فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال سوم | شماره چهارم | زمستان ۱۴۰۳ | شماره پیاپی ۱۲
وبگاه مجله: https://sanad.iau.ir/journal/cyberlaw
ISSN: 2821-126X

# Artificial Intelligence as a Predictor of Cybercrimes: Opportunities and Challenges

**Fatemeh fallah tafti**
Assistant Professor of Jurisprudence and Islamic Law, Allameh Tabatabaei University, Tehran, Iran (Corresponding Author) Email: f.fallah@atu.ac.ir

**DOI: 10.71488/cyberlaw.2025.1184064**

**Keywords:**
Artificial Intelligence, Cybercrime, Prediction, Shia Islamic jurisprudence Iranian Law, Privacy, Regulation

## Abstract

With the ever-increasing expansion of information technology and the complexity of cybercrimes, the need for smart tools to deal with these threats is felt more and more. Artificial intelligence, with the capabilities of analyzing large and complex data, has been proposed as a powerful tool in this field. This research examines the role of artificial intelligence in predicting and preventing cybercrimes, its challenges and regulatory solutions. The findings show that artificial intelligence can predict the occurrence of cybercrimes by analyzing behavioral patterns and historical data. However, challenges such as privacy, algorithmic bias, and prediction uncertainty limit its use. However, challenges such as privacy, algorithmic bias, and prediction uncertainty limit its use. To manage these challenges, it is necessary to develop appropriate legal and ethical frameworks. Imamiyyah jurisprudence with general principles such as harm and justice can lead the way in this field. Finally, artificial intelligence can play an effective role in the fight against cybercrime, but for its optimal use, challenges must be identified and appropriate regulatory solutions considered. Combining the principles of Imamiyyah jurisprudence and Iran's legal laws can help to formulate a comprehensive and efficient framework for the use of artificial intelligence in the prevention of cybercrimes.

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license: http://creativecommons.org/licenses/by/4.0/

فصلنامه علمی
مطالعات حقوقی فضای مجازی
صفحات مقاله ۱ الی ۲۰

# هوش مصنوعی در خدمت پیشگیری از جرایم سایبری: رویکردی فقهی–حقوقی

**فاطمه فلاح تفتی**

استاد گروه فقه و حقوق اسلامی،دانشگاه علامه طباطبایی، تهران، ایران.

پست الکترونیک: f.fallah@atu.ac.ir

تاریخ دریافت : ۲۷ شهریور ۱۴۰۳ تاریخ پذیرش: ۲۹ آذر ۱۴۰۳

## چکیده

**با گسترش روزافزون فناوری اطلاعات و پیچیدگی جرایم سایبری، نیاز به ابزارهای هوشمند برای مقابله با این تهدیدات بیش از پیش احساس می‌شود. هوش مصنوعی با قابلیت‌های تحلیل داده‌های حجیم و پیچیده، به عنوان یک ابزار قدرتمند در این حوزه مطرح شده است. این پژوهش به بررسی نقش هوش مصنوعی در پیش‌بینی و پیشگیری از جرایم سایبری، چالش‌های آن و راهکارهای تنظیم‌گری می‌پردازد.یافته‌ها نشان می‌دهد که هوش مصنوعی می‌تواند با تحلیل الگوهای رفتاری و داده‌های تاریخی، وقوع جرایم سایبری را پیش‌بینی کند. با این حال، چالش‌هایی همچون حریم خصوصی، تعصب الگوریتمی و عدم قطعیت در پیش‌بینی، استفاده از آن را محدود می‌کند. برای مدیریت این چالش‌ها، ضرورت دارد چارچوب‌های قانونی و اخلاقی مناسبی تدوین شود. فقه امامیه با اصول کلی همچون لاضرر و عدالت می‌تواند در این زمینه راهگشا باشد.در نهایت، هوش مصنوعی می‌تواند نقش مؤثری در مبارزه با جرایم سایبری ایفا کند، اما برای بهره‌برداری بهینه از آن، باید چالش‌ها شناسایی شده و راهکارهای تنظیم‌گری مناسب در نظر گرفته شود. تلفیق اصول فقه امامیه و قوانین حقوقی ایران می‌تواند به تدوین چارچوبی جامع و کارآمد برای استفاده از هوش مصنوعی در پیشگیری از جرایم سایبری کمک کند.**

**واژگان کلیدی:** هوش مصنوعی، جرایم سایبری، پیشگیری، فقه امامیه، حقوق ایران، حریم خصوصی، تنظیم‌گری

**مقدمه**

در عصر دیجیتال کنونی، فناوری اطلاعات و ارتباطات به طور بنیادی ساختارهای اجتماعی، اقتصادی و سیاسی را متحول کرده است. گسترش بی‌سابقه اینترنت، شبکه‌های اجتماعی و سایر پلتفرم‌های دیجیتال، ضمن فراهم آوردن فرصت‌های بی‌نظیر، چالش‌های جدیدی به ویژه در حوزه امنیت سایبری ایجاد کرده است. جرائم سایبری، از جمله حملات سایبری، کلاهبرداری‌های آنلاین و سرقت اطلاعات، به تهدیدی جدی برای افراد، سازمان‌ها و دولت‌ها تبدیل شده است. با توجه به رشد تصاعدی این جرائم و خسارات هنگفت ناشی از آن‌ها، ضرورت یافتن راهکارهای نوین برای مقابله با این تهدیدات بیش از پیش احساس می‌شود.

یکی از راهکارهای مؤثر در این زمینه، بهره‌گیری از هوش مصنوعی است. هوش مصنوعی با قابلیت‌های منحصر به فرد خود در تحلیل حجم عظیمی از داده‌ها، شناسایی الگوهای پیچیده و اتوماسیون فرآیندها، می‌تواند به طور مؤثری در پیش‌بینی، تشخیص و مقابله با تهدیدات سایبری به کار گرفته شود. سیستم‌های مبتنی بر هوش مصنوعی قادرند با تحلیل رفتار کاربران، ترافیک شبکه و سایر داده‌های مرتبط، حملات سایبری را در مراحل اولیه شناسایی کرده و از وقوع خسارات گسترده جلوگیری کنند.

با این حال، توسعه و استقرار سیستم‌های هوش مصنوعی در حوزه امنیت سایبری مستلزم توجه به ابعاد حقوقی، اخلاقی و اجتماعی آن است. حفظ حریم خصوصی کاربران، جلوگیری از سوءاستفاده از داده‌ها و تضمین شفافیت در تصمیم‌گیری‌های الگوریتمی از جمله چالش‌های مهم در این زمینه محسوب می‌شوند. در این راستا، تلفیق دانش فنی هوش مصنوعی با اصول فقهی و حقوقی می‌تواند به تدوین چارچوب‌های قانونی و اخلاقی مناسب برای استفاده از این فناوری در حوزه امنیت سایبری کمک شایانی نماید.

بررسی‌های پیشین در حوزه کاربرد هوش مصنوعی در پیشگیری از جرم عمدتاً بر جرایم سنتی و جنبه‌های فنی این فناوری متمرکز بوده است. به عنوان مثال، ابراهیمی (۱۴۰۱) به بررسی مقتضیات و محدودیت‌های استفاده از هوش مصنوعی در پیشگیری از تکرار جرم پرداخته و آورزمانی و صفایی نبات (۱۳۹۵) به نقش داده‌کاوی و هوش مصنوعی در پیشگیری از جرایم خشن اشاره کرده‌اند.

پژوهش حاضر با تمرکز بر جرایم سایبری و رویکردی میان‌رشته‌ای، به بررسی ابعاد حقوقی، فقهی و فنی این موضوع می‌پردازد. هدف اصلی این پژوهش، ارائه یک چارچوب جامع برای استفاده از هوش مصنوعی در پیشگیری از جرایم سایبری با تأکید بر حفظ حقوق شهروندی و رعایت اصول اخلاقی است.

سوالات پژوهش شامل موارد زیر است: چگونه می‌توان از قابلیت‌های هوش مصنوعی برای پیش‌بینی و تشخیص دقیق‌تر حملات سایبری استفاده کرد؟ چه چالش‌های حقوقی و اخلاقی در استفاده از هوش مصنوعی در حوزه امنیت سایبری وجود دارد و چگونه می‌توان آن‌ها را مدیریت کرد؟ چگونه می‌توان اصول فقه امامیه را با فناوری هوش مصنوعی در جهت ارتقای امنیت سایبری تلفیق کرد؟ و چه راهکارهای نظارتی و قانونی برای تضمین استفاده ایمن و مؤثر از هوش مصنوعی در این حوزه ضروری است؟

از اینرو در این مقاله، ابتدا به بررسی مفاهیم پایه و چالش‌های موجود در حوزه امنیت سایبری پرداخته می‌شود. سپس، قابلیت‌های هوش مصنوعی در پیش‌بینی و تشخیص حملات سایبری تحلیل می‌شود. در ادامه، چالش‌های حقوقی و اخلاقی مرتبط با استفاده از هوش مصنوعی در این حوزه بررسی شده و راهکارهای فقهی و حقوقی برای رفع این چالش‌ها ارائه می‌گردد. در نهایت، چارچوبی جامع برای تنظیم‌گری و نظارت بر استفاده از هوش مصنوعی در حوزه امنیت سایبری پیشنهاد می‌شود.

## ۱- مبانی نظری

### ۱-۲ بررسی مفهوم هوش مصنوعی

هوش مصنوعی (AI) به معنای ظهور هوشی است که توسط سیستم‌های ماشینی ایجاد می‌شود و در تقابل با هوش طبیعی موجودات زنده، از جمله انسان‌ها، قرار دارد. مفهوم "هوش" به توانایی استدلال و پردازش اطلاعات اشاره دارد و این که آیا AI می‌تواند به چنین توانایی‌هایی دست یابد، موضوعی است که در میان محققان بحث‌برانگیز است. برخی متون علمی این حوزه را به عنوان مطالعه بر روی "عوامل هوشمند" تعریف می‌کنند؛ سیستم‌هایی که می‌توانند محیط خود را تحلیل کرده و اقداماتی را انجام دهند که شانس موفقیت آن‌ها در دستیابی به اهداف را افزایش می‌دهد. (Kaplan & Haenlein, ۲۰۱۹, pp. ۱۵-۲۵) برخی منابع، AI را به عنوان تقلید از عملکردهای شناختی انسان، نظیر یادگیری و حل مسئله، توصیف می‌کنند، اما این تعریف به طور گسترده‌ای توسط پژوهشگران معتبر این حوزه مورد انتقاد قرار گرفته است. (Kaplan & Haenlein, ۲۰۱۹, pp. ۱۵-۲۵)طبق تعریف سند ملی هوش مصنوعی، این فناوری به توانایی ماشین‌ها برای انجام فعالیت‌های خودکار و نظام‌مند اشاره دارد که شامل یادگیری، درک، استنتاج، پیش‌بینی و تصمیم‌گیری است. هوش مصنوعی دارای ویژگی‌های داده‌محوری، شبکه‌ای، الگوریتمی و یکپارچه است و تأثیرات عمیقی بر روابط انسانی و محیط زیست، چه در عرصه فیزیکی و چه در فضای مجازی، دارد.(مصوبه شورای عالی انقلاب فرهنگی، ۱۴۰۳، ص ماده ۱)

### ۱،۱. تبیین جرم و جرم سایبری از منظر فقه و حقوق ایران

جرم، از ریشه عربی ج ر م، به معانی قطع کردن، چیدن میوه از درخت، حمل کردن، کسب کردن، ارتکاب گناه و وادار کردن به کاری ناپسند به کار رفته است.(ابن اثیر، ۱۳۶۷، ج ذیل ماده؛ ابن منظور، ۱۴۱۴، ج ذیل ماده؛ طریحی، ۱۳۷۵، ج ذیل ماده؛ فراهیدی، ۱۴۰۹، ج ۶، ص ۱۱۹) در اصطلاح فقهی، جرم عبارت است از هر نوع عملی که در شرع ممنوع، و دارای کیفر دنیوی، همچون حد، تعزیر، قصاص، دیه و کفاره و یا اخروی باشد.(فیض، ۱۳۸۵، صص ۷۰-۶۹) بنابراین، جرم در اصطلاح فقهی مرادف معصیت است؛ بنابراین، ترک واجبات یا ارتکاب محرمات شرعی، جرم محسوب می‌شود. در اصطلاح حقوقی نیز، جرم به فعل یا ترک عملی که بر اساس قانون، قابل کیفر و یا مستلزم اقدامات تأمینی و تربیتی باشد، تعریف شده است.(گرجی، ۱۳۶۹، ج ۱، ص ۵۸) بنابراین، تعریف حقوقی جرم با تعریف فقهی تا حدودی همپوشانی دارد، اما تفاوت‌هایی نیز وجود دارد. برخی افعال ممنوع شرعی، از منظر حقوقی جرم محسوب نمی‌شوند.

در حقوق جزای ایران، جرم دارای سه رکن است: ۱) عنصر قانونی (جرم باید در قانون تصریح شده باشد)، ۲) عنصر مادی (تحقق خارجی اقدام خلاف قانون)، ۳) عنصر روانی (قصد و انگیزه مرتکب). این سه رکن در تحقق جرم ضروری هستند (رحیمی نژاد، ۱۳۹۱، ج ۱، ص ۳۹؛ فیض، ۱۳۸۵، ج ۱، ص ۱۷۹-۱۷۳؛ نوربها، ۱۳۸۵، ج ۱، ص ۱۸۹-۱۸۴).

در مورد جرایم سایبری نیز، همین اصول و ارکان حاکم است. جرایم سایبری به جرایمی گفته می‌شود که در محیط غیرفیزیکی و با استفاده از فناوری اطلاعات ارتکاب می‌یابند.(ر.ک. بیابانی و هادیانفر، ۱۳۸۴، ص ۲۲۵؛ جلالی فراهانی، ۱۳۸۹، ص ۴۸) این جرایم می‌توانند هم در حوزه فقهی و هم در حوزه حقوقی مصداق داشته باشند. جرم سایبری در فقه اسلامی به طور خاص مورد بحث قرار نگرفته است، چرا که این پدیده در زمان‌های گذشته وجود نداشته است. با این حال، فقها معتقدند که هر عملی که در فضای مجازی انجام شود و به نوعی به نفس، مال، آبرو یا سایر حقوق افراد تجاوز کند، حرام و شرعاً جرم محسوب می‌شود.

برخی از مصادیق جرم سایبری از منظر فقه به شرح زیر است:

۱. هک کردن و نفوذ به سیستم‌های کامپیوتری: این عمل به عنوان نوعی تجاوز به حریم خصوصی افراد تلقی می‌شود و از نظر شرعی حرام است. نفوذ غیرمجاز به سیستم‌ها نه تنها نقض حقوق مالکیت دیجیتال است، بلکه می‌تواند عواقب اجتماعی و اقتصادی جدی نیز به همراه داشته باشد.

۲. سرقت اطلاعات: هرگونه برداشت یا استفاده غیرمجاز از داده‌ها و اطلاعات افراد، تحت عنوان سرقت اطلاعات، جرم محسوب می‌شود. این عمل به معنای نقض حقوق فردی و حریم خصوصی است و از نظر فقهی غیرقابل قبول است.
۳. کلاهبرداری اینترنتی: فریب افراد و برداشت اموال آن‌ها از طریق اینترنت، به عنوان کلاهبرداری اینترنتی شناخته می‌شود و این عمل شرعاً حرام است. کلاهبرداری‌های آنلاین، نه تنها به اعتماد عمومی آسیب می‌زنند، بلکه منجر به خسارات مالی و روحی به قربانیان می‌شوند.

٤. نشر محتوای غیرمجاز: انتشار مطالب و تصاویری که مغایر با اصول شرعی و اخلاق اسلامی باشد، حرام و جرم محسوب می‌شود. این نوع فعالیت‌ها می‌تواند به ترویج فساد و انحرافات اجتماعی منجر شود و از نظر فقهی قابل مجازات است.
۵. توهین و افترا: توهین و فحاشی به دیگران در فضای مجازی، همانند دنیای واقعی، حرام و شرعاً جرم است. این رفتارها به تضعیف حیثیت افراد و ایجاد تنش‌های اجتماعی منجر می‌شود و باید تحت پیگرد قانونی قرار گیرد.

قانون جرایم رایانه‌ای مصوب ۱۳۸۸ به تعریف و جرم‌انگاری این مصادیق پرداخته و برای هر یک مجازات‌های خاصی تعیین کرده است. این قانون به‌طور جامع به بررسی جرایم سایبری مانند هک کردن، سرقت اطلاعات، کلاهبرداری اینترنتی و نشر محتوای غیرمجاز می‌پردازد و تلاش دارد تا با ایجاد یک چارچوب حقوقی مناسب، به مقابله با این جرائم بپردازد.
علاوه بر مجازات‌های کیفری، قانون جرایم رایانه‌ای تدابیر پیشگیرانه‌ای نیز برای مقابله با جرایم سایبری در نظر گرفته است. از جمله این تدابیر می‌توان به ایجاد پلیس فتا، آموزش فرهنگ استفاده صحیح از فضای مجازی، و حمایت از شرکت‌های تولیدکننده نرم‌افزارهای امنیتی اشاره کرد. این اقدامات به منظور ارتقاء آگاهی عمومی و تقویت زیرساخت‌های امنیت سایبری طراحی شده‌اند تا از وقوع جرایم سایبری جلوگیری شود و امنیت فضای مجازی حفظ گردد.

نقش هوش مصنوعی در پیش‌بینی و پیشگیری از جرائم سایبری

در دنیای دیجیتالی امروز، جرایم سایبری به یکی از بزرگ‌ترین تهدیدات برای افراد، سازمان‌ها و دولت‌ها تبدیل شده است. با پیچیده‌تر شدن حملات سایبری و افزایش حجم داده‌ها، تشخیص و پیش‌بینی این تهدیدات به چالشی جدی تبدیل شده است. در همین راستا، هوش مصنوعی (AI) به‌عنوان یک فناوری نوظهور، نقش مهمی در مقابله با این تهدیدات ایفا می‌کند.

هوش مصنوعی با توانایی پردازش حجم عظیمی از داده‌ها، شناسایی الگوهای پیچیده و یادگیری مداوم، ابزاری قدرتمند برای تحلیل رفتارهای مشکوک در شبکه‌ها و پیش‌بینی حملات سایبری به شمار می‌رود. این فناوری به سیستم‌های امنیتی اجازه می‌دهد تا تهدیدات را در مراحل اولیه شناسایی کرده و از وقوع خسارات جدی جلوگیری کنند.

تحلیل رفتار کاربران با هوش مصنوعی

هوش مصنوعی با بهره‌گیری از الگوریتم‌های یادگیری ماشین، تحولی شگرف در حوزه امنیت سایبری ایجاد کرده است. یکی از کاربردهای کلیدی هوش مصنوعی، تحلیل رفتار کاربران است. با جمع‌آوری داده‌های متنوعی از قبیل فعالیت‌های کاربران در سیستم‌ها، شبکه‌ها و وب‌سایت‌ها، هوش مصنوعی الگوهای رفتاری نرمال را شناسایی می‌کند و هرگونه انحراف از این الگوها را به عنوان یک تهدید بالقوه در نظر می‌گیرد( Lopes, Mamede, Reis, & Santos, ۲۰۲٤, pp. ۷٦۱-۷۹٤).

این فرآیند شامل چندین مرحله است: ابتدا، داده‌های خام جمع‌آوری و پیش‌پردازش می‌شوند. سپس، ویژگی‌های کلیدی که نشان‌دهنده رفتارهای کاربران هستند، استخراج می‌شوند. در مرحله بعد، با استفاده از الگوریتم‌های مناسب، مدلی ساخته

می‌شود که قادر به تشخیص رفتارهای غیرعادی است. این مدل با داده‌های آموزشی تغذیه شده و به مرور زمان بهبود می‌یابد.

هوش مصنوعی قادر است انواع مختلفی از رفتارهای غیرعادی را شناسایی کند، از جمله تلاش‌های مکرر برای ورود به سیستم با رمز عبور اشتباه، دانلود فایل‌های با حجم بالا در مدت زمان کوتاه و دسترسی به منابع سیستم در خارج از ساعات کاری. این قابلیت، به سازمان‌ها کمک می‌کند تا حملات سایبری را به موقع شناسایی کرده و از خسارات احتمالی جلوگیری کنند. هوش مصنوعی با تحلیل رفتار کاربران، یک لایه دفاعی قدرتمند در برابر تهدیدات سایبری ایجاد می‌کند و به سازمان‌ها این امکان را می‌دهد تا به طور مؤثرتری از دارایی‌های دیجیتال خود محافظت کنند( Scarfone & ۲۰۲٤mitre, ; ۱-۳, pp. ۲۰۰۷Mell,).

استفاده از هوش مصنوعی در تحلیل رفتار کاربران دارای مزایای متعددی است. این فناوری قادر است تهدیدات را پیش از اینکه به سیستم آسیب جدی وارد کنند، شناسایی کند و همچنین با کاهش تعداد هشدارهای کاذب، تمرکز را بر روی تهدیدات واقعی قرار دهد. به علاوه، این ابزار به تحلیلگران امنیت کمک می‌کند تا زمان بیشتری را به تحلیل تهدیدات پیچیده اختصاص دهند و در نتیجه کارایی آن‌ها به‌طور چشمگیری افزایش یابد.( ۲۷-۳, pp. ۲۰۰۲Axelsson,)

### ۱,۲. تشخیص نفوذ با هوش مصنوعی

هوش مصنوعی با بهره‌گیری از الگوریتم‌های پیشرفته، به یک ابزار قدرتمند در تشخیص نفوذ در شبکه‌های کامپیوتری تبدیل شده است. این فناوری با تحلیل حجم عظیمی از داده‌های شبکه، الگوهای رفتاری نرمال را شناسایی کرده و هرگونه انحراف از این الگوها را به عنوان یک تهدید بالقوه در نظر می‌گیرد.

فرآیند تشخیص نفوذ با جمع‌آوری داده‌های مختلف از شبکه آغاز می‌شود. این داده‌ها شامل ترافیک شبکه، لاگ‌های سیستم و فعالیت‌های کاربران است. پس از پیش‌پردازش داده‌ها، ویژگی‌های کلیدی که نشان‌دهنده رفتارهای مشکوک هستند، استخراج می‌شوند. سپس، یک مدل یادگیری ماشین با استفاده از این ویژگی‌ها آموزش داده می‌شود تا بتواند بین رفتارهای نرمال و غیرعادی تمایز قائل شود.

هوش مصنوعی قادر است انواع مختلفی از حملات سایبری را تشخیص دهد، از جمله حملات DDoS ، اسکن پورت، تزریق SQL و نفوذ به سیستم. با استفاده از هوش مصنوعی، سازمان‌ها می‌توانند به سرعت به تهدیدات پاسخ دهند و از بروز خسارات جدی جلوگیری کنند(محمودی و بحرکاظمی، ۱٤۰۳، صص ۹۹-۱۰۰).

هوش مصنوعی با تحلیل الگوهای شناخته شده حملات (روش مبتنی بر امضا) و تشخیص انحراف از رفتار نرمال (روش مبتنی بر ناهنجاری)، یا ترکیبی از هر دو، به شناسایی سریع‌تر و دقیق‌تر حملات سایبری کمک می‌کند. این فناوری با کاهش هشدارهای کاذب و توانایی تشخیص حملات پیچیده، امنیت سیستم‌ها را به‌طور قابل توجهی افزایش می‌دهد. همچنین، قابلیت یادگیری و سازگاری هوش مصنوعی با تهدیدات جدید، آن را به ابزاری قدرتمند در مقابله با حملات سایبری تبدیل کرده است(ر.ک. دولت آبادی و دولت آبادی، ۱٤۰۰؛ دیدبان، ۱٤۰۳؛ ونگ، بی‌تا).

### ۱,۳. پیش‌بینی حملات سایبری با هوش مصنوعی

پیش‌بینی حملات سایبری، همانند پیش‌بینی آینده، چالش‌برانگیز اما ضروری است. هوش مصنوعی با توانایی پردازش حجم عظیمی از داده‌ها و شناسایی الگوهای پیچیده، به ابزاری قدرتمند در این زمینه تبدیل شده است.

فرآیند پیش‌بینی با جمع‌آوری داده‌های مختلف از جمله ترافیک شبکه، لاگ‌های سیستم و اطلاعات آسیب‌پذیری‌ها آغاز می‌شود. پس از آماده‌سازی داده‌ها، ویژگی‌های کلیدی حملات استخراج شده و یک مدل یادگیری ماشین ایجاد می‌شود. این مدل با استفاده از الگوریتم‌های پیشرفته، مانند شبکه‌های عصبی، داده‌ها را تحلیل کرده و الگوهای رفتاری را شناسایی می‌کند.

با استفاده از این مدل، می‌توان حملات را به دو روش اصلی پیش‌بینی کرد: اول، با شناسایی الگوهای شناخته‌شده حملات (روش مبتنی بر امضا) و دوم، با تشخیص هرگونه انحراف از رفتار نرمال (روش مبتنی بر ناهنجاری). علاوه بر این، رویکردی جامع‌تر به نام تحلیل ریشه نیز وجود دارد که به بررسی علل اصلی حملات می‌پردازد.

با کمک هوش مصنوعی، می‌توان حملات را زودتر شناسایی کرده و از خسارات ناشی از آن‌ها جلوگیری کرد. همچنین، می‌توان به طور مداوم مدل‌ها را بهبود بخشید و آن‌ها را با تهدیدات جدید سازگار کرد. در نتیجه، هوش مصنوعی نقش مهمی در ارتقای امنیت سایبری و حفاظت از زیرساخت‌های حیاتی ایفا می‌کند(ر.ک. عبدی پور و مصاحب طلب، ۱۴۰۳).

مزایای پیش‌بینی حملات با هوش مصنوعی شامل کاهش زمان پاسخگویی، افزایش دقت تشخیص، کاهش هزینه‌ها و اتوماسیون فرآیندهای امنیتی است. با پیش‌بینی حملات، اقدامات لازم قبل از وقوع آن‌ها انجام می‌شود و از خسارات جلوگیری می‌کند. هوش مصنوعی قادر است با دقت بالایی حملات سایبری را شناسایی کند و شناسایی زودهنگام حملات به کاهش هزینه‌های مربوط به مقابله با آن‌ها کمک می‌کند. بسیاری از فرآیندهای امنیتی را می‌توان با استفاده از هوش مصنوعی خودکار کرد که به بهبود کارایی و سرعت در واکنش به تهدیدات کمک می‌کند. در نهایت، ادغام هوش مصنوعی در فرآیند پیش‌بینی حملات سایبری می‌تواند به تقویت امنیت دیجیتال و کاهش ریسک‌های مرتبط با حملات سایبری کمک شایانی نماید.( Buczak & Guven, ۲۰۱۶, pp. ۱۱۷۶-۱۱۵۳; Mitnick & Simon, ۲۰۱۱)

### ۱,٤. تحلیل داده‌های بزرگ در پیش‌بینی جرائم سایبری

در دنیای دیجیتال امروزی، جرایم سایبری به تهدیدی جدی برای افراد، سازمان‌ها و دولت‌ها تبدیل شده است. پیچیدگی روزافزون این حملات و حجم عظیم داده‌های تولید شده، نیازمند رویکردهای نوینی برای شناسایی و پیش‌بینی آن‌ها است. تحلیل داده‌های بزرگ با استفاده از هوش مصنوعی، به‌عنوان یک ابزار قدرتمند، به کمک ما آمده است.

با جمع‌آوری داده‌های متنوعی از منابع مختلف مانند شبکه‌ها، سیستم‌ها و کاربران، می‌توانیم الگوهای پنهانی را شناسایی کنیم که ممکن است نشان‌دهنده یک حمله سایبری باشد. این داده‌ها پس از پیش‌پردازش و استخراج ویژگی‌های کلیدی، به مدل‌های یادگیری ماشین تغذیه می‌شوند. این مدل‌ها با یادگیری از داده‌های گذشته، قادر به تشخیص رفتارهای غیرعادی و پیش‌بینی حملات آینده هستند( Bochie, Gonzalez, Giserman, Campista, & Costa, ۲۰۲۰).

مزایای استفاده از هوش مصنوعی در تحلیل داده‌های بزرگ برای پیش‌بینی جرایم سایبری بسیار زیاد است. از جمله این مزایا می‌توان به موارد زیر اشاره کرد:

- شناسایی سریع‌تر و دقیق‌تر حملات: هوش مصنوعی می‌تواند با سرعت و دقت بسیار بالایی، حجم عظیمی از داده‌ها را تحلیل کرده و حملات را در مراحل اولیه شناسایی کند.
- کاهش هشدارهای کاذب: با استفاده از الگوریتم‌های پیشرفته، می‌توان تعداد هشدارهای کاذب را کاهش داده و تمرکز را بر روی تهدیدات واقعی قرار داد.

- تشخیص حملات پیچیده: هوش مصنوعی قادر است حملات پیچیده و هدفمند را که به روش‌های سنتی قابل شناسایی نیستند، تشخیص دهد.
- سازگاری با تهدیدات جدید: مدل‌های یادگیری ماشین می‌توانند به‌طور مداوم خود را با تهدیدات جدید سازگار کنند و به این ترتیب، همواره یک قدم جلوتر از مهاجمان باشند.

با توجه به مزایای ذکر شده، می‌توان گفت که تحلیل داده‌های بزرگ با هوش مصنوعی، یک راهکار بسیار موثر برای مقابله با جرایم سایبری است. با استفاده از این فناوری، می‌توانیم امنیت سیستم‌های اطلاعاتی خود را به طور قابل توجهی افزایش داده و از داده‌های ارزشمند خود محافظت کنیم(نوروزی و بیرانوند، ۱۴۰۲، صص ٤٤-٥٥).

کاربردهای تحلیل داده‌های بزرگ در پیش‌بینی جرائم سایبری شامل تشخیص نفوذ، که به شناسایی تلاش‌های غیرمجاز برای دسترسی به سیستم‌ها و شبکه‌ها می‌پردازد، کشف بدافزار، که انواع مختلف بدافزارها را شناسایی و طبقه‌بندی می‌کند، پیش‌بینی حملات هدفمند به سازمان‌ها و افراد، تحلیل رفتار کاربران برای شناسایی رفتارهای غیرعادی که ممکن است نشانه‌ای از یک حمله باشد، و همچنین کشف آسیب‌پذیری‌های سیستم‌ها و نرم‌افزارها می‌باشد. در مجموع، تحلیل داده‌های بزرگ به‌عنوان ابزاری کارآمد در پیش‌بینی و مقابله با جرائم سایبری، نقش حیاتی در تأمین امنیت سایبری ایفا می‌کند. (Sicari, Rizzardi, Grieco, & Coen-Porisini, ۲۰۱۵, pp. ۱۴۶-۱۶۴).

## ۲- چالش‌ها و محدودیت‌های استفاده از هوش مصنوعی در پیشگیری از جرائم سایبری

با وجود تمام مزایای استفاده از هوش مصنوعی در پیشگیری از جرائم سایبری، این فناوری با چالش‌ها و محدودیت‌هایی نیز همراه است. در ادامه به برخی از مهم‌ترین این چالش‌ها می‌پردازیم:

۱. کیفیت داده‌ها

دقت و کارایی مدل‌های هوش مصنوعی در تشخیص تهدیدات سایبری به شدت به کیفیت و کمیت داده‌های آموزشی وابسته است. داده‌های ناکافی، نادرست یا نامتعادل می‌توانند به نتایج نادرست و تشخیص‌های اشتباه منجر شوند. برای دستیابی به بهترین عملکرد، مدل‌ها باید با مجموعه‌ای متنوع از داده‌ها، شامل نمونه‌های سالم و آلوده، آموزش ببینند. همچنین، به‌روزرسانی مداوم داده‌های آموزشی برای مقابله با تهدیدات جدید و در حال تکامل ضروری است.

۲. پیچیدگی حملات سایبری

حملات سایبری امروزی، پیچیدگی و تنوع بالایی پیدا کرده‌اند. این حملات اغلب هدفمند و طراحی شده برای بهره‌برداری از نقاط ضعف خاص سیستم‌ها هستند. یکی از مهم‌ترین چالش‌ها در این زمینه، حملات روز صفر است که از آسیب‌پذیری‌های ناشناخته نرم‌افزارها سوءاستفاده می‌کنند. این نوع حملات به دلیل ناشناخته بودن، تشخیص و مقابله با آن‌ها بسیار دشوار است.

علاوه بر این، مهاجمان سایبری به طور مداوم تاکتیک‌ها و روش‌های خود را تغییر می‌دهند تا از شناسایی توسط سیستم‌های امنیتی جلوگیری کنند. این تحولات مداوم، باعث می‌شود که مقابله با تهدیدات سایبری به یک بازی موش و گربه تبدیل شود.

برای مقابله با این چالش‌ها، سازمان‌ها باید رویکردهای پیشگیرانه و تحلیلی را در پیش بگیرند. این رویکردها شامل به‌روزرسانی مداوم سیستم‌ها، آموزش کارکنان، استفاده از ابزارهای تشخیص نفوذ و تحلیل رفتار کاربران است. همچنین، همکاری با سایر سازمان‌ها و اشتراک‌گذاری اطلاعات تهدیدات، می‌تواند در مقابله با حملات سایبری موثر باشد.

۳. هزینه‌ها

پیاده‌سازی سیستم‌های هوش مصنوعی نیازمند سرمایه‌گذاری قابل توجهی است. این هزینه‌ها از چند بخش اصلی تشکیل می‌شود:

- زیرساخت‌های سخت‌افزاری: این سیستم‌ها به سخت‌افزارهای قدرتمندی مانند پردازنده‌های گرافیکی(GPU) ، حافظه‌های با ظرفیت بالا و سیستم‌های ذخیره‌سازی پیشرفته نیاز دارند تا بتوانند حجم عظیمی از داده‌ها را پردازش کنند و مدل‌های پیچیده را آموزش دهند.
- نرم‌افزارهای تخصصی: علاوه بر سخت‌افزار، نرم‌افزارهای تخصصی نیز برای توسعه، آموزش و استقرار مدل‌های هوش مصنوعی مورد نیاز است. این نرم‌افزارها معمولاً هزینه‌های مجوز و پشتیبانی بالایی دارند.
- نیروی انسانی: برای توسعه، آموزش و نگهداری سیستم‌های هوش مصنوعی به متخصصان ماهری در زمینه‌های هوش مصنوعی، یادگیری ماشین و داده‌کاوی نیاز است. هزینه‌های استخدام و آموزش این متخصصان می‌تواند بخش قابل توجهی از هزینه‌های کل را تشکیل دهد (ر.ک. محمدحسینی، قافله باشی، و هادی زاده، ۱۳۹۹).

در مجموع، پیاده‌سازی سیستم‌های هوش مصنوعی نیازمند سرمایه‌گذاری اولیه قابل توجهی است. با این حال، مزایای این سیستم‌ها در بلندمدت می‌تواند به طور قابل توجهی بیشتر از هزینه‌های اولیه باشد

٤. حریم خصوصی

استفاده از هوش مصنوعی در حوزه امنیت سایبری، به رغم مزایای فراوان، چالش‌های جدی در زمینه حریم خصوصی ایجاد می‌کند. جمع‌آوری حجم عظیمی از داده‌ها، از جمله داده‌های شخصی کاربران، برای آموزش و بهبود عملکرد مدل‌های هوش مصنوعی ضروری است. این امر نگرانی‌هایی را درباره حریم خصوصی افراد به وجود می‌آورد. کاربران ممکن است نگران باشند که اطلاعات شخصی آن‌ها بدون اجازه جمع‌آوری و مورد سوءاستفاده قرار گیرد.

از سوی دیگر، سوءاستفاده از داده‌های جمع‌آوری شده نیز یک تهدید جدی است. در صورت عدم وجود تدابیر امنیتی مناسب، این داده‌ها ممکن است به دست افراد سودجو افتاده و برای اهداف غیرقانونی مانند سرقت هویت یا کلاهبرداری مورد استفاده قرار گیرند. این امر می‌تواند عواقب جدی برای افراد و سازمان‌ها داشته باشد(محمودی و بحرکاظمی، ۱٤۰۳، صص ۹۳-۹٤).

برای رفع این چالش‌ها، سازمان‌ها باید به طور جدی به موضوع حریم خصوصی توجه کرده و اقدامات لازم را برای محافظت از داده‌های کاربران انجام دهند. این اقدامات شامل شفافیت در مورد نحوه جمع‌آوری و استفاده از داده‌ها، اخذ رضایت صریح کاربران، استفاده از روش‌های رمزنگاری قوی برای محافظت از داده‌ها و رعایت قوانین و مقررات مربوط به حریم خصوصی است

۵. مسائل مرتبط با نیروی انسانی

استفاده از اتوماسیون در امنیت سایبری، به عنوان یک ابزار قدرتمند برای تشخیص و مقابله با تهدیدات سایبری، به طور فزاینده‌ای مورد توجه قرار گرفته است. با این حال، اتوماسیون بی‌حد و حصر، چالش‌های قابل توجهی را نیز به همراه دارد که نیازمند بررسی دقیق و مدیریت هوشمندانه است.

یکی از مهم‌ترین چالش‌ها، کاهش توانایی نیروی انسانی در تشخیص تهدیدات جدید و پیچیده است. وابستگی بیش از حد به سیستم‌های خودکار، ممکن است منجر به تحلیل رفتن مهارت‌های تحلیلگران امنیت سایبری شود. همچنین، اتوماسیون

می‌تواند به کاهش فرصت‌های شغلی در این حوزه منجر شود و به این ترتیب، نیروی کار متخصص را با چالش‌های جدی مواجه کند.از سوی دیگر، اعتماد بیش از حد به سیستم‌های هوش مصنوعی، خطرات قابل توجهی را به همراه دارد. خطاهای انسانی در طراحی، پیاده‌سازی و نگهداری این سیستم‌ها می‌تواند منجر به نتایج نادرست و تصمیم‌گیری‌های اشتباه شود. علاوه بر این، الگوریتم‌های هوش مصنوعی ممکن است حاوی تعصباتی باشند که منجر به تبعیض و بی‌عدالتی شوند. (ر.ک. کشاورز و حسینی، ۱۴۰۲).

در صورت وقوع یک حمله سایبری، تعیین مسئولیت بین سیستم‌های هوش مصنوعی و انسان‌ها نیز می‌تواند چالش‌های قانونی و اخلاقی جدی ایجاد کند. این مسئله، به ویژه در مواردی که سیستم‌های خودکار تصمیم‌گیری‌های حیاتی انجام می‌دهند، اهمیت بیشتری پیدا می‌کند.برای رفع این چالش‌ها، سازمان‌ها باید به یک تعادل مناسب بین اتوماسیون و دخالت انسان دست یابند. به عبارت دیگر، اتوماسیون باید به عنوان مکمل و تقویت‌کننده توانایی‌های انسان مورد استفاده قرار گیرد. همچنین، سازمان‌ها باید به آموزش مداوم نیروی انسانی خود اهمیت دهند تا آن‌ها بتوانند با تغییرات فناوری و ظهور تهدیدات جدید، همگام شوند. باید توجه داشت که هوش مصنوعی یک ابزار است و به تنهایی نمی‌تواند تمام مشکلات امنیت سایبری را حل کند. برای ایجاد یک فضای سایبری امن، نیاز به یک رویکرد جامع داریم که در آن، فناوری، انسان و فرآیندهای مدیریتی به صورت یکپارچه با هم عمل کنند.

## ۳- راهکارهای تنظیم‌گری هوش مصنوعی برای جرائم سایبری از منظر فقه امامیه و حقوق ایران

با پیشرفت روزافزون فناوری هوش مصنوعی و کاربرد گسترده آن در حوزه‌های مختلف، از جمله امنیت سایبری، نیاز به تنظیم‌گری و نظارت بر این فناوری بیش از پیش احساس می‌شود. از یک سو، هوش مصنوعی می‌تواند نقش موثری در پیشگیری و کشف جرایم سایبری ایفا کند و از سوی دیگر، سوءاستفاده از این فناوری می‌تواند تهدیدات جدی برای امنیت اطلاعات و حریم خصوصی افراد ایجاد کند. در این بخش مقاله، به بررسی راهکارهای تنظیم‌گری و نظارت بر استفاده از هوش مصنوعی در حوزه امنیت سایبری از منظر فقه امامیه و حقوق ایران پرداخته می‌شود.

### ۳,۱. تحلیل دیدگاه‌های فقهی امامیه در خصوص کاربرد هوش مصنوعی برای پیشگیری از جرائم

با توجه به ماهیت نوظهور هوش مصنوعی، به طور مستقیم به این فناوری در فقه امامیه اشاره‌ای نشده است. با این حال، می‌توان با استناد به اصول و قواعد کلی فقه به بررسی جایگاه استفاده از هوش مصنوعی در پیشگیری از جرایم پرداخت.

#### ۳,۱,۱. قاعده لاضرر

قاعده لاضرر، که در آیات و روایات اسلامی به‌ویژه در آیه ۹۳ سوره نساء و روایت مشهور «لاضرر و لاضرار فی الاسلام»(کلینی، ۱٤۲۹، ج ۵، ص ۲۹٤) به‌روشنی تأکید شده، یکی از اصول بنیادین حقوقی و اخلاقی در اسلام است که به جلوگیری از اضرار به دیگران و حفظ حقوق اجتماعی کمک می‌کند. این قاعده به‌ویژه در زمینه پیشگیری از جرایم سایبری، که به صورت مستقیم یا غیرمستقیم به افراد، سازمان‌ها و جوامع آسیب می‌زند، اهمیت ویژه‌ای پیدا می‌کند. اضرار به غیر در متون دینی به شدت نهی شده و خداوند متعال از بندگانش می‌خواهد که به هیچ ضرری، چه از جانب خود و چه از جانب دیگران، راضی نباشند.

محققان در تحلیل قاعده لاضرر، سه معنا را برای آن مطرح می‌کنند: نخست، نفی ضرر به‌عنوان تحریم؛ دوم، نفی به‌عنوان عدم مشروعیت ضرر در دین اسلام؛ و سوم، نفی ماهیت ضرر به‌طور کلی. (نراقی، ۱٤۱۷، ص ۵۰) در این راستا، ضرر در این قاعده به‌طور خاص به ضرر شخصی اشاره دارد، به این معنا که حکمی ممکن است برای یک شخص ضررآور و برای

دیگری غیرضررآور باشد. .(رضایی اصفهانی، محمدعلی، ۱۳۹۲، ج ۱، ص ۱۱۰) این ضرر باید واقعی باشد، زیرا احکام برای موضوعات واقعی وضع شده‌اند و مقید به علم و جهل نیستند. (عبداللهی، بی‌تا، ۲۶۳-۲۶۲) بنابراین، حکمی که موجب ضرر برای مکلف باشد، اعم از اینکه مکلف عالم به آن ضرر باشد یا جاهل، باید مورد توجه قرار گیرد. (ایروانی، بی‌تا، ج ۱، ص ۱۶۹).

در زمینه جرایم سایبری، قاعده لاضرر می‌تواند به‌عنوان یک ابزار فقهی برای ارزیابی و تحلیل اثرات استفاده از هوش مصنوعی در پیشگیری از این جرایم عمل کند. جرایم سایبری می‌توانند شامل سرقت اطلاعات، تخریب داده‌ها، اخلال در خدمات و تهدید به جان افراد باشند. به همین دلیل، پیشگیری از این جرایم نه‌تنها به معنای جلوگیری از ضرر به افراد بلکه به معنای حفظ امنیت اجتماعی و حقوق عمومی نیز هست.

هوش مصنوعی با توانایی تحلیل حجم عظیمی از داده‌ها و شناسایی الگوهای پیچیده، نقش مهمی در پیشگیری از جرایم سایبری ایفا می‌کند. این فناوری می‌تواند به تشخیص حملات سایبری، شناسایی آسیب‌پذیری‌ها و پیش‌بینی تهدیدات کمک کند. با این حال، در استفاده از هوش مصنوعی برای پیشگیری از جرایم سایبری، ضروری است که به اصل لاضرر توجه شود. این به معنای آن است که باید اطمینان حاصل کرد که استفاده از این فناوری به حقوق افراد آسیب نرساند و منجر به نقض حریم خصوصی یا تبعیض نشود.

به‌طور خاص، طراحان و توسعه‌دهندگان سیستم‌های هوش مصنوعی باید به نکات زیر توجه کنند: اول، کاربردهای هوش مصنوعی باید به گونه‌ای طراحی شوند که به حریم خصوصی افراد و حقوق مالکیت معنوی آسیب نرسانند. دوم، الگوریتم‌های هوش مصنوعی نباید به گونه‌ای طراحی شوند که علیه گروه‌های خاصی تبعیض قائل شوند. سوم، سازندگان و کاربران این الگوریتم‌ها باید پاسخگوی تصمیمات و اقدامات خود باشند.

در نهایت، قاعده لاضرر به‌عنوان یک چارچوب اخلاقی و فقهی می‌تواند به توسعه و استفاده از هوش مصنوعی در پیشگیری از جرایم سایبری کمک کند. با رعایت این قاعده، می‌توان اطمینان حاصل کرد که استفاده از هوش مصنوعی نه‌تنها به حداقل ممکن به افراد و جامعه آسیب می‌زند، بلکه به تأمین منافع عمومی و ارتقای عدالت اجتماعی نیز کمک می‌کند. این رویکرد نه‌تنها به پیشگیری از جرایم سایبری کمک می‌کند، بلکه به تقویت اعتماد عمومی به فناوری‌های نوین نیز منجر خواهد شد.

### ۳,۲. قاعده عدالت

قاعده عدالت به‌عنوان یک اصل بنیادین در متون دینی (مائده: ۸؛ نساء: ۵۸؛ نحل: ۹۰؛ ص: ۲۶؛ حدید: ۲۵؛ شوری: ۱۵) و فقه اسلامی، نقش مهمی در شکل‌دهی به رویکردهای اخلاقی و قانونی در زمینه‌های مختلف اجتماعی، سیاسی و اقتصادی دارد. در عصر حاضر، با ظهور فناوری‌های نوین، به‌ویژه هوش مصنوعی، این قاعده می‌تواند به‌عنوان چارچوبی برای پیشگیری از جرایم سایبری عمل کند. مفهوم عدالت در این قاعده نه‌تنها به مصادیق خاص محدود نمی‌شود، بلکه در هر زمان و مکانی با توجه به شرایط و مقتضیات مختلف، تفسیر و تطبیق می‌شود. (صادق زاده طباطبایی، ۱۳۹۳، ص ۱۵۷)

استفاده از هوش مصنوعی در پیشگیری از جرایم سایبری باید به‌گونه‌ای باشد که به عدالت اجتماعی کمک کند. به این معنا که فناوری‌های نوین نباید به تبعیض، نقض حقوق بشر یا نابرابری در دسترسی به خدمات منجر شوند. در این راستا، هوش

مصنوعی می‌تواند به شناسایی الگوهای جرایم و پیش‌بینی وقوع آن‌ها از طریق تحلیل داده‌های کلان کمک کند، اما باید توجه داشت که این تحلیل‌ها باید با رعایت اصول عدالت و احترام به حریم خصوصی افراد انجام شود.

قاعده عدالت به فقیه و مجتهد اجازه می‌دهد تا با توجه به تحولات اجتماعی و فناوری‌های نوین، احکام را به‌گونه‌ای استنباط کند که نه‌تنها با موازین شرعی هم‌خوانی داشته باشد، بلکه به تحقق عدالت در جامعه نیز کمک کند. بنابراین، در استفاده از الگوریتم‌های هوش مصنوعی، باید تعادلی بین منافع مختلف برقرار شود؛ به‌عنوان مثال، افزایش امنیت سایبری نباید به قیمت کاهش حریم خصوصی افراد تمام شود.

علاوه بر این، الگوریتم‌های هوش مصنوعی باید شفاف و قابل فهم باشند تا بتوان به درستی عملکرد آن‌ها را ارزیابی کرد و از سوءاستفاده‌های احتمالی جلوگیری نمود. سازندگان و کاربران این الگوریتم‌ها باید پاسخگوی تصمیمات و اقدامات خود باشند تا اطمینان حاصل شود که استفاده از این فناوری‌ها به تحقق عدالت اجتماعی کمک می‌کند و نه به تضعیف آن.

در نهایت، قاعده عدالت به‌عنوان معیاری برای سنجش صحت و درستی احکام فقهی، می‌تواند به‌عنوان خط قرمزی در فرآیند استنباط فقهی تلقی شود. (ر.ک محامد ۱۳۸۵، ۲۳۹؛ صادق زاده طباطبایی ۱۳۹۳، ۱۵۷)تمامی برداشت‌های فقهی و کاربردهای هوش مصنوعی در پیشگیری از جرایم سایبری باید با این قاعده سنجیده شوند. با رعایت این قاعده، می‌توان از سوءاستفاده از فناوری‌های نوین جلوگیری کرده و به ایجاد یک فضای سایبری امن‌تر و عادلانه‌تر کمک کرد.

### ۳،۳. قاعده‌ی دفع ضرر محتمل

قاعده‌ی دفع ضرر محتمل به‌عنوان یک اصل عقلانی و اخلاقی در فقه اسلامی، بر لزوم جلوگیری از ضررهای احتمالی تأکید دارد. طبق این قاعده، عقل حکم می‌کند که هرگونه ضرر محتمل باید دفع شود و این حکم مستقل از شرع نیز معتبر است. (طباطبایی، بی‌تا، ج ۱۳، ص ۵۷۷) در این راستا، مقصود از این قاعده، وجوب عقلانی دفع ضرر است، به‌طوری که عقل به‌طور مستقل بر لزوم اقدام برای جلوگیری از ضرر تأکید می‌کند. ضرر در اینجا شامل ضرر دنیوی و اخروی است و برخی محققان، ضرر دنیوی را به موارد جدی و غیرقابل جبران، مانند از دست دادن جان یا اعضای بدن، محدود کرده‌اند.

در فضای سایبری، انواع مختلفی از ضرر محتمل وجود دارد، از جمله سرقت اطلاعات شخصی، اخلال در عملکرد سیستم‌ها، تخریب داده‌ها و ایجاد اختلال در خدمات الکترونیکی. استفاده از هوش مصنوعی در پیشگیری از جرایم سایبری می‌تواند به کاهش این نوع ضررها کمک کند. قاعده دفع ضرر محتمل، استفاده از ابزارها و فناوری‌هایی مانند هوش مصنوعی را برای پیشگیری از جرایم سایبری توجیه می‌کند. به عبارت دیگر، این قاعده به ما می‌گوید که باید از ابزارهایی که می‌توانند از وقوع ضررهای احتمالی جلوگیری کنند، استفاده کنیم. (هاشمی شاهرودی، ۱۳۸۲، ج ٦، ص ٤٤٥)

با این حال، در استفاده از هوش مصنوعی برای پیشگیری از جرایم سایبری، باید بین منافع مختلفی مانند امنیت، حریم خصوصی و آزادی‌های فردی تعادل برقرار کرد. قاعده دفع ضرر محتمل به ما می‌گوید که باید به دنبال راه‌حل‌هایی باشیم که بیشترین منفعت را با کمترین ضرر ایجاد کند. همچنین، استفاده از هوش مصنوعی در حوزه امنیت سایبری مسئولیت‌هایی را برای طراحان، توسعه‌دهندگان و استفاده‌کنندگان از این فناوری ایجاد می‌کند. این افراد باید اطمینان حاصل کنند که استفاده از هوش مصنوعی منجر به ایجاد ضرر برای دیگران نشود و در این راستا، باید به اصول اخلاقی و قانونی پایبند باشند تا از بروز تبعات منفی جلوگیری کنند.

قاعده دفع مفسده أولی از جلب المصالح

قاعده فقهی «درء المفاسد أولی من جلب المصالح» به‌عنوان یکی از اصول بنیادین در فقه اسلامی، از فروعات قاعده اصلی «لاضرر و لاضرار» محسوب می‌شود. این قاعده به‌طور گسترده‌ای در متون فقهی به‌کار می‌رود و شامل احکام مرتبط با جلب منافع و دفع مفاسد است. حفظ ضروریات پنجگانه (دین، نفس، عقل، نسب و مال) در این قاعده نیز به‌روشنی مشهود است(فتوحی حنبلی، ١٤٠٠ق، ٤٤٣). محل اعمال این قاعده در مواقعی است که مصالح و مفاسد در تعارض قرار می‌گیرند و به‌این‌ترتیب، این قاعده به‌عنوان ابزاری برای حمایت از مصالح عمومی و دفع ضرر از جامعه طراحی شده است. اهمیت این قاعده در فقه مقاصد به‌ویژه در عرصه‌های اجتماعی و اخلاقی بسیار بارز است و در طول تاریخ توسط بسیاری از علما به‌صورت اصولی یا فرعی مورد بحث و بررسی قرار گرفته است. اولین اشاره به این قاعده از سوی «علی ابن خلف بن بطال» (متوفی ٤٤٩ ق) در کتب اصول فقه و فقه او ثبت شده است (ابن حجر هیتمی، ١٣٨٩ق: ٩٣). همچنین، در کتب اصولیین و فقهای شیعه، مانند آخوند خراسانی در «کفایهٔ الاصول» (آخوند خراسانی، ١٤٠٩، ص ٢٧٧) و جواد مغنیه در «فقه امام صادق»(مغنیه، بی‌تا، ج ٦، ص ٣٦٨) به این قاعده استناد شده است.

معنای اجمالی قاعده «درء المفاسد أولی من جلب المصالح» این است که در مواردی که مفسده و مصلحت در یک امر دینی یا دنیایی تعارض می‌کنند، اصل بر دفع مفسده است. به عبارت دیگر، از بین بردن مفسده از جلب مصلحت مهم‌تر است. این قاعده به‌دلیل قبح مفسده و تأثیرات منفی آن بر انسان، نشان‌دهنده اهمیت شارع در دفع مفاسد است. به‌ویژه در مواردی که جلب مصلحت و دفع مفسده در تعارض هستند، شریعت دفع مفسده را مقدم می‌داند. فقهای امامیه در بحث اجتماع امر و نهی در اصول فقه، از وجوه تقدم نهی بر امر، به قاعده «دفع مفسده مقدم بر جلب منفعت» اشاره کرده‌اند. در این راستا، فقیه باید جانب حرمت و نهی را که از مفسده حکایت دارد، بر جانب وجوب که حاکی از مصلحت است مقدم بدارد. (علیدوست، ١٣٨٨، ص ٥١٩).

در مواردی که فردی در لزوم انجام یا ترک فعلی شک کند، باید در صورت جمع مفسده و مصلحت، ابتدا دفع مفسده را انتخاب کند. اگر مکلفی در مورد واجب یا حرام بودن فعلی شک کند، انجام عمل ممکن است به مصلحتی منجر شود، هرچند که ممکن است واقعاً حرام باشد و او را در مفسده بیندازد. اما اگر عمل را ترک کند، ممکن است مفسده‌ای را از خود دور کند، هرچند که احتمال دارد مصلحتی از او فوت شود. در این موارد، دفع مفسده در نزد عقل و شرع برتر است، زیرا دفع مفسده قطعی از جلب منفعت قطعی بهتر است(وزیری و سعیدیانی، ١٣٩٦، ص ١٠٦). با این حال، فقهای امامیه تأکید کرده‌اند که چنین قاعده‌ای نزد عقلا ثابت نشده و لذا این قاعده کلیت ندارد(آخوند خراسانی، ١٤٠٩، ص ١٧٧؛ حکیم، ١٣٩١، ص ٥٤٤)؛ زیرا ممکن است عقلا جلب مصلحت زیاد را بر دفع مفسده کم مقدم بدانند (همان).

در دنیای دیجیتال و فضای سایبری، مفاسد مختلفی از جمله سرقت اطلاعات، تخریب داده‌ها و اخلال در خدمات وجود دارد. استفاده از هوش مصنوعی برای پیشگیری از این مفاسد، در واقع عملیاتی کردن قاعده دفع مفسده است. در بسیاری از موارد، استفاده از هوش مصنوعی برای افزایش امنیت سایبری با ملاحظاتی چون حریم خصوصی و آزادی‌های فردی در تعارض است. در این موارد، قاعده دفع مفسده به ما می‌گوید که باید به دنبال راه‌حل‌هایی باشیم که بیشترین مفسده را کاهش دهد، حتی اگر به معنای کاهش برخی منافع باشد. قاعده دفع مفسده أولی از جلب المصالح بر اهمیت پیشگیری از وقوع جرم تأکید می‌کند. استفاده از هوش مصنوعی برای پیش‌بینی و جلوگیری از حملات سایبری در راستای این قاعده است. همچنین، استفاده از هوش مصنوعی در حوزه امنیت سایبری مسئولیت‌هایی را برای طراحان، توسعه‌دهندگان و استفاده‌کنندگان از این فناوری ایجاد می‌کند. این افراد باید اطمینان حاصل کنند که استفاده از هوش مصنوعی منجر به ایجاد مفاسد جدیدی نشود.

با توجه به قاعده دفع مفسده أولی از جلب المصالح، کاربردهای هوش مصنوعی در پیشگیری از جرایم سایبری می‌تواند

در صورتی جایز باشد که منجر به کاهش مفاسد سایبری شود و کمترین آسیب را به حقوق افراد وارد کند. همچنین، الگوریتم‌های هوش مصنوعی باید شفاف و قابل فهم باشند و در صورت بروز هرگونه خطا یا خسارت، باید سازوکارهای پاسخگویی و جبران خسارت وجود داشته باشد. در نهایت، با توجه به پیچیدگی‌ها و چالش‌های موجود در فضای سایبری، لازم است که رعایت اصول اخلاقی و قانونی در استفاده از فناوری‌های نوین، به‌ویژه هوش مصنوعی، در اولویت قرار گیرد تا از بروز مفاسد جدید جلوگیری شود و امنیت و حقوق افراد به‌طور مؤثر حفظ گردد.

حریم خصوصی

حریم خصوصی در لغت عرب از ریشه‌ی «حَرَمَ» به معنای منع و تشدید است. ابن فارس حریم را به معنای منع تفسیر کرده و صاحب المحیط فی اللغة نیز تعریفی مشابه ارائه داده است(فراهیدی، ۱٤۰۹، ج ۳، ص ۲۲۲). در اقرب الموارد آمده است که حریم به معنای چیزی است که انسان از آن دفاع می‌کند و به دیگران اجازه‌ی ورود نمی‌دهد (شرتونی، ۱٤۰۳، ج۱: ۱۸٤). این تعریف به‌نوعی تسامحی است، زیرا بین «حَرَمَ» و «مَنَعَ» تفاوت‌هایی وجود دارد. به‌طور مثال، در کتاب «تحقیق در کلمات قرآن» گفته شده است که «حَرَمَ» به معنای ممنوعیت از اصل و ریشه است، در حالی که «مَنَعَ» ناظر به بعد از ظهور و وجود است(مصطفوی، ۱۳٦۸، ج ۲، ص ۲۰٤). بنابراین، حریم به‌طور خلاصه به معنای هر آنچه است که هتک آن به هر شکلی از ابتدا ممنوع و حرام شده باشد. در فقه، حریم به معنای منع است و به چیزی اشاره دارد که نزدیک‌شدن به آن برای غیرصاحبش ممنوع است(مجلسی، ۱٤۰۳، ج ٦، ص ۲٤۱). موضوع حریم در فقه از دو جنبه‌ی اقتصادی و اخلاقی مورد بحث قرار می‌گیرد. جنبه‌ی اقتصادی به مسئله‌ی مال مربوط می‌شود و جنبه‌ی اخلاقی به مالک مال. فقها معمولاً دو مصداق برای حریم ذکر کرده‌اند: یکی در مورد اموال و دیگری در مورد انسان. مورد اول در باب‌های «احیاء موات، تجارت، بیع» و مصداق دوم در باب‌های «جهاد» و «حدود» مطرح شده است(علامه حلی، ۱٤۱۳، ج ۲، ص ٤۱۰)

واژه‌ی حریم به‌عنوان یک اصطلاح حقوقی، نخستین بار در ماده‌ی ۱۳٦ قانون مدنی مصوب سال ۱۳۰۷ تعریف شد: «حریم مقداری از اراضی اطراف ملک و قنات و نهرها است که برای کمال انتفاع از آن ضرورت دارد». این تعریف به‌نوعی همان تعریفی است که فقها برای کاربرد نخست حریم ارائه کرده‌اند. برخی حقوقدانان ایرانی نیز بر این باورند که زبان حقوقی هر کشور، ساخته‌ی عالمان حقوق است و قانونگذار نیز از آن پیروی می‌کند(کاتوزیان، ۱۳۷٦، ص ۲۱٦). با این حال، تعریف مستقلی از حریم ارائه نکرده‌اند. در مورد کاربرد دوم حریم، یعنی در مورد انسان، چون در قانون نیامده است، حقوقدانان آن را تعریف نکرده‌اند و صرفاً به اصطلاح «حرمت منازل» اکتفا کرده‌اند و در تعریف آن گفته‌اند: «حرمة المنازل یعنی احترام منازل مسکونی مردمان و هتک حرمت آن‌ها نکردن»(جعفری لنگرودی، ۱۳۷۸، ج ۳، ص ۱٦۵) خصوصی در لغت به معنای ویژه و اختصاصی است و در زبان عربی برای بیان این معنا، واژه «الخاصه» به‌کار می‌رود(طریحی، ۱۳۷۵ ذیل واژه). حریم خصوصی به قلمروی از زندگی هر فرد اشاره دارد که آن فرد انتظار دارد دیگران بدون رضایت او به اطلاعات راجع به آن دسترسی نداشته باشند یا به آن وارد نشوند اشکالی که به این تعریف وارد است، عبارت «انتظار دارد» است، چراکه این عبارت بار معنایی حقوقی ندارد و مفهوم حریم خصوصی را نسبی می‌کند. در لایحه‌ی حریم خصوصی، چنین تعریف شده است: «حریم خصوصی قلمروی از زندگی هر شخص است که آن شخص عرفاً یا با اعلان قبلی در چارچوب قانون، انتظار دارد تا دیگران بدون رضایت وی به آن وارد نشوند یا به آن نظارت یا نگاه نکنند» (لایحه حریم خصوصی، بند ۱، ماده ۲). با اضافه‌شدن قید «در چارچوب قانون»، اشکالات قبلی به این تعریف وارد نمی‌شود و به‌طور کلی، این تعریف قابل قبولی از حریم خصوصی است.

پذیرش و شناخت حریم خصوصی به‌عنوان یک حق انسانی در قوانین الهی و بشری مورد توجه قرار گرفته است. نیاز به حریم خصوصی امری ریشه‌دار و فطری است که تنها به انسان محدود نمی‌شود. تفکیک حوزه خصوصی از عمومی

به‌نوعی قدمتی به امتداد حیات انسانی دارد. به‌طور مثال، آدم و حوا در قرآن پس از خوردن از میوه‌ی ممنوعه و آشکار شدن زشتی‌هایشان در صدد پوشاندن آن برآمدند (اعراف/۲۲) که این خود اشاره‌ای به فطری بودن این مسئله برای انسان است. اگرچه اصطلاح "حریم خصوصی" حقیقت شرعیه ندارد و در فقه مطرح نشده، اما مقولات و مسائل آن با مبانی محکم مورد حمایت قرار گرفته‌اند. در اسلام، حریم خصوصی علاوه بر اموال و اماکن، شامل حریم‌های جان، خانواده، مسلمان و اسلام می‌شود (نجفی، ١٤٠٤، ج ٢٦، ص ٧٥). در آیات متعددی از قرآن مجید بر لزوم رعایت حریم خصوصی اشخاص تأکید شده است، از جمله آیه ۱۲ سوره حجرات و آیات ۱۹ و ۲۷ الی ۳۰ سوره نور. سنت نبوی و سیره‌ی ائمه‌ی اطهار نیز سرشار از توصیه‌هایی در پرهیز از نقض حریم خصوصی افراد است. ممنوعیت تجسس، تحسس و تفتیش، سوءظن، هجو، قذف و سبّ، نمیمه و غیبت، و استراق سمع از رایج‌ترین اصطلاحاتی است که در آیات و روایات اسلامی درباره‌ی حریم خصوصی به‌کار رفته است این موضوع نشان‌دهنده‌ی اهمیت بالای حریم خصوصی در فرهنگ اسلامی و ضرورت احترام به آن در زندگی اجتماعی و فردی است.

در این راستا، استفاده از هوش مصنوعی در پیشگیری از جرایم سایبری به جمع‌آوری و تحلیل داده‌های شخصی نیاز دارد که این امر می‌تواند با حریم خصوصی افراد در تعارض باشد. فقه امامیه به‌طور خاص بر حفظ حریم خصوصی تأکید دارد و لذا استفاده از هوش مصنوعی در حوزه امنیت سایبری باید به گونه‌ای باشد که کمترین آسیب را به این حریم وارد کند. حفظ حریم خصوصی در عصر دیجیتال نه‌تنها به‌عنوان یک حق انسانی بلکه به‌عنوان یک عنصر کلیدی در ایجاد اعتماد عمومی و امنیت سایبری شناخته می‌شود. ایجاد تعادل میان امنیت و حریم خصوصی ضروری است و می‌تواند به‌عنوان یک راهکار مؤثر در پیشگیری از جرایم سایبری عمل کند.

استفاده از هوش مصنوعی در حوزه امنیت سایبری، مسئولیت‌هایی را برای طراحان، توسعه‌دهندگان و کاربران این فناوری ایجاد می‌کند. این افراد باید اطمینان حاصل کنند که استفاده از هوش مصنوعی منجر به نقض حریم خصوصی افراد نشود. به‌علاوه، باید سازوکارهایی برای پاسخگویی در صورت بروز خطا یا خسارت وجود داشته باشد. کاربردهای هوش مصنوعی در پیشگیری از جرایم سایبری می‌تواند در صورتی جایز باشد که کمترین آسیب به حریم خصوصی وارد شود، اطلاعات جمع‌آوری‌شده به‌صورت محرمانه نگهداری شود، الگوریتم‌ها شفاف و قابل فهم باشند و در صورت بروز هرگونه خطا، سازندگان و کاربران پاسخگو باشند. این الزامات نه‌تنها به حفظ حریم خصوصی کمک می‌کند بلکه به ایجاد اعتماد در جامعه و استحکام زیرساخت‌های امنیت سایبری نیز منجر خواهد شد.

بررسی قوانین و مقررات حقوقی ایران در زمینه نظارت بر استفاده از هوش مصنوعی

در حقوق ایران، قوانین و مقررات مختلفی در رابطه با نظارت بر استفاده از فناوری‌های نوظهور مانند هوش مصنوعی وجود دارد که می‌تواند در زمینه استفاده از هوش مصنوعی برای پیشگیری از جرائم سایبری نیز مؤثر باشد:

قانون حمایت از حقوق کاربران در فضای مجازی به‌عنوان یک چارچوب قانونی مهم، بر حفظ حریم خصوصی کاربران تأکید ویژه‌ای دارد. این قانون به‌خصوص در زمینه استفاده از فناوری‌های نوین مانند هوش مصنوعی برای پیشگیری از جرایم سایبری، ضرورت رعایت حریم خصوصی افراد را مورد تأکید قرار می‌دهد. به‌عبارت دیگر، هرگونه جمع‌آوری و تحلیل داده‌های شخصی باید با رعایت اصول و قوانین مربوط به حریم خصوصی انجام شود. این امر نه‌تنها به حفظ حقوق فردی کاربران کمک می‌کند، بلکه موجب تقویت اعتماد عمومی به خدمات دیجیتال نیز می‌شود.علاوه بر این، امنیت اطلاعات یکی دیگر از محورهای کلیدی این قانون است. هوش مصنوعی می‌تواند به‌عنوان ابزاری مؤثر در افزایش امنیت اطلاعات کاربران عمل کند، اما باید به این نکته توجه داشت که خود این فناوری نیز ممکن است هدف حملات سایبری قرار گیرد. بنابراین، استفاده از هوش مصنوعی باید به‌گونه‌ای باشد که ضمن تقویت امنیت اطلاعات، از بروز تهدیدات

جدید جلوگیری کند و اطلاعات کاربران را در برابر خطرات سایبری محافظت نماید.
مسئولیت‌پذیری از دیگر اصول بنیادین این قانون است. این قانون به‌وضوح مسئولیت ارائه‌دهندگان خدمات در فضای مجازی را مشخص می‌کند. در خصوص هوش مصنوعی، سازندگان و کاربران این فناوری باید مسئولیت نتایج و پیامدهای ناشی از استفاده از آن را بر عهده بگیرند. این مسئولیت‌پذیری شامل تضمین امنیت و حریم خصوصی کاربران و همچنین پاسخگویی در برابر هرگونه نقص یا سوءاستفاده از داده‌ها می‌شود.(ر.ک. «طرح قانون حمایت از حقوق کاربران و خدمات پایه کاربردی فضای مجازی»، ۱۴۰۰)

تعیین سند راهبردی امنیت فضای تولیدو تبادل اطلاعات کشورنیز به‌عنوان یک ابزار قانونی دیگر، استانداردهای امنیتی لازم برای فعالیت در فضای سایبری را تعیین می‌کند. هوش مصنوعی می‌تواند در اجرای این استانداردها و بهبود امنیت سیستم‌ها نقش مهمی ایفا کند. این آیین‌نامه همچنین به نظارت بر فناوری‌های نوین اشاره دارد و استفاده از هوش مصنوعی در پیشگیری از جرایم سایبری باید مطابق با این استانداردها و الزامات باشد. این نظارت می‌تواند به شناسایی و مدیریت ریسک‌ها و چالش‌های مرتبط با فناوری‌های نوین کمک کند.(ر.ک. «سند راهبردی امنیت فضای تولیدو تبادل اطلاعات کشور»، ۱۳۸۷)

سیاست‌های کلی نظام در حوزه فضای مجازی بر توسعه هوشمندسازی تأکید دارند. هوش مصنوعی به‌عنوان یکی از ابزارهای کلیدی در این راستا می‌تواند در شناسایی الگوهای جرایم سایبری و پیشگیری از آن‌ها نقش مؤثری ایفا کند. این سیاست‌ها همچنین بر اهمیت حفاظت از حریم خصوصی و امنیت اطلاعات تأکید دارند، به‌طوری‌که استفاده از هوش مصنوعی در این حوزه باید با رعایت این اصول انجام شود. این رویکرد می‌تواند به ایجاد یک فضای امن و مطمئن برای کاربران کمک کند.(ر.ک. «سیاست‌های کلی فضای مجازی»، ۱۳۹۳)قانون جرائم رایانه‌ای به‌طور خاص به جرایم سایبری و روش‌های مقابله با آن‌ها می‌پردازد. هوش مصنوعی می‌تواند در شناسایی و پیشگیری از این جرایم نقش مهمی داشته باشد و به‌عنوان ابزاری کارآمد در افزایش امنیت سایبری و حفاظت از زیرساخت‌های اطلاعاتی کشور عمل کند. این قانون به‌ویژه بر اهمیت ایجاد زیرساخت‌های امن و مقاوم در برابر تهدیدات سایبری تأکید دارد و هوش مصنوعی می‌تواند در این زمینه به‌عنوان یک راهکار مؤثر در شناسایی و مدیریت تهدیدات عمل کند.(ر.ک. «قانون جرائم رایانه ای»، ۱۳۸۸)

برای بحث درباره کاربرد هوش مصنوعی در پیشگیری از جرایم سایبری، می‌توان از این قوانین به طرق مختلف بهره‌برداری کرد. نخست، این قوانین چارچوب قانونی لازم برای استفاده از هوش مصنوعی در پیشگیری از جرایم سایبری را مشخص می‌کنند. همچنین، این قوانین به شناسایی چالش‌های موجود در استفاده از هوش مصنوعی در این حوزه کمک می‌کنند و الزامات لازم برای این استفاده را تعیین می‌کنند. به‌علاوه، این قوانین به ارزیابی ریسک‌های مرتبط با استفاده از هوش مصنوعی نیز کمک می‌کنند و با توجه به آن‌ها می‌توان سیاست‌ها و راهبردهای لازم برای توسعه و استفاده از هوش مصنوعی در این حوزه را تدوین کرد.

در نتیجه، قوانین و مقررات موجود در کشور ما بستری مناسب برای استفاده از هوش مصنوعی در پیشگیری از جرایم سایبری فراهم می‌کنند. با توجه به این قوانین، می‌توان از هوش مصنوعی برای افزایش امنیت سایبری، حفاظت از حریم خصوصی و مبارزه با جرایم سایبری بهره برد. با این حال، برای استفاده مؤثر از هوش مصنوعی در این حوزه، نیاز به تدوین قوانین و مقررات دقیق‌تر و همچنین ایجاد زیرساخت‌های لازم احساس می‌شود. به‌طور کلی، ایجاد توازن بین امنیت و حریم خصوصی در دنیای دیجیتال امری ضروری است که می‌تواند به تقویت اعتماد عمومی و بهبود کیفیت خدمات دیجیتال منجر شود.

نتیجه‌گیری

هوش مصنوعی با قابلیت‌های بی‌نظیر خود در پردازش حجم عظیمی از داده‌ها، شناسایی الگوهای پیچیده و یادگیری ماشین، تحولی بنیادین در حوزه امنیت سایبری ایجاد کرده است. این فناوری به عنوان یک ابزار قدرتمند، با ارائه راهکارهای هوشمند و خودکار، توانمندسازی سیستم‌های امنیتی در پیش‌بینی، تشخیص و مقابله با تهدیدات سایبری را به طور چشمگیری ارتقا بخشیده است.

یکی از مهم‌ترین کاربردهای هوش مصنوعی در امنیت سایبری، تشخیص زودهنگام تهدیدات است. الگوریتم‌های یادگیری ماشین با تحلیل رفتار کاربران، ترافیک شبکه و داده‌های مختلف، قادر به شناسایی انحرافات از الگوهای معمول و تشخیص حملات سایبری در مراحل اولیه هستند. این قابلیت، به ویژه در مواجهه با تهدیدات نوظهور و پیچیده، از اهمیت بالایی برخوردار است.

با این حال، گسترش کاربرد هوش مصنوعی در امنیت سایبری با چالش‌هایی نیز همراه است. مسائلی مانند حفظ حریم خصوصی کاربران، تعصب الگوریتمی و هزینه بالای توسعه و پیاده‌سازی سیستم‌های هوش مصنوعی، از جمله مهم‌ترین موانع پیش روی این فناوری محسوب می‌شوند. علاوه بر این، نیاز به نیروی انسانی متخصص و با تجربه برای طراحی، توسعه و مدیریت سیستم‌های هوش مصنوعی، یک ضرورت اجتناب‌ناپذیر است.

از منظر فقهی، استفاده از هوش مصنوعی در امنیت سایبری باید با رعایت اصول اخلاقی و قانونی صورت گیرد. اصول مهمی مانند لاضرر، عدالت، دفع ضرر محتمل و دفع مفسده أولی، ضرورت توجه به حریم خصوصی افراد و تطابق با قوانین و مقررات حاکم بر فضای سایبری را مورد تأکید قرار می‌دهند.

در نهایت آنکه هوش مصنوعی پتانسیل بالایی برای ارتقای امنیت سایبری دارد، اما برای بهره‌برداری بهینه از این فناوری، نیازمند یک رویکرد جامع و چندجانبه هستیم. این رویکرد باید بر پایه تعامل مؤثر بین متخصصان امنیت سایبری، توسعه‌دهندگان هوش مصنوعی، قانون‌گذاران و فقها شکل گیرد. با توجه به اهمیت روزافزون امنیت سایبری و نقش حیاتی هوش مصنوعی در این حوزه، توسعه چارچوب‌های قانونی و اخلاقی مناسب برای استفاده از این فناوری، یک ضرورت اجتناب‌ناپذیر است.

در راستای مقاله حاضر، می‌توان پیشنهادات کاربردی و علمی زیر را برای گسترش استفاده از هوش مصنوعی در پیشگیری از جرایم سایبری ارائه داد:

۱. توسعه سیستم‌های تشخیص نفوذ مبتنی بر هوش مصنوعی: این سیستم‌ها باید شامل استفاده از شبکه‌های عصبی عمیق برای تشخیص الگوهای پیچیده در ترافیک شبکه و شناسایی حملات صفر روزه باشند. همچنین، مدل‌سازی رفتار طبیعی کاربران و تشخیص انحرافات از این الگوها به شناسایی فعالیت‌های مشکوک کمک می‌کند. علاوه بر این، استفاده از هوش مصنوعی برای شناسایی و طبقه‌بندی انواع مختلف بدافزارها و ویروس‌ها ضروری است.

۲. بهبود سیستم‌های مدیریت رویدادهای امنیتی (SIEM): در این راستا، هوش مصنوعی می‌تواند برای همبستگی رویدادهای امنیتی مختلف و شناسایی حملات پیچیده به کار رود. همچنین، استفاده از الگوریتم‌های یادگیری ماشین برای اولویت‌بندی هشدارهای امنیتی و تمرکز بر تهدیدات جدی و خودکارسازی برخی از فرآیندهای پاسخگویی به تهدیدات از دیگر اقدامات مؤثر است.

۳. حفاظت از زیرساخت‌های حیاتی: هوش مصنوعی می‌تواند برای شناسایی حملات سایبری هدفمند به زیرساخت‌های

حیاتی مانند نیروگاه‌ها و شبکه‌های برق استفاده شود. علاوه بر این، استفاده از مدل‌های پیش‌بینی برای پیش‌بینی حملات آینده و اتخاذ اقدامات پیشگیرانه می‌تواند به تقویت امنیت این زیرساخت‌ها کمک کند.

٤. آموزش و ارتقای آگاهی کارکنان: استفاده از هوش مصنوعی برای ایجاد شبیه‌سازی‌های واقع‌بینانه از حملات سایبری به منظور آموزش کارکنان و انجام آزمون‌های نفوذ خودکار برای شناسایی نقاط ضعف سیستم‌ها، می‌تواند به افزایش آمادگی سازمان‌ها کمک کند.

۵. همکاری بین‌المللی و اشتراک‌گذاری اطلاعات: ایجاد پایگاه داده‌های مشترک برای تبادل اطلاعات در مورد تهدیدات سایبری بین سازمان‌ها و کشورها و توسعه استانداردهای مشترک برای استفاده از هوش مصنوعی در امنیت سایبری از جمله این اقدامات هستند.

٦. تحقیقات و توسعه: سرمایه‌گذاری در تحقیقات برای توسعه الگوریتم‌های هوش مصنوعی با قابلیت‌های پیشرفته‌تر و بررسی اثرات اجتماعی و اخلاقی استفاده از این فناوری در امنیت سایبری، می‌تواند به بهبود عملکرد و کاهش ریسک‌ها کمک کند.

۷. تدوین قوانین جامع امنیت سایبری: لازم است قوانینی جامع و مشخص در زمینه امنیت سایبری تدوین شود که شامل تعاریف دقیق از جرایم سایبری، مجازات‌ها و مسئولیت‌های سازمان‌ها و افراد باشد. این قوانین باید به‌روز و متناسب با تحولات فناوری باشند.

۸. ایجاد نهادهای نظارتی و اجرایی: تأسیس نهادهای مستقل برای نظارت بر رعایت قوانین امنیت سایبری و اجرای سیاست‌های مربوطه ضروری است. این نهادها باید مسئولیت‌های خود را به‌طور شفاف و مؤثر انجام دهند.

## منابع


۱. آخوند خراسانی، محمدکاظم. (۱٤۰۹). *کفایه الاصول*. قم: موسسهٔ آل البیت (علیهم السلام) لإحیاء التراث.

۲. ابن اثیر، مبارک بن محمد. (۱۳٦۷). *النهایهٔ فی غریب الحدیث و الأثر*. (طاهر احمد زاوی و محمود محمد طناحی، مصححین). قم: اسماعیلیان.

۳. ابن منظور، محمد بن مکرم. (۱٤۱٤). *لسان العرب*. بیروت: دار صادر.

٤. ایروانی، باقر. (بی‌تا). *دروس تمهیدیهٔ فی الفقه الاستدلالی علی المذهب الجعفری*. مؤسسهٔ الفقه للطباعهٔ و النشر.

۵. بیابانی، غلام حسین؛ و هادیانفر، سیدکمال. (۱۳۸٤). *فرهنگ توصیفی علوم جنایی*. تهران: انتشارات مرکز تحقیقات کاربردی کشف جرایم و امنیت معاونت آگاهی ناجا.

٦. جعفری لنگرودی، محمد جعفر. (۱۳۷۸). *مبسوط در ترمینولوژی حقوق*. تهران: گنج دانش.

۷. جلالی فراهانی، امیرحسین. (۱۳۸۹). *درآمدی بر آیین دادرسی کیفری جرایم سایبری*. تهران: انتشارات خرسندی.

۸. حکیم، سید محسن. (۱۳۹۱). مستمسک عروهٔ الوثقی. بیروت: دار إحیاء التراث العربی.

۹. دولت آبادی، سروش؛ و دولت آبادی، مسرور. (۱٤۰۰). مقاله تشخیص نفوذ با استفاده از هوش مصنوعی

۱۰. دیدبان. (۱٤۰۳). تمامی کاربردهای هوش مصنوعی در امنیت. بازیابی ۱۸ شهریور ۱٤۰۳، از https://didbaan.com/ai-in-security/

۱۱. رحیمی نژاد، اسمعیل. (۱۳۹۱). آشنایی با حقوق جزا و جرم‌شناسی. قم: پژوهشگاه فرهنگ و اندیشه اسلامی.

۱۲. *رضایی اصفهانی، محمدعلی. (۱۳۹۲). وسائل العباد فی یوم التناد (ج ۱). قم: پژوهشهای تفسیر و علوم قرآن.*

۱۳. *سند راهبردی امنیت فضای تولیدو تبادل اطلاعات کشور. (۱۳۸۷). بازیابی ۲۰ شهریور ۱٤۰۳، از* https://rc.majlis.ir/fa/law/show/۱۳۵۸۳۵

۱٤. *سیاست‌های کلی فضای مجازی. (۱۳۹۳). بازیابی ۲۰ شهریور ۱٤۰۳، از -اولیه سیاست‌های-کلی-فضای-مجازی ایده* https://maslahat.ir/fa/news/۵۵۳٤/

۱۵. *صادق زاده طباطبایی، سیدمحمود. (۱۳۹۳). درآمدی بر تطبیق قاعده عدالت. فقه و اصول، (۹۸)، ۱٤۳-۱۵۸.*

۱٦. *طباطبایی، سید محمدحسین. (بی‌تا). تفسیر المیزان (ترجمه). (محمد باقر موسوی، مترجم). جامعه مدرسین حوزه علمیه قم. دفتر انتشارات اسلامی.*

۱۷. طرح قانون حمایت از حقوق کاربران و خدمات پایه کاربردی فضای مجازی. (۱٤۰۰ زمستان). بازیابی ۲۰ شهریور ۱٤۰۳، از طرح-حمایت-از-حقوق – کاربران https://www.shenasname.ir/laws/۸۷۸۰

۱۸. طریحی، فخرالدین بن محمد. (۱۳۷۵). مجمع البحرین. تهران: مکتبهٔ المرتضویهٔ.

۱۹. عبدی پور، مهدی؛ و مصاحب طلب، علی. (۱٤۰۳). هوش مصنوعی ، کاربردهای آن و امنیت سایبری. کنفرانس بین المللی مطالعات بین رشته ای در مدیریت و مهندسی، ۱۰(۱۰)، ۸۹٦-۹۰٦.

۲۰. علامه حلی، حسن بن یوسف. (۱٤۱۳). قواعد الأحکام. (جامعه مدرسین حوزه علمیه قم. دفتر انتشارات اسلامی). قم: مؤسسهٔ النشر الإسلامی.

۲۱. علیدوست، ابوالقاسم. (۱۳۸۸). فقه و مصلحت. قم: پژوهشگاه فرهنگ و اندیشه اسلامی.

۲۲. فراهیدی، خلیل بن احمد. (۱٤۰۹). العین. قم: مؤسسهٔ دار الهجرهٔ.

۲۳. فیض، علیرضا. (۱۳۸۵). مقارنه و تطبیق در حقوق جزای عمومی اسلام. تهران: سازمان چاپ و انتشارات وزارت فرهنگ و ارشاد اسلامی.

۲٤. قانون جرائم رایانه ای. (۱۳۸۸). بازیابی ۲۰ شهریور ۱٤۰۳، از https://rc.majlis.ir/fa/law

۲۵. کاتوزیان، ناصر. (۱۳۷٦). *حقوق مدنی: قواعد عمومی قراردادها*. تهران: شرکت سهامی انتشار.

۲۶. کشاورز، زهرا؛ و حسینی، حمیدرضا. (۱٤۰۲). هوش مصنوعی در امنیت سایبری (کاربردها، چالش ها و فرصت ها). *ششمین همایش ملی فناوریهای نوین در مهندسی برق، کامپیوتر و مکانیک ایران*.

۲۷. کلینی، محمدبن یعقوب. (۱٤۲۹). *کافی*. قم: دارالحدیث.

۲۸. گرجی، ابوالقاسم. (۱۳٦۹). *مقالات حقوقی*. تهران: دانشگاه تهران.

۲۹. مجلسی، محمدباقر. (۱٤۰۳). *بحار الأنوار*. بیروت: دار إحیاء التراث العربی.

۳۰. محامد، علی. (۱۳۸۵). بررسی قاعده عدل و انصاف و آثار آن. *پژوهشهای فلسفی-کلامی*، (۳۰)، ۲۳۵-۲۷۰.

۳۱. محمدحسینی، بابک؛ قافله باشی، سید فهیم؛ و هادی زاده، مرتضی. (۱۳۹۹). پیشرانهای ارائه خدمات سایبری پایدار در دولت با تاکید بر حفظ امنیت از طریق هوش مصنوعی. *آینده پژوهی ایران*، ۹(۵)، ۳٦-٦۵.

۳۲. محمودی، امیررضا؛ و بحرکاظمی، مریم. (۱٤۰۳). هوش مصنوعی و تاثیر آن بر امنیت سایبری و حفاظت از داده ها. *پژوهش های بنیادین در حقوق*، ۳(۲)، ۸۷-۱۰٤.

۳۳. مصطفوی، حسن. (۱۳٦۸). *التحقیق فی کلمات القرآن الکریم*. تهران: وزارت فرهنگ و ارشاد اسلامی.

۳٤. مصوبه شورای عالی انقلاب فرهنگی. (۱٤۰۳، ۳۰ تیر). سند ملی هوش مصنوعی جمهوری اسلامی ایران.

۳۵. مغنیه، محمدجواد. (بی‌تا). *فقه الإمام جعفر الصادق*. انصاریان.

۳٦. نجفی، محمدحسن. (۱٤۰٤). *جواهر الکلام*. بیروت - لبنان: دار إحیاء التراث العربی.

۳۷. نراقی، احمد بن محمدمهدی. (۱٤۱۷). *عوائد الأیام*. قم: دفتر تبلیغات اسلامی.

۳۸. نوربها، رضا. (۱۳۸۵). *زمینه حقوق جزای عمومی*. تهران: گنج دانش.

۳۹. نوروزی، عرفانه؛ و بیرانوند، آریا. (۱٤۰۲). تاثیر هوش مصنوعی در ارتقا توانمندی های زیر سامانه های الکترونیکی، مخابراتی و سایبری در بستر جنگ الکترونیک. *نخبگان علوم و مهندسی*، ٤٤(۸)، ٤٤-۵۵.

٤۰. هاشمی شاهرودی، محمود. (۱۳۸۲). *فرهنگ فقه مطابق مذهب اهل بیت علیهم السلام*. قم: مؤسسه دائرة المعارف فقه اسلامی بر مذهب اهل بیت (علیهم السلام).

۴۱. ونگ. (بی‌تا). سیستم تشخیص نفوذ مبتنی بر ناهنجاری. بازیابی ۱۸ شهریور ۱٤۰۳، از

https://fa.wikipedia.org/wiki

42. Axelsson, Stefan. (2002). Intrusion Detection Systems: A Survey and Taxonomy.
43. Bochie, Kaylani; Gonzalez, Ernesto R.; Giserman, Luiz F.; Campista, Miguel Elias M.; & Costa, Luís Henrique M. K. (2020). Detecção de Ataques a Redes IoT Usando Técnicas de Aprendizado de Máquina e Aprendizado Profundo. In Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg) (pp. 257-270). SBC. https://doi.org/10.5753/sbseg.2020.19242
44. Buczak, Anna L.; & Guven, Erhan. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Communications Surveys & Tutorials, 18(2), 1153-1176. https://doi.org/10.1109/COMST.2015.2494502
45. Kaplan, Andreas; & Haenlein, Michael. (2019). Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. Business Horizons, 62(1), 15-25. https://doi.org/10.1016/j.bushor.2018.08.004
46. Lopes, António; Mamede, Henrique S.; Reis, Leonilde; & Santos, Arnaldo. (2024). Common Techniques, Success Attack Factors and Obstacles to Social Engineering: A Systematic Literature Review. Emerging Science Journal, 8(2), 761-794. https://doi.org/10.28991/ESJ-2024-08-02-025
47. Mitnick, Kevin D.; & Simon, William L. (2011). The Art of Deception: Controlling the Human Element of Security. John Wiley & Sons.
48. mitre. (2024). MITRE ATT&CK®. Retrieved January 12, 2025, from https://attack.mitre.org/
49. Scarfone, Karen; & Mell, Peter. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). National Institute of Standards and Technology. https://doi.org/https://doi.org/10.6028/NIST.SP.800-94
50. Sicari, S.; Rizzardi, A.; Grieco, L.; & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Comput. Networks, 76, 146-164.