مجله مطالعات حقوق

شماره ۵۱،
دوره ۱۱،
سال پنجم،
مستان ۱۴۰۲،
صص ۱-۱۸

تاثیر هوش مصنوعی در ارتکاب جرایم سایبری

سارا صوفی[۱]، صابر صالح نژاد بهرستاقی[۲]

چکیده

هدف تحقیق حاضر، بررسی تاثیر فناوری هوش مصنوعی در ارتکاب جرایم سایبری است. تکنولوژی هوش مصنوعی به‌عنوان یکی از پیشرفت‌های چشم‌گیر در دهه‌های اخیر، تأثیرات عمیقی بر انواع فعالیت‌های انسانی، از جمله جرایم سایبری، گذاشته است. این تأثیرات ممکن است به دو صورت مثبت و منفی باشند. از یک طرف، سیستم‌های هوش مصنوعی می‌توانند بهبودهای قابل توجهی در امنیت سایبری و جلوگیری از جرایم آنلاین ایجاد کنند. به عنوان مثال، توانایی تشخیص الگوهای ناشناخته و ردیابی فعالیت‌های مشکوک از طریق الگوریتم‌های یادگیری ماشین، می‌تواند به مقابله با حملات سایبری کمک کند. از سوی دیگر، همان‌طور که توانایی‌های هوش مصنوعی بهبود می‌یابد، متخصصان جرم‌شناسی نیز نگرانی‌هایی را در مورد استفاده از آن در جرایم سایبری ابراز کرده‌اند. مثلاً، ابزارهای هوش مصنوعی می‌توانند برای ایجاد حملات سایبری پیچیده‌تر و موثرتر توسط مهاجمان استفاده شوند. بر همین اساس سوالی که مطرح می‌گردد این است که هوش مصنوعی چه تاثیری در ارتکاب جرایم سایبری دارد؟ یافته‌های تحقیق نشان از آن دارد که، تاثیر هوش مصنوعی در ارتکاب جرایم سایبری به چندین شکل ممکن است مورد بررسی قرار گیرد. این تاثیرات می‌توانند هم در ابزارها و تکنولوژی‌های مورد استفاده توسط مجرمان سایبری و هم در راهکارهای دفاعی مورد استفاده برای کاهش این حملات مشاهده شوند. به عبارتی، هوش مصنوعی همچنین می‌تواند هم به عنوان یک ابزار برای ارتکاب جرایم سایبری و هم به عنوان یک ابزار برای دفاع در برابر آنها مورد استفاده قرار گیرد. اما برای مقابله با این چالش‌ها، نیاز به توسعه راهکارهای مبتنی بر هوش مصنوعی برای تشخیص، پیشگیری و مهار کردن حملات سایبری بیشتر است.

کلمات کلیدی: هوش مصنوعی، جرم، سایبر، اینترنت.

[۱] کارشناسی ارشد، گروه حقوق جزاء و جرم شناسی، واحد پردیس، دانشگاه آزاد اسلامی ، تهران، ایران (نویسنده مسئول) s.soufi1981@gmail.com

[۲] دکتری تخصصی، گروه فلسفه تعلیم و تربیت، واحد شهید مفتح، دانشگاه فرهنگیان، تهران، ایران saber.salehnezhad@gmail.com

[Downloaded from jlawst.ir on 2026-09-08]

شماره ۵۱،
دوره ۱۱،
سال پنجم،
مستان ۱۴۰۲،
صص ۱–۱۸

مقدمه

هوش مصنوعی (AI) یکی از فناوری‌های پیشرفته و پرکاربرد در دنیای امروز است که تأثیر عمیقی بر زندگی انسان‌ها و جوامع داشته است. با توجه به رشد سریع در زمینه توسعه فناوری و پیشرفت‌های بزرگ در الگوریتم‌های هوش مصنوعی، این فناوری به یکی از مهم‌ترین عوامل تغییر و تحول در بسیاری از صنایع تبدیل شده است. مفهوم هوش مصنوعی به عنوان یک شاخه علمی و فناوری، به دهه‌های اوایل قرن بیستم برمی‌گردد، اما ریشه‌های آن را می‌توان در افکار و آرمان‌های انسان‌ها از دیرباز یافت. پس از آن، با پیشرفت‌های علمی و فناوری در دهه‌های بعد، مفهوم هوش مصنوعی به تدریج شکل گرفت. اولین مفهوم سیستم هوش مصنوعی توسط جان مک‌کارتی در دهه ۱۹۵۰ میلادی مطرح شد. هوش مصنوعی به دو دسته تقسیم می‌شود: هوش مصنوعی ضعیف و هوش مصنوعی قوی. در هوش مصنوعی ضعیف، سیستم‌ها تنها وظیفه‌های خاص و محدودی را انجام می‌دهند و اغلب بر اساس قوانین و الگوریتم‌های مشخص عمل می‌کنند. اما در هوش مصنوعی قوی، سیستم‌ها قادر به تفکر، یادگیری، حل مسئله و انجام وظایف پیچیده‌تر هستند. در اینده‌ای نزدیک، یادگیری عمیق، یادگیری تقویتی، شبکه‌های عصبی مصنوعی، الگوریتم‌های ژنتیک، و همچنین روش‌های پردازش زبان طبیعی از جمله روش‌های مورد استفاده در هوش مصنوعی خواهند بود (نظرپور و همکاران،۱۳۹۹: ۲٤).

هوش مصنوعی در بسیاری از صنایع و حوزه‌ها کاربردهای فراوانی دارد. به عنوان مثال، در حوزه پزشکی، هوش مصنوعی می‌تواند در تشخیص بیماری‌ها، طراحی داروهای جدید، و بهبود روش‌های درمانی موثر باشد. در حوزه خودروسازی، خودروهای خودران با استفاده از تکنولوژی هوش مصنوعی در حال توسعه هستند. در علوم اجتماعی، هوش مصنوعی می‌تواند به تحلیل داده‌های اجتماعی و پیش‌بینی رفتارهای انسانی کمک کند. هوش مصنوعی به عنوان یکی از فناوری‌های کلیدی در دنیای امروز، توانسته است به طور چشمگیری در زندگی ما تأثیر بگذارد. با پیشرفت روزافزون در این حوزه، انتظار می‌رود که کاربردهای هوش مصنوعی در آینده‌ای نزدیک به صورت گسترده‌تری در صنایع مختلف بکار گرفته شود و به بهبود کیفیت زندگی انسان‌ها کمک کند(قاید رحمتی، ۱۳۹۵، ۱۱).

هوش مصنوعی از دهه‌های گذشته تا کنون تحولات چشمگیری را تجربه کرده است و با پیشرفت‌های علمی و تکنولوژیکی، انتظار می‌رود که نقش و اهمیت آن در جامعه به طور روزافزون افزایش یابد. گسترش استفاده از هوش مصنوعی، عدم شناخت و آگاهی کاربران از بعد فنی این موضوع و همه گیر گشتن تعاملات از طریق آنها و درگیر نمودن قسمتی از زندگی افراد، موجب وقوع جرائم گوناگونی از جمله جعل، کلاهبرداری، تقلب در آزمون‌ها و.... در این رابطه گردیده است. استفاده از این فناوری، گرچه فرصت شایسته‌ای را جهت به اشتراک گذاری علوم گوناگون، سوابق شغلی و حرفه‌ای به وجود آورده است، ولی تبعات ناخوشایندی از جمله ارتکاب جرایم را نیز به دنبال داشته است، که در عصر کنونی در رسانه‌ها شاید و ناظر وقوع جرائم در این حوزه هستیم. به علت پیشرفت روز افزون فناوری هوش مصنوعی، همیشه جرائم جدید و نوپدیدی ارتکاب یافته که گاه بعضی از آنان به طور مستقیم در قانون پیش‌بینی نشده‌اند و این موضوع کار دستگیری این مجرمان و قضاوت در این قبیل پرونده‌ها را دشوار می‌سازد. از جمله این جرائم می‌توان به جرایم ارتکابی از طریق هوش مصنوعی اشاره کرد. آن طور که بیان گردید، بعضی از این جرائم در قانون پیش بینی نشده است و با دقت به اینکه هوش مصنوعی و استحکام بنیان آن برای تأمین کارکردهای آن، از جایگاه خاصی برخوردار است و از سویی احتمال وقوع جرائم گوناگون نیز قابل تصور است (قایدرحمتی،۱۳۹۵، ۱۲).

تاثیر هوش مصنوعی در ارتکاب جرایم سایبری یک مسئله اجتماعی و فناوری است که با گسترش روزافزون فناوری‌های هوش مصنوعی، ابعاد جدیدی را به جرم‌های سایبری اضافه کرده است. با پیشرفت هوش مصنوعی و الگوریتم‌های پیچیده، متخصصان جرایم سایبری قادر به ایجاد ابزارها و روش‌های جدید برای نفوذ به سیستم‌ها، دزدیدن اطلاعات حساس، تقلب مالی، ترویج

[Downloaded from jlawst.ir on 2026-09-08]

شماره ۵۱،
دوره ۱۱،
سال پنجم،
مستان ۱۴۰۲،
صص ۱-۱۸

تبلیغات تقلبی و حتی توسعه برنامه‌های رباتیک برای حملات گسترده‌تر شده‌اند. یکی از مواردی که هوش مصنوعی می‌تواند در ارتکاب جرایم سایبری تاثیرگذار باشد، استفاده از الگوریتم‌های یادگیری ماشینی برای شناسایی ضعف‌ها و نقاط آسیب‌پذیر در سیستم‌هاست. این الگوریتم‌ها می‌توانند به طور خودکار به دنبال ضعف‌های امنیتی در نرم‌افزارها یا سیستم‌های شبکه بگردند و از آنها به عنوان نقطه ورود برای حملات سایبری استفاده کنند. به طور کلی، هوش مصنوعی می‌تواند به عنوان یک ابزار قدرتمند برای افزایش پیچیدگی و تأثیرگذاری جرایم سایبری عمل کند. از طرف دیگر، استفاده از هوش مصنوعی نیز می‌تواند به عنوان یک راه حل برای تشخیص و پیشگیری از این جرایم مورد استفاده قرار گیرد. اما با این حال، همانطور که توانایی‌های هوش مصنوعی افزایش می‌یابد، نیاز به توسعه استراتژی‌ها و سیاست‌های امنیتی مناسب برای مقابله با تهدیدات سایبری نیز بیشتر می‌شود. اما مسئله مهم و قابل بحث، تاثیرگذاری هوش مصنوعی در ارتکاب جرایم سایبری است اینکه این فناوری چه تاثیری بر ارتکاب جرایم دارد؟

۱-تعاریف

۱-۲-هوش مصنوعی

هوش مصنوعی، به معنای هوش و توانایی‌هایی است که توسط ماشین‌ها و سیستم‌های کامپیوتری برای انجام فعالیت‌های هوشمندانه و تصمیم‌گیری استفاده می‌شود. این فراداده به ماشین‌ها امکان می‌دهد تا الگوها را تشخیص داده، داده‌ها را تحلیل کرده و مسائل را مدیریت کنند. هوش مصنوعی شامل مجموعه‌ای از تکنیک‌ها و الگوریتم‌ها است که به ماشین‌ها این قابلیت را می‌دهد تا با بررسی و تحلیل داده‌ها، الگوهای پنهان در آن‌ها را شناسایی کنند و بر اساس آن‌ها تصمیم‌گیری کنند. این فناوری در حال حاضر در بسیاری از زمینه‌ها مانند رباتیک، پردازش زبان طبیعی، تشخیص تصویر، پشتیبانی تصمیم‌گیری، خودران‌سازی و سیستم‌های هوشمند به کار می‌رود. هدف اصلی هوش مصنوعی ایجاد سیستم‌هایی است که قادر به انجام وظایفی مشابه به انسان باشند و در برخی موارد حتی بتوانند عملکرد بهتری نسبت به انسان داشته باشند. به عبارتی، هوش مصنوعی به مجموعه‌ای از تکنیک‌ها، الگوریتم‌ها و فرآیندهای کامپیوتری اشاره دارد که به کامپیوترها و سیستم‌های مصنوعی امکان می‌دهد کارهایی را انجام دهند که به نظر می‌رسد نیازمند انسانیت و هوش ذهنی باشند. هدف اصلی هوش مصنوعی، شبیه‌سازی و تقلید عملکرد انسانی در زمینه‌هایی مانند تصمیم‌گیری، یادگیری، استدلال، تشخیص الگو، پردازش زبان طبیعی و بینایی ماشینی می‌باشد. تکنیک‌ها و روش‌های مختلفی در دسته‌بندی هوش مصنوعی وجود دارد که شامل موارد زیر می‌شود:

-یادگیری ماشینی: این رویکرد به کامپیوترها امکان می‌دهد از داده‌ها یاد بگیرند و با استفاده از الگوریتم‌های مختلف، پتانسیل تشخیص الگوها و انجام پیش‌بینی‌ها را داشته باشند.

-شبکه‌های عصبی مصنوعی: این مدل‌ها به تقلید از ساختار مغز انسان پرداخته‌اند. اطلاعات با استفاده از نورون‌های مصنوعی در لایه‌های مختلف پردازش می‌شود و این مدل‌ها برای مسائل پیچیده‌تر مانند تصویربرداری و تشخیص الگو بسیار مؤثر هستند.

-پردازش زبان طبیعی: این حوزه به کامپیوترها امکان می‌دهد تا متون و گفتار انسانی را تشخیص داده و تفسیر کنند. این امر شامل ترجمه ماشینی، تولید متن خودکار، تحلیل مضمون متون و مکالمات با کامپیوترها می‌شود.

-بینایی ماشین: این زمینه به کامپیوترها امکان می‌دهد تصاویر و ویدئوها را تحلیل و تشخیص دهند. این شامل تشخیص و شناسایی اشیاء، چهره‌ها، شناسایی وضعیت و ویژگی‌های تصاویر می‌شود.

-منطق فازی: در این رویکرد، مفاهیمی مانند صحیح یا غلط با در نظر گرفتن ابهامات و مبهمی‌ها تعریف می‌شوند. این به کامپیوترها امکان می‌دهد با مفاهیم پیچیده‌تر و واقع‌نزدیک‌تر کار کنند.

هوش مصنوعی به صورت یکی از فناوری‌های پیشرفته و چالش‌برانگیز، در مختلف صنایع و زمینه‌ها مورد استفاده قرار می‌گیرد و بهبودهای چشمگیری در کارکردها و امکانات مختلف ارائه داده است(قائدرحمتی،۱۳۹۵: ۲۴-۲۵).

[Downloaded from jlawst.ir on 2026-09-08]

شماره ۵۱،
دوره ۱۱،
سال پنجم،
مستان ۱۴۰۲،
صص ۱-۱۸

۲-جرم

جرم در لغت به معنای «گناه» آمده است و در اصطلاح، علیرغم تعاریف زیادی که از جرم شده، هنوز هم این موفقیت بدست نیامده تا از جرم، آن چنان تعریفی به عمل آید که مورد قبول همگان قرار گیرد و در زمان و مکان واجد ارزش باشد و دلیل این امر نیز این است که پدیده جرم، برحسب نظر دانشمندان و محققان، دارای مبانی و صور گوناگون است. به سخنی دیگر، آنچه که از نظر یکی جرم محسوب می‌شود، برحسب دیگری نه تنها ممکن است عنوان جرم به خود نگیرد، بلکه امکان دارد که حتی عملی پسندیده به شمار آید (شامبیاتی، ۱۴۰۲، ۲۳).

عده‌ای از حقوقدانان معتقدند که نقص قانون هر کشوری در اثر عمل خارجی، در صورتی که انجام وظیفه یا اعمال آن را تجویز نکند و مستوجب مجازات هم باشد، جرم نامیده می‌شود (دانش،۱۳۸۵، ۴۳).

سهم دورکیم در نظریه پردازی درباره جرم و کیفر بسیار مهم است که بیشتر در کتاب «تقسیم کار در جامعه» و «قواعد و روش جامعه شناسی» منعکس می‌باشد. دورکیم معتقد است که هر عملی که درخور مجازات باشد، جرم است. به بیان دیگر، هر فعل یا ترک فعلی که نظم، صلح وآرامش اجتماعی را مختل سازد و قانون نیز برای آن مجازاتی تعیین کرده باشد، «جرم» محسوب می‌شود. به نظر دورکیم «ما کاری را بخاطر جرم بودن محکوم نمی‌کنیم، بلکه از آنجایی که آن را محکوم می‌کنیم، جرم تلقی می‌شود» (دورکیم، ۱۳۸۹، ۸۰)

جرم یک پدیده «معمولی» جامعه است، زیرا که بر حسب احساس تنفر و انزجاری که بزهکار در جامعه بر می‌انگیزد، معین می‌گردد. هدف از کیفر، بیشتر معطوف به افراد غیر مجرم است، زیرا که بیشتر احساس همبستگی و یگانگی افراد بی گناه را تقویت می‌کند، پیش از اینکه مجرمان را متنبه سازد. کیفر ممکن است نقش عدم ترغیب و تضعیف و دلسردی مجرمان را نیز فراهم آورد؛ لیکن احساس انزجار در قبال پاره‌ای از اعمال کیفرپذیر در میان بعضی از مردم ضعیف است و در نتیجه آنان در معرض ارتکاب جرم قرار می‌گیرند. بنابراین کیفر نمی‌تواند از وقوع جرم پیشگیری کند. هیچ جرمی جرم محسوب نمی‌شود، مگر اینکه کیفری در کار باشد. در نتیجه کیفر قانونی نمی‌تواند اعمال شود، مگر اینکه در قبال اعمالی که قانوناً تعریف دقیق داشته باشند. اگر اعمال ناپسند و مذموم از سوی قانون دقیقاً تعریف نشده باشند، ولی در میان افراد احساس انزجار و تنفر پدید آورند، چنین اعمالی که از سوی قانون محکوم نشده باشند، جرم شمرده نمی‌شود. مثلاً پدیده چند زنی در میان روشنفکران. شاید اغراق نباشد که بگوییم تئوری جامعه شناختی جرم در پی طرح و تاکید دورکیم، امروزه بدین پایه رسیده است (شیخاوندی،۱۳۸۵، ۶۰).

جرم در معنی عام کلمه فعل یا ترک فعل انسان است که جامعه آن را به دلیل اخلال در نظام اجتماعی به قید ضمانت اجرای کیفری منع کرده است (اردبیلی،۱۴۰۲، ج ۱، ۱۳).

از نظر قانونی، جرم عبارت از عمل یا ترک عملی که قانون آن را پیش بینی نموده و برای ترک یا ارتکاب آن مجازات تعیین نموده باشد. به عبارت دیگر جرم، عمل یا خودداری از عملی است که مخالف نظم و صلح و آرامش اجتماعی بوده و از همین حیث مجازاتی برای آن تعیین نموده باشند (شامبیاتی،۱۴۰۲، ج ۱، ۲۲۲).

علیرغم وجود دیدگاه‌ها و رویکردهای مختلف در زمینه بررسی پدیده جرم، هنوز تعریف جامع، کامل و روشنی از جرم ارائه نشده است که مورد تأیید همگان باشد.

ماده ۲ قانون مجازات اسلامی ۱۳۷۰ بیان می‌داشت: «جرم عبارت است از هر فعل یا ترک فعلی که در قانون برای آن مجازات تعیین شده باشد».

اما ماده ۲ قانون مجازات اسلامی مصوب ۱۳۹۲ در مقام تعریفی از جرم بیان می‌دارد: «هر رفتاری اعم از فعل یا ترک فعل که در قانون برای آن مجازات تعیین شده است، جرم محسوب می‌شود».

[Downloaded from jlawst.ir on 2026-09-08]

شماره ۵۱،
دوره ۱۱،
سال پنجم،
مستان ۱۴۰۲،
صص ۱-۱۸

مزایای هوش مصنوعی در دنیای امروز

هوش مصنوعی دارای مزایا و فواید فراوانی است که تأثیر قابل توجهی در جوامع و صنایع دارد. در زیر، به برخی از مزایای کلیدی هوش مصنوعی اشاره خواهم کرد:

۱- قدرت پردازش و تحلیل بزرگ‌تر

هوش مصنوعی قادر به پردازش حجم عظیمی از داده‌ها و تحلیل آنهاست. این امر به کارآمدی بیشتر در تصمیم‌گیری‌ها، پیش‌بینی‌ها و بهبود فرآیندهای کسب و کار منجر می‌شود. به عبارتی، هوش مصنوعی امکان پردازش حجم عظیمی از داده‌ها و تحلیل آنها را داراست. از طریق تکنیک‌های مختلفی مانند یادگیری ماشین، شبکه‌های عصبی عمیق، الگوریتم‌های استنتاج و داده‌کاوی، هوش مصنوعی قادر است به تجزیه و تحلیل داده‌های بزرگ و استخراج الگوها و ارتباطات مهم از آنها. با پردازش حجم عظیمی از داده‌ها، هوش مصنوعی می‌تواند الگوهای پنهان و ارتباطات پیچیده‌تر را کشف کند و اطلاعات ارزشمندی را از داده‌های به نظر اولیه بی‌ارزش استخراج کند. این امر می‌تواند در تصمیم‌گیری‌های استراتژیک، پیش‌بینی روندها، بهبود فرآیندهای کسب و کار، بهبود تجربه کاربری و بهبود عملکرد سیستم‌ها و خدمات مختلف مفید باشد. با توجه به پیشرفت‌های اخیر در زمینه هوش مصنوعی و قدرت محاسباتی بالا، قدرت پردازش و تحلیل داده‌ها به طور عمده افزایش یافته است. این امکان به سازمان‌ها و کسب و کارها کمک می‌کند تا از داده‌های خود بهره‌برداری بهتری داشته باشند و تصمیم‌گیری‌های بهتری را بر اساس اطلاعات قابل استخراج از داده‌ها انجام دهند (نجاتی و همکاران، ۱۴۰۰: ۸-۹).

۲-اتخاذ تصمیمات بهتر

با توجه به توانایی هوش مصنوعی در تجزیه و تحلیل داده‌ها و استخراج الگوها، این فناوری قادر به ارائه تصمیمات بهتر و مبتنی بر شواهد و داده‌های واقعی است. این مزیت بهبود قابل توجهی در عملکرد و کارایی سازمان‌ها و سیستم‌های مختلف به همراه دارد. هوش مصنوعی با توانایی تجزیه و تحلیل داده‌ها و استخراج الگوها می‌تواند تصمیمات بهتر و مبتنی بر شواهد و داده‌های واقعی را ارائه کند. با استفاده از الگوریتم‌ها و مدل‌های هوش مصنوعی، می‌توان داده‌های بزرگ را به صورت خودکار و سریع تحلیل کرده و نتایجی که بر اساس آنها تصمیم‌گیری می‌شود، ارائه داد. با تکیه بر شواهد و داده‌های واقعی، تصمیمات گرفته شده توسط هوش مصنوعی می‌توانند به دقت و قابلیت پیش‌بینی بالا دست یابند. این تصمیمات مبتنی بر داده‌های واقعی می‌توانند به مدیران و تصمیم‌گیرندگان کمک کنند تا از تصمیم‌گیری‌های احساسی و بر اساس حدس و گمان خودداری کنند و به جای آن، تصمیماتی را اتخاذ کنند که بر اساس آمار و شواهد قابل ارائه هستند. با تصمیمات بهتر و مبتنی بر داده‌های واقعی، سازمان‌ها و سیستم‌ها می‌توانند عملکرد و کارایی خود را بهبود بخشند. این بهبود می‌تواند به دلیل بهبود فرآیندها، کاهش هزینه‌ها، افزایش بهره‌وری، بهبود تجربه کاربری و افزایش رقابت‌پذیری سازمان باشد. همچنین، با توجه به قابلیت پیش‌بینی هوش مصنوعی، می‌توان مشکلات و خطرات آینده را پیش‌بینی کرده و اقدامات مناسبی را در جهت پیشگیری از آنها انجام داد (سهرابی و همکاران،۱۴۰۱: ٤٠).

۳-افزایش دقت و کارایی

هوش مصنوعی قادر به انجام کارها با دقت بالا و کارایی بیشتر است. در بسیاری از حوزه‌ها مانند تشخیص الگو، تشخیص تصاویر و صدا، ترجمه زبانی، پردازش زبان طبیعی و خودران‌سازی، هوش مصنوعی به دقت و کارایی بهتری نسبت به روش‌های سنتی دست پیدا کرده است. هوش مصنوعی با قابلیت‌های خود می‌تواند در بسیاری از حوزه‌ها دقت بالا و کارایی بهتری نسبت به روش‌های سنتی ارائه دهد. در زمینه تشخیص الگو، مانند تشخیص چهره، تشخیص اشیا، تشخیص الگوهای زمانی، هوش مصنوعی با استفاده از شبکه‌های عصبی عمیق و یادگیری ماشین قادر است به دقت بالایی در تشخیص و تحلیل الگوها برسد. در حوزه تشخیص تصاویر و صدا، هوش مصنوعی می‌تواند با استفاده از شبکه‌های عصبی عمیق و الگوریتم‌های پیچیده دقت

[Downloaded from jlawst.ir on 2026-09-08]

شماره ۵۱،
دوره ۱۱،
سال پنجم،
مستان ۱۴۰۲،
صص ۱-۱۸

بالایی در تشخیص و تحلیل تصاویر و صداها داشته باشد. به عنوان مثال، در تشخیص تصاویر پزشکی مثل سرطان، هوش مصنوعی قادر است به طور دقیق و با کارایی بیشتری در تشخیص و تفسیر تصاویر کمک کند. در زمینه ترجمه زبانی و پردازش زبان طبیعی، هوش مصنوعی می‌تواند با استفاده از مدل‌های زبانی پیشرفته، دقت بالا در ترجمه متون و تفسیر متون مختلف را به ارمغان آورد. همچنین، در حوزه خودران‌سازی، هوش مصنوعی با استفاده از الگوریتم‌های مبتنی بر شبکه‌های عصبی و یادگیری تقویتی، قادر است به دقت و کارایی بیشتری در کنترل خودروها و سیستم‌های خودران شود. به طور کلی، با توجه به توانایی هوش مصنوعی در استفاده از الگوریتم‌های پیچیده و پردازش داده‌های بزرگ، می‌تواند دقت و کارایی در بسیاری از حوزه‌ها را بهبود بخشد و نتایج بهتری نسبت به روش‌های سنتی ارائه دهد. با ادغام هوش مصنوعی در فرآیندهای کسب و کار، می‌توان به بهبود عملکرد و افزایش توانایی‌های سازمان‌ها و سیستم‌ها دست یافت (طهماسبی،۱۳۸۵: ۱۳۵).

٤-امکانات خودکارسازی

هوش مصنوعی قادر به خودکارسازی فرآیندها و وظایف است. این امکان به سازمان‌ها کمک می‌کند تا فرآیندهای خود را بهبود داده و بهبود کارایی و بهره‌وری را تجربه کنند. همچنین، خودران‌سازی بخشی از تکنولوژی هوش مصنوعی است که در صنایع مانند خودرو، تولید، حمل و نقل و سلامت بسیار کاربرد دارد. با استفاده از هوش مصنوعی، می‌توان الگوریتم‌ها و مدل‌هایی را طراحی کرد که به طور خودکار و بدون نیاز به دخالت انسانی، وظایف و فرآیندهای مختلف را انجام دهند. در صنایع مختلف، مانند خودروسازی، تولید، حمل و نقل و سلامت، خودران‌سازی به عنوان بخشی از تکنولوژی هوش مصنوعی به کار می‌رود. در صنعت خودرو، برای مثال، هوش مصنوعی می‌تواند در خودروهای خودران که با استفاده از سیستم‌های حسگری و پردازش تصویر و صدا کار می‌کنند، به کار رود. این خودروها قادرند به طور خودکار رانندگی کنند و فرآیندهای مربوط به تشخیص موانع، تصویربرداری، تشخیص علائم راهنمایی و رانندگی ایمن را انجام دهند. همچنین، در صنعت تولید، هوش مصنوعی می‌تواند در خودکارسازی فرآیندهای تولید و کنترل کیفیت کمک کند. با استفاده از الگوریتم‌ها و مدل‌های هوش مصنوعی، می‌توان فرآیندهای تولید را به صورت خودکار و با دقت بالا اجرا کرده و نیاز به دخالت انسانی را کاهش داد. در حوزه حمل و نقل، هوش مصنوعی می‌تواند در بهبود کارایی و کاهش ترافیک و مصرف سوخت کمک کند. با استفاده از الگوریتم‌ها و مدل‌های هوش مصنوعی، می‌توان به طور هوشمند ترافیک را کنترل کرده، بهینه‌سازی مسیرها و زمان‌بندی را انجام داد و مصرف سوخت را بهینه کرد. در حوزه سلامت، هوش مصنوعی می‌تواند در تشخیص بیماری‌ها، پیش‌بینی خطرات سلامت و بهبود فرآیندهای درمانی کمک کند. با استفاده از الگوریتم‌ها و مدل‌های هوش مصنوعی، می‌توان به طور دقیق تشخیص بیماری‌ها را ارائه داد و مداخلات درمانی را بهبود بخشید. با استفاده از خودران‌سازی و خودکارسازی فرآیندها و وظایف، سازمان‌ها قادرند بهبود کارایی، کاهش خطاها، افزایش بهره‌وری و کاهش هزینه‌ها را تجربه کنند. همچنین، با خودران‌سازی در صنایع مختلف، امکاناتی مانند کاهش حوادث رانندگی، بهبود فرآیندهای تولید، حمل و نقل هوشمندتر و بهره‌وری انرژی بیشتر فراهم می‌شود (ربیعی زاده،۱۳۹٦: ۲۹).

۵-ارتباطات هوشمند

هوش مصنوعی در سیستم‌های ارتباطی هوشمند مانند ربات‌ها، مساعدت‌کننده‌های صوتی مانند سیری و آلکسا و سیستم‌های مبتنی بر گفتار استفاده می‌شود. این سیستم‌ها قادر به تفسیر و پاسخ به دستورات صوتی انسان هستند و تجربه ارتباطی بسیار نزدیکتری را برای کاربران ایجاد می‌کنند. این سیستم‌ها از الگوریتم‌ها و مدل‌های یادگیری ماشین برای تفسیر دستورات صوتی انسان استفاده می‌کنند و سعی می‌کنند به طور خودکار و هوشمندانه به آن‌ها پاسخ دهند. یکی از روش‌های استفاده از هوش مصنوعی در این سیستم‌ها، تشخیص الگوهای صوتی است. با استفاده از مدل‌های یادگیری عمیق، سیستم‌ها قادر به تشخیص و شناسایی الگوهای صوتی مختلف می‌شوند و می‌توانند دستورات صوتی را تفسیر کنند. سپس با تحلیل و پردازش دستورات،

[Downloaded from jlawst.ir on 2026-09-08]

شماره ۵۱،
دوره ۱۱،
سال پنجم،
زمستان ۱۴۰۲،
صص ۱-۱۸

سیستم‌ها تلاش می‌کنند به درخواست‌ها و نیازهای کاربران پاسخ دهند. هوش مصنوعی در این سیستم‌ها به طور مداوم در حال بهبود است و تلاش می‌شود تا تفاهم بیشتری در مورد دستورات صوتی انسان به وسیله استفاده از پردازش زبان طبیعی و تکنیک‌های مرتبط با هوش مصنوعی به دست آید. این سیستم‌ها با ارائه پاسخ‌های منطقی و مفهومی به دستورات صوتی کاربران، تجربه ارتباطی نزدیکتری را فراهم می‌کنند و به کاربران امکان می‌دهند تا با سیستم‌ها به صورت طبیعی و صمیمی‌تر ارتباط برقرار کنند (موسایی و همکاران، ۱٤۰۰: ۱۰۹).

٦-خودکارسازی و اتوماسیون

هوش مصنوعی قادر است وظایف و فرآیندهای مختلف را خودکارسازی کند و این امکان بهبود بهره‌وری و کارایی در صنایع و سازمان‌ها را به همراه دارد. مثال‌هایی که ارائه دادید، از جمله خودران‌سازی در خط تولید، خودروهای خودران و رباتیک، عملکردهای رایجی از هوش مصنوعی هستند. در خطوط تولید، هوش مصنوعی و رباتیک می‌توانند برای خودران‌سازی فرآیندها و وظایف مورد استفاده قرار بگیرند. با استفاده از سامانه‌های هوشمند و ربات‌ها، می‌توان فرآیندهای تولید را به طور خودکار و بدون نیاز به دخالت انسانی انجام داد. این منجر به کاهش خطاها، افزایش سرعت و دقت تولید، و بهبود بهره‌وری می‌شود. همچنین، خودروهای خودران نیز از تکنولوژی هوش مصنوعی بهره می‌برند. سیستم‌های هوشمند درون خودروها، با استفاده از حسگرها، داده‌ها را جمع‌آوری کرده و تحلیل می‌کنند تا بتوانند خودرو را بدون نیاز به راننده به طور خودکار کنترل کنند. این شامل اموری مانند تشخیص علائم راهنمایی و رانندگی، تشخیص موانع و خطرات و کنترل سرعت و فاصله از خودروهای دیگر است. به طورکلی، هوش مصنوعی در بسیاری از صنایع و سازمان‌ها، امکان خودکارسازی و بهبود بهره‌وری را فراهم می‌کند. این فناوری در طول فرآیندهای مختلف مانند تولید، خدمات مشتری، مدیریت منابع، تصمیم‌گیری‌های استراتژیک و غیره، تأثیر قابل توجهی دارد (شهبازی و همکاران، ۱٤۰۱: ۱۳-۱٤).

۷-سازماندهی و مدیریت داده‌ها

هوش مصنوعی قادر است به سازماندهی و مدیریت داده‌های بزرگ کمک کند. با توجه به توانایی‌های پردازشی قوی و الگوریتم‌های پیشرفته، هوش مصنوعی می‌تواند به طور خودکار داده‌های بزرگ را تحلیل و سازماندهی کند. هوش مصنوعی می‌تواند الگوها، روابط و اطلاعات مفید را در داده‌های بزرگ شناسایی کند. با استفاده از روش‌های یادگیری ماشینی و شبکه‌های عصبی، هوش مصنوعی قادر است الگوهای پنهان و ارتباطات میان داده‌ها را کشف کند که به صورت سنتی ممکن نبوده است. علاوه بر آن، هوش مصنوعی می‌تواند در وظیفه‌هایی مانند ترتیب‌بندی، تصفیه و تهیه خلاصه اطلاعات از داده‌های بزرگ کمک کند. به طور مثال، با استفاده از الگوریتم‌های خوشه‌بندی، هوش مصنوعی می‌تواند داده‌های مشابه را در گروه‌های جداگانه دسته‌بندی کند و اطلاعات خلاصه شده‌ای از هر گروه ارائه دهد. با استفاده از هوش مصنوعی در سازماندهی و مدیریت داده‌های بزرگ، امکان دسترسی سریع‌تر و دقیق‌تر به اطلاعات موجود فراهم می‌شود. این باعث می‌شود تصمیم‌گیران و مدیران بتوانند تصمیمات بهتری بگیرند و بهبود عملکرد سازمان را تجربه کنند. به هر حال، استفاده مؤثر از هوش مصنوعی در سازماندهی داده‌های بزرگ نیازمند آماده‌سازی و پیش‌پردازش مناسب داده‌ها، انتخاب الگوریتم‌ها و مدل‌های مناسب، و نظارت و ارزیابی مداوم بر عملکرد سیستم هوش مصنوعی است (عظیمی و اسماعیلی،۱٤۰۰: ۹۷).

جرایم ارتکابی با هوش مصنوعی

به دلیل پیشرفت روز افزون تکنولوژی همواره جرائم جدیدی رخ می‌دهد که گاه برخی از آنان مستقیماً در قانون پیش بینی نشده‌اند و این امر کار دستگیری این مجرمان و قضاوت در این قبیل پرونده‌ها را دشوار می‌نماید. در نتیجه تغییر و به روز رسانی قوانین در این حوزه بیش از سایر حوزه‌ها ضروری به نظر می‌رسد. البته اهمیت موضوع فقط در جرم انگاری جرائم نیست، بلکه نحوه جمع آوری ادله الکترونیکی و تکالیف کسب و کارهای الکترونیکی نیز از مسایلی است که خوشبختانه به

[Downloaded from jlawst.ir on 2026-09-08]

شماره ۵۱،
دوره ۱۱،
سال پنجم،
مستان ۱۴۰۲،
صص ۱-۱۸

درستی مورد توجه قانون گذار در ایران واقع شده‌اند. لازم به ذکر است جز آنچه در قوانین و مقررات موجود به طور خاص مورد توجه قرار گرفته‌اند؛ جرایمی وجود دارند که در برخی کشورهای دنیا به شکل ویژه‌ای تعیین مجازات شده‌اند و بهتر بود در ایران نیز قانونگذار به این موضوعات نگاه متفاوتی می‌داشت. برای مثال، مسایلی هم چون جرائم جنسی در قوانین مورد بحث قرار گرفته‌اند. متاسفانه میان جرائم جنسی علیه کودکان و بزرگسالان در قوانین ما تفکیک چندانی صورت نگرفته است. در حالی که این موضوع در خصوص کودکان اهمیت دو چندان داشته و در نتیجه برخورد جدی‌تری را می‌طلبد. این موضوع درجرایم جنسی صورت گرفته علیه کودکان در فضای سایبری با توجه به امکان افزایش تعداد بزهدیدگان و آثار مخرب شدیدتر آن علاوه بر دقت بیشتر در نظارت و پیشگیری‌های لازم مجازات‌های شدیدتری را برای مجرمان ایجاب می‌نماید (اسلامی،۱۳۹۱، ۱۵-۱۶).

مهم‌ترین جرائم نوپدید با بهره گیری از فناوری هوش مصنوعی به قرار زیر می‌باشند:

۱-سوءاستفاده جنسی

از دیگر خطرات جدی هوش مصنوعی به عنوان منشأ جرائم رایانه‌ای در فضای مجازی، سوءاستفاده جنسی است، که در دوران کنونی بیشتر متوجه کودکان و نوجوانان است. کودکان و نوجوانان، به خصوص در جوامع پیشرفته که استفاده از اینترنت در خانه و مدرسه برای آنان میسر است، خاصه از طریق اتاق‌های چت و گپ زنی مورد اغفال و سواستفاده جنسی قرار می‌گیرند. گاه افرادی با ضبط تصاویر خصوصی و احیاناً غیر اخلاقی از طریق دوربین اینترنتی[1] و یا به دست آوردن اطلاعات و عکس‌های خصوصی بزه‌دیدگان آنان را وادار به پذیرش رابطه جنسی فیزیکی می‌کنند و یا پس از آشنایی از طریق چت با قرار گذاشتن و حضور فیزیکی دختران در محل، آنان را مورد تجاوز قرار می‌دهند. در مواردی با ارسال تصاویر مستهجن، افراد به ویژه نوجوانان را ترغیب به برقراری رابطه نامشروع جنسی می‌کنند. در مواردی اغفال دختران و نوجوانان به صورت باندی صورت می‌گیرد (فرهمند،۱۳۸۷، ۱۳۹).

بنابر مطالعاتی که در غرب در این زمینه انجام گرفته است، اغلب نوجوانانی که مورد اغفال و سوءاستفاده جنسی واقع می‌شوند، زیر ۱۸ سال سن دارند و در بیشتر موارد تصاویر تحریک کننده‌ای از طریق چت یا تلفن همراه برایشان ارسال و سپس از آنها برای حضور فیزیکی در محل خاصی دعوت شده و بدین ترتیب فریب خورده و مورد تجاوز جنسی واقع می‌شوند. این مسئله در حال حاضر، به یکی از معضلات جدی در مغرب زمین مبدل شده است؛ چندان که غالب دانشمندان و سیاست‌گذاران به این امر بیش از پیش وقوف و توجه داشته‌اند و مقالات، کتاب‌ها و همایش‌های متعددی در ارتباط با آن برگزار کرده‌اند. برای مثال، ده سال پس از تصویب کنوانسیون حقوق کودک توسط سازمان ملل در سال ۱۹۸۹ م؛ یعنی در سال ۱۹۹۹ م گردهمایی جهانی تحت عنوان کارشناسی برای حمایت کودکان در برابر سوء استفاده جنسی از طریق اینترنت برگزار گردید، که منجر به صدور قطعنامه‌ای شد که در آن آمده است: «هر چه اینترنت بیشتر توسعه پیدا کند، کودکان بیشتر در معرض محتویات خطرناک آن قرار خواهند گرفت. فعالیت‌های مجرمانه مربوط به فحشای کودکان و پورنوگرافی آنان، که از طریق اینترنت مورد سوءاستفاده واقع می‌شوند، اکنون از مسائل حاد به شمار می‌رود. اگر چه سودمندی‌های هوش مصنوعی از زیان‌های بالقوه آن بیشتر است، در عین حال نباید از شناخت خطرات آن، غفلت کرد. در صورتی که برای مقابله با این خطرات، اقدامی صورت نگیرد، تهدیدهای سنگین آن بر کودکان باقی خواهد ماند و سبب بازداری از کاربرد صحیح هوش مصنوعی در آینده خواهند شد (دوران[2]،۲۰۱٤، ۲۳).

۲-انحرافات جنسی

[1]- Web Cam

[2]- Duran

[Downloaded from jlawst.ir on 2026-09-08]

شماره ۵۱،
دوره ۱۱،
سال پنجم،
مستان ۱۴۰۲،
صص ۱–۱۸

از جمله آثار مخرب هوش مصنوعی، به ویژه جرائم مرتبط با محتوا (به قول قانون مجازات جرائم رایانه‌ای) به وجود آمدن انحرافات جنسی و اختلالات جنسی است. هوش مصنوعی به دلیل رویکرد آزاد اندیشی در روابط جنسی از سوی گردانندگان اصلی آن (یعنی غرب و به ویژه آمریکا) و نگرش تجاری نسبت به مسائل جنسی موجب پدید آمدن پدیده کثیفی به نام هرزه نگاری و هنر پلید شهوانی و رواج سرسام آور آن گردید، که مرزهای اخلاقی را درهم می‌شکند و تهدیدی برای فرهنگ‌ها، به ویژه فرهنگ‌های دینی، چون فرهنگ اسلامی است. اصولاً، پورنوگرافی به عنوان نمایش تصویری و یا کلامی، رفتارهای جنسی است که با هدف ارضای خواسته‌های جنسی دیگران تعریف می‌شود. این گونه مطالب و تصاویر که در پی تحریک جنسی دیگران عرضه می‌گردد، معمولاً به ارضای غیر طبیعی جنسی مراجعه کنندگان آن می‌انجامد. نکته دیگر اینکه رجوع به اینترنت برای دسترسی به مطالب مستهجن صرفاً به افراد نابهنجار خلاصه نمی‌شود و حجم قابل توجهی از مراجعان را افراد طبیعی تشکیل می‌دهند. اصولاً هوش مصنوعی به جوی دامن زده که در سایه ویژگی‌های خاص خود به تدریج به شکل گیری ناهنجاری‌های جنسی در کاربران خود می‌انجامد و منشأ به وجود آمدن بسیاری از جرائم رایانه‌ای (به ویژه محتوایی) و مقدمه‌ای برای جرائم جنسی می‌گردد. دلایل رجوع و اقبال مردم به این گونه مطالب را در عرصه اینترنت می‌توان در این موارد خلاصه نمود:

الف– گمنامی: ناشناخته ماندن مراجعان در عرصه اینترنت، به نوعی اعتماد به نفس در افراد را دامن می زند و این حالت، نوعی رفتار غیرمسئولانه را در فرد شکل می‌دهد. مراجعان در چنین شرایطی است که به خود اجازه می‌دهند تا برخلاف رفتارهای طبیعی به راحتی از دسترس زوج اینترنتی خود دور شوند و یا بلافاصله به فرد دیگری روی آورند. حتی در چنین شرایطی، مردان به خود اجازه می‌دهند تا در خلوت خود به فکر داشتن تجربه سکسی با مردان هم بیندیشند. در چنین فضایی است که فرد بدون هیچ گونه دردسری و به نحوی ناشناخته می‌تواند با مفاهیمی، چون سکس گروهی، همجنس بازی، مبدل پوشی جنسی و. . آشنا شود. اصولاً در چنین فضایی است که فرد می‌تواند در معرفی خود هرگونه که می‌خواهد عمل کند و همین ویژگی، خود محرکی است تا کاربران اینترنتی به استفاده از هویت جعلی روی آورند و این را می‌توان از جمله ویژگی‌های فرهنگی فضای مجازی برشمرد، که این خود زمینه‌ای برای ارتکاب جرائم فضای سایبر نیز هست(شیرزاد،۱۳۹۰، ٦٩) .

ب–سهولت: مطالب شهوانی و تصاویر سکسی به آسانی در دسترس همگان قرار دارند. عرضه گسترده این مطالب و وجود تعداد بی شمار اتاق‌های گفتگوی سکسی، هر کاربری را به داشتن اولین تجربه در این حوزه تحریک می ند. یک زن یا شوهر کنجکاو به راحتی و دور از دیدگان همسرش وارد این فضاها می‌شود و گفتگوهای سکسی با دیگران را تجربه می‌کند چنین سهولتی است که بسیاری را به تجربه رفتارهای ناهنجاری جنسی نه در فضای فیزیکی، بلکه در فضای مجازی هدایت می‌کند. به ویژه اگر نظارت نهادهای مسئول در کشورها در این زمینه کم رنگ و ناتوان باشند(کوثری،۱۳۸۷: ۹٤).

ج–گریز از واقعیت: مراجعه کنندگان به این سایت‌ها، تجربه داشتن نوعی ارضای جنسی اینترنتی را دلیل اصلی رجوعشان معرفی می‌کنند. مطالعات نیز نشان می‌دهد که ارضای جنسی دلیل اولیه درگیر شدن فرد به سکس مجازی است. اما از جمله پیامدهای این رفتار، واقعیت گریزی و گسترش چنین تجربه‌ای است. به عنوان مثال یک زن تنها، ناگهان در چنین فضایی، نوعی گریز عقلانی را تجربه کرده و شخصیت و هویت جدیدی را در چنین فضایی در خود شکل می‌دهد، که خود منشأ به وجود آمدن رفتارهای نابهنجار و اباحه گری جنسی می‌گردد. با اعتیاد به این مسائل، به ویژه به صورت مجازی افراد دچار اختلالات و انحرافات گوناگون جنسی می‌شوند، که نتیجه آن به خطر افتادن سلامت روانی و حتی جسمی جامعه خواهد بود. از جمله انحرافات جنسی ناشی از این فضا، اعتیاد جنسی، خود ارضایی که در کاربران مطالب مستهجن شیوع زیادی دارد ارضای جنسی به وسیله اشیاء اباحه گری جنسی، همجنس بازی، از بین رفتن حیای اخلاقی است(عالی پور،۱۳۹۰، ۱۲۵–۱۲٦).

[Downloaded from jlawst.ir on 2026-09-08]

شماره ۵۱،
دوره ۱۱،
سال پنجم،
مستان ۱۴۰۲،
صص ۱-۱۸

البته شیوع انحرافات جنسی از این قبیل، به ویژه با گسترش هوش مصنوعی و شیوع استفاده از آن در میان جوانان، آثار مخرب اجتماعی نیز خواهد داشت که تا حدی بقای جامعه و نسل بشری را نیز به خطر خواهد انداخت.

۳-فیشینگ

در صورت ارتباط با کامپیوتر و دنیای اینترنت ممکن است با اصطلاحی به نام فیشینگ برخورد کرده اما معنای آن را به خوبی متوجه نشده باشید. فیشینگ[۱]، عبارت است از به‌دست آوردن اطلاعات شخصی افراد مانند نام کاربری، گذرواژه، اطلاعات حساب بانکی و... از طریق جعل یک وب‌گاه، نشانی پست الکترونیک و... . به عبارت دیگر روشی است تا افراد سودجو با ایجاد وب‌گاه‌ها یا پست الکترونیک‌های قلابی به تحریک و ترغیب شما بپردازند و اطلاعات حساس و شخصی‌تان را به منظور سرقت یا کلاهبرداری دریافت کنند. در فیشینگ ابتدا فرد از طریق پست الکترونیک، آگهی‌های تبلیغاتی یا صفحات قلابی پایگاه‌های گوناگون به یک صفحه ساختگی راهنمایی می‌شود. سپس از او خواسته می‌شود تا اطلاعات حساسی را مانند اطلاعات کارت اعتباری در آنجا وارد کند. در صورت گمراه شدن فرد و وارد کردن اطلاعات، فیشرها (مرتکبان فیشینگ) به اطلاعات شخص دسترسی پیدا و به این ترتیب از او کلاهبرداری می‌کنند، مانند اینکه افرادی نشانی وب‌گاه یک بانک را با کمی تغییر و بسیار شبیه نشانی اصلی جعل و به این ترتیب از اطلاعات شخصی مراجعه کنندگان به پایگاه آگاه می‌شوند و از آن اطلاعات سودجویی می‌کنند. فیشینگ به صورت‌های گوناگونی اجرامی شوداما برخی راه‌ها رایج‌تر است و بیشتر از بقیه مورد استفاده قرار می‌گیرند. پست الکترونیک‌های قلابی از طرف افرادی که ادعا می‌کنند همکار شما بوده یا شما را می‌شناسند، تبلیغات دروغین و غیرواقعی در شبکه‌های اجتماعی، وب‌گاه‌های قلابی برای امور خیریه و تأسیس وب‌گاه‌هایی با نام‌های مشابه وب‌گاه‌های شناخته‌شده از اصلی‌ترین روش‌های اجرای این نوع کلاهبرداری است. فراموش نکنید که این افراد به طورمعمول پایگاه‌هایی با ظاهری آراسته و تیترهای رسمی از سازمان‌ها، شرکت‌ها، بانک‌ها یا مؤسسات مالی ایجاد می‌کنند، زیرا برای فریب مردم لازم است همه چیز تا آنجا که ممکن است واقعی به نظر برسد. فیشینگ جز رواج بی‌اعتمادی بین مردم، تحصیل مال نامشروع و اختلال و بی نظمی در ساختار اقتصادی و اجتماعی جامعه اثری ندارد؛ به همین دلیل قانونگذار آن را جرم دانسته و برای مرتکبان مجازات در نظر گرفته است. مواد ۱۲ و ۱۳ قانون جرائم رایانه‌ای مصوب ۱۳۸۹ به موارد کلاهبرداری اینترنتی می‌پردازد و مجازات آن را بیان می‌کند. این قانون در ماده ۱۳ در مقام بیان مجازات کلاهبرداری اینترنتی بیان می‌کند که مرتکبان علاوه بر رد مال به صاحب آن به حبس از یک تا پنج سال یا جزای نقدی از بیست تا یکصد میلیون ریال یا هر دو مجازات محکوم خواهند شد (اوجاقلو و زندی،۱۳۹٦، ٤۹).

فیشینگ راهی است که تبهکاران، اطلاعاتی نظیر کلمه کاربری، رمز عبور، شماره ۱٦ رقمی عابر بانک، رمز دوم را از طریق ابزارهای الکترونیکی ارتباطات به سرقت می‌برند. شبکه‌های حراجی و درگاه‌های پرداخت آنلاین نمونه‌ای از ابزارهای الکترونیکی ارتباطات می‌باشد. کلاهبرداری فیشینگ از طریق ایمیل‌ها و پیام‌ها صورت می‌پذیرد و قربانیان به صورت مستقیم اطلاعات حساس و محرمانه خود را در یک وب سایت‌های جعلی که در ظاهر کاملاً شبیه وب سایت‌های سالم و قانونی می‌باشد وارد می‌نماید. انواع تکنیک‌های حقه فیشینگ عبارتنداز:

۱- دستکاری و تقلب در لینک‌ها و آدرس‌ها: یکی از شیوه‌های متداول و رایج در فیشینگ ارسال لینک‌ها و آدرس متعلق به سازمان‌های غیرواقعی و جعلی از طریق ایمیل می‌باشد. آدرس‌هایی که تنها تفاوت آنها با آدرس اصلی یک یا دو حرف است یا از دامین‌های فرعی گمراه کننده برای ایجاد آنها استفاده گردیده است.

۲- دور زدن فیلتر: فیشرها با استفاده کردن از عکس به جای متن، کار فیلترهای ضد فیشینگ را که برای شناسایی متن‌هایی که عموماً در ایمیل‌های حاوی آدرس‌های جعلی یافت می‌شوند، را سخت کند

[۱]- Phishing

[Downloaded from jlawst.ir on 2026-09-08]

شماره ۵۱،
دوره ۱۱،
سال پنجم،
مستان ۱۴۰۲،
صص ۱-۱۸

۳- فیشینگ تب نبینگ: در واقع جدیدترین روش است که این برنامه از صفحاتی که کاربر باز کرده استفاده می‌کند و به‌طور آهسته کاربر را به سایت ساختگی ارجاع می‌دهد(ربیعی زاده،۱۳۹۶: ۱۰۲).

٤- دوقلوهای شرور[1] : روشی است که در واقع یک فیشر، یک شبکه بی سیم (وایرلس) ساختگی ایجاد می‌کند. این شبکه همانند شبکه‌های معتبر عمومی و و قانونی می‌تواند در مکان‌هایی مانند فرودگاه‌ها، هتل‌ها، و کافی‌شاپ‌ها وجود داشته باشد. . وقتی که یک نفر وارد شبکه جعلی می‌شود، کلاهبرداران سعی می‌کنند رمزهای عبور و یا سایر اطلاعات مرتبط با کارت اعتباری او را ثبت و ضبط کنند.

۳- حمله نفوذگر[2]: حمله نفوذگر به منظور تغییر ترافیک وب سایت به یک وب سایت جعلی دیگر است. در این بخش از شیادی، با دستگاری سرویس دهنده DNS توسط فرد شیاد که در اصطلاح فنی به «سمی[1]» شدن سرویس دهنده DNS کاربر معروف است. منجر می‌شود. کاربر به تصور این‌که وارد سایت اصلی بانک می‌شود وارد سایت جعلی فرد شیاد شده و اطلاعات محرمانه بانکی اعم از شماره حساب، شماره کارت و کلمه عبور را وارد می‌کند و آن‌گاه فرد شیاد به راحتی می‌تواند نسبت به سوء استفاده اقدام کند(فرجیها و علمداری،۱۳۹٦: ۵۷).

٤- فرآیند کپی کردن[3]: فرآیند کپی کردن اطلاعات نوار مغناطیسی کارت اعتبار مشتری از طریق کشیدن کارت از میان کارت‌خوان و استفاده از اطلاعات جهت ساخت کارت تقلبی توسط فرد شیاد را می‌نامند.

۵- دزدیدن کلمه عبور[4]: دزدیدن کلمه عبور دارنده کارت هنگام استفاده از دستگاه خودپرداز یا پایانه فروش از طریق مشاهده کاراکترهای وارد شده توسط کاربر را شامل می‌شود.

٦- سرقت کارت و کلمه عبور[5]: شیاد با قرار دادن یک قطعه در مدخل ورودی کارت‌خوان و قرار گرفتن پشت سر مشتری نسبت به سرقت کارت و کلمه عبور اقدام می‌کند. لایه بیرونی این قطعه مشابه دستگاه است و در آن نواری تعبیه شده است که اجازه نمی‌دهد کارت داخل قسمت‌های درونی دستگاه وارد شود و با کشیدن لایه بیورنی، کارت نیز با آن بیرون می‌اید. در این روش پس از گیر کردن کارت مشتری درون کارت‌خوان و عدم انجام عملیات، مشتری کلیدهای مختلفی را فشار داده و زمانی که مشتری مستاصل می‌شد به پیشنهاد شیاد دوباره کلمه عبور توسط مشتری به منظور رفع مشکل وارد می‌شود که کلمه عبور کارت در این شرایط سرقت می‌شود. مشتری بنابر پیشنهاد مجدد فرد شیاد به منظور اطلاع متصدیان امور بانکی از محل خودپرداز دور می‌شود که فرد شیاد نسبت به خروج قطعه به همراه کارت اقدام و از دستگاه خودپرداز دیگر وجوه موجود از حساب مشتری را سرقت می‌کند یا می‌رباید شایان ذکر است که در مطالعه و تحقیقی که توسط دیوید کارتر پرفسور و استاد دانشگاه میشگان صورت گرفته است شایع‌ترین جرمی که در سالهای اخیر در فضای سایبر یا سایبرسپیس[1] گزارش شده اسه کلاهبرداری کارت اعتباری بوده است(نادرخانی،۱۳۸۹: ۲۸).

۷- سوء استفاده از صندوق‌های پرداخت: این‌گونه کلاهبرداری از قدیم با استفاده از کارت‌های مسروقه، (کارت بانک) صورت می‌گرفت ولی امروزه با استفاده گسترده از سخت‌افزار و نرم‌افزار ویژه کامپیوتری، اطلاعات الکترونیکی کذب به صورت کد روی لبه‌های مغناطیسی کارت‌های بانک و اعتبار ثبت شده مورد سوء استفاده قرار می‌گیرد. مرتکبین این نوع کلاهبرداری شماره‌های محرمانه ضروری برای سوء استفاده از کارت‌ها را اغلب از طریق تجاوز به مکامه تلفنی، از طریق تدارک صفحه کلید جعلی، نفوذ کردن و یا مختل نمودن خطوط مخابرات داده‌ها را به دست می‌آورند.

---

[1]- Eviltwins
[2]- Pharming
[3]- Skimming
[4]- Shoulder surfing
[5]- Lebanese Loop

[Downloaded from jlawst.ir on 2026-09-08]

شماره ۵۱،
دوره ۱۱،
سال پنجم،
مستان ۱۴۰۲،
صص ۱-۱۸

۸- لینک‌های فیشینگ برای سازمان خیریه[۱]:هکرها با ارسال ایمیل خود را جای سازمان خیریه جا می‌زنند و لینک موجود در ایمیل شما را به دست سایت جعلی هدایت کرده و اطلاعات هویتی و کارت اعتباری شما را به سرقت می‌برند.

۹- پیش فاکتورهای جعلی با نام سرویس‌های پستی معتبر[۲]: از سرویس‌های پستی مانند UPS و فدرال اکسپرس ایمیل دریافت می‌کنید و در آن فاکتوری دیده می‌شود که درب خانه شما مثلاً یک تلویزیون می‌آید و باید هزینه پست را پرداخت کنید و شما نیز هول شده و پول را پرداخت می‌کنید در حالی که فاکتور با بدافزارها نصب شده روی سیستم شما به حساب حمله کننده می‌رود.

۱۰-سرقت آنلاین هویت و مشخصات فردی و بانکی[۳]: استفاده از سیستم وایرلس در کافی شاپ و اسکن کامپیوتر توسط هکرهایی که اطراف شما نشسته‌اند و سرقت اطلاعات. با توجه به موارد اشاره شده در مطالب فوق الذکر که راه‌هایی است که مرتکبین کلاهبرداری رایانه‌ای با ارتکاب این اعمال به وجه مال دسترسی پیدا می‌کنند.

٤-فارمینگ

فارمینگ، یک نوع حمله هکرهاست که موجب هدایت ترافیک یک وب سایت به سایت جعلی دیگر می‌شود. عبارت pharming یک واژه جدید بر اساس واژگان farming و phishing است. فارمینگ یک حمله مهندسی اجتماعی است برای دسترسی به گواهینامه‌های دستیابی مانند نام کاربری و اسم رمز. در سال‌های اخیر فارمینگ برای دسترسی به گواهینامه‌های دستیابی در سرقت‌های آنلاین به کار رفته‌اند. فارمینگ تبدیل به یکی از نگرانی‌های عمده برای تجارت الکترونیک و وب سایت‌های بانکداری آنلاین شده‌است. اقدامات پیشرفته‌ای که با عنوان anti-pharming شناخته شده‌اند، برای مقابله با این سرقت‌ها نیاز است. نرم‌افزارهای ضدویروس (رایانه) و نرم‌افزارهای پاک‌کننده جاسوس افزارها نمی‌توانند علیه فارمینگ حفاظت کنند. می‌تواند از طریق تغییر فایل‌های میزبان در یک کامپیوتر قربانی یا از طریق بهره‌برداری از قابلیت آسیب‌پذیری نرم‌افزارهای سامانه نام دامنه (DNS) صورت گیرد. درحالی که یک تشخیص نام دامنه بدخواهانه می‌تواند از به خطر انداختن تعداد زیادی از گره‌های مطمئن، که در name lookup شرکت کرده‌اند، به دست آید، اکثر نقاط آسیب پذیر در نزدیکی گره‌های آخر اینترنت قرار دارد. به عنوان مثال ورودی‌های نادرست در فایل‌های میزبان دستکتاپ که name lookup را با تبدیل نام محلی خود به آدرس IP به دام می‌اندازد، یک هدف محبوب برای بدافزارها می‌باشد. دسکتاپ‌ها، غالباً هدف‌های بهتری برای فارمینگ هستند، زیرا سرورهای اینترنتی مدیریت ضعیف‌تری روی آن‌ها دارند. بدتر از حملات فایل میزبان، به خطر افتادن یک رهیاب محلی است. وظیفه رهیاب‌ها این است که یک سامانه نام دامنه مطمئن جهت دسترسی به شبکه برای کارخواه‌ها تعیین کنند. حال اطلاعات نادرست در اینجا می‌تواند موجب خرابی جستجوها برای کل شبکه محلی شود. برخلاف بازنویسی‌های فایل میزبان، به خطر افتادن مسیریاب‌های محلی به سختی کشف می‌شود. رهیاب‌ها می‌توانند اطلاعات بدسامانه نام دامنه را به دو روش عبور دهند: با پیکربندی بد و نادرست محیط‌های موجود یا بازنویسی کامل نرم‌افزارهای تعبیه شده بسیاری از رهیاب‌ها برای ادمینستورها امکان تعیین یک سامانه نام دامنه ویژه و قابل اعتماد را در مکان پیشنهاد شده توسط گره‌های بالادستی مانند (ISP) فراهم می‌کنند (قابل دسترسی در http://irandad.org/tag).

یک حمله‌کننده می‌تواند یک سامانه نام دامنه را تحت کنترل خود درآورد و همه رزولوشن‌های بعدی از سرور نادرست عبور می‌کنند. یک سناریو شامل java script بد اندیش است که سامانه نام دامنه مسیریاب را تغییر می‌دهد. از سوی دیگر بسیاری از مسیریاب‌ها دارای توانایی جایگزینی سفت افزار (یعنی نرم‌افزار داخلی که سرویس‌های پیچیده‌تر دستگاه را انجام می‌دهند) خود هستند. مانند بدافزار در دسکتاپ‌ها، جایگزینی یک سفت افزار هم به سختی می‌تواند کشف شود. فارمینگ تنها یکی از

---

[۱]- Charityphishing

[2]- Fake invoices from delivery services

[3]- On line identity theft

[Downloaded from jlawst.ir on 2026-09-08]

شماره ۵۱،
دوره ۱۱،
سال پنجم،
مستان ۱۴۰۲،
صص ۱-۱۸

انواع حملات است که می‌تواند سفت افزار نادرست نصب کند، سایر موارد شامل حمله مردی در میان، شنود، و... است. همانند پیکربندی نامناسب کل شبکه محلی در معرض این رفتارها قرار می‌گیرند. این روش‌های فارمینگ به خودی خود فقط از نظر آکادمیک مورد توجه هستند. درحالی که مشتریان رهیاب‌های بی‌سیم‌ها در همه جا هستند و این خودنوعی آسیب‌پذیری کلان به وجود می‌آورد. دسترسی اجرایی به صورت بی‌سیم در اکثر این دستگاه‌ها امکان پذیر است. علاوه بر این چون این رهیاب‌ها غالباً با محیط‌های پیش‌فرض خود کار می‌کنند، رمزهای اجرایی معمولاً بدون تغییر باقی می‌مانند. حتی زمانی که رمزهای اجرایی تغییر می‌کنند بسیاری از آن‌ها از طریق حملات قابل حدس زدن هستند، چون بیشتر مشتریان رهیاب‌های بی سیم خطاهای زمانی را برای ورود به سیستم ناموفق نشان نمی‌دهند. وقتی دستیابی اجرایی تائید شد، همه محیط‌های رهیاب حتی خود سفت افزار ممکن است تغییر کند. این فاکتورها برای به خطر انداختن رهیاب‌ها استفاده می‌شوند. این حملات به سختی ردیابی می‌شوند، زیرا خارج از خانه یا ادارات کوچک و خارج از اینترنت روی می‌دهند (قابل دسترسی در وب سایت: https://pvlearn.com).

۵-هک یا دسترسی غیرمجاز

با پیشرفت علم و فراگیر شدن استفاده از هوش مصنوعی و عدم وجود محدودیت سنی و جسیتی و قومیتی برای استفاده از این فضا، باعث شده است که هر فردی با هر عقیده و دیدگاهی از این فضا استفاده کند و این یک جنبهٔ مثبتی است که هیچ کس از محرومیتی برخوردار نیست. در مقابل؛ بالطبع این فراگیری باعث ورود افراد سودجو و تبهکار می‌شود و این خود جنبهٔ منفی این شمول است. با تصویب قانون مبارزه با جرایم رایانه‌ای در کشور ما و جرم انگاری آن توسط مقنن این موضوع را روشن می‌کند که مسألهٔ هک کردن و دسترسی غیر مجاز به اطلاعات در شبکه‌های اجتماعی و فضای مجازی یک معضل و مشکلی را به وجود آورده است. هرچند تمام کشورها از این قاعده مستثنی نیستند و تمام آن‌ها درگیر این مشکل شده اند. هک کردن، به معنی سود بردن از یک روش سریع و هوشمندانه برای حل یک مشکل در رایانه است. در علوم رایانه‌ای هک مساوی، کِرک است که معنی رمز گشایی می‌دهد. گستردگی واژه هک فقط منحصر به رایانه نیست و توسط افراد گوناگون در زمینه‌هایی از قبیل: موسیقی، نقاشی و... بکار می‌رود. این واژه برای اولین بار در مؤسسه فناوری ماساچوست در سال ۱۹۶۰بکار رفت. معنی اصلی آن سود بردن از یک روش سریع و هوشمندانه برای حل مشکل تکنیکی بوده است. در دهۀ اخیر دانشمندان توانسته‌اند که حتی سلول‌های بدن انسان را نیز هک کنند (خالقی و احمدی شریفی،۱۳۹۶، ۳).

منظور از دسترسی غیرمجاز به اطلاعات فضای مجازی و شبکه‌های اجتماعی این است که فرد بزهکار با نقض تدابیر امنیتی و به صورت غیرمجاز به داده‌های حفاظت شده دست یابد. برخی دسترسی غیرمجاز را در زیر مجموعۀ جرایم علیه فناوری محض قرار می دهند. برخی دیگر آن را در زمرۀ جرایم علیه محرمانگی و تمامیت و در دسترس بودن سیستم ها و داده های رایانه ای قلمداد می کنند. دسترسی غیرمجاز را از منظر حقوق کیفری رایانه‌ای را می‌توان در زمرۀ جرم های رایانه‌ای محض دانست؛ زیرا، اولا از جرم‌های مرتبط با سیستم های رایانه ای است، ثانیا تنها در محیط سامانه های رایانه ای و فضای سایبر ارتکاب یافتنی است. از منظر حقوق کیفری برخی دسترسی غیرمجاز را در زمره جرم های علیه اموال می پندارند و برخی دیگر آن را از مقوله جرم های مالی یا اقتصادی می دانند(جلالی فراهانی،۱۳۸۸، ۱۹).

بنا به نظریه ای مفهوم جرم دسترسی غیرمجاز با توجه به موضوع آن و تعریف گفته شده و آنچه که در زمینه آن ارائه شده، به مفهوم جرایم علیه امنیت و اسایش عمومی نزدیک‌تر می‌نماید تا جرایم علیه اموال (عبدالهی، ۱۳۸۹، ٤۲).

به موجب ماده یک قانون جرایم رایانه‌ای مصوب ۱۳۸۸، به طور خاص دسترسی غیرمجاز را که یکی از مظاهر تجاوز به حریم خصوصی افراد در شبکه‌های اجتماعی و فضای مجازی است، جرم انگاری شده است. منطوق این ماده: «ماده۱ـ هرکس به طور غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی که به وسیله تدابیر امنیتی حفاظت شده است دسترسی یابد، به حبس

[Downloaded from jlawst.ir on 2026-09-08]

شماره ۵۱،
دوره ۱۱،
سال پنجم،
مستان ۱۴۰۲،
صص ۱-۱۸

از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون (۵/۰۰۰/۰۰۰) ریال تا بیست میلیون (۲۰/۰۰۰/۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد».

این رکن قانونی جرم دسترسی غیرمجاز به اطلاعات اشخاص است که ایراداتی نیز برآن وارد است. من جمله این ایرادات؛ عدم تعریف اصطلاحات غیرمجاز و تدابیر امنیتی که این امر تاحدی ابهام آمیز بودن ماده فوق را می‌رساند چرا که روشن نیست مقصود از غیرمجاز چه بوده و تدابیر امنیتی چه مواردی را در بر می‌گیرد. حال آن که می‌دانیم قانون باید واضح و شفاف باشد. ایراد دیگری که مطرح است مربوط به کیفر جزای نقدی است که به نظر می‌رسد میزان آن از بازدارندگی لازم در پیشگیری از این جرم برخوردار نباشد.

٦-هتک حیثیت و نشر اکاذیب

در کشور ما نیز همسو با تحولات جهانی با توسعه فناوری‌های مربوط به ضبط و انتشار تصویر و صوت گسترش اینترنت سبب شده تا هر روزه شاهد سوء استفاده از این وسایل علیه حیثیت و آبرو و حریم خصوصی افراد شویم که اگر تدبیر قانونی در این زمینه ظهور نکند دیری نخواهد پایید حریم خصوصی تبدیل به صحنه سوءاستفاده عمومی شده و روی سیاه فناوری اطلاعات، هویدا شده و باعث انتقاد همگانی به پیشرفت‌های بشری از یکسو و بی اعتمادی عمومی به دولت و قانونگذار در حفظ حریم خصوصی افراد از سوی دیگر خواهد شد. در بررسی حمایت قانونی از حیثیت افراد می‌توان به قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت‌های غیرمجاز می‌نمایند مصوب ۱۳۷۲ و ماده ٦٤٠ قانون مجازات اسلامی (تعزیرات حکومتی) اشاره کرد. همچنین با توجه به اشاره ماده ٦٩٨ این قانون به جرم نشر اکاذیب به عنوان جرمی عمومی باید متذکر شد که این جرم موضوع ماده (۱۷) لایحه جرائم رایانه‌ای هم می‌باشد. توهین رایانه‌ای، نوع جدیدی از جرم توهین سنتی است که در آن وسیله ارتکاب، رایانه می‌باشد. جرم توهین رایانه‌ای، به معنای نسبت دادن هر امر وهن‌آور اعم از دروغ یا راست به‌وسیله رایانه یا انجام فعلی که در نظر عرف و عادت موجب کسر شأن و یا باعث تخفیف و پست شدن فرد گردد. می‌توان هتک حرمت را نتیجه حاصل از توهین رایانه‌ای دانست. توهین رایانه‌ای از طریق رفتار، گفتار، اشارات و کلیه اظهارات شفاهی و کتبی توهین‌آمیز به‌وسیله رایانه صورت می‌گیرد. در توهین، خلاف واقع بودن اظهارات ضروری نیست؛ زیرا ممکن است اظهار توهین‌آمیز، اظهار واقعیت نیز باشد. در تشخیص رفتار و گفتار و اشارات موهن باید به عرف زمان و مکان وقوع جرم رجوع کرد. (میرمحمدصادقی،۱٤۰۲، ۱٦).

شخصیت طرفی که مورد اهانت واقع شده نیز در قضاوت عرف مؤثر است. در این جرم باید مخاطب معین باشد؛ توهین به یک مخاطب کلی، جرم نیست. همچنین مخاطب توهین رایانه‌ای باید شخص حقیقی باشد. این امر از لفظ «افراد» مذکور در ماده ٦۰۸ قانون مجازات اسلامی۱۳۹۲ استفاده می‌گردد و همچنین از کلماتی مثل صوت، تصویر و فیلم که در ماده «٦٤۰» قانون مجازات اسلامی‌آمده است؛ زیرا شخص حقوقی فاقد صوت و تصویر و فیلم است و شخصیتی اعتباری داشته، شخصیت و وجود مادی ندارد. زنده بودن مخاطب نیز شرط دیگری است که از ماده ٦۰۸ قانون مجازات اسلامی مستفاد می‌شود؛ زیرا فرد مرده، زنده تلقی نمی‌شود. حضوری یا علنی بودن، جز در موارد تصریح‌شده در قانون شرط تحقق جرم توهین نیست و از سوی دیگر، طبق قانون استفساریه ۱۳۷۹/۱۰/۱۰ نسبت به کلمه اهانت، توهین و یا هتک حرمت مندرج در مقررات جزائی مواد: ٦۰۸ و ٦۰۹ قانون مجازات اسلامی و بندهای ۷ و ۸ ماده ٦ و مواد ۲٦ و ۲۷ قانون مطبوعات توهین باید صریح باشد. ارتجالی بودن توهین رایانه‌ای نیز ضرورتی ندارد. توهین رایانه‌ای، هم شامل توهین بدوی و هم توهینی که در جواب دیگری است، می‌شود. توهین رایانه‌ای، مقید به نتیجه نیست. بنابراین، از جرائم مطلق می‌باشد؛ اما در توهین رایانه‌ای وسیله ارتکاب حتماً باید رایانه باشد. جرم توهین نیاز به عنصر روانی، یعنی عمد در توهین کردن دارد، که مستلزم معرفت داشتن فاعل نسبت به موهن بودن رفتار خود می‌باشد. البته سوءنیت خاص، مثل قصد اذیت و متألم کردن طرف، شرط نمی‌باشد. (میرمحمد صادقی، ۱٤۰۲، ۱۵۸).

[Downloaded from jlawst.ir on 2026-09-08]

شماره ۵۱،
دوره ۱۱،
سال پنجم،
مستان ۱۴۰۲،
صص ۱–۱۸

به عبارت دیگر، اولاً، مرتکب باید در فعل خود عامد باشد؛ نه این‌که در حالت خواب، بیهوشی، هیپنوتیزم و یا مستی و... باشد و در هر حال، باید با اراده و اختیار مرتکب رفتار موهن گردد. ثانیاً، از موهن بودن رفتار خود آگاه باشد. پس اگر به دلایلی مثل تفاوت فرهنگی و یا زبانی نسبت به امر جاهل باشد، توهین کیفری محقق نگشته است. از آنجا که جرم توهین رایانه‌ای صراحتاً در هیچ ماده‌ای از قوانین ذکر نشده و بدون مجازات ماندن مرتکبان این جرم نیز بر ارتکاب روزافزون آن خواهد افزود، به نظر می‌رسد باید طبق ماده۱۶ قانون جریم رایانه‌ای مصوب ۱۳۸۸ مرتکبان این جرم را به‌عنوان یکی از مصادیق هتک حرمت، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون ریال تا چهل میلیون ریال یا هر دو مجازات محکوم کرد. اما آنچه مدنظر است، ماده ٦٠٨ قانون مجازات اسلامی در خصوص توهین ساده و ماده ٦٠٩ در مورد توهین مشدد می‌باشد. مجازات توهین ساده بر اساس ماده ٦٠٨ شلاق تا ٧٤ ضربه و یا پنجاه هزار ریال تا یک میلیون ریال جزای نقدی است و مجازات توهین مشدد، حبس از ٣ تا ٦ ماه و یا تا ٧٤ ضربه شلاق و یا پنجاه هزار ریال تا یک میلیون ریال جزای نقدی می‌باشد. انتشار و اشاعۀ اخبار دروغ و وقایع خلاف واقع به قصد اضرار به غیر یا تشویش اذهان عمومی یا مقامات رسمی را نشر اکاذیب گویند. به عبارت دیگر، مقصود از اشاعه اکاذیب آن است که مرتکب مطالب و کارهایی را که می‌داند حقیقت ندارد عالماً و عامداً علیه شخص حقیقی یا حقوقی یا مقامات رسمی شایع و اظهار کند و بدون اینکه اعمال معینی را به افراد معینی نسبت دهد، اخبار یا مطالب بی اساس و دروغ را بیان کند(وروایی و همکاران،۱۳۹۳: ۵۹–٦٠).

عنصر مادی این جرم، اظهار و نشر اکاذیب یا نسبت دادن عمل خلاف حقیقت به شخص حقیقی یا حقوقی یا مقامات رسمی در شبکه‌های اجتماعی است که به یکی از راه‌های مذکور در ماده ۱۸ قانون جرایم رایانه ای محقق می‌شود. در حقیقت دو جرم در این ماده بیان شده است: اظهار اکاذیب و نسبت دادن مطلب غیر واقعی به شخص یا اشخاص حقوقی یا مقامات رسمی. اشاعه اکاذیب باید به وسیله نامه، شکوائیه، عریضه، گزارش یا توزیع هر گونه اوراق چاپی یا خطی با امضا یا بدون امضا یا بدون امضا یا به عنوان نقل و قول صریح یا ضمنی از شخص حقیقی یا حوقی یا مقامات رسمی صورت گیرد. (میر محمد صادقی،١٤٠٢، ٢٣٤).

از مصادیق مذکور در این ماده می‌توان استنباط کرد که اظهارات شفاهی از شمول ماده خارج است و ظاهراً رویه قضایی نیز همین را تأیید می‌کند. با توجه به فلسفه تشریح مواد مذکور که حفظ حیثیت و شئون افراد است، به نظر می‌رسد این جرم با هر وسیله ای که بتوان اکاذیبی را اظهار و حیثیت افراد جریحه دار ساخت از قبل اینترنت و ... قابل تحقق است. البته حتی اگر به مقید به مصادیق ذکر شده در ماده ٦٩٨ قانون مجازات اسلامی باشیم، باز هم امکان تحقق آن از طریق رایانه وجود دارد. مثلاً در مصداق «مراسلات»، مقصود از مراسله هر نوع مکتوبی است که اشخاص برای دیگری از طریق تلفنگرام و یا حتی از طریق پست الکترونیکی می‌فرستند. نظریه اراده حقوقی قوه قضائیه نیز مؤیّد این مطلب است :اگر به وسیله اینترنت یا مشابه به آن هم جرمی به کسی نسب داده شود و نسبت دهنده نتواند صحت آن انتساب و اسناد را ثابت نماید، مورد مشمول ماده ٦٩٧ قانون مجازات اسلامی خواهد بود.

نتیجه گیری

با پیشرفت سریع فناوری و گسترش استفاده از هوش مصنوعی، این فناوری نه تنها در بهبود زندگی روزمره و ارتقای کارایی در صنایع مختلف موثر بوده است، بلکه مورد سوءاستفاده مجرمان سایبری نیز قرار گرفته است. جرایم سایبری یکی از بزرگترین چالش‌های امنیتی دنیای مدرن است و با ورود هوش مصنوعی، این چالش‌ها پیچیده‌تر و مخرب‌تر شده‌اند. هوش مصنوعی امکان اجرای حملات پیچیده‌تر و هدفمندتر را فراهم می‌کند. الگوریتم‌های یادگیری ماشینی می‌توانند به تحلیل داده‌های بزرگ بپردازند و الگوهای رفتاری کاربران را شناسایی کنند. این تحلیل‌ها به مهاجمان اجازه می‌دهد تا حملات فیشینگ و بدافزارها را

[Downloaded from jlawst.ir on 2026-09-08]

شماره ۵۱،
دوره ۱۱،
سال پنجم،
زمستان ۱۴۰۲،
صص ۱-۱۸

با دقت بیشتری طراحی و اجرا کنند، که این امر منجر به افزایش موفقیت‌آمیز بودن این حملات می‌شود. هوش مصنوعی می تواند برای ایجاد بدافزارهایی استفاده شود که توانایی پنهان ماندن از سیستم‌های تشخیص نفوذ و دیگر ابزارهای امنیتی را دارند. این بدافزارها می‌توانند خود را با تغییرات محیطی و تدابیر امنیتی تطبیق دهند و شناسایی و حذف آنها را دشوارتر کنند. در نهایت، تاثیر هوش مصنوعی در ارتکاب جرایم سایبری نشان می‌دهد که لازم است تدابیر امنیتی جدید و پیشرفته‌تری برای مقابله با این تهدیدات اتخاذ شود. همچنین، افزایش آگاهی عمومی و آموزش کاربران در خصوص تهدیدات جدید و نحوه مقابله با آنها از اهمیت ویژه‌ای برخوردار است.

منابع

اردبیلی، محمدعلی(۱٤۰۲). حقوق جزای عمومی، تهران: میزان.

دانش، تاج زمان(۱۳۸۵)، مجرم کیست جرم شناسی چیست؟، موسسه کیهان، تهران.

ربیعی زاده، احمد (۱۳۹٦). کاربرد هوش مصنوعی در علوم اسلامی، فصلنامه نور، سال اول، شماره ۷۵.

سهرابی، ایمان و اکبرنژاد، حسن (۱٤۰۱). نقش هوش مصنوعی در فرهنگ نوین تمدن اسلامی، جستارنامه فرهنگ و هنر اسلامی، دوره اول، شماره ۲.

شامبیاتی هوشنگ (۱٤۰۲)، حقوق جزای عمومی، انتشارات ژوبین، تهران.

عظیمی، محمدحسن و اسماعیلی، سمیرا (۱٤۰۰). شناسایی مؤلفه‌های هوش مصنوعی در پایگاه‌های اطلاعاتی ایرانی. مجله دانش شناسی، دوره ۱٤، شماره ٥٤.

فرجیها، محمد و علمداری، علی(۱۳۹٦)، مطالعه تطبیقی معیارهای جرم‌انگاری در فضای سایبر در نظام کیفری ایران و آلمان، مطالعات حقوق تطبیقی، شماره ۲ .

قایدرحمتی، الهام(۱۳۹۵)، نقش شبکه های اجتماعی در جرم زدایی، اولین همایش ملی آینده پژوهی، علوم انسانی و امنیت اجتماعی.

کوثری، مسعود(۱۳۸۷)، اینترنت و آسیبهای اجتماعی، نشر سلمان، تهران.

موسایی، زینب و کریمی نیا مهدی، انصاری مقدم، مجتبی (۱٤۰۰). تحلیلی بر کارکردهای هوش مصنوعی در علوم اسلامی، پیشرفت‌های نوین در روانشناسی، سال ٤، شماره ٤۳.

میرمحمد صادقی، حسین(۱٤۰۲)، جرائم علیه امنیت و آسایش عمومی، انتشارات میزان، تهران.

نجاتی، نریمان؛ کلانتری، سعیده و بمانیان، محمدرضا (۱٤۰۰). آموزش طراحی معماری مبتنی بر هوش مصنوعی، مجله معماری نوین، دوره اول، شماره ۱.

نظرپور، محمد؛ موسوی، سیدحسن و حسینی، میرسعید (۱۳۹۹). کاربرد هوش مصنوعی در حسابرسی مالیاتی. دانش حسابرسی، سال ۲۰، شماره ۸۱.

وروایی، اکبر و همکاران(۱۳۹۳)، تأثیر اخلاق در جرم انگاری و جرم زدایی در نظام حقوق کیفری اسلامی ایران، پژوهش حقوق کیفری، شماره ۸.

Duran, Maria Garcia (2014): Internet Addiction Disorder, AllPsych Journal, 14 December.

[Downloaded from jlawst.ir on 2026-09-08]

مجله مطالعات حقوق

شماره ۵۱،
دوره ۱۱،
سال پنجم،
مستان ۱۴۰۲،
صص ۱-۱۸

The Impact of Artificial Intelligence on Cybercrime

Sara Soufi[۱], Saber Salehnezhad Behrestaghi[۲]

Abstract

The aim of this research is to investigate the impact of artificial intelligence technology on cybercrime. Artificial intelligence technology, as one of the remarkable advancements in recent decades, has had profound effects on various human activities, including cybercrimes. These effects may be both positive and negative. On the one hand, artificial intelligence systems can make significant improvements in cybersecurity and prevent online crimes. For example, the ability to detect unknown patterns and track suspicious activities through machine learning algorithms can help combat cyber attacks. On the other hand, as artificial intelligence capabilities improve, forensic experts have also expressed concerns about its use in cybercrimes. For instance, artificial intelligence tools can be used by attackers to create more complex and effective cyber attacks. Therefore, the question arises: What impact does artificial intelligence have on committing cybercrimes? Research findings indicate that the impact of artificial intelligence on committing cybercrimes can be examined in several ways. These impacts can be observed both in the tools and technologies used by cybercriminals and in defensive strategies used to mitigate these attacks. In other words, artificial intelligence can also be used both as a tool for committing cybercrimes and as a tool for defense against them. However, to address these challenges, there is a need to further develop artificial intelligence-based solutions for detecting, preventing, and mitigating cyber attacks.

Keywords: Artificial Intelligence, Crime, Cyber, Internet.

[۱] Master's degree, Department of Criminal Law and Criminology, Campus Branch, Islamic Azad University, Tehran, Iran (Responsible Author)

[۲] Ph.D, Department of Philosophy of Education, Shahid Muftah Branch, Farhangian University, Tehran, Iran

[Downloaded from jlawst.ir on 2026-09-08]