Legal Studies in Cyberspace

مطالعات حقوقی فضای مجازی

Received: 2025/05/31
Accepted: 2025/11/29
Publish: 2025/12/28
Pages: 50 - 68

ISSN: 2821-126X
https://sanad.iau.ir/journal/cyberlaw :وبگاه مجله

Volume 4, Issue 15, Fall 2025
Article Type: **Research**
DOI: 10.71488/cyberlaw.2025.1229828

The Role of Artificial Intelligence in Cyber Fraud and Preventive Measures Against It[1]

Ali Forotani
Department of Law, Ta.C., Islamic Azad University, Tabriz, Iran
Baharak Shahed
Department of Law, Ur.C., Islamic Azad University, Urmia, Iran
(Corresponding Author) Baharakshahed@iau.ac.ir
Jamal Beigi
Department of Law, Mar.C., Islamic Azad University, Maragheh, Iran
Keyvan Heydarnejad
Department of Law, Shab.C., Islamic Azad University, Shabestar, Iran

Abstract
In today's technology-driven world, cyber fraud is one of the most significant cybercrimes and crimes resulting from the misuse of information technology. On the other hand, artificial intelligence, as an advanced emerging technology under development, has transformed cyberspace and technological innovations. The objective of the present article is to examine the role of artificial intelligence in the commission and occurrence of cyber fraud, as well as countermeasures against it, employing a descriptive and analytical method to investigate the topic. Currently, artificial intelligence-based technologies have significantly provided new tools for criminals, enabling cybercriminals to leverage AI-related methods in their activities. From another perspective, artificial intelligence is one of the fields that can enhance cybersecurity, thereby aiding in the identification, detection of crimes, and prevention thereof, proving impactful in countering cyber fraud. These preventive measures are addressed in two frameworks: social prevention and situational prevention. In social prevention, through education, awareness-raising, and formulation of behavioral codes; and in situational prevention, through user behavior analysis, intrusion detection, botnet identification, email security, user information protection, authentication, and fraud detection in pursuit of data and network security—these are among the most important actions of artificial intelligence. In other words, artificial intelligence can be utilized both as a tool for committing cyber fraud and as a tool for defending against it.

Keywords: Cybersecurity, Social Prevention, Situational Prevention, Cyber Fraud, Artificial Intelligence

❋Citation (APA): Forotani, A. Shahed, B. Beigi, J. Heydarnejad, K. (2025). The Role of Artificial Intelligence in Cyber Fraud and Preventive Measures Against It. *Cyberspace legal studies, 4(15),* 50 - 68

[1] - This article is an excerpt from a doctoral dissertation titled "Criminological Analysis of Cyber Fraud and Its Necessities in Iran's Criminal Policy."

مطالعات حقوقی فضای مجازی
Legal Studies in Cyberspace
ISSN: 2821-126X
ویگاه مجله: https://sanad.iau.ir/journal/cyberlaw
تاریخ دریافت: ۱۴۰۴/۰۳/۱۰
تاریخ پذیرش: ۱۴۰۴/۰۹/۰۸
تاریخ انتشار: ۱۴۰۴/۱۰/۰۷
صفحه: ۵۰ الی ۶۸
دوره ۴ / شماره ۱۵ / پاییز ۱۴۰۴
نوع مقاله: پژوهشی
DOI: 10.71488/cyberlaw.2025.1229828

نقش هوش مصنوعی در کلاهبرداری سایبری و تدابیر پیشگیرانه در قبال آن[۱]

علی فروتنی
گروه حقوق، واحد تبریز، دانشگاه آزاد اسلامی، تبریز، ایران
بهارک شاهد
گروه حقوق، واحد ارومیه، دانشگاه آزاد اسلامی، ارومیه، ایران
Baharakshahed@iau.ac.ir (نویسنده مسئول)
جمال بیگی
گروه حقوق، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران
کیوان حیدرنژاد
گروه حقوق، واحد شبستر، دانشگاه آزاد اسلامی، شبستر، ایران

چکیده
در دنیای تکنولوژی امروزه، کلاهبرداری سایبری یکی از مهم ترین جرائم سایبری و جرائم ناشی از سوء استفاده از فناوری اطلاعات است. از طرفی، هوش مصنوعی به عنوان یک فناوری پیشرفته نوظهور در حال توسعه که فضای سایبر و نوآوری های فناوری را دستخوش تغییر نموده است. هدف مقاله ی حاضر، بررسی نقش هوش مصنوعی در ارتکاب و وقوع کلاهبرداری سایبری و نیز مقابله با آن می باشد که به روش توصیفی و تحلیلی به بررسی موضوع پرداخته می شود. در حال حاضر، فناوری های مبتنی بر هوش مصنوعی به طور قابل توجّهی، ابزارهای جدیدی برای مجرمان فراهم کرده است که کلاهبرداران سایبری از روش های مرتبط با هوش مصنوعی برای فعالیّت های خود بهره می برند. و از منظر دیگر، هوش مصنوعی یکی از حوزه هایی است که می توان به کمک آن، امنیّت سایبری را بالا برد و از این طریق، کمک به شناسایی، کشف جرم و در عین حال، پیشگیری از جرم، در مقابله با کلاهبرداری سایبری تأثیرگذار باشد و این تدابیر پیشگیرانه در دو قالب پیشگیری اجتماعی و پیشگیری وضعی مطرح می باشد. در پیشگیری اجتماعی از طریق آموزش، آگاهی بخشی و تدوین کدهای رفتاری و در پیشگیری وضعی از طریق تحلیل رفتار کاربران، تشخیص تهاجم، شناسایی بات نت ها، امنیّت ایمیل، حفاظت از اطلاعات کاربران و احراز هویّت و تشخیص فریب در راستای امنیّت داده و شبکه از مهم ترین اقدامات هوش مصنوعی محسوب می گردد. به عبارتی هوش مصنوعی، هم می تواند به عنوان یک ابزار برای ارتکاب کلاهبرداری سایبری و هم یک ابزار برای دفاع در برابر آن، مورد استفاده قرار گیرد..

کلمات کلیدی: امنیّت سایبری، پیشگیری اجتماعی، پیشگیری وضعی، کلاهبرداری سایبری، هوش مصنوعی.

*استناددهی (APA): فروتنی ، علی. شاهد ، بهارک. بیگی، جمال. حیدرنژاد، کیوان. (۱۴۰۴). نقش هوش مصنوعی در کلاهبرداری سایبری و تدابیر پیشگیرانه در قبال آن. *مطالعات حقوقی فضای مجازی*، ۴(۱۵)، ۵۰ – ۶۸

---

[۱]- این مقاله مستخرج از رساله دکتری با عنوان " تحلیل جرم شناختی کلاهبرداری سایبری و بایسته های آن در سیاست جنایی ایران" است.

مقدمه

با ورود کلاهبرداری سایبری در اثر پیدایش و تکوین فناوری اطلاعات به عرصه ی حقوق جزای اختصاصی اصول و قواعد حاکم بر کلاهبرداری سنّتی به چالش کشیده شده است. تفاوت کلاهبرداری کلاسیک با کلاهبرداری سایبری در این است که تحقّق کلاهبرداری کلاسیک مستلزم اغفال یا فریب قربانی جرم است و موجب می‌شود قربانی جرم مالش را با دستان خود و حتّی با التماس و اصرار فراوان در اختیار مرتکب نهد؛ در حالی که کلاهبرداری سایبری، بدون فریفتن قربانی و از طریق مداخله ناروا در داده‌های رایانه‌ای یا عملکرد سیستم رایانه‌ای حادث می‌گردد. ضمن اینکه کلاهبرداری سایبری، علاوه بر تحصیل مال ممکن است تحصیل منفعت، خدمت و یا امتیاز مالی را به همراه داشته باشد (بابایی، ۱۴۰۱، ۱۳۲ –۱۳۱).

هوش مصنوعی، یکی از برجسته ترین فناوری های نوظهور عصر حاضر، دارای پتانسیل قابل توجّهی برای تغییر و تحوّل ابعاد مختلف زندگی بشری و یکی از فناوری های پیشرفته و پرکاربرد در دنیای امروز است که تأثیر عمیقی بر زندگی انسان ها و جوامع داشته است. مفهوم هوش مصنوعی به عنوان یک شاخه ی علمی و فناوری، به دهه های اوایل قرن بیستم برمی گردد، امّا ریشه های آن را می توان در افکار و آرمان های انسان ها از دیرباز یافت (صوفی و صالح نژاد بهرستاقی،۱۴۰۲، ۲).

اصطلاح هوش مصنوعی به معنای واقعی به جان مک کارتی نسبت داده می شود که به همراه ماروین مینسکی ، ناتانائیل روچستر و کلود شانون در سال ۱۹۵۶ میلادی یک کنفرانس تابستانی را در کالج دارتموث ترتیب دادند. البتّه، برخی از دانشمندان حاضر گمان می کردند عبارت "هوش مصنوعی" به ذهن اشخاص، این مسئله که همه چیز مصنوعی و ساختگی است و هیچ چیز واقعی وجود ندارد را متبادر می کند، به همین دلیل فعّالیّت های خود در این زمینه را با نام پردازش اطلاعات پیچیده منتشر نمودند؛ امّا هوش مصنوعی عبارتی بود که ماندگار شد (میرشکاری و همکاران، ۱۴۰۳، ۷۴). تأثیر هوش مصنوعی در ارتکاب جرایم سایبری یک مسئله اجتماعی و فناوری است که با گسترش روزافزون فناوری های هوش مصنوعی، ابعاد جدیدی را به جرم های سایبری اضافه کرده است.گسترش استفاده از هوش مصنوعی، عدم شناخت، اطلاع و آگاهی کاربران از بعد فنّی این موضوع و همه گیر گشتن تعاملات از طریق آن ها و درگیر نمودن قسمتی از زندگی افراد، موجب وقوع جرائم گوناگونی از جمله جعل، کلاهبرداری و.... در این رابطه گردیده است (صوفی و صالح نژاد بهرستاقی،۱۴۰۲، ۲).

در عصر دیجیتال کنونی، فنّاوری اطلاعات و ارتباطات به طور بنیادی ساختارهای اجتماعی، اقتصادی و سیاسی را متحوّل کرده است. گسترش بی سابقه اینترنت، شبکه های اجتماعی و سایر پلتفرم های دیجیتال، ضمن فراهم آوردن فرصت های بی نظیر، چالش های جدیدی به ویژه در حوزه ی امنیّت سایبری ایجاد کرده است. جرائم سایبری، از جمله حملات سایبری، کلاهبرداری های آنلاین و سرقت اطلاعات، به تهدیدی جدی برای افراد، سازمان ها و دولت ها تبدیل شده است. هوش مصنوعی در کنار مزایایی که برای ما به همراه آورده، دردسرهایی هم به دنبال داشته و ما را در معرض کلاهبرداری های متعدّدی قرار داده است. استفاده از هوش مصنوعی در کلاهبرداری سایبری به عنوان یک روش نوین برای تقلّب و کلاهبرداری در امور آنلاین به کار گرفته می‌شود. با توجه به رشد تصاعدی این جرائم و خسارات هنگفت ناشی از آن ها، ضرورت یافتن راهکارهای نوین برای مقابله با این تهدیدات بیش از پیش احساس می شود. یکی از راهکارهای مؤثر در این زمینه، بهره گیری از هوش مصنوعی است. این مقاله در پاسخ به این سؤال اساسی است که هوش مصنوعی چه نقشی در ارتکاب کلاهبرداری سایبری یا پیشگیری از آن می تواند داشته باشد. لذا ابتدا مفاهیم پایه و سپس، به بررسی تأثیر و نقش هوش مصنوعی در ارتکاب و وقوع کلاهبرداری سایبری و نیز اتّخاذ تدابیر پیشگیرانه در قبال آن پرداخته می شود.

۱. مفهوم شناسی متغیّرهای تحقیق

۱-۱. فضای سایبر

واژه «سایبر» در دهه ی ۱۹۹۰ میلادی جایگزین عناوین دیگری مانند فناوری اطلاعات و ارتباطات، حقوق انفورماتیک و... گردید و مشتقات زیادی از آن از جمله «سایبر اسپیس» و «سایبرلا» ساخته شد که واژه «سایبر اسپیس (فضای سایبر)»، نخستین بار توسط «ویلیام فورد گیبسون» نویسنده داستان های علمی تخیّلی در کتاب نورومنسر برای نشان دادن شبکه های رایانه ای دنیای آنلاین، به کار گرفته شد(قاجارقیونلو،۱۳۹۱، ۱۳۲). فضای سایبر در معنا به مجموعه هایی از ارتباطات درونی انسان ها از طریق کامپیوتر و مسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می شود. یک سیستم آنلاین یا یک تلفن همراه یا یک دستگاه خودپرداز نمونه ای از فضای سایبر است که کاربران آن می توانند از طریق آن با یکدیگر ارتباط برقرار کنند. بر خلاف فضای واقعی، در فضای سایبر نیاز به جا به جایی های فیزیکی نیست و کلیه اعمال فقط از طریق فشردن کلید ها یا حرکات ماوس صورت می گیرد (عاملی، ۱۳۹۰، ۲۳).

۱-۲. کلاهبرداری سایبری

با پیشرفت تکنولوژی و فناوری اطلاعات، جرمی به وجود آمده است که به آن کلاهبرداری سایبری می گویند؛ این کلاهبرداری یکی از جرائم ناشی از سوء استفاده از فناوری اطلاعات است. فناوری اطلاعات، پدیده منحصر به فرد عصر کنونی بوده که موجب رونق، پیشرفت و تغییر و تحوّل عمیق و عظیمی در تمامی ابعاد و شئون زندگی انسان ها گردیده است. این پدیده با طرح مسائل نو و جدید، بسیاری از علوم را با چالش های جدی روبرو ساخته و آن ها را تحت تأثیر قرار داده است. چرا که این پدیده نه تنها امکان ارتکاب رفتار و اعمال مجرمانه ی جدیدی را به وجود آورده که قبل از این به هیچ وجه امکان پذیر نبوده، بلکه با خلق دنیای جدیدی به نام فضای سایبر، ارتکاب بسیاری از رفتارهای مجرمانه را تسهیل نموده است (خرّم آبادی، ۱۳۸۶، ۸۴). امروزه اختراع رایانه و دیگر دستگاه های الکترونیکی (تلفن هوشمند همراه، فضای مجازی و...) امکان ارتکاب جرایمی را فراهم کرده است که بیش از آن وقوع آن ها امکان‌پذیر نبود. بردن متقلبانه اموال متعلق به غیر تا قبل از اختراع رایانه، موضوع جرم کلاهبرداری سنّتی قرار می‌گرفت. با پیدایش رایانه، تعرّض متقلّبانه به داده های پردازش شده در رایانه که نماینده آن اموال محسوب می‌شوند، دیگر نمی‌تواند ذیل همان عنوان سنّتی مورد مطالعه قرار بگیرد (میرمحمدصادقی و شایگان، ۱۳۸۹، ۱۳۸).

کلاهبرداری سایبری مهم ترین و شایع ترین جرم اقتصادی فضای سایبری (فضای مجازی و رایانه) محسوب شده و از جمله جرایمی است، علیه اموال و مالکیّت افراد، با این تفاوت که در کلاهبرداری سنّتی، فرد قربانی بر اثر مانورهای متقلبانه طرف مقابل، فریب خورده و مال خویش را با میل و رغبت خود در اختیار کلاهبردار قرار می دهد؛ امّا در جرم کلاهبرداری سایبری، دیگر نیاز به مانورهای متقلّبانه و فریب قربانی نیست. بلکه بزهکار از راه تغییر و محو و ... در سیستم پردازش داده ها، اموال یا منفعت و ... قربانی را به نفع خود یا دیگری تصاحب می کند؛ بنابراین در تعریف جرم کلاهبرداری سایبری می توان گفت: «هرگونه محو، ورود، پردازش، متوقّف سازی، مداخله در سیستم و برنامه های رایانه ای در فضای سایبری به منظور بردن مال غیر و اخذ منافع مالی برای خود یا دیگری کلاهبرداری سایبری می باشد» (اوجاقلو و زندی، ۱۴۰۰، ۲۴۶).

۱-۳. هوش مصنوعی

علی رغم توجّه فزاینده ای که هوش مصنوعی و روش های توسعه یافته ی آن در رسانه ها، تحقیقات چند رشته ای و سیاست گذاری ها به خود جلب می کند، توافق روشن و واضحی در مورد این که چگونه هوش مصنوعی باید به بهترین شکل تعریف

شود، وجود ندارد. ظاهراً این موضوع نه تنها با توجه به برداشت عمومی، بلکه به علم کامپیوتر و قانون مرتبط است. به عنوان مثال، گاسر و آلمیدا اعتقاد دارند که یکی از دلایل دشواری تعریف هوش مصنوعی از منظر فنّی، این است که هوش مصنوعی یک فناوری واحد نیست، بلکه مجموعه ای از تکنیک ها و زیرشاخه ها از حوزه هایی مانند تشخیص گفتار و بینایی رایانه گرفته تا حافظه و دقّت توجه است. گروه تخصّصی هوش مصنوعی کمیسیون اتّحادیّه اروپا، هوش مصنوعی را چنین تعریف نمودند: هوش مصنوعی به سیستم هایی اطلاق می شود که با تجزیه و تحلیل محیط خود و انجام اقدامات با درجاتی از خود مختاری برای دستیابی به اهداف خاص، رفتار هوشمندانه ای را نشان می دهند. سیستم های مبتنی بر هوش مصنوعی می توانند صرفاً مبتنی بر نرم افزار باشند و در دنیای مجازی عمل کنند (مانند نرم افزار تحلیل تصویر، دستیارهای صوتی، موتورهای جستجو، سیستم های تشخیص چهره و گفتار) یا هوش مصنوعی را می توان در دستگاه های سخت افزاری تعبیه کرد؛ مانند: اتومبیل های خودران، روبات های پیشرفته، پهپادها یا برنامه های کاربردی اینترنت اشیا (فرج پور و همکاران، ۱۴۰۳، ۴۰). لذا هنوز تعریف دقیقی از هوش مصنوعی که تمامی دانشمندان بر روی آن توافق داشته باشند ارائه نشده، ولی اکثر تعریف‌ها را جهت تبیین بیشتر، می‌توان به شکل زیر بیان کرد.

هوش مصنوعی که برخی از آن به اختصار " هومص" یاد کرده اند، در لغت انگلیسی متشکل از دو بخش بوده و در زبان فارسی به عنوان هوش مصنوعی ترجمه گشته است (ذوالقدر، ۱۴۰۴، ۵۲ و ۵۳). پیشگامانی مانند جان مک‌کارتی در سال ۱۹۵۶، هوش مصنوعی را به عنوان علم و مهندسی خلق ماشین‌های هوشمند تعریف کردند (حافظ ، ۲۰۲۵،۱).

همچنین، برابر تعریف سند ملی هوش مصنوعی، این فنّاوری، به توانایی ماشین برای انجام عملکرد های خودکار و نظام مند از جمله یادگیری، درک، استنتاج، حلّ مسأله، پیش‌بینی، تصمیم‌گیری و اقدام از طریق به کارگیری دانش و اطلاعات و پردازش داده گفته می‌شود که منشأ اثرگذاری های گسترده بر انسان و روابط انسانی در محیط فیزیکی یا مجازی و همچنین بازتاب های زیست محیطی است. هوش مصنوعی ماهیّتی داده ای، شبکه ای، الگوریتمی، خوشه ای، لایه ای و یکپارچه، مبتنی بر منطق های کلاسیک و سایر منطق های نوین دارد (فلاح تفتی، ۱۴۰۳، ۴).

اساساً یادگیری در هوش مصنوعی به سه دسته ی هوش مصنوعی محدود ، عمومی و فوق العاده (سوپر) تقسیم می شود. این سه دسته، بیشتر نشان دهنده ی روند تکامل هوش مصنوعی در طول زمان هستند؛ به این صورت که در هوش مصنوعی محدود، این هوش برای عملی محدود و معیّن و دستوری خاصّ طرّاحی شده و نمی تواند به طور مستقل مهارت هایی فراتر از طرّاحی آن را بیاموزد. آن ها اغلب از یادگیری ماشینی و الگوریتم های شبکه عصبی مانند: گوگل ترنسلیت و سیستم تشخیص چهره یا چت بات های عادّی برای تکمیل این وظایف مشخص شده استفاده می کنند. منظور و هدف از طرّاحی هوش مصنوعی عمومی این است که بتوان ماشین هایی ایجاد کرد که قادر به انجام وظایف چند منظوره باشند و به عنوان دستیاران واقعی و به همان اندازه هوشمند برای انسان ها در زندگی روزمره عمل کنند. هوش مصنوعی فوق العاده یا ابر هوش مصنوعی راهی به سوی آینده است. برای ایجاد آن باید این هوش از انسان پیشی بگیرد و توانایی بیشتری از انسان داشته باشد (میرشکاری و همکاران، ۱۴۰۳، ۷۶-۷۵). و در یک تقسیم بندی دیگر، هوش مصنوعی به هوش مصنوعی ضعیف و هوش مصنوعی قوی تقسیم می شود؛ در هوش مصنوعی ضعیف، سیستم ها تنها وظیفه های خاصّ و محدودی را انجام می دهند و اغلب بر اساس قوانین و الگوریتم های مشخص عمل می کنند (منصور بیگ و شیری، ۱۴۰۴، ۲۴). امّا در هوش مصنوعی قوی، سیستم ها قادر به تفکّر، یادگیری، حلّ مسئله و انجام وظایف پیچیده تر هستند (صوفی و صالح نژاد بهرستاقی، ۱۴۰۲، ۲).

۱-۴. پیشگیری اجتماعی

تدابیر پیشگیرانه که برخی آن را نوعی مداخله از طریق اتّخاذ تدابیر برای جلوگیری یا کاهش خطرات ارتکاب یا کاهش نتایج احتمالی می دانند. موریس کوسن، جرم شناسی کانادایی، پیشگیری را چنین تعریف می کند: «مجموعه اقدام ها و تدابیر غیر قهرآمیز که با هدف خاصّ مهار بزهکاری، کاهش احتمال جرم، کاهش وخامت جرم، پیرامون علل جرایم اتخاذ می شود». در این تعریف، اقدام پیشگیرانه، اقدام غیر قهرآمیزی است که بر عوامل جرم زا اعمال می گردد (ابراهیمی، ۱۳۹۶، ۳۸). می توان در نوشتگان اختصاص یافته به پیشگیری از بزهکاری، دو جهت گیری کلّی را ملاحظه کرد: الف) "بینشِ موسّع و فراگیر" که «هر اقدامی در زمینه مبارزه با بزهکاری، حتّی پاسخ های کیفری (ضمانت اجراهای کیفری) و جبران خسارت از بزه دیدگان را پیشگیرانه محسوب می کند. در این تعریف، در واقع فقط به نتیجه توجه می شود؛ یعنی هر روش، صرف نظر از محتوی، خواه کیفری، خواه غیرکیفری، که منجر به کاهش نرخ بزه کاری می شود. اما مراد از "معنای مضیّق"، همان پیشگیری های معمول در جرم شناسی است که عمدتاً در دو گونه ی پیشگیری اجتماعی و پیشگیری وضعی- فنّی، مطالعه و به صورت موردی نسبت به یک جرم خاصّ و یا کلّی، نسبت به بزهکاری به شکل ترکیبی اعمال می شود (ابراهیمی، ۱۳۹۶، ۳۹). پیشگیری اجتماعی به آن نوع اقدامات پیشگیرانه ای گفته می شود که عمدتاً بر تغییر شرایط جرم زای محیط اجتماعی تأکید می کند. به عبارت دیگر، پیشگیری اجتماعی از بزهکاری، عبارت است از: جلوگیری از ارتکاب جرم از طریق از بین بردن عوامل اجتماعی تکوین جرم (رحیمی نژاد، ۱۳۹۵، ۱۲۱ و ۱۲۲).

۱-۵. پیشگیری وضعی

پیشگیری وضعی از جرم به یک رویکرد پیشگیرانه ای اشاره دارد که نه بر توسعه ی جامعه و نهادهای آن، بلکه صرفاً بر کاهش موقعیّت ها و فرصت های ارتکاب جرم مبتنی است. به عبارت دیگر، در پیشگیری وضعی، ما با استفاده از شیوه ها و روش هایی همچون تقویت آماج ها و سیبل های جرم ، استفاده از تکنولوژی مراقبتی و کنترلی و مدیریّت و طرّاحی محیطی به دنبال کاهش فرصت ها و موقعیّت های ارتکاب جرم و تسلّط بر شرایط و اوضاع و احوال پیرامونی جرم و نتیجتاً جلوگیری از وقوع جرم هستیم (رحیمی نژاد، ۱۳۹۵، ۱۲۲ و ۱۲۴).

۲. نقش هوش مصنوعی در وقوع کلاهبرداری سایبری

انقلاب فنّاوری به دلیل چندین فنّاوری توانمندساز کلیدی، مانند هوش مصنوعی، به سرعت در حال توسعه است (بتوش ،۲۰۲۵، ۱). هوش مصنوعی در کنار مزایا و تأثیر زیادی که بر زندگی و فعّالیّت‌های ما گذاشته، درد سرهایی هم به دنبال داشته و حتی در دنیای تبهکاری نیز با استقبال روبه رو شده و ما را در معرض کلاهبرداری های متعدّدی قرار داده است. نیازی نیست با شنیدن نام کلاهبرداری های مبتنی بر هوش مصنوعی، به سناریوهای عجیب و غریب و تخیّلی فکر شود. این نوع کلاهبرداری ها همان کلاهبرداری های قدیمی و آشنا هستند که به لطف هوش مصنوعی ساده تر، ارزان تر و قانع‌کننده تر از قبل شده اند. در حال حاضر، فناوری های مبتنی بر هوش مصنوعی به طور قابل توجّهی ابزارهای جدیدی برای مجرمان فراهم کرده است که کلاهبرداران سایبری از این فناوری برای بهینه سازی حملات، ایجاد بدافزار خودکار و مهندسی اجتماعی و نیز از روش های مرتبط با هوش مصنوعی برای فعّالیّت های خود بهره می برند. لذا به تعدادی از آن به قرار ذیل اشاره می گردد:

۲-۱. کلاهبرداری فیشینگ با استفاده از هوش مصنوعی

هکرها از هوش مصنوعی برای ساخت و ارسال پیام‌های فیشینگ به کاربران با هدف دریافت اطلاعات حساس یا ورود به حساب کاربری آن‌ها استفاده می‌کنند. به طور مثال، پیام فیشینگ با استفاده از هوش مصنوعی می‌تواند به شکل یک ایمیل باشد که به صورت خودکار توسط هوش مصنوعی ارسال شده و در آن برای کاربران نام کاربری و رمز عبور خود را وارد کنند.

استفاده از الگوریتم های یادگیری ماشین و تحلیل داده: در این روش، هکرها با استفاده از مجموعه ای از الگوریتم های یادگیری ماشین، می توانند به داده های مربوط به یک فرد در فضای سایبری دسترسی پیدا کنند و با تحلیل و بررسی این داده ها، اطلاعات حسّاس را پیدا کنند. به عنوان مثال، هکرها با استفاده از هوش مصنوعی به جستجوی افرادی می‌پردازند که احتمال وابستگی شدیدی به یک شبکه اجتماعی دارند. با تحلیل پیام های ایمیل، پیام های خصوصی، پیام های تلفنی و داده های مرتبط با شبکه های اجتماعی، می توانند به اطلاعات شخصی و حسّاس فرد دسترسی پیدا کنند که باعث کلاهبرداری از این افراد می شود. حملات فیشینگ پیشرفته یکی از پرکاربرد ترین روش‌های حمله است، امّا اکنون با کمک هوش مصنوعی بسیار پیچیده‌تر و مؤثرتر شده است. مهاجمان با استفاده از ابزارهایی مانند چت جی پی تی ، پیام‌هایی بسیار قانع کننده تولید می‌کنند که احتمال فریب قربانیان را به طور چشمگیری افزایش می‌دهد.

۲-۲. کلاهبرداری جعل عمیق (دیپ‌فیک)

یکی از روش های دیگر کلاهبرداری، توانایی هوش مصنوعی مدرن برای جعل هویّت افراد است. اگرچه، قدمت دستکاری رسانه های دیداری و شنیداری به میزان عمر خود رسانه هاست؛ اما ورود اخیر جعل عمیق یک جهش قابل توجّه و رو به جلو و نقطه عطفی در این زمینه بوده است. جعل عمیق یا دیپ فیک ترکیبی از "یادگیری عمیق" و "محتوای جعلی" است که به استفاده از هوش مصنوعی برای ساخت، دستکاری محتواهای صوتی- بصری برای معتبر جلوه دادن، اشاره دارد. مجرمان سایبری در حال حاضر از این فناوری برای تولید محتوای مستهجن جعلی و غیرقانونی افراد مشهور یا انتشار اطلاعات غلط سیاسی استفاده می‌کنند و حتّی یک شرکت انرژی مستقر در بریتانیا را فریب داده‌اند تا در سال ۲۰۱۹ مبلغ ۲۲۰۰۰۰ یورو را به یک حساب بانکی مجارستان منتقل کند.

جعل عمیق، محتوای رسانه ای فریبنده بوده که توسط فناوری های هوش مصنوعی ایجاد شده و ابزاری مهم برای انتشار اطلاعات غلط و جعل هویّت دیجیتالی و به عبارت دیگر آلودگی داده ها محسوب می شود. که تشخیص آن، حتّی برای اشخاص خبره و متخصّص نیز سخت و مشکل است. جعل عمیق توسط الگوریتم های یادگیری ماشینی در دو قسمت شبکه های عصبی و شبکه مولّد تخاصمی ترکیب شده با نرم افزار نقشه برداری چهره ایجاد می گردند که می توانند آن داده ها را بدون اجازه در محتوای دیجیتال وارد کنند. اوّلین و بیشترین استفاده از آن، تغییر تصاویر افراد برای کلاهبرداری است. از جمله نرم افزارهایی که به صورت رایگان در اختیار همگان قرار گرفته و برای تغییر چهره کاربرد دارد می توان ری فیس و دیپ فیس لب را نام برد. دیگر مورد استفاده از جعل عمیق که می تواند موجب ایجاد چالش در زمینه حریم خصوصی شود، توانایی این فناوری در فریب سامانه های احراز هویّت بیومتریک است که از آن می توان برای دستیابی به اطلاعات محرمانه اشخاص مانند جعل هویّت برای ورود و دستیابی به اطلاعات شرکت های رمز ارز مانند بایننس استفاده نمود (میرشکاری و همکاران، ۱۴۰۳، ۸۱). این نوع فریب، از توانایی هوش مصنوعی برای دستکاری آسان محتوای بصری یا صوتی و قانونی جلوه دادن آن استفاده می کند. این شامل استفاده از صدا و تصویر ساختگی برای جعل هویّت شخص دیگری است. سپس می‌توان محتوای اصلاح شده را به‌طور

گسترده در عرض چند ثانیه به صورت آنلاین توزیع کرد، از جمله در پلتفرم های رسانه های اجتماعی تأثیرگذار برای ایجاد زمینه های کلاهبرداری سایبری قرار گیرد.

هوش مصنوعی مولّد سبب شده است تا دیپ فیک، گامی رو به جلو داشته باشد و تصاویر، ویدئوها و صداهای مصنوعی واقعی‌تر همیشه به نظر برسند. روش دیگری که کلاهبرداران از دیپ فیک استفاده می‌کنند، دور زدن سیستم های تأیید است. بانک‌ها و صرافی‌های ارز دیجیتال از این سیستم‌ها برای تأیید هویّت واقعی مشتریان شان استفاده می‌کنند. آن ها از کاربران جدید می‌خواهند در حالی که مدرک شناسایی فیزیکی خود را در مقابل دوربین نگه داشته‌اند، از خود عکس بگیرند؛ اما تبهکاران اپلیکیشن‌هایی را در پلتفرم هایی مانند تلگرام عرضه کرده اند که به مردم اجازه می دهد تا نیازشان را بدون طی کردن این مرحله برطرف کنند. می‌توان انتظار داشت که در آینده، کلاهبرداران از دیپ فیک های واقعی استفاده کنند تا بتوانند احراز هویّت پیچیده تری انجام دهند.

۲-۳. ارائه خدمات جیل‌بریک (شکستن قفل سیستم محافظ)

شرکت های هوش مصنوعی تدابیر حفاظتی مختلفی را برای جلوگیری از انتشار اطلاعات مضر یا خطرناک مدل هایشان در نظر گرفته‌اند. تبهکاران سایبری به جای ساخت مدل های هوش مصنوعی خود بدون این پادمان‌ها که گران، وقت‌گیر و دشوار است، روند جدیدی را پیش گرفته‌اند که عبارت است از ارائه خدمات جیل‌بریک. اکثر مدل ها قوانینی در مورد نحوه استفاده از جیل‌بریک دارند که به کاربران اجازه می‌دهد تا سیستم هوش مصنوعی را دست‌کاری کنند و خروجی‌هایی تولید کنند که این سیاست‌ها را نقض می‌کند. به عنوان مثال، برای نوشتن کد باج افزار یا تولید متنی که می‌تواند در ایمیل‌های کلاهبرداری استفاده شود. سرویس‌های جیل‌بریک از ترفندهای مختلفی برای شکستن مکانیسم‌های ایمنی استفاده می‌کنند؛ مانند طرح سؤالات فرضی یا پرسیدن سؤال به زبان‌های خارجی. بازی دائمی موش و گربه‌ای بین شرکت های هوش مصنوعی وجود دارد که سعی می‌کنند مدل‌هایشان از رفتار نادرست جلوگیری کنند و بازیگران بدخواه با اعلان‌های خلاقانه تری برای جیل‌بریک کردن مواجه شوند.

۲-۴. شکستن رمز عبور با هوش مصنوعی

مجرمان سایبری از یادگیری ماشینی و هوش مصنوعی برای بهبود الگوریتم‌های حدس زدن رمز عبور کاربران استفاده می‌کنند. درحالی‌که برخی از الگوریتم‌های شکستن رمز عبور از قبل وجود دارند، مجرمان سایبری قادر خواهند بود مجموعه داده های رمز عبور بزرگ‌تری را تجزیه وتحلیل کنند و تغییرات عمده و متفاوتی در تحلیل رمز عبور ایجاد کنند.

۲-۵. طرح های مهندسی اجتماعی توسط هوش مصنوعی

این طرح بر دستکاری روانی تکیه می‌کند تا افراد را فریب دهند تا اطلاعات حساس را فاش کنند یا اشتباهات امنیتی دیگری انجام دهند. این طیف گسترده ای از دسته بندی های فعّالیّت های جعلی را شامل می شود، از جمله کلاهبرداری های فیشینگ، ویشینگ و ایمیل های تجاری. هوش مصنوعی به مجرمان سایبری اجازه می دهد تا بسیاری از فرآیندهای مورد استفاده در حملات مهندسی اجتماعی را خودکار کنند و همچنین پیام های شخصی‌تر، پیچیده تر و مؤثرتر را برای فریب قربانیان نا آگاه ایجاد کنند. این بدان معناست که مجرمان سایبری می توانند حجم بیشتری از حملات را در زمان کمتری ایجاد کنند و نرخ موفقیت بالاتری را تجربه کنند.

۳. تدابیر پیشگیرانه از طریق هوش مصنوعی در قبال کلاهبرداری سایبری

فعّالیّت های کلاهبرداری به یک مشکل فراگیر و پرهزینه در دنیای به هم پیوسته امروزی تبدیل شده است که ثبات و اعتماد را تهدید می کند. ظهور تاکتیک های پیچیده کلاهبرداری و ماهیّت دائماً در حال تحوّل رفتارهای متقلّبانه، راه حل‌های نوآورانه و تطبیقی را برای کشف کلاهبرداری ضروری می‌کند. هوش مصنوعی ثابت کرده است که در نبرد با کلاهبرداری قدرتمند است و قابلیّت‌های امیدوارکننده ای را برای افزایش کارایی و دقت سیستم‌های تشخیص ارائه می‌کند (کوتیاپان و راجاسکار ،۲۰۲۳،۱). و نیز در دنیای تکنولوژی امروزه، کلاهبرداری سایبری به یکی از بزرگ ترین تهدیدات مالی برای افراد تبدیل شده است. با پیچیده تر شدن این حملات سایبری و افزایش حجم داده ها، تشخیص و پیش بینی این تهدیدات به چالشی جدی تبدیل شده است. در همین راستا، هوش مصنوعی به عنوان یک فناوری نوظهور، نقش مهمّی در مقابله با این تهدیدات می تواند ایفا کند. هوش مصنوعی با توانایی پردازش حجم عظیمی از داده ها، شناسایی الگوهای پیچیده و یادگیری مداوم، ابزاری قدرتمند برای تحلیل رفتارهای مشکوک در شبکه ها و پیش بینی حملات سایبری به شمار می رود. این فناوری به سیستم های امنیتی اجازه می دهد تا تهدیدات را در مراحل اولیه شناسایی کرده و از وقوع کلاهبرداری سایبری پیشگیری کنند (فلاح تفتی، ۱۴۰۳، ۵).

۱-۳. تدابیر پیشگیرانه اجتماعی

پیشگیری اجتماعی مرسوم ترین نوع پیشگیری غیر کیفری بوده که بر مبنای رویکرد عوامل بزهکاری مبتنی است و به دنبال تعیین عوامل بزهکاری، سازماندهی برنامه هایی به منظور مقابله با آن و تغییر شرایط اجتماعی، اقتصادی نامناسبی است که فرد در آن زندگی می کند و منشاء رفتارهای ضداجتماعی وی می شود (ابراهیمی، ۱۳۹۶، ۵۱). اهمّ تدابیر پیشگیرانه از طریق هوش مصنوعی در قبال کلاهبرداری سایبری؛ تدابیری هم چون آموزش و آگاهی و تدوین کدهای رفتاری به شرح ذیل مورد سنجش و بررسی قرار می گیرد.

۱-۱-۳. آموزش و آگاهی بخشی

به رغم گسترش روز افزون ابزارهای فنّاورانه ی مخابراتی و ارتباطاتی و کاربری فراگیر و گسترده ی آن ها در امور گوناگون زندگی، افراد بسیاری هستند که از تهدیدهای ناشی از کاربری های نا امن خود ناآگاه اند. و گمان می برند فضای سایبری، همه چیز جلوه ای غیر واقعی دارد و در صورت مواجه با تهدیدها، چیزی از دست نمی دهند. زیرا اغلب افرادی که در فضای سایبر، بزه دیده ی این جرم می شوند از تهدیدات این فضا نسبت به حفظ اطلاعات و داده ها بی خبرند یا حداقل آگاهی را دارند. در نتیجه به سادگی، داشته ها و اطلاعات ارزشمند مالی الکترونیکی را به اشتراک یا زمینه ی آسیب پذیری و بزه دیدگی کلاهبرداری خود را فراهم می آورند (جلالی فراهانی و منفرد، ۱۳۹۲، ۱۶۲). بنابراین جهت جلوگیری از قربانی شدن، نیاز به آگاهی بخشی جدی در این حوزه باید وجود داشته باشد. در نتیجه، اوّلین و نخستین گام و مرحله در تدابیر و اقدامات پیشگیرانه از طریق هوش مصنوعی در کلاهبرداری در فضای سایبری، آموزش و آگاهی دادن به کاربران و مردم درباره تهدیدات علیه اطلاعات و داده ها است. خوشبختانه مسئولین ذیربط نیز در متون قانونی و اسناد بالادستی که به عنوان سیاست جنایی فراتقنینی (بالاتر از مجلس) مطرح می باشد، ضمنی و به عنوان یک اصول کلّی در حوزه ی سایبری به آموزش و آگاهی عموم مردم پرداخته است که در ذیل به برخی از این مقرره ها اشاره می شود.

۱. بند دوّم اصل سوم قانون اساسی ، سیاست های کلی نظام در خصوص شبکه های اطلاع رسانی رایانه ای در مورخ ۱۳۸۰/۰۳/۰۹ ، بند (۸) ابلاغیه ی سیاست های کلی نظام در امور«امنیّت فضای عمومی در حوزه افتا » در مورخ ۱۳۸۹/۱۱/۲۶

، ماده ی (۲) اساسنامه ی مرکز ملی فضای مجازی مورخ ۱۳۹۱/۰۴/۳۱ که این مقررها، جرم کلاهبرداری در فضای سایبر را نیز شامل می گردد.

۲. سند ملّی هوش مصنوعی

در بند ۵ ماده ی ۲ این سند ملّی، توّجه به عدالت، کرامت، حقوق و سلامت جسمی، روحی و روانی انسان ها در سازوکار آموزش و به کارگیری هوش مصنوعی شده است. و نیز در بند ۶ اهداف کلان این سند؛ نقش آفرینی فعّال در تعاملات و همکاری های آموزشی، علمی، فنّاورانه و اقتصادی بین المللی با اولویّت کشورهای همسو در راستای منافع ملی و جهان اسلام گردیده است. و نیز آموزش نیروی انسانی برای مدیریت سیستم های پیشرفته هوش مصنوعی به عنوان راهکارهای تقویت امنیّت سایبری با هوش مصنوعی.

۲-۱-۳. تدوین کردارنامه ها (کدهای رفتاری)

از دیگر تدابیر پیشگیرانه ی اجتماعی در خصوص کلاهبرداری سایبری، تدوین کدهای رفتاری یا کردارنامه ها از سوی دست اندرکاران حوزه ی سایبری است تا به این طریق، با ماهیّت کار خود آشنا شده و سپس عواقب ناشی از نقض شرایط حاکم بر آن را بپذیرند و زیربنای اصلی آن ها، بر آگاه بخشی و هشدار دهی مخاطبان شان استوار است. به عبارتی دیگر منظور از کردار نامه، مجموعه قواعد وضع شده برای متصدیّان یک حوزه ی خاص است تا با ماهیّت کار خود و هم چنین عواقبی آن آشنا شوند که در اثر شرایط حاکم بر آن متحمّل خواهند شد (ذبیح اله نژاد، ۱۵۷،۱۳۹۷).

به صورت کلّی با تدوین کردارنامه ها، می توان گروه های خاص و ویژه ای که وظیفه و تعهّد خاصّی بر عهده آنان گذاشته شده است در مقابل اعمال و اقدامات خود، مسئول و پاسخ گو نگه داشت. از قبیل گروه های شغلی و حرفه ای که در حوزه های مختلف به فعّالیّت مشغول می باشند و چون که به متصدیّان شبکه ای خود داده و اطلاعات، دارای ارزش و اعتبار را واگذار نموده اند، تا با رعایت سه اصل تمامیّت ، محرمانه بودن و دسترس پذیری در فضای سایبر منتشر و توزیع کنند، ضروری و مهّم است که مناسب و متناسب با حرفه و شغل، نوع و میزان اطلاعات آن ها، کد رفتاری مرتبط را تدوین نمایند. این کدها، مقنّن را حجم فراوان تقنین نجات می دهد. صنوف از جمله صنف رایانه ای، مخابراتی و ... با خود تنظیمی ، بایدها و نبایدهای شغلی را تبیین می کنند و این اقدام باعث ترویج اخلاق رایانه ای یا سایبری می گردد که در اسناد جهانی «اعلامیّه اصول، ایجاد و ساخت جامعه اطلاعاتی، چالش جهانی هزاره ی جدید» با (۶۷ ماده) و «طرح اقدام» (با ۲۹ ماده و ۱۱ خط عمل) در سال ۲۰۰۳ در ژنو و نیز اسناد «تعهّد تونس» و «دستور جلسه تونس برای جامعه ی اطلاعاتی» (سال ۲۰۰۵) مورد تأکید قرار گرفته است (محمدزاده و همکاران، ۱۴۰۲، ۱۲۱).

کدهای رفتاری که با عناوینی هم چون منشورهای اخلاقی و حرفه ای شناخته می شوند، بر دو قسم اند. کدهای رفتاری بزهکار مدار و کدهای رفتارهای بزه دیده مدار. کدهای رفتاری بزهکارمدار عموماً برای بزهکاران بالقوه با هدف بازدارندگی آن ها از روی آوردن به بزهکاری با یادآوری پیامدهایی که در انتظار آنان خواهد بود (از قبیل: ضمانت اجراهای قراردادی، مقرراتی، مدنی و کیفری) تدوین می شود. کدهای رفتاری بزه دیده مدار برای بزه دیدگان بالقوه نیز بهره برداری و تهدیدهای پیش روی آن ها را گوشزد می کند. ضمن این که این آسیب ها برای شان ممکن است مسئولیّت هایی به دنبال داشته باشد که در این صورت با جدیّت بیشتری به توصیه های ایمنی و امنیتی پایبند خواهد بود (جلالی فراهانی و منفرد، ۱۳۹۲، ۱۶۴ -۱۶۳).

با توجّه به مزایای بیان شده برای کدهای رفتاری، به نظر می رسد در خصوص جرم کلاهبرداری در فضای سایبر، آیین نامه ی دفاتر خدمات اینترنت و آیین نامه ی واحدهای ارائه کننده ی خدمات اطلاع رسانی و اینترنت مصوب شورای عالی انقلاب فرهنگی می باشد که مفاد این دو آیین نامه نیز بیشتر در زمینه ی اعمال نظارت فیزیکی بر کاربران اینترنتی در ارائه ی خدمات به آن ها و اعلام اسامی سایت هایی است که محتوای مجرمانه به مراجع ذی صلاح دارند و می توان آن ها را جزو کدهای رفتاری محسوب نمود.

۲-۳. تدابیر پیشگیرانه وضعی

پیشگیری وضعی یعنی تغییر اوضاع و احوال و شرایط خاص که احتمال ارتکاب جرم در آن زیاد است، به منظور دشوار نمودن، پر خطر کردن یا جاذبه زدایی ارتکاب جرم. این رویکرد سه هدف را دنبال می کند: افزایش خطرات دستگیری، افزایش دشواری ها و کاهش منافع. این نوع از پیشگیری، بر مبنای یک افق کوتاه مدت، کارایی و فایده مندی بی درنگ و زودهنگام تدابیر پیشگیری مبتنی است (ابراهیمی، ۱۳۹۶، ۸۶).

تدابیر پیشگیرانه ی وضعی از طریق هوش مصنوعی در قبال کلاهبرداری سایبری می توان به تدابیر امنیّت سایبری داده و شبکه اشاره نمود که به شرح ذیل بیان می گردد.

۱-۲-۳. امنیّت سایبری داده و شبکه توسط هوش مصنوعی

بهره گیری از هوش مصنوعی در شناسایی و جلوگیری از تهدیدات سایبری و جلوگیری از ورود مهاجمان به شبکه به یکی از راهکارهای اساسی در امنیّت سایبری تبدیل شده است. امنیّت سایبری به مجموعه‌ای از اقدامات و فرآیند هایی اشاره دارد که برای محافظت از سیستم ها، شبکه ها و داده ها در برابر حملات سایبری طرّاحی شده‌اند. ابزارهای هوش مصنوعی می توانند داده ها را مورد بررسی قرار داده و داده های ناهنجار را که از دید انسان پنهان مانده است، تشخیص دهند. یکی از کارکرد های هوش مصنوعی در زمینه امنیّت داده، شناسایی و جلوگیری از نشت داده می باشد. این امر می تواند به دلیل اتّصال کاربران غیرمجاز به سیستم، سطح دسترسی های نادرست به اطلاعات، سیستم های مجهز به هوش مصنوعی با شناسایی نظارت و مراقبت از اطلاعات موجود در حافظه و همچنین مراقبت از داده هایی که در شبکه ها در حال جا به جایی هستند، امنیت داده ها را افزایش می دهد و درصورت وجود رفتار غیرعادی به طور خودکار هشدار داده و از ادامه آن رفتار جلوگیری می کند (کاوه و بارانی، ۱۴۰۴، ۱۹۷).

امروزه نبود امنیّت کافی در فضای وب، خطر حملات سایبری، سرقت اطلاعات شخصی و مالی و اختلال در سیستم های حیاتی را به همراه دارد. امنیّت سایبری با محافظت از داده‌ها و زیرساخت‌ها، کمک می‌کند تا از تهدیدات مخرب در امان بمانند و اعتماد کاربران به خدمات دیجیتال را تقویت می‌کند. در حال حاضر هوش مصنوعی و امنیّت سایبری ارتباطی عمیق و دو سویه دارند. از یک سو، هوش مصنوعی می‌تواند با تحلیل داده های حجیم و شناسایی الگوهای مشکوک، به بهبود سیستم‌های امنیتی و مقابله با تهدیدات سایبری کمک کند. الگوریتم‌های یادگیری ماشین می‌توانند به سرعت حملات را پیش‌بینی و به آن‌ها پاسخ دهند. از سوی دیگر، خود هوش مصنوعی نیز ممکن است هدف حملات سایبری قرار گیرد. مهاجمان می‌توانند از نقاط ضعف موجود در مدل‌های هوش مصنوعی سوءاستفاده کرده و با حملاتی مانند دستکاری داده‌ها یا حملات تداخلی، این سیستم‌ها را فریب دهند. بنابراین، تعامل نزدیک میان متخصصان هوش مصنوعی و امنیت سایبری برای حفاظت از این فناوری‌های حساس و بهبود امنیت آن‌ها ضروری است. برای مثال در صنعت مالی، بانک‌ها با استفاده از هوش مصنوعی به تشخیص تراکنش‌های مشکوک و

پیشگیری از کلاهبرداری می‌پردازند. به عنوان نمونه، با بهره‌گیری از الگوریتم‌های یادگیری ماشین، رفتار مشتریان را تحلیل و فعالیت‌های غیرعادی را شناسایی می‌کند. این سیستم ها قادرند تهدیدات را به سرعت کشف و پیش از وقوع حملات سایبری، آن‌ها را خنثی کنند.

در ادامه کاربردهای هوش مصنوعی در امنیّت شبکه (سایبری) به عنوان اقدامات پیشگیرانه از کلاهبرداری سایبری به شرح ذیل توضیح داده می شود.

۲-۲-۳. تحلیل رفتار کاربران با هوش مصنوعی

سیستم های مدرن تشخیص کلاهبرداری از مجموعه‌ای پیچیده از فنّاوری‌های هوش مصنوعی، شامل الگوریتم های یادگیری ماشین، شبکه های عصبی عمیق و پردازش زبان طبیعی ، استفاده می‌کنند (ولوو ،۲۰۲۵، ۲۲۸).

یادگیری (فراگیری) ماشین، یک نوع هوش مصنوعی است که سیستم ها را قادر می سازد از داده ها بدون برنامه ریزی صریح یاد بگیرند. الگوریتم های یادگیری ماشین بر روی مجموعه ی داده های بزرگی از ترافیک پیچیده برای شناسایی الگوها و تهدیدات بالقوه آموزش داده می شوند (محمودی و بحر کاظمی، ۱۴۰۳، ۱۰۰). یادگیری ماشین می‌تواند تکنیک هایی را برای توسعه، مدل هایی ارائه دهد که روند های جدید در آن، شامل طرح‌های " داپ مل" است که قادر به شناسایی الگوهای پیچیده‌تر بر روی حجم عظیمی از داده‌ها هستند (زیوویروس ،۲۰۲۵، ۱۴۸۲۵).

هوش مصنوعی با بهره گیری از الگوریتم های یادگیری ماشین، تحوّلی شگرف در حوزه ی امنیّت سایبری ایجاد که یکی از کاربردهای کلیدی آن، تحلیل رفتار کاربران است. با جمع آوری داده های متنوعی از قبیل فعّالیّت های کاربران در فضای سایبری، هوش مصنوعی الگوهای رفتاری نرمال را شناسایی می کند و هرگونه انحراف از این الگوها را به عنوان یک تهدید بالقوه در نظر می گیرد. این فرآیند شامل مراحلی است: ابتدا، داده های خام جمع آوری و پیش پردازش شده و سپس، ویژگی های کلیدی که نشان دهنده رفتارهای کاربران هستند، استخراج می شوند. در مرحله بعد، با استفاده از الگوریتم های مناسب، مدلی ساخته می شود که قادر به تشخیص رفتارهای غیرعادی است. این مدل با داده های آموزشی تغذیه شده و به مرور زمان بهبود می یابد. هوش مصنوعی قادر است انواع مختلف و متفاوتی از اعمال و رفتارهای غیرعادی را شناسایی کند، از جمله تلاش های مکرّر برای ورود به سیستم با رمز عبور اشتباه و... هوش مصنوعی با تحلیل رفتار کاربران، یک لایه دفاعی قدرتمند در برابر تهدیدات سایبری ایجاد و این امکان را می دهد تا به طور مؤثرتری از دارایی های دیجیتال محافظت کنند (فلاح تفتی، ۱۴۰۳، ۶ -۵).

۳-۲-۳. تشخیص تهاجم، نفوذ یا تهدید توسط هوش مصنوعی

سیستم تشخیص تهاجم یا نفوذ، یک ابزار مؤثر جهت شناسایی و تشخیص هرگونه استفاده ی غیرمجاز سوءاستفاده و یا آسیب رسانی در شبکه را برعهده دارد. برای ایجاد امنیّت کامل در یک سیستم رایانه ای یا سایبری، علاوه بر دیوارهای آتشین و دیگر تجهیزات جلوگیری از نفوذ، سیستم های دیگری نیز نیاز است تا بتوان درصورت عبور نفوذگر از دیواره آتشین، آنتی ویروس و سایر تجهیزات امنیّتی، آن ها را تشخیص داده و راه حلی برای مقابله با آن تعبیه نمود. به دلیل ماهیّت غیرالگوریتمی روش های نفوذ در شبکه های رایانه ای، راهکارهای مطرح شده برای مقابله با ناهنجاری ها نیز باید دارای ماهیت غیرالگوریتمی باشد. هوش مصنوعی به ویژه شبکه عصبی که جزء سیستم های یاد گیرنده تلقی می شود، توانسته در زمینه ی شناسایی و جلوگیری از این ناهنجاری ها تأثیر به سزایی داشته باشد (کاوه و بارانی، ۱۴۰۴، ۱۹۸).

سیستم های تشخیص تهدید مبتنی بر هوش مصنوعی می توانند خطرها و تهدید ها را دقیق تر، سریع تر و کارآمد تر مورد شناسایی قرار دهد. این سیستم های تشخیص تهدید از حجم عظیمی از داده ها یاد می گیرند و الگویی را پیدا می کنند که می توانند به خطرات احتمالی با استفاده از الگوریتم ها و تکنیک های یادگیری ماشین اشاره کنند. یادگیری عمیق، فرآیند یادگیری مغز انسان را با استفاده از شبکه های عصبی شبیه سازی می کند که به الگوریتم ها اجازه می دهد در طول زمان با شناسایی و یادگیری از نقاط داده جدید دقیق تر شوند. این سیستم ها می توانند به طور هم زمان داده ها را از چندین منبع تجزیه و تحلیل و آن ها را قادر سازد تهدیدات را در سیستم ها و شبکه های مختلف شناسایی و ردیابی کنند. بسته به نوع داده ها و الگوریتم های مورد استفاده، سیستم تشخیص تهدید مبتنی بر هوش مصنوعی می توانند خطرات مختلفی را شناسایی کنند. این فنّاوری برای مثال می توانند بدافزارها، کلاهبرداری فیشینگ و سایر خطرات آنلاین را تشخیص دهند (محمودی و بحرکاظمی، ۱۴۰۳، ۹۹).

۴-۲-۳. شناسایی بات نت ها

بات نت ها از مجموعه ای از رایانه ها و یا سیستم های آلوده تشکیل یافته اند که توسط یک بدافزار هدایت می شوند. افرادی که بدافزارها را ایجاد کرده اند، می توانند به جای این که به یک رایانه ی آلوده به صورت مستقیم متصل شوند، از بات نت ها برای مدیریت خودکار حجم زیادی از این رایانه های آلوده استفاده کنند که از طریق یک کانال فرمان و کنترل به یکدیگر وصل شده اند. یکی از مشکلات کشف بات نت ها شباهت زیاد ترافیک بات نت با ترافیک واقعی شبکه است؛ بنابراین به آسانی و با استفاده از روش های سنّتی نمی توان آن ها را شناسایی نمود. الگوریتم های یادگیری ماشین در دو نوع با ناظر و بدون ناظر یکی از ابزارهای هوش مصنوعی در شناسایی بات نت ها هستند. شناسایی بات نت ها نمونه ای از مسائل طبقه بندی است که با هدف تعیین کلاس یک بسته یا توالی بسته ها به ترافیک بات نت ها و یا ترافیک معمولی مورد بررسی قرار می گیرند. از طرف دیگر جهت گروه بندی ترافیک باتوجه به ویژگی های مشابه و شناسایی ترافیک های مشکوک می توان از مدل های یادگیری ماشین بدون ناظر استفاده کرد (کاوه و بارانی، ۱۴۰۴، ۱۹۸).

محقّقان سایبری از تکنیک‌های طبقه‌بندی مبتنی بر هوش مصنوعی استفاده کرده‌اند. که برای مدیریت موثر حجم زیادی از داده‌ها و پردازش سریع آنها بسیار مناسب هستند. با الهام از این رویکرد، هدف ارائه مدلی مبتنی بر تکنیک‌های پیشرفته هوش مصنوعی، به ویژه یادگیری عمیق، برای شناسایی بات نت ها به عنوان منبع قابل توجّه حملات سایبری است (دجانه ،۲۰۲۳، ۷).

۵-۲-۳. امنیّت ایمیل

کاربردهای هوش مصنوعی در امنیّت ایمیل از دو طریق شناسایی هرزنامه و شناسایی حملات فیشینگ انجام می شود. هرزنامه یا اسپم به پیام الکترونیکی اطلاق می شود که بدون درخواست گیرنده و برای افراد زیاد فرستاده می شود. هرزنامه به نوعی سوء استفاده از سامانه انتقال پیام است. جهت شناسایی هرزنامه، استراتژی های هوش مصنوعی متفاوتی وجود دارد که یکی از رایج ترین و ساده ترین آن ها شبکه های عصبی است. از قابلیت های دیگری همچون ماشین های بردار پشتیبان (به ویژه برای اسپم های تصویری)، شبکه های بیز و همچنین استفاده از فناوری های پردازش زبان طبیعی می توان در این زمینه بهره برد (کاوه و بارانی، ۱۴۰۴، .۱۹۹- ۱۹۸)

فیشینگ یکی از بزرگ ترین تهدیدات سایبری است که همه کسب و کارها با آن روبرو هستند. زمانی که هوش مصنوعی در کنار راهکارهای امنیّتی ایمیل قرار می گیرد، سازمان ها را قادر به شناسایی موارد مشکوک و پیام های غیر عادی می نماید. در این صورت است که می توان محتوای ایمیل را تجزیه و تحلیل نمود تا به سرعت تشخیص داد پیام مورد نظر، اسپم است یا خیر. به

عنوان مثال؛ هوش مصنوعی می تواند به سرعت و سادگی، نشانه های فیشینگ مانند جعل ایمیل ، فرستنده های جعلی و نام دامنه اشتباه تایپی را شناسایی کند. چالش اساسی در زمینه‌ی فیشینگ با ایمیل‌ها و پیام‌های اسپم این است که چنین پیام‌هایی شما را ترغیب می‌کنند تا روی لینک ارسال‌شده کلیک کنید؛ بنابراین اگر به هویت ارسال‌کننده یا جعلی‌بودن پیام مشکوک هستید، هرگز آن را باز نکنید.

۶-۲-۳. حفاظت از حساب ها و اطلاعات کاربران

یکی از نقاط ضعف در محافظت از حساب ها و اطلاعات کاربران، محافظت ضعیف از رمز عبور آن هاست. هرچند امروزه در راستای افزایش امنیّت اطلاعات و حساب های کاربران، راهکارهایی؛ ازجمله ارسال پیام و یا ایمیل به کاربر در حین اتّصال سیستم دیگری به حساب مربوطه مطرح شده است، با این حال، این فعّالیّت ها، واکنشی هستند که با شناسایی دسترسی های غیرمجاز، سیستم در قالب هشدار، واکنشی را نشان داده و باعث بسته و یا معلّق شدن حساب کاربر می گردد. این سیستم های هشدار واکنشی، معمولاً با مجموعه ای از محرک های پیش فرض و مرتبط با رویدادها فعّال می شوند که برای تمامی کاربران یکسان هستند. به عبارت دیگر، این سیستم ها در شناسایی رفتار کاربران تلاشی نکرده تا بتوانند براساس الگوی رفتاری هر فرد عمل نمایند. علاوه بر این، سیستم های واکنشی، آینده را مشابه با گذشته در نظر می گیرند و توانایی سازگاری سریع با تغییرات را ندارند. اتّخاذ یک رویکرد پیشگیرانه برای حفاظت حساب و اطلاعات کاربران می تواند مثمر ثمر واقع شود. در اینجاست که هوش مصنوعی با استفاده از روش های مختلف داده کاوی و یادگیری ماشین جهت بهره برداری از داده های ساختار یافته و یا غیر ساختاری استخراج شده از منابع ناهمگون سازمان به کار می آید، هوش مصنوعی با شروع تجزیه و تحلیل داده های گذشته قادر به نشان دادن الگوهای نهفته، برآورد رفتارهای آینده کاربران و شناسایی به موقع تلاش های احتمالی برای کلاهبرداری سایبری است (کاوه و بارانی، ۱۴۰۴، ۱۹۹).

۷-۲-۳. احراز هویّت و تشخیص فریب آن توسط هوش مصنوعی

احراز هویّت فرآیندی است که طی آن صحّت و درستی هویّت یک فرد شناسایی و تأیید می گردد. بنابراین زمانی که کاربر بخواهد وارد سیستم شده و یا به منبعی دسترسی پیدا کند، ابتدا باید خود را اثبات نماید. احراز هویّت به صورت روش های متفاوتی، ازقبیل سؤال های؛ امنیّتی رمزهای عبور توکن ها، دستگاه های فیزیکی و ویژگی های بیومتریک انجام می گیرد. در حال حاضر احراز هویّت از طریق ویژگی های بیومتریک بسیار مطرح شده است. منظور از ویژگی های بیومتریک در احراز هویت، ویژگی های فیزیکی منحصر به فرد مانند عنبیه ی چشم، چهره، اثر انگشت و صداست که از طریق آن می توان افراد را شناسایی و ردیابی نمود. هوش مصنوعی با استفاده از تکنولوژی های بینایی ماشین و تشخیص گفتار، تحوّل شگرفی در این زمینه ایجاد نموده است که می تواند با تلفیق با علم داده کاوی الگوهای رفتاری مانند نحوه تایپ مطالب و دست خط و یا الگوی امضاکردن را نیز شناسایی کند و از آن برای صحّه گذاری هویّت افراد بهره ببرد. با پیشرفت تکنولوژی علاوه بر ایجاد راهکارهایی جهت تأمین امنیّت بیشتر در فضای دیجیتال می توان ادعا نمود که به همان میزان حملات و کلاهبرداری های سایبری نیز پیچیده تر و پیشرفته تر شده است. جعل در تصاویر ازجمله جعل در صحبت کردن و عدم رعایت الگوی مورد نظر در صحبت می باشد. با ظهور فنّاوری دیپ فیک و مدل هایی مانند مدل های مولد تخاصمی می توان تصاویری از افراد ایجاد کرد که هرگز حضور فیزیکی نداشته اند و سیستم های مربوط به احراز هویّت را فریب داد. در این راستا، فرآیندی تحت عنوان صحّت سنجی یا تشخیص زنده بودن مطرح شده که عبارت است از مجموعه ای از عملیات که تصاویر ویدیویی را مورد پردازش قرار داده و تشخیص می دهد که ویدیوی دریافت شده از فرد جعلی نبوده و مورد دستکاری عامدانه قرار نگرفته است. این مورد یکی از

جالب ترین کاربردهای هوش مصنوعی در امنیّت سایبری است که به نوعی این فناوری را در مقابل خود قرار می دهد (کاوه و بارانی، ۱۴۰۴، ۲۰۰-۱۹۹).

در تشخیص عکس های جعلی و عکس های جایگزین، یک الگوریتم تشخیص می دهد که آیا چهره یک فرد در عکس با عکس شخص دیگری جایگزین شده است یا خیر. این ویژگی به ویژه برای احراز هویّت بیومتریک از راه دور در خدمات مالی مفید است. این از کلاهبرداران از ایجاد عکس ها یا فیلم های جعلی و معرفی خود به عنوان شهروندان قانونی که می توانند وام دریافت کنند، جلوگیری می کند. مهم ترین اقدامات پیشگیرانه برای جلوگیری از کلاهبرداری به روش جعل هویّت، استفاده از احراز هویّت چندعاملی است؛ روشی که در آن هرگونه فعالیت جدید در حساب شما به تلفن همراه تان ارسال می‌شود و ورودهای مشکوک یا تلاش برای تغییر رمز عبور را می‌توانید در ایمیل خود ببینید. به خاطر داشته باشید که هرگونه پیام هشداری را که در این زمینه برایتان ارسال می‌شود جدی بگیرید؛ به خصوص اگر تعداد این پیام ها بالا است و به‌طور مرتب برای شما ارسال می‌شود.

هوش مصنوعی سیستم ها را قادر می‌سازد تا وظایفی مانند شناسایی، تشخیص و تشخیص ناهنجاری را انجام دهند (ژانگ ،۲۰۲۵، ۳). برای مثال، در احراز هویّت بیومتریک، هوش مصنوعی از فنّاوری‌های یادگیری عمیق و دید رایانه ای برای احراز هویّت کاربران استفاده می‌کند، ابتدا با تشخیص و سپس مقایسه ویژگی‌های بیومتریک آنها (کودیتوواککو ،۲۰۱۵، ۱۱۳). در احراز هویت پیوسته، هوش مصنوعی از فناوری گراف برای مدل‌سازی روابط و پردازش زبان طبیعی برای تجزیه و تحلیل داده‌های متنی به منظور تشخیص الگوهای کلاهبرداری در داده های ساختار یافته (مانند سوابق تراکنش‌ها) و داده‌های بدون ساختار (مانند محتوای رسانه‌های اجتماعی) استفاده می‌کند که امکان احراز هویّت در زمان واقعی و تطبیقی را فراهم می‌کند (بیگ و اسکلند ،۲۰۲۱، ۵۹۶۷).

نتیجه گیری

با پیشرفت سریع فنّاوری و گسترش استفاده از هوش مصنوعی، این فنّاوری نه تنها در بهبود زندگی روزمره و ارتقای کارایی در صنایع مختلف مؤثر بوده است، بلکه ابزارهای قدرتمندی را در اختیار مجرمان سایبری قرار داده است تا حملاتی را با کارایی و پیچیدگی بیشتر انجام دهند. کلاهبرداری سایبری یکی از بزرگترین چالش های جرایم سایبری 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 هدفمند تر را فراهم می کند. الگوریتم های یادگیری ماشینی می توانند به تحلیل داده های بزرگ بپردازند و الگوهای رفتاری کاربران را شناسایی کنند. این تحلیل ها به مهاجمان اجازه می دهد تا حملات فیشینگ، جعل عمیق (دیپ فیک)، ارائه ی خدمات جیل بریک، شکستن رمز عبور توسط هوش مصنوعی را با دقّت بیشتری جهت وقوع کلاهبرداری سایبری، طرّاحی و اجرا کنند، که این امر منجر به افزایش موفقیّت آمیز بودن این حملات می شود. و از منظر دیگر نیز، هوش مصنوعی به عنوان یک فنّاوری نوظهور و با قابلیّت های منحصر به فرد خود، می تواند نقش مؤثری در پیش بینی، تشخیص و مقابله با کلاهبرداری سایبری ایفا کند. که این اقدامات را به صورت تدابیر پیشگیرانه ی اجتماعی از طریق آموزش و آگاهی بخشی به کاربران و مردم درباره ی تهدیدات علیه اطلاعات و داده ها و تدوین کدهای رفتاری یا کردارنامه ها از سوی دست اندرکاران حوزه ی سایبری است و نیز اتّخاذ تدابیر پیشگیرانه ی وضعی از طریق تدابیر امنیّت سایبری و شبکه به صورت تحلیل رفتار کاربران، تشخیص تهاجم، نفوذ یا تهدید، شناسایی بات نت ها، امنیّت ایمیل، حفاظت از حساب ها و اطلاعات کاربران، احراز هویّت و تشخیص فریب توسط هوش مصنوعی از وقوع کلاهبرداری سایبری پیشگیری نمود. هوش مصنوعی با توانایی های شگفت‌انگیز خود در تحلیل داده ها و یادگیری از تجربیات، به سرعت به یکی از ابزارهای کلیدی در زندگی مدرن تبدیل شده است. در پایان باید گفت که هوش مصنوعی می‌تواند به تشخیص و پیش‌گیری از حملات سایبری، تحلیل و پاسخگویی به تهدیدات و ارتقای مهارت‌های انسانی کمک کند. در مقابل هم ممکن است به عنوان ابزاری برای انجام حملات سایبری، ایجاد تقلّب و فریب و اختلال در سیستم‌های حساس و کلاهبرداری سایبری استفاده شود. پس برای بهره‌برداری از هوش مصنوعی برای امنیّت سایبری، لازم است که چالش‌هایی مانند کمبود داده‌های کافی و معتبر، نیاز به همکاری و مسائل اخلاقی و قانونی حل شوند. به عبارت دیگر، هوش مصنوعی می‌تواند هم به‌عنوان ابزار و هم به عنوان تهدید عمل کند؛ برای استفاده ی بهینه و امن از هوش مصنوعی برای امنیّت سایبری، لازم است که چالش‌های موجود را شناسایی و راه‌حل‌های مناسب ارائه شوند. در واقع هوش مصنوعی می‌تواند شریکی قدرتمند برای افزایش امنیّت سایبری باشد، البته به شرطی که با دقّت و مسئولیت‌پذیری از آن استفاده شود.

پیشنهادها

در نهایت با توجه به یافته های پژوهش، مواد ذیل را می توان به عنوان پیشنهادهای عملیّاتی و کاربردی ارائه نمود که عبارتند از:

۱. این فنّاوری نه تنها روش های جدیدی برای بهبود کیفیّت زندگی و افزایش بهره وری ارائه می کند، بلکه به ما امکان می دهد تا با پیچیدگی های دنیای دیجیتال به شیوه ای مؤثرتر و هوشمندانه تر برخورد کنیم. با این حال، همچنان نیازمند توجه و نظارت مستمر هستیم تا اطمینان حاصل کنیم که پیشرفت‌های هوش مصنوعی به شیوه ای مسئولانه و ایمن به کار گرفته شوند.

۲. تأثیر هوش مصنوعی در ارتکاب جرایم کلاهبرداری نشان می دهد که ضروری است تدابیر امنیّتی جدید و پیشرفته تری برای مقابله با این تهدیدات اتّخاذ شود.

۳. تأثیر این فناوری نوین در ارتکاب جرایم سایبری به خصوص کلاهبرداری سایبری، مستلزم تدوین و به روز رسانی قوانین متناسب جهت اقدامات پیشگیرانه از این جرایم توسط هوش مصنوعی در راستای سیاست جنایی تقنینی و فراتقنینی، بایستی مورد توجّه ویژه ای قرار گیرد.

۴. آموزش نیروی انسانی قضایی متخصّص (قضات) جهت شناخت و آگاهی بیشتر در راستای رسیدگی به پرونده های کلاهبرداری سایبری به وسیله ی هوش مصنوعی

۵. اهمیّت ویژه ی افزایش آگاهی های عمومی و آموزش کاربران در خصوص تهدیدات جدید (کلاهبرداری و...) به وسیله هوش مصنوعی و نحوه مقابله با آن ها

منابع

۱. ابراهیمی، شهرام. (۱۳۹۶). جرم شناسی پیشگیری، جلد اوّل، چاپ چهارم، تهران، نشر میزان

۲. اوجاقلو، صالح و زندی، محمدرضا. (۱۴۰۰). پیشگیری از کلاهبرداری سایبری در سیاست جنایی ایران با نگاهی به رویّه قضایی، فصلنامه علمی مطالعات پیشگیری از جرم، دوره شانزدهم، شماره ۵۸، صفحات ۲۶۱ -۲۴۳

۳. بابایی، جواد. (۱۴۰۱)، جرایم رایانه ای و آیین دادرسی حاکم بر آن، چاپ هفتم، تهران، نشر مرکز مطبوعات و انتشارت قوه قضاییه

۴. جلالی فراهانی، امیرحسین و منفرد، محبوبه. (۱۳۹۲). حمایت قانونی از آسیب دیدگان سایبری، فصلنامه مجلس و راهبرد، سال بیستم، شماره هفتاد و سه، صفحات ۱۹۹-۱۵۶

۵. خرّم آبادی، عبدالصمد. (۱۳۸۶). کلاهبرداری رایانه ای از دیدگاه بین المللی و وضعیّت ایران، فصل نامه حقوق مجله ی دانشکده حقوق و علوم سیاسی دانشگاه تهران، سال ۳۷، شماره ۲، صفحات ۱۱۲-۸۳

۶. ذبیح اله نژاد، وحید.(۱۳۹۷). کشف علمی جرایم سایبری و نقش پلیس فتا استان مازندران در حوزه پیش گیری و امنیت سایبری، فصلنامه علمی تخصصی دانش انتظامی مازندران، سال نهم، شماره دوم (پیاپی ۳۳)، صفحات ۱۷۰-۱۳۵

۷. ذوالقدر، محمدجواد. (۱۴۰۴). امکان سنجی اعطای شخصیت حقوقی به هوش مصنوعی، نوبت دوم، وزارت دادگستری، انتشارات دادگستری کل استان تهران

۸. رحیمی نژاد، اسمعیل. (۱۳۹۵). جرم شناسی، چاپ پنجم، تهران، انتشارات فروزش

۹. صوفی، سارا و صابر صالح نژاد بهرستاقی. (۱۴۰۲) تأثیر هوش مصنوعی در ارتکاب جرایم سایبری، مجله مطالعات حقوق، شماره ۵۱، دوره ۱۱، سال پنجم، صفحات ۱۸-۱

۱۰. عاملی، سعید رضا. (۱۳۹۰). رویکرد دو فضایی به آسیب ها، جرائم و قوانین و سیاست های فضای مجازی، چاپ اوّل، تهران، انتشارات امیرکبیر

۱۱. فرج پور، رضا، عامری نیا، محمد باقر و گرجی نیا، معصومه. (۱۴۰۳). الزامات اخلاقی در سیر تصویب قانون هوش مصنوعی اتحادیه اروپا، فصلنامه علمی مطالعات حقوقی فضای مجازی، دانشگاه آزاد اسلامی واحد مراغه، سال سوم، شماره چهارم، شماره پیاپی ۱۲، صفحات ۵۳-۳۷

۱۲. فلاح تفتی، فاطمه. (۱۴۰۳). هوش مصنوعی در خدمت پیشگیری از جرایم سایبری: رویکردی فقهی حقوقی، فصلنامه علمی مطالعات حقوقی فضای مجازی، دانشگاه آزاد اسلامی واحد مراغه، سال سوم، شماره چهارم، شماره پیاپی ۱۲، صفحات ۲۰-۱

۱۳. قاجارقیونلو، سیامک، (۱۳۹۱)، مقدّمه حقوق سایبر، جلد اول، تهران، نشر میزان

۱۴. کاوه، محمّدهادی و بارانی، محمّد. (۱۴۰۴). به کارگیری هوش مصنوعی برای مقابله با جرایم رایانه ای و بهبود عملکرد امنیت سایبری، فصلنامه فقه جزای تطبیقی، دوره پنجم، شماره اوّل، صفحات ۲۰۵-۱۹۳

۱۵. محمّدزاده، اکرم، بیگی، جمال و احدی، فاطمه. (۱۴۰۲). مکانیسم پیشگیری از کلاهبرداری رفاهی در فضای مجازی، دو فصلنامه علمی-تخصصی اقتصاد توسعه و برنامه ریزی، سال دهم، شماره دوّم، صفحات ۱۳۲-۱۰۷

۱۶. محمودی، امیررضا و بحر کاظمی، مریم. (۱۴۰۳). هوش مصنوعی و تأثیر آن بر امنیّت سایبری و حق بر حریم خصوصی، پژوهش های بنیادین در حقوق، شماره سوم، صفحات ۱۰۴-۸۶

۱۷. میرشکاری، عباس، ثابت قدم، فاطمه و اصغرنیا، مرتضی. (۱۴۰۳). درآمدی بر چالشهای فناوری هوش مصنوعی در حوزه حریم خصوصی، فصلنامه علمی مطالعات حقوقی فضای مجازی، دانشگاه آزاد اسلامی واحد مراغه، سال سوم، شماره چهارم، شماره پیاپی ۱۲، صفحات ۸۹-۷۰

۱۸. میرمحمد صادقی، حسین و شایگان، محمد رسول. (۱۳۸۹). بررسی تطبیقی کلاهبرداری سنتی و رایانه ای و مجازات های آن ها در نظام حقوقی ایران- دیدگاه های حقوقی، فصلنامه دانشگاه علوم قضایی و خدمات اداری، سال پانزدهم، ش ۵۱، صفحات ۱۶۲-۱۳۷

۱۹. منصور بیگ، ریبوار و شیری، امید.(۱۴۰۴). آثار هوش مصنوعی بر سیستم قضائی، چاپ اوّل، تهران، انتشارات کتاب آوا

20.F. Baig and S. Eskeland, "Security, Privacy, and Usability in Continuous Authentication: a survey," Sensors, vol. 21, no. 17, p. 5967, Sep. 2021, doi: 10.3390/s21175967
21.Btoush. Eyad, Zhou. Xujuan, Gururajan. Raj, Ching Chan.Ka & Alsodi. Omar (2025)." Achieving Excellence in Cyber Fraud Detection: A Hybrid ML+DL Ensemble Approach for Credit Cards". Appl. Sci. 2025, 15, 1081. https:// doi.org/10.3390/app15031081
22.Djenna, Amir. Barka, Ezedin. Benchikh, Achouak & Khadir, Karima." Unmasking Cybercrime with Artificial-Intelligence-Driven Cybersecurity Analytics". Sensors 2023, 23, 6302
23.Hafez, Ibrahim Y. Hafez ,Ahmed Y. Saleh, Ahmed. Abd El-Mageed, Amr A. Abd & Abohany , Amr A. " A systematic review of AI-enhanced techniques in credit card fraud detection". Hafez et al. Journal of Big Data (2025 (
24.Kuttiyappan Damodharan, Rajasekar V. "AI-Enhanced Fraud Detection: Novel Approaches and Performance Analysis". IACIDS 2023, November 23-25, Lavasa, India. DOI 10.4108/eai.23-11-2023.2343170
25.Kodituwakku S. R,"Biometric authentication: A review," International Journal of Trend in Research and Development, vol. 2, no.4, pp.113–123, 2015
26.Olowu, Olawale. Adeleye, Ademilola Olowofela. Omokanye ,Abraham Okandeji. Ajayi ,Akintayo Micheal. Adepoju ,Adebayo Olabode. Omole , Olayinka Mary & Chianumba , Ernest C. " AI-driven fraud detection in banking: A systematic review of data science approaches to enhancing cybersecurity" GSC Advanced Research and Reviews, 2024, 21(02),Pp 227–237
27.Zhang, Chuo Jun . Gill Asif Q, Liu Bo , Anwa Memoona. " AI-BASED IDENTITY FRAUD DETECTION: A SYSTEMATIC REVIEW". arXiv:2501.09239v1 [cs.AI] 16 Jan 2025
28.Zioviris , Georgios. Kolomvatsos, Kostas .Stamoulis, George. " An intelligent sequential fraud detection model based on deep learning".The Journal of Supercomputing (2024) 80: Pp 14824–14847
29.https://www.darianet.com/ai-in-cyber-security
30.https://www.khabaronline.ir/news/1921039 /
31.https://rc.majlis.ir/fa/law/show/820227
32.https://rc.majlis.ir/fa/law/show/1811432
33.https://hamrah.academy/blog/cyber-security-artificial-intelligence /
34.https://www.ressis.net/artificial-intelligence-in-cybersecurity /
35.https://fata.gov.ir/node/166144