

بسترهای تحقق جرائم حوزه سایبری با به کارگیری هوش مصنوعی در ایران

(تاریخ دریافت ۱۴۰۴/۰۲/۱۷، تاریخ تصویب ۱۴۰۴/۰۳/۲۶)

حسین دانشفر

چکیده

هدف تحقیق حاضر، بررسی تاثیر فناوری هوش مصنوعی در ارتکاب جرایم سایبری است. تکنولوژی هوش مصنوعی به عنوان یکی از پیشرفتهای چشمگیر در دهه های 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. بر همین اساس سوالی که مطرح میگردد این است که هوش مصنوعی چه تأثیری در ارتکاب جرایم سایبری دارد؟ یافته های تحقیق نشان از آن دارد که تاثیر هوش مصنوعی در ارتکاب جرایم سایبری به چندین شکل ممکن است مورد بررسی قرار گیرد. این تأثیرات 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. جرایم سایبری مرتبط با هوش مصنوعی یکی از موضوعات مهم و چالشبرانگیز در دنیای دیجیتال امروز است. با پیشرفت فناوری و افزایش استفاده از هوش مصنوعی در بخشهای مختلف، جرایم سایبری نیز پیچیده تر و پیشرفته تر شده اند. در این مقاله به بررسی برخی از جنبه های مهم این نوع جرایم می پردازیم.

واژگان کلیدی: هوش مصنوعی، جرم، سایبر، اینترنت

مقدمه

هوش مصنوعی (AI) به عنوان یک فناوری پیشرفته و قدرتمند، به دسترسی به اطلاعات حساس و مهم در دنیای دیجیتال کمک می کند، اما همچنین با خود ریسک های امنیتی جدیدی را به وجود می آورد. جرایم سایبری مرتبط با هوش مصنوعی به عنوان یکی از چالش های امنیتی جدید، به دنبال شناسایی، پیشگیری و مقابله با این نوع تهدیدات می باشد. یکی از انواع جرایم سایبری مرتبط با هوش مصنوعی، حملات افزایش یافته با استفاده از الگوریتم های هوش مصنوعی می باشد. در این نوع حملات، هکرها از الگوریتم های هوش مصنوعی برای شناسایی ضعف های سیستم ها و نفوذ به آنها استفاده می کنند. این نوع حملات می تواند منجر به دسترسی غیرمجاز به اطلاعات حساس، سرقت اطلاعات مالی یا حتی کنترل سیستم های حیاتی شود. یک نوع دیگر از جرایم سایبری مرتبط با هوش مصنوعی، فریبندگی های هوش مصنوعی می باشد. در این نوع جرم، هکرها از الگوریتم های هوش مصنوعی برای ارسال پیام های تقلبی و فریبنده به کاربران استفاده می کنند تا آنها را به ارائه اطلاعات حساس یا پرداخت وجه متقلب وادار کنند. برای مقابله با جرایم سایبری مرتبط با هوش مصنوعی، اهمیت افزایش آگاهی و آموزش کاربران در مورد روش های حفاظتی و امنیتی بسیار بالا است. همچنین، استفاده از فناوری های امنیتی پیشرفته و تکنیک های تشخیص و پیشگیری از حملات سایبری می تواند به کاهش خطرات مرتبط با هوش مصنوعی کمک کند. در نهایت، هوش مصنوعی به عنوان یک فناوری نوظهور، به امنیت دیجیتال چالش های جدیدی را ایجاد کرده است. برای مقابله با جرایم سایبری مرتبط با هوش مصنوعی، ضرورت افزایش آگاهی و استفاده از روش های امنیتی پیشرفته بسیار حیاتی است.

نقش هوش مصنوعی در افزایش جرایم سایبری طی سال های گذشته هوش مصنوعی مولد (AI) به عنوان ابزاری قدرتمند و موثر در زمینه های مختلف، از جمله امنیت سایبری ظهور کرده است. این فناوری که بر اساس الگوریتم های یادگیری عمیق

عمل می کند توانایی های متعدد مانند تولید محتوای واقعی و غیرواقعی به صورت متن، تصویر و ویدئو دارد. درحالی که هوش مصنوعی مولد نویدبخش افزایش امنیت سایبری است، قادر به ایجاد مخاطرات جدی برای این حوزه نیز هست. تکنولوژی و پیشرفت هایش باعث قدرتمندتر شدن مجرمان سایبری شده و خدماتی را به آن ها ارائه می دهد. یکی از این چالش ها استفاده از مدل های زبانی مانند ChatGPT برای نوشتن کدهای مخرب است. ۷۶ درصد از شرکت ها بر اساس آمار فوربس و تحقیقات شرکت بلک بری، هوش مصنوعی و یادگیری ماشینی را در اولویت های بودجه مختص فناوری اطلاعات خود قرار داده اند تا بتوانند حجم زیادی از داده ها را برای شناسایی و کاهش تهدیدات سایبری تجزیه و تحلیل کنند؛ در نتیجه هوش مصنوعی هم برای مجرمین سایبری و هم مبارزه با جرایم سایبری ابزاری ضروری است. دولت ها و شرکت ها برای مدیریت بهتر آینده بهتر است مخاطرات و کاربردهای هوش مصنوعی را در امنیت سایبری شناخته و راه هایی برای مقابله با چالش های آن در نظر بگیرند.

بخش اول: تعاریف

۱- هوش مصنوعی

هوش مصنوعی به معنای هوش و توانایی هایی است که توسط ماشینها و سیستمهای کامپیوتری برای انجام فعالیتهای هوشمندانه و تصمیم گیری استفاده می شود این فراداده به ماشینها امکان میدهد تا الگوها را تشخیص داده ، داده ها را تحلیل کرده و مسائل را مدیریت کنند. هوش مصنوعی شامل مجموعه ای از تکنیکها و الگوریتمها است که به ماشینها این قابلیت را میدهد تا با بررسی و تحلیل داده ها الگوهای پنهان در آنها را شناسایی کنند و بر اساس آنها تصمیم گیری کنند. این فناوری در حال حاضر در بسیاری از زمینه ها مانند ریاتیک پردازش زبان ،طبیعی تشخیص تصویر پشتیبانی تصمیم گیری خودران سازی 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 مجموعه ای 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 شبیه سازی و تقلید عملکرد انسانی در زمینه هایی مانند تصمیم گیری یادگیری استدلال تشخیص الگو پردازش زبان طبیعی و بینایی ماشینی میباشد. تکنیکها و روشهای مختلفی در دسته بندی هوش مصنوعی وجود دارد که شامل موارد زیر میشود یادگیری ماشینی این رویکرد به کامپیوترها امکان میدهد از داده ها یاد بگیرند و با استفاده از الگوریتمهای مختلف، پتانسیل تشخیص الگوها و انجام پیشبینیها را داشته باشند شبکه های عصبی مصنوعی این مدلها به تقلید از ساختار مغز انسان پرداخته اند اطلاعات با استفاده از نورونهای مصنوعی در لایه های مختلف پردازش میشود و این مدلها برای مسائل پیچیده تر مانند تصویر برداری 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 ماشینی: این زمینه به کامپیوترها امکان میدهد تصاویر و ویدئوها را تحلیل و تشخیص دهند این شامل تشخیص و شناسایی اشیاء چهره ها شناسایی وضعیت و ویژگیهای تصاویر می شود منطق فازی در این رویکرد، مفاهیمی مانند صحیح یا غلط با در نظر گرفتن ابهامات و مبهمی ها تعریف می شوند. این به کامپیوترها امکان میدهد با مفاهیم پیچیده تر و واقع نزدیک تر کار کنند. به صورت یکی از فناوریهای پیشرفته و چالش برانگیز در مختلف صنایع و زمینه ها مورد استفاده قرار میگیرد هوش و بهبودهای چشمگیری در کارکردها و امکانات مختلف ارائه داده است. (قائد رحمتی ۱۳۹۵ (۲۴-۲۵)

۲- جرم

جرم لغت به معنای گناه آمده است و در اصطلاح علیرغم تعاریف زیادی که از جرم شده هنوز هم این موفقیت بدست جرم در 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 بر حسب نظر دانشمندان و محققان دارای مبانی و صور گوناگون است. به سخنی دیگر، آنچه که از نظر یکی جرم محسوب می شود، بر حسب دیگری نه تنها ممکن است عنوان جرم به خود نگیرد، بلکه امکان دارد که حتی عملی پسندیده به شمار آید، (شامبیاتی ۱۴۰۲، ۲۳) عده ای 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 و آرامش 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 می شود (دورکیم، ۱۳۸۹، ۸۰) گناه را در جرم یک پدیده معمولی جامعه است زیرا که بر حسب احساس تنفر و انزجاری که بزهکار در جامعه بر می انگیزد، معین میگردد هدف از کیفر، بیشتر معطوف به افراد غیر مجرم است زیرا که بیشتر احساس همبستگی و یگانگی افراد کند پیش از اینکه مجرمان را متنبه سازد. کیفر ممکن است نقش عدم ترغیب و تضعیف و دلسردی مجرمان را نیز تقویت فراهم آورده لیکن احساس انزجار در قبال پاره ای از اعمال کیفر پذیر در میان بعضی از مردم ضعیف است و در نتیجه آنان معرض ارتکاب جرم قرار میگیرند بنابر این کیفر نمیتواند از وقوع جرم پیشگیری کند هیچ جرمی جرم محسوب نمیشود مگر اینکه کیفری در کار باشد. در نتیجه کیفر قانونی نمی تواند 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 دیدگاه ها 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.

۳- جرایم سایبری

جرایم سایبری از مباحث مطرح شده در حقوق جزا بوده و به جرایمی گفته می شود که در محیطی غیرفیزیکی علیه فناوری اطلاعات با حالات شبیه سازی و مجازی سازی ارتکاب می یابد. جرایم سایبری به جهت گسترش خود، رفته رفته جانشین عباراتی چون جرم های رایانه ای و جرم های اینترنتی می شوند. به جرایم سایبری، جرایم علیه فناوری اطلاعات نیز گفته می شود. تفاوت جرایم سایبری و جرایم کلاسیک در زمان ارتکاب جرم، مکان ارتکاب

جرم، بزه‌دیده و تعداد بزه‌دیدگان است. جرایم سایبری را می‌توان به چهار دسته: جرایم کلاسیک با توصیف سایبری، جرایم علیه محرمانه بودن داده‌ها و سیستم‌ها، جرایم علیه صحت و تمامیت داده‌ها و سیستم‌ها و جرایم مرتبط با محتوا تقسیم کرد. تقسیم‌بندی جرائم سایبری به دسته‌های جداگانه کار ساده‌ای نیست زیرا اغلب آن‌ها با هم در ارتباط هستند. با این حال، به طور کلی انواع زیر قابل تشخیص است:

۳-۱ جرائم مالی

جای تعجب نیست که بسیاری از مجرمان فضای مجازی از اینترنت برای کسب منافع مالی از طریق انجام حملات زیر استفاده می‌کنند:

۳-۲ فیشینگ

مجرمان سایبری دوست دارند هنگام آلوده کردن رایانه‌های کاربران، راه ساده‌ای را انتخاب کنند. به همین دلیل، ایمیل یک وسیله مناسب برای حمله است. ماهیت کلاهبرداری فیشینگ، مجبور کردن گیرنده برای کلیک بر روی لینک وب، باز کردن فایل پیوست یا تکمیل فرم آنلاین است. پیام‌ها اغلب از طرف یک سازمان بزرگ و معتبر مانند خدمات مالیاتی، بانک‌ها و فروشگاه‌های آنلاین ارسال می‌شود. در بسیاری از موارد کلاهبرداران می‌خواهند کلمات عبور شما را بدست آورند یا دستگاه را با بدافزار آلوده کنند.

۳-۳ باج‌خواهی آنلاین

یکی دیگر از جرائم سایبری با انگیزه مالی، اخاذی است. پس از آلوده کردن کاربر یا شرکتی به بدافزار، همه پرونده‌ها مسدود می‌شوند. سپس مجرمان پیشنهادی را برای بازگرداندن پرونده‌ها در ازای پاداش پولی ارسال می‌کنند. بیشتر اوقات، هکرها خواستار پرداخت‌هایی با رمزارزها هستند.

۳-۴ تقلب

تقلب مالی پیچیده شامل هک کردن شبکه‌های خرده‌فروشی برای به دست آوردن اطلاعات کارت اعتباری مشتریان آن‌ها است. روش‌های دیگر می‌تواند فیشینگ هدفمند برای جعل

هویت مدیران کسب و کارها و انتشار دستور از طرف آنها باشد. لازم به ذکر است کشف برخی از انواع تقلب‌های مالی بسیار دشوار است.

۳-۵ نقض قوانین کپی‌رایت

این یکی از رایج‌ترین شکل‌های جرم آنلاین است. استفاده از محتوای محافظت شده از حق چاپ برای منافع شخصی به طور گسترده در وب سایت‌های تورنت مشاهده می‌شود. همچنین سایت‌های زیادی محتوایی که دارای کپی‌رایت است را به صورت غیرقانونی منتشر می‌نمایند.

۳-۶ جرائم مربوط به نفوذ به حریم‌های خصوصی

هدف از انجام چنین جرائمی دستیابی به اطلاعات محرمانه است. انواع مختلفی از چنین تخلفاتی وجود دارد. بعضی اوقات هکرها با انگیزه‌های عمیق‌تر مانند پول یا نفوذ سیاسی هدایت می‌شوند. روش این نوع حملات دور زدن قوانین و یافتن آسیب‌پذیری در فناوری‌هایی است که باید از داده‌های محرمانه محافظت کنند.

۳-۷ سرقت هویت

سرقت اطلاعات شخصی با هدف تعویض هویت دیجیتالی یک قربانی رخ می‌دهد. به عنوان مثال، کلاهبرداران اطلاعات شخصی یک قربانی (شماره تلفن، آدرس و غیره) را بدست می‌آورند و برای دریافت وام بانکی بزرگ اقدام می‌کنند.

۳-۸ جاسوسی

جاسوسی و نظارت مخفی بر زندگی افراد ممکن است شامل هک شدن دوربین‌های مدار بسته، نفوذ به کانال‌های ارتباطی مانند پیام کوتاه، ایمیل و غیره باشد.

۳-۹ هرزنامه‌ها

اسپم یک نوع بسیار رایج از جرایم رایانه‌ای است. هرزنامه‌ها ممکن است از ایمیل‌های ناخواسته، پیام کوتاه و سایر کانال‌های ارتباطی استفاده کنند. به طور کلی به هر پیام ارسال شده بدون دریافت رضایت قبلی کاربر، اسپم یا هرزنامه گفته می‌شود.

۳-۱۰ فعالیت‌های سیاسی و اجتماعی غیرقانونی آنلاین

برخی از انواع جرائم با هدف تغییر نگرش سیاسی یا ایجاد آسیب و یا کاهش تأثیر افراد یا گروه‌ها انجام می‌شود.

۳-۱۱ آزار و اذیت و نفرت‌پراکنی

ایمیل‌های توهین‌آمیز و پیام‌های فوری علیه یک فرد یا گروهی از افراد اغلب بر اساس ویژگی‌های نژادی، جنسیتی، مذهبی افراد انجام می‌شود.

۳-۱۲ تروریسم سایبری

سازمان‌های افراطی و افراد متخاصم به طور فزاینده‌ای از فضای مجازی برای آسیب رساندن به زیرساخت‌های فناوری اطلاعات، بحث در مورد اقدامات ترور، گسترش تبلیغات و غیره استفاده می‌کنند.

تعداد روز افزون مشاغل، خدمات و دستگاه‌های مرتبط، همه اهداف بالقوه تروریست‌های سایبری را به وجود می‌آورد.

۳-۱۳ تحقیر سایبری

استفاده از دستگاه‌های متصل به منظور تحقیر یا ارباب، در دسته حمله سایبری قرار می‌گیرد. خط بین جرائم آزار و اذیت و نفرت و تحقیر سایبری گاهی مبهم است. برخی از انواع حمله سایبری، مانند انتشار تصاویر حساس از کودکان، غیرقانونی است و به آن استثمار کودکان گفته می‌شود.

۳-۱۴ سایر فعالیت‌های غیرقانونی

قسمت بد اینترنت که وب تاریک نامیده می‌شود، برای انجام انواع مختلفی از فعالیت‌های غیرقانونی استفاده می‌شود.

۳-۱۵ محتوای غیر اخلاقی

انتشار محتوای غیر اخلاقی از طریق اینترنت در بسیاری از کشورها به عنوان یک جرم تعبیر می‌شود. در برخی از مناطق، فقط خشونت شدید و یا محتوای مربوط به حیوانات ممنوع

است. گسترش محتوای غیر اخلاقی کودکان در اکثر کشورها ممنوع است.

۳-۱۶ توزیع اسلحه و مواد مخدر

بازارهای بی شماری که در وب تاریک وجود دارند، به مجرمان کمک می کنند تا در حالی که دور از چشم پلیس می ماند به فروش مواد مخدر و اسلحه بپردازند.

۳-۱۷ روش های حمله

سه روش معمول وجود دارد که هکرها از آن استفاده می کنند.

مورد اول مبتنی بر استفاده از بدافزار است. بسیاری از سیستم عامل ها و نرم افزارهای آسیب پذیر وجود دارد. استفاده از اقدامات امنیتی پیچیده، تنظیم گذرواژه های طولانی و اجرای نسخه پشتیبان و به روزرسانی منظم بسیار مهم است.

راه دوم به حملات منع سرویس توزیع شده یا DDoS متکی است. یک مهاجم تعداد زیادی درخواست را به سرور ارسال می کند که باعث اضافه بار آن شده و آفلاین می شود. هیچ بدافزاری برای قربانی ارسال نمی شود. هدف اصلی این است که سرویس برای بازدیدکنندگان از دسترس خارج شود.

روش سوم ترکیبی از کد مخرب و مهندسی اجتماعی است. مشهورترین شکل این حمله، فیشینگ است که در بالا به آن اشاره شده است. یک قربانی فریب خورده و روی پیوند کلیک کرده و یا فرم آنلاین را پر کرده است، که منجر به سرقت هویت می شود.

بخش دوم: مزایای هوش مصنوعی

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 خواهیم کرد :

۱- قدرت پردازش و تحلیل بزرگتر

هوش مصنوعی قادر به پردازش حجم عظیمی از داده ها و تحلیل آنهاست این امر به کارآمدی بیشتر در تصمیم گیریها، پیش بینی ها و بهبود فرآیندهای کسب و کار منجر می شود به عبارتی هوش مصنوعی امکان پردازش حجم عظیمی از داده ها و تحلیل آنها را

داراست از طریق تکنیکهای مختلفی مانند یادگیری ماشین شبکه های عصبی، عمیق الگوریتم های استنتاج و داده کاوی، هوش مصنوعی قادر است به تجزیه و تحلیل داده های بزرگ و استخراج الگوها و ارتباطات مهم از آنها با پردازش عظیمی از داده ها. هوش مصنوعی میتواند الگوهای پنهان و ارتباطات پیچیده تر را کشف کند و اطلاعات ارزشمندی را حجم از داده های به نظر اولیه بی ارزش استخراج کند این امر میتواند در تصمیم گیریهای استراتژیک پیش بینی 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 داده های خود بهره برداری بهتری داشته باشند و تصمیم گیریهای بهتری را بر اساس اطلاعات قابل استخراج از داده ها انجام دهند (نجاتی و همکاران ۱۴۰۰، ۹۸)

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 داده های 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 داده ها و استخراج الگوها میتواند تصمیمات بهتر و مبتنی بر شواهد و داده های واقعی را ارائه کند با استفاده از الگوریتمها و مدلهای هوش مصنوعی میتوان دادههای بزرگ را به صورت خودکار ده و نتایجی که بر اساس آنها تصمیم گیری می.شود ارائه داد با تکیه بر شواهد و داده های واقعی، تصمیمات گرفته شده توسط هوش مصنوعی میتوانند به دقت و قابلیت پیش بینی بالا دست یابند این تصمیمات مبتنی بر داده های واقعی تحلیل کرده و سریع می توانند به مدیران و تصمیم گیرندگان کمک کنند تا از تصمیم گیریهای 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 توانند عملکرد و کارایی خود را بهبود بخشند.

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 خودران سازی، 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 اشیاء، 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 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 خودران سازی 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

۴- امکانات خود کار ساز

هوش مصنوعی قادر به انجام کارها با دقت بالا و کارایی بیشتر است در بسیاری از حوزه ها مانند تشخیص الگو، تشخیص تصاویر و صدا، ترجمه، زبانی پردازش زبان طبیعی و خودران، سازی هوش مصنوعی به دقت و کارایی بهتری نسبت به روشهای سنتی دست پیدا کرده است. هوش مصنوعی با قابلیت‌های خود میتواند در بسیاری از حوزه ها دقت بالا و کارایی بهتری نسبت به روشهای سنتی ارائه دهد در زمینه تشخیص الگو، مانند تشخیص چهره تشخیص اشیاء تشخیص الگوهای زمانی هوش مصنوعی با استفاده از شبکه های 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 مجله مطالعات حقوق ۵۸ 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 خودران سازی هوش مصنوعی با استفاده از الگوریتم های مبتنی بر شبکه های 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 حوزه ها 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 ۱۳۸۶ ۱۳)

۵- ارتباطات هوشمند

هوش مصنوعی در سیستمهای ارتباطی هوشمند مانند رباتها مساعدت کننده های صوتی مانند سیری و آلسا و سیستم های مبتنی بر گفتار استفاده می شود. این سیستم ها قادر به تفسیر و پاسخ به دستورات صوتی انسان هستند و تجربه ارتباطی بسیار نزدیکتری را برای کاربران ایجاد میکنند. این سیستمها از الگوریتم ها و مدل های یادگیری ماشین برای تفسیر دستورات صوتی انسان استفاده می کنند و سعی می کنند به طور خودکار و هوشمندانه به آنها پاسخ دهند یکی از روشهای استفاده از هوش الگوهای صوتی است. با استفاده از مدل های یادگیری عمیق سیستمها قادر به تشخیص و شناسایی الگوهای صوتی مختلف است و با استفاده از مدل های 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 سیستم ها 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. (همکاران ۱۴۰۰، ۱۰۹)

۶- خودکار سازی و اتوماسیون

هوش مصنوعی قادر است وظایف و فرآیندهای مختلف را خودکار سازی کند و این امکان بهبود بهره وری و کارایی در صنایع و سازمانها را به همراه دارد مثلهایی که ارائه دادید از جمله خودران سازی در خط تولید، خودروهای خودران و رباتیک، هستند. در خطوط تولید هوش مصنوعی و رباتیک میتوانند برای خودران سازی فرآیندها عملکردهای رایجی از هوش و ش مصنوعی 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 بهره وری می شود. همچنین خودروهای خودران نیز از تکنولوژی هوش مصنوعی بهره میبرند سیستمهای هوشمند درون خودروها با استفاده از حسگرها داده ها را جمع آوری 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 طور کلی، هوش مصنوعی در بسیاری از صنایع و سازمانها امکان خود کارسازی و بهبود بهره وری را فراهم در کند. این فناوری در طول فرآیندهای مختلف مانند تولید خدمات درست منابع تصویر گیری های استراتژیک و غیره تأثیر قابل توجهی دارد. (شهبازی و همکاران، ۱۴۰۱: ۱۳-۱۴)

۷- سازماندهی و مدیریت داده ها

هوش مصنوعی قادر است به سازماندهی و مدیریت دادههای بزرگ کمک کند. با توجه به تواناییهای پردازشی قوی و الگوریتم های پیشرفته هوش مصنوعی میتواند به طور خودکار دادههای بزرگ را تحلیل و سازماندهی کند. هوش مصنوعی میتواند الگوها روابط و اطلاعات مفید را در داده های بزرگ شناسایی کند با استفاده از روشهای یادگیری ماشینی و شبکه های 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 وظیفه هایی مانند: ترتیب بندی تصفیه و تهیه خلاصه اطلاعات از داده های بزرگ کمک کند. به طور مثال با استفاده از الگوریتمهای خوشه بندی هوش مصنوعی میتواند داده های مشابه را در گروه های جداگانه دسته بندی کند و اطلاعات خلاصه شده ای از هر گروه ارائه دهد با استفاده از هوش مصنوعی در سازماندهی و مدیریت دادههای بزرگ، امکان دسترسی سریع تر و دقیقتر به اطلاعات موجود فراهم میشود. این باعث میشود تصمیم گیران و مدیران بتوانند تصمیمات بهتری بگیرند و بهبود عملکرد سازمان را تجربه کنند به هر حال استفاده

مؤثر از هوش مصنوعی در سازماندهی داده های بزرگ نیازمند آماده سازی و پیش پردازش مناسب، داده ها انتخاب الگوریتمها و مدل‌های مناسب، و نظارت و ارزیابی مداوم بر عملکرد سیستم هوش مصنوعی است. (عظیمی و اسماعیلی، ۱۴۰۰: ۹۷).

بخش سوم: جرایم ارتكابی با هوش مصنوعی

به دلیل پیشرفت روز افزون تکنولوژی همواره جرائم جدیدی رخ میدهد که گاه برخی از آنان مستقیماً در قانون پیش بینی نشده اند و این امر کار دستگیری این مجرمان و قضاوت در این قبیل پرونده ها را دشوار مینماید در نتیجه تغییر و به روز رسانی قوانین در این حوزه بیش از سایر حوزه ها ضروری به نظر میرسد البته اهمیت موضوع فقط در جرم انگاری جرائم درستی مورد توجه قانون گذار در ایران واقع شده اند. لازم به ذکر است جز آنچه در قوانین و مقررات موجود به طور خاص مورد توجه قرار گرفته اند جرایمی وجود دارند که در برخی کشورهای دنیا به شکل ویژه ای تعیین مجازات شده اند و بهتر بود در ایران نیز قانونگذار به این موضوعات نگاه متفاوتی می داشت. برای مثال مسایلی هم چون جرائم جنسی در قوانین مورد بحث قرار گرفته اند متأسفانه 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 جدی تری را میطلبد این موضوع در جرایم 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)

مهم ترین جرائم نوپدید با بهره گیری از فناوری هوش مصنوعی به قرار زیر می باشند:

۱- سوء استفاده جنسی

از دیگر خطرات جدی هوش مصنوعی به عنوان منشأ جرائم رایانه ای در فضای مجازی سوء استفاده 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 و یا به دست آوردن اطلاعات و عکسهای خصوصی بزه دیدگان 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. (فرهمنده، ۱۳۸۷، ۱۳۹۰)

بنابر مطالعاتی که در غرب در این زمینه انجام گرفته است، اغلب نوجوانانی که مورد اغفال و سوء استفاده جنسی واقع میشوند زیر ۱۸ سال سن دارند و در بیشتر موارد تصاویر تحریک کننده ای 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 سیاست گذاران به این وقوف و توجه داشتهاند و، مقالات کتابها و همایشهای متعددی در ارتباط با آن برگزار کرده اند. برای مثال امر بیش ده سال پس از تصویب کنوانسیون حقوق کودک توسط سازمان ملل در سال ۱۹۸۹ م یعنی در سال ۱۹۹۹م گردهمایی جهانی تحت عنوان کارشناسی برای حمایت کودکان در برابر سوء استفاده جنسی از طریق اینترنت برگزار گردید که منجر به صدور قطعنامه ای 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 زبانهای 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 ۲۰۱۴، ۸).

۲- انحرافات جنسی

از جمله آثار مخرب هوش مصنوعی به ویژه جرائم مرتبط با محتوا (به قول قانون مجازات جرائم رایانه ای) به وجود آمدن انحرافات جنسی و اختلالات جنسی است. هوش مصنوعی به دلیل رویکرد آزاد اندیشی در روابط جنسی از سوی گردانندگان 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 در هم می شکند 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 خواسته های جنسی دیگران تعریف میشود. این گونه مطالب و تصاویر که در پی تحریک جنسی دیگران عرضه می گردد. معمولاً به ارضای غیر طبیعی جنسی مراجعه کنندگان آن می انجامد. 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 می انجامد و منشأ به وجود آمدن بسیاری از جرائم رایانه ای به ویژه محتوایی و مقدمه ای 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 میزند و این حالت نوعی رفتار غیر مسئولانه 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 زمینه ای برای ارتکاب جرائم فضای سایبر نیز هست (شیرزاد، ۱۳۹۰، ۶۹)

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 میند. 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، ۹۴)

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 تجربه ای 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 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. (عالی پور ۱۲۵-۱۲۶-۱۳۹۰)

۳- هتک یا دسترسی غیر مجاز

با پیشرفت علم و فراگیر شدن استفاده از هوش مصنوعی و عدم وجود محدودیت سنی و جنسیتی 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 جنبه مثبتی است که هیچ کس از محرومیتی برخوردار نیست در مقابل بالطبع این فراگیری باعث ورود افراد سودجو و تبهکار میشود و این خود جنبه منفی این شمول است. با تصویب قانون مبارزه با جرایم رایانه ای در کشور ما و جرم انگاری آن توسط مقنن این موضوع را روشن میکند که مسأله هک کردن و دسترسی غیر مجاز به اطلاعات در شبکه های 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 رایانه ای هک مساوی کرک است که معنی رمز گشایی میدهد گستردگی واژه هک فقط منحصر به رایانه نیست و توسط افراد گوناگون در زمینه هایی از قبیل، موسیقی، نقاشی و.... بکار میرود این واژه برای اولین بار در مؤسسه فناوری ماساچوست در سال ۱۹۶۰ بکار رفت معنی اصلی آن سود بردن از یک روش سریع و هوشمندانه برای حل مشکل تکنیکی بوده است. در دهه اخیر دانشمندان توانسته اند که حتی سلولهای بدن انسان را نیز هک کنند. (خالقی و احمدی شریفی ۱۳۹۶، ۳).

منظور از دسترسی غیر مجاز به اطلاعات فضای مجازی و شبکه های اجتماعی این است که

فرد بزهکار با نقض تدابیر امنیتی و به صورت غیر مجاز به داده های حفاظت شده دست یابد. برخی دسترسی غیر مجاز را در زیر مجموعه جرایم علیه فناوری محض قرار می دهند. برخی دیگر آن را در زمره جرایم علیه محرمانگی و تمامیت و در دسترس بودن سیستم ها و داده های رایانه ای کنند دسترسی غیر مجاز را از منظر حقوق کیفری رایانه ای را میتوان در زمره جرمهای رایانه ای محض دانست؛ زیرا اولاً از جرم های مرتبط با سیستمهای رایانه ای است، ثانیاً: تنها در محیط سامانه های رایانه ای و فضای سایبر ارتکاب یافتنی است. از منظر حقوق کیفری برخی دسترسی غیر مجاز را در زمره جرمهای علیه اموال می پندارند و برخی دیگر آن را از مقوله جرم های مالی یا اقتصادی میدانند (جلالی فراهانی ۱۳۸۸، ۱۹)

بنا به نظریه ای مفهوم جرم دسترسی غیر مجاز با توجه به موضوع آن و تعریف گفته شده و آنچه که در زمینه آن ارائه شده، به مفهوم جرایم علیه امنیت و آسایش عمومی نزدیک تر مینماید تا جرایم علیه اموال (عبدالهی ۱۳۸۹، ۴۲) به موجب ماده یک قانون جرایم رایانه ای مصوب ۱۳۸۸ به طور خاص دسترسی غیر مجاز را که یکی از مظاهر تجاوز به حریم خصوصی افراد در شبکه های اجتماعی و فضای مجازی است جرم انگاری شده است. منطوق این ماده: «ماده ۱- هرکس به مجاز به داده ها با سامانه های رایانه ای با مخابراتی که به وسیله تدابیر امنیتی حفاظت شده است دسترسی یابد، به حبس 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 غیر مجاز به اطلاعات اشخاص است که ایراداتی نیز بر آن وارد است. من جمله این ایرادات عدم تعریف اصطلاحات غیر مجاز و تدابیر امنیتی که این امر تاحدی ابهام آمیز بودن ماده فوق را میرساند چرا که روشن نیست مقصود از غیر مجاز 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.

۴- هتک حیثیت و نشر اکاذیب

حریم 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 سوء استفاده 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 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 غیر مجاز مینمایند مصوب ۱۳۷۲ و ماده ۶۴۰ قانون مجازات اسلامی تعزیرات حکومتی اشاره کرد. همچنین با توجه به اشاره ماده ۶۹۸ این قانون به جرم نشر اکاذیب به عنوان جرمی عمومی باید متذکر شد که این جرم موضوع ماده ۱۷ لایحه جرائم رایانه ای هم میباشد. توهین رایانه ای نوع جدیدی از جرم توهین سنتی است که در آن وسیله ارتکاب رایانه میباشد. جرم توهین رایانه ای به معنای نسبت دادن هر امر وهن آور اعم از دروغ یا راست به وسیله 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 رایانه ای دانست توهین رایانه ای از طریق، رفتار، گفتار اشارات و کلیه اظهارات شفاهی و کتبی توهین آمیز به وسیله رایانه صورت میگیرد. در توهین خلاف واقع بودن اظهارات ضروری نیست زیرا ممکن است اظهار توهین آمیز، اظهار واقعیت نیز باشد. در تشخیص رفتار و گفتار و اشارات موهن باید به عرف زمان و مکان وقوع جرم رجوع کرد . (میر محمد صادقی ۱۴۰۲، ۱۶) شخصیت طرفی که مورد امانت 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 رایانه ای باید شخص حقیقی باشد. این امر از لفظ «افراد مذکور در ماده مچنین از کلماتی مثل صوت تصویر و فیلم که در ماده ۶۴۰۰ قانون ۶۰۸

قانون مجازات اسلامی ۱۳۹۲ استفاده می‌گردد و همچنین مجازات اسلامی آمده حقوقی فاقد صور و تصویر و فیلم است و شخصیتی اعتباری داشته شخصیت وجود مادی ندارد زنده بودن مخاطب نیز شرط دیگری است که از ماده ۶۰۸ قانون مجازات اسلامی مستفاد می‌شود؛ زیرا فرد، مرده زنده تلقی نمیشود حضوری یا علنی بودن جز در موارد تصریح شده 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 ۶۰۸ و ۶۰۹ قانون مجازات اسلامی و بندهای ۷ و ۸ ماده ۶ و مواد ۲۶ و ۲۷ قانون مطبوعات توهین باید صریح باشد. ارتجالی بودن توهین رایانه ای نیز ضرورتی ندارد توهین رایانه ای هم شامل توهین بدوی و هم توهینی که در جواب دیگری است میشود. توهین رایانه ای مقید به نتیجه نیست، بنابراین از جرائم مطلق میباشد اما در توهین رایانه ای 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 سوء نیت خاص مثل قصد اذیت و متألم کردن طرف شرط نمیباشد. (میر محمد صادقی ۱۴۰۲، ۱۵۸) به عبارت دیگر، اولاً، مرتکب باید در فعل خود عامد باشد نه این که 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 رایانه ای صراحتاً در هیچ ماده ای از قوانین ذکر نشده و بدون مجازات ماندن مرتکبان این جرم نیز بر ارتکاب روزافزون آن خواهد افزود، به نظر میرسد باید طبق ماده ۱۹ قانون جرم رایانه‌ای مصوب ۱۳۸۸ مرتکبان این جرم را به عنوان 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 ۶۰۸ قانون مجازات اسلامی در خصوص توهین ساده و ماده ۶۰۹ در مورد توهین مشده میباشد مجازات توهین ساده بر

اساس ماده ۶۰۸ شلاق تا ۷۴ ضربه و یا پنجاه هزار ریال تا یک میلیون ریال جزای نقدی است و مجازات توهین مشدد حبس از ۳ تا ۶ ماه و یا تا ۷۴ ضربه شلاق و یا پنجاه هزار ریال تا یک میلیون ریال جزای نقدی میباشد انتشار و اشاعه اخبار دروغ و وقایع خلاف واقع به قصد اضرار به غیر یا تشویش اذهان عمومی با 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 (و روایی و همکاران ۱۳۹۳ ۶۰۵۹) عنصر مادی این جرم اظهار و نشر اکاذیب یا نسبت دادن عمل خلاف حقیقت به شخص حقیقی یا حقوقی یا مقامات رسمی در شبکه های اجتماعی است که به یکی از راههای مذکور در ماده ۱۸ قانون جرایم رایانه ای محقق می شود. در حقیقت دو جرم در این ماده بیان شده است اظهار اکاذیب و نسبت دادن مطلب غیر واقعی به شخص یا اشخاص حقوقی با مقامات رسمی اشاعه اکاذیب باید به وسیله نامه شکوائیه عریضه گزارش یا توزین 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 حقوقی با مقامات رسمی صورت گیرد (میر محمد صادقی، ۱۴۰۲، ۲۳۴). 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 می کند 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 ۶۹۸ 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 می فرستند. نظریه اراده حقوقی قوه قضائیه نیز مؤید 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 ۱۹۷ قانون مجازات اسلامی خواهد بود.

نتیجه گیری

همانطور که می بینید، جرائم سایبری دامنه وسیعی از اقدامات غیرقانونی را شامل می شود، از قاچاق مواد مخدر و جرائم تحقیر و نفرت پراکنی گرفته تا سرقت اطلاعات شخصی و کلاهبرداری. باز هم تاکید می کنیم که گاهی اوقات جدا کردن این جرائم از هم کار دشواری است. به عنوان مثال: حمله فیشینگ می تواند با هدف سرقت داده های شخصی انجام شود و هویت جدید جعلی می تواند متعاقباً برای گرفتن پول برای تروریست ها مورد استفاده قرار گیرد. درک این نکته ضروری است که جرائم سایبری همیشه با طرح های پیشرفته همراه نیست. با ایجاد عادات اساسی امنیتی و آگاهی در مورد تهدیدات مدرن، می توان از بیشتر حملات جلوگیری کرد. 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 سوء استفاده مجرمان سایبری نیز قرار گرفته است. جرایم سایبری یکی از بزرگترین چالش های امنیتی دنیای مدرن است و با ورود هوش مصنوعی این چالش ها پیچیده تر و مخرب تر شده اند. هوش مصنوعی امکان اجرای حملات پیچیده تر و هدفمندتر را فراهم میکند. الگوریتم های یادگیری ماشینی میتوانند به تحلیل داده های بزرگ بپردازند و الگوهای رفتاری کاربران را شناسایی کنند این تحلیلها به مهاجمان اجازه میدهد تا حملات فیشینگ و بدافزارها را دقت بیشتری طراحی و اجرا کنند که این امر منجر به افزایش موفقیت آمیز بودن این حملات میشود هوش مصنوعی می تواند برای ایجاد بدافزارهایی استفاده شود که توانایی پنهان ماندن از سیستم های 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 پیشرفته تری 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 ویژه ای برخوردار است.

منابع و مأخذ

- اردبیلی، محمد علی (۱۴۰۲). حقوق جزای عمومی: تهران. میزان
- دانش تاج زمان (۱۳۸۵)، مجرم کیست جرم شناسی چیست؟ موسسه کیهان، تهران
- ربیعی زاده، احمد (۱۳۹۶) کاربرد هوش مصنوعی در علوم، اسلامی فصلنامه نور، سال اول شماره ۷۵
- سهرابی، ایمان و اکبرنژاد حسن (۱۴۰۱) نقش هوش مصنوعی در فرهنگ نوین تمدن، اسلامی جستار نامه فرهنگ و هنر، اسلامی دوره اول شماره ۲
- شامبیاتی هوشنگ، (۱۴۰۲) حقوق جزای عمومی انتشارات ژوبین، تهران
- عظیمی، محمدحسن و اسماعیلی، سمیرا (۱۴۰۰). علمداری شناسایی مؤلفه‌های هوش مصنوعی در پایگاه‌های اطلاعاتی ایرانی مجله دانش شناسی دوره ۱۴ شماره ۵۴
- فرجیها محمد و علمداری علی (۱۳۹۶)، مطالعه تطبیقی معیارهای جرم انگاری در فضای سایبر در نظام کیفری ایران و آلمان مطالعات حقوق تطبیقی شماره ۲
- قاید رحمتی الهام (۱۳۹۵) نقش شبکه‌های 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 (۱۴۰۰). تحلیلی بر کارکردهای هوش مصنوعی در علوم اسلامی، پیشرفتهای نوین در روانشناسی، سال ۴، شماره ۴۳
- میر محمد صادقی، حسین (۱۴۰۲)، جرائم علیه امنیت و آسایش عمومی انتشارات میزان تهران
- نجاتی نریمان، کلانتری، سعیده و بمانیان، محمدرضا (۱۴۰۰) آموزش طراحی

- معماری مبتنی بر هوش مصنوعی، مجله معماری نوین دوره اول شماره ۱ .
- نظریور، محمد؛ موسوی، سیدحسن و حسینی، میرسعید (۱۳۹۹). کاربرد هوش مصنوعی در حسابرسی مالیاتی، دانش حسابرسی، سال ۲۰، شماره ۸۱
 - ورورایی، اکبر و همکاران (۱۳۹۳)، تأثیر اخلاق در جرم انگاری و جرم زدایی در نظام حقوق کیفری اسلامی ایران، پژوهش حقوق کیفری شماره ۸