارآمدی خدمات آنلاین شده است، اما هم‌زمان شیوه‌های جدیدی از ارتکاب کلاهبرداری اینترنتی را ایجاد کرده که نظام‌های حقوقی را با چالش‌های جدی مواجه ساخته است. بررسی انجام‌شده نشان داد که ویژگی‌هایی مانند توانایی تولید محتوای متقاعدکننده، تقلید تعامل انسانی، پاسخ‌گویی سریع و فعالیت در مقیاس گسترده، ربات‌های گفت‌وگو را به ابزاری مؤثر برای ارتکاب رفتارهای متقلبانه تبدیل کرده است؛ با این حال، استفاده از این فناوری به‌تنهایی نمی‌تواند موجب ایجاد مسئولیت کیفری شود، بلکه تحقق مسئولیت نیازمند احراز عناصر قانونی، مادی و معنوی جرم و تعیین دقیق نقش اشخاص انسانی دخیل در فرآیند ارتکاب جرم است.یافته‌های پژوهش نشان می‌دهد که مهم‌ترین چالش در این حوزه، مسئله انتساب رفتار مجرمانه است؛ زیرا برخلاف جرائم سنتی که معمولاً میان مرتکب و نتیجه مجرمانه رابطه مستقیم وجود دارد، در جرائم مبتنی بر ربات‌های گفت‌وگو، زنجیره‌ای از عوامل شامل کاربر، توسعه‌دهنده، مالک سامانه و ارائه‌دهنده خدمات ممکن است در شکل‌گیری نتیجه مجرمانه نقش داشته باشند. بر این اساس، نمی‌توان مسئولیت کیفری را به‌صورت یکسان بر تمامی عوامل تحمیل کرد، بلکه باید میزان کنترل، آگاهی، نقش مؤثر، امکان پیشگیری و درجه تقصیر هر شخص به‌صورت جداگانه مورد ارزیابی قرار گیرد.همچنین، تحلیل مباحث نشان داد که شناسایی مسئولیت کیفری مستقل برای ربات‌های گفت‌وگو در وضعیت فعلی با اصول سنتی حقوق کیفری سازگار نیست؛ زیرا این سامانه‌ها فاقد اراده آزاد، قصد مجرمانه و قابلیت سرزنش اخلاقی هستند. بنابراین، رویکرد مناسب آن است که هوش مصنوعی به‌عنوان ابزار یا محیط ارتکاب جرم مورد توجه قرار گیرد و مسئولیت کیفری بر اشخاص انسانی دارای نقش واقعی در طراحی، کنترل یا بهره‌برداری مجرمانه از این فناوری متمرکز شود.در نهایت، مقابله مؤثر با کلاهبرداری‌های اینترنتی مبتنی بر ربات‌های گفت‌وگو، نیازمند ترکیبی از اصلاحات تقنینی، توسعه قواعد اختصاصی مسئولیت فناوری، ایجاد الزامات نظارتی برای ارائه‌دهندگان سامانه‌های هوشمند و ارتقای توان فنی نهادهای تحقیقاتی و قضایی است. به نظر می‌رسد اتخاذ الگوی «مسئولیت انسانی مبتنی بر میزان کنترل و خطرپذیری فناوری» می‌تواند ضمن حفظ اصول بنیادین حقوق کیفری، پاسخ مناسبی برای چالش‌های ناشی از استفاده مجرمانه از ربات‌های گفت‌وگو ارائه دهد.

Diamantis [۱]

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

Print ISSN: 2717-1469 | Online ISSN: 2717-1477

ISC | SID | NOORMAGS | MAGIRAN | Google Scholar

منابع

۱. ابراهیمی، ف. (۱۳۹۹). «فلسفه اخلاق اسلامی و مسئولیت در فناوری‌های دیجیتال». مجله حقوق فناوری، ۳(۲)، ۵۵-۷۸.

۲. احمدی، م. (۱۳۹۷). تحلیل اقتصادی و حقوقی جرایم سایبری. تهران: پژوهشگاه فناوری اطلاعات.

۳. حسینی، س. (۱۳۹۹). «الزامات قانونی و پیشگیری از فیشینگ». مجله حقوق فناوری، ۳(۲)، ۵۵-۷۸.

۴. حسینی، س. (۱۳۹۹). فلسفه حقوق و پاسخگویی در سیستم‌های هوش مصنوعی. تهران: نشر عدالت.

۵. رضایی، م. (۱۳۹۸). فلسفه حقوق و فناوری‌های نوین. تهران: انتشارات دانشگاه تهران.

۶. رضایی، م. (۱۳۹۸). قانون جرایم رایانه‌ای و چالش‌های حقوقی. تهران: انتشارات دانشگاه تهران.

۷. رضایی، م. (۱۳۹۹). «مسئولیت قانونی و کیفری در محیط دیجیتال». مجله حقوق و فناوری، ۲(۱)، ۴۵-۶۷.

۸. رضایی، م. (۱۳۹۹). فناوری‌های نوین و هزینه‌های جرایم دیجیتال. تهران: انتشارات دانشگاه تهران.

۹. سلطانی، م. و کامکار، م. (۱۴۰۳). «فناوری‌های نوین و فیشینگ: بررسی حقوقی استفاده از هوش مصنوعی و اتوماسیون در کلاهبرداری». حقوق سایبری، ۱(۲)، ۴۱-۶۵.

۱۰. کریمی، ف. و موسوی، ع. (۱۳۹۹). «دکترین حقوقی و مسئولیت فناوری‌های نوین». مجله علوم اجتماعی، ۵(۱)، ۱۲-۳۸.

۱۱. محمدی، س. (۱۳۹۹). «مسئولیت بر اساس تقصیر و مسئولیت محض در جرایم سایبری». مجله حقوق و فناوری، ۳(۱)، ۲۳-۵۵.

۱۲. Jaff, A. S., Ali, K. A., Rashed, S. M., & Ahmed, D. S. (۲۰۲۶). Criminal liability for manipulation of generative artificial intelligence. Scientific Culture, ۱۲(۱), ۲۵۵۳.

۱۳. Al-Jizani, H. K. A., Heidari, M., Ali, H. H., & Saeedi, Y. (۲۰۲۵). Criminal liability arising from offenses committed by robots. Qarar Journal for Scientific Research, ۵(۱۵), ۴۱۴–۴۴۲.

۱۴. Chen, Y., & Liu, H. (۲۰۲۶). Criminal responsibility for generative AI in cross-border financial fraud. Computer Law & Security Review, ۵۸, ۱۰۶۰۳۲.

۱۵. Delfino, R. A. (۲۰۲۴). Deepfake fraud and the limits of criminal attribution in the digital age. UCLA Law Review, ۷۱(۲), ۴۱۰–۴۶۵.

۱۶. Diamantis, M. E. (۲۰۲۴). Corporate criminal liability for artificial intelligence. Washington Law Review, ۹۹(۳), ۷۸۹–۸۳۲.

۱۷. Fajrin, N., Suryani, A. I., Rato, D., & Ohoiwutun, Y. A. T. (۲۰۲۶). Legal certainty of criminal responsibility for artificial intelligence scam through electronic communications in Indonesia. Rechtenstudent, ۷(۲).

۱۸. Hallevy, G. (۲۰۲۴). Liability for crimes committed by AI systems: A modern approach. Criminal Law Forum, ۳۵(۱), ۱–۳۵.

۱۹. Kilovaty, I. (۲۰۲۵). Hacking generative AI. Loyola of Los Angeles Law Review, ۵۸, ۵۲۱.

۲۰. Nerantzi, E., & Sartor, G. (۲۰۲۵). Crimes without criminals: In search of criminal liability for harms caused by AI systems. In Research Handbook on the Law of Artificial Intelligence.

۲۱. Parlangeli, O., Curro', F., Palmitesta, P., & Guidi, S. (۲۰۲۴). Moral judgements of errors by AI systems and humans in civil and criminal law. Behaviour & Information Technology, ۴۳(۹), ۱۷۱۸–۱۷۲۸.

۲۲. Schultz, D. (۲۰۲۵). Personhood, crimes, and criminal liability in the age of artificial intelligence. Bulletin of the Transilvania University of Brasov, ۱۸(Suppl), ۳۰۱–۳۰۸.

۲۳. Zhang, F. (۲۰۲۵). The dilemma and solutions in

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

Print ISSN: 2717-1469 | Online ISSN: 2717-1477

ISC | SID | NOORMAGS | MAGIRAN | Google Scholar

applying criminal law to generative AI fraud crimes: The case of Sora. Studies in Law and Justice, ۴(۵), ۷۸–۸۷.