Archive of SID.ir

JOURNAL OF CYBER LAW
نشریه حقوق سایبری

Received: 14/05/2024
Review: 10/08/2024
Accepted: 10 /09/2024
DOI: 10.22054/jocl.2025.85333.2714

Journal of Cyber Law
No(2),Vol(1), 41-65.
ISSN: 0972-6934
www.jocl.ir

Emerging Technologies and Phishing: A Legal Analysis of the Use of Artificial Intelligence and Automation in Fraud

Mahdieh Soltani [1], Majid Kamkar [*2]

1- M.A. Student in Law, Islamic Azad University, Yazd, Iran.

2*- M.A. Student in Law, Islamic Azad University, Yazd, Iran

ABSTRACT

Emerging technologies have brought significant transformations across economic, social, and legal domains, and the advent of artificial intelligence and automation has introduced new opportunities and challenges in the digital landscape. One of the most critical challenges is cyber fraud, particularly phishing, which poses a serious threat to information security and user assets, leading to financial losses and a decline in public trust. This study addresses the question of how the legal system can, by integrating philosophical, legal, ethical, and economic principles, determine liability and preventive measures for frauds based on emerging technologies and fill existing legislative gaps. The importance of this topic stems from the rapid growth of technology and the complexity of cyber fraud methods, which render existing laws insufficient and highlight the necessity of updating and developing comprehensive legal, ethical, and economic frameworks. The aim of this article is to provide a comprehensive analysis of the role of emerging technologies in cyber fraud and to propose legal and managerial strategies to mitigate risks and compensate for damages. The research method is descriptive-analytical and relies on a documentary study of domestic and international legal, philosophical, economic, and scholarly sources. The findings indicate that combining fault-based liability, strict liability, and employer liability, together with preventive regulations and security standards, can provide an effective framework for addressing cybercrime. Moreover, the results show that economic analysis of such crimes and investment in user education and system security can reduce the financial and social impacts of phishing and AI-based fraud. The innovation of this study lies in integrating philosophical, legal, ethical, and economic perspectives to propose a comprehensive framework for managing digital risks and legal responsibility.

Keywords:
emerging technologies, phishing, artificial intelligence, automation, legal liability

How to Cite: Soltani, M. and Kamkar, M. (2024). Emerging Technologies and Phishing: A Legal Analysis of the Use of Artificial Intelligence and Automation in Fraud. Cyber Law, 1(2), 41-65.
DOI: 10.22054/jocl.2025.85333.2714

Journal of Cyber Lawin Development and Evolution is licensed under a Creative Commons Attribution-Non Commercial 4.0 International License.

© Authors

* Corresponding Author: majid.kamkar@iauyazd.ac.ir

Archive of SID.ir

Archive of SID.ir

نشریه حقوق سایبری
JOURNAL OF CYBER LAW

نشریه حقوق سایبری
شماره (۲) ۴۱-۶۵
دوره ۱۴۰۳

تاریخ دریافت: ۱۴۰۳/۰۲/۲۵
تاریخ اصلاح: ۱۴۰۳/۰۵/۲۰
تاریخ پذیرش: ۱۴۰۳/۰۶/۲۰

فناوری‌های نوین و فیشینگ: بررسی حقوقی استفاده از هوش مصنوعی و اتوماسیون در کلاهبرداری

مهدیه سلطانی [۱]، مجید کامکار [۲*]

۱- دانشجوی کارشناسی ارشد حقوق، دانشگاه آزاد اسلامی یزد، ایران.

۲ - دانشجوی کارشناسی ارشد حقوق، دانشگاه آزاد اسلامی یزد، ایران.

چکیده

فناوری‌های نوین در دهه‌های اخیر تحولات گسترده‌ای در حوزه‌های اقتصادی، اجتماعی و حقوقی ایجاد کرده‌اند و به‌ویژه با ظهور هوش مصنوعی و اتوماسیون، فرصت‌ها و چالش‌های جدیدی در فضای دیجیتال پدید آورده‌اند. یکی از چالش‌های مهم مرتبط با این تحولات، کلاهبرداری‌های سایبری از جمله فیشینگ است که تهدیدی جدی برای امنیت اطلاعات و سرمایه کاربران به شمار می‌رود و موجب زیان‌های مالی و کاهش اعتماد عمومی می‌شود. پژوهش حاضر در پی پاسخ به این پرسش است که چگونه نظام حقوقی می‌تواند با استفاده از مبانی فقهی، حقوقی، فلسفی و اقتصادی، مسئولیت و راهکارهای پیشگیری از کلاهبرداری‌های مبتنی بر فناوری‌های نوین را تعیین کند و خلأهای قانونی موجود را پر نماید. اهمیت این موضوع از آنجا ناشی می‌شود که رشد سریع فناوری و پیچیدگی روش‌های کلاهبرداری، قوانین موجود را ناکافی ساخته و ضرورت بازنگری و توسعه چارچوب‌های حقوقی، اخلاقی و اقتصادی را آشکار می‌سازد. هدف این مقاله، تحلیل جامع نقش فناوری‌های نوین در کلاهبرداری‌های سایبری و ارائه راهکارهای قانونی و مدیریتی برای کاهش ریسک و جبران خسارات است. روش پژوهش در این مقاله توصیفی–تحلیلی و مبتنی بر مطالعه اسنادی است و از منابع حقوقی، فقهی، اقتصادی و پژوهش‌های علمی داخلی و خارجی بهره گرفته شده است. نتایج تحقیق نشان می‌دهد که ترکیب نظریه‌های مسئولیت بر اساس تقصیر، مسئولیت بدون تقصیر و مسئولیت کارفرما، همراه با تدوین مقررات پیشگیرانه و استانداردهای امنیتی، می‌تواند چارچوب مؤثری برای مقابله با جرایم سایبری فراهم آورد. همچنین یافته‌ها بیانگر آن است که تحلیل اقتصادی این جرایم و سرمایه‌گذاری در آموزش کاربران و تقویت سامانه‌های امنیتی، اثرات منفی مالی و اجتماعی ناشی از فیشینگ و سوءاستفاده از هوش مصنوعی را کاهش می‌دهد. نوآوری این مقاله در تلفیق دیدگاه‌های فلسفی، فقهی، حقوقی و اقتصادی برای ارائه یک چارچوب جامع جهت مدیریت ریسک‌های دیجیتال و مسئولیت قانونی است.

کلیدواژه‌ها:

فناوری‌های نوین، فیشینگ، هوش مصنوعی، اتوماسیون، مسئولیت حقوقی

نحوه استناد:

سلطانی, مهدیه و کامکار, مجید . (۱۴۰۳). فناوری‌های نوین و فیشینگ: بررسی حقوقی استفاده از هوش مصنوعی و اتوماسیون در کلاهبرداری. حقوق سایبری, ۱(۲), ۴۱-۶۵.

نشریه حقوق سایبری در توسعه و تکامل تحت مجوز کریتیو کامنز انتساب – غیرتجاری ۴,۰ بین‌المللی منتشر شده است.

©نویسندگان

* ایمیل نویسنده مسئول: majid.kamkar@iauyazd.ac.ir

Archive of SID.ir

Archive of SID.ir

مقدمه

در دنیای امروز، فناوری‌های نوین به‌ویژه هوش مصنوعی و اتوماسیون، به‌عنوان ابزارهایی تحول‌آفرین در عرصه‌های مختلف اقتصادی، اجتماعی و حقوقی شناخته می‌شوند. اما همزمان با این پیشرفت‌ها، تهدیدات جدیدی نیز در قالب جرایم سایبری، به‌ویژه فیشینگ، ظهور کرده‌اند که چالش‌های جدی برای نظام‌های حقوقی ایجاد کرده‌اند. فیشینگ به‌عنوان یکی از روش‌های متداول کلاهبرداری اینترنتی، با بهره‌گیری از فناوری‌های نوین، به‌طور فزاینده‌ای پیچیده‌تر و گسترده‌تر شده است. این مسأله ضرورت بررسی و تحلیل ابعاد حقوقی آن را در نظام حقوقی ایران ایجاب می‌کند.در نظام حقوقی ایران، با وجود پیشرفت‌های قابل توجه در زمینه فناوری اطلاعات و ارتباطات، همچنان خلأهای قانونی و چالش‌هایی در مواجهه با جرایم سایبری وجود دارد. ماده ۷۲۹ قانون مجازات اسلامی، به‌عنوان یکی از مواد قانونی مرتبط با جرایم رایانه‌ای، به‌طور کلی به جرایم رایانه‌ای پرداخته است. اما این ماده با توجه به تحولات سریع فناوری و ظهور روش‌های نوین کلاهبرداری، نیازمند بازنگری و به‌روزرسانی است. همچنین، قانون جرایم رایانه‌ای مصوب ۱۳۸۸ نیز به‌عنوان یکی از قوانین اصلی در این حوزه، با وجود برخی نقاط قوت، در مقابله با تهدیدات جدید ناکافی به‌نظر می‌رسد.اهمیت موضوع فیشینگ و چالش‌های حقوقی آن در ایران، به‌ویژه با توجه به رشد روزافزون استفاده از فناوری‌های نوین، بر کسی پوشیده نیست. این تهدیدات نه‌تنها امنیت اطلاعات شخصی و مالی افراد را به مخاطره می‌اندازند، بلکه اعتماد عمومی به سیستم‌های دیجیتال را نیز کاهش می‌دهند. بنابراین، تحلیل حقوقی این مسأله و ارائه راهکارهای قانونی مؤثر، امری ضروری است.پیشینه پژوهش‌های انجام‌شده در این زمینه نشان می‌دهد که محققانی چون دکتر محمدرضا بهرامی، دکتر سارا حسینی، دکتر علی‌اکبر موسوی، دکتر فاطمه کریمی و دکتر مهدی رضایی، مطالعاتی در حوزه جرایم سایبری و فیشینگ انجام داده‌اند. نتایج این پژوهش‌ها حاکی از آن است که با وجود تلاش‌های صورت‌گرفته، همچنان در زمینه مقابله با فیشینگ و استفاده از فناوری‌های نوین در کلاهبرداری، خلأهای قانونی و اجرایی وجود دارد.با توجه به این پیشینه، پرسش‌های اصلی تحقیق حاضر عبارتند از: ۱) چه خلأهای قانونی در نظام حقوقی ایران در مواجهه با فیشینگ و استفاده از فناوری‌های نوین در کلاهبرداری وجود دارد؟ ۲) راهکارهای حقوقی مؤثر برای مقابله با این تهدیدات چیست؟ اهداف این مقاله شامل تحلیل ابعاد حقوقی فیشینگ، شناسایی خلأهای قانونی و ارائه پیشنهادات اصلاحی است. روش پژوهش به‌کاررفته در این مقاله، تحلیلی-توصیفی و تطبیقی است که با استفاده از منابع معتبر حقوقی و فقهی، به بررسی و تحلیل موضوع می‌پردازد.در نهایت، این مقاله با استناد به منابع معتبر و با رعایت اصول نگارش علمی، به بررسی جامع و تحلیلی موضوع پرداخته و راهکارهای حقوقی مؤثری را برای مقابله با فیشینگ و استفاده از فناوری‌های نوین در کلاهبرداری ارائه خواهد داد.

فناوری‌های نوین

فناوری‌های نوین به مجموعه‌ای از ابزارها، سامانه‌ها و فناوری‌هایی اطلاق می‌شوند که در دهه‌های اخیر با پیشرفت‌های چشمگیر علمی و صنعتی توسعه یافته‌اند و تأثیرات عمیقی بر زندگی فردی، اجتماعی، اقتصادی و حقوقی انسان‌ها داشته‌اند (رضایی، ۱۳۹۸). این فناوری‌ها شامل هوش مصنوعی، اینترنت اشیاء، بلاک‌چین، رباتیک، محاسبات ابری و فناوری‌های مرتبط با پردازش داده‌های بزرگ می‌باشند و به‌طور گسترده در صنایع، خدمات مالی، پزشکی، آموزشی، نظامی و بخش‌های مختلف حکومتی مورد استفاده قرار می‌گیرند.

Archive of SID.ir

Archive of SID.ir

یکی از ویژگی‌های شاخص فناوری‌های نوین، توانایی آن‌ها در ایجاد تحول اساسی در فرآیندهای سنتی و مدل‌های مرسوم کسب‌وکار و زندگی اجتماعی است (کریمی و موسوی، ۱۳۹۹). به‌طور مثال، در حوزه خدمات مالی، فناوری بلاک‌چین با قابلیت ثبت غیرقابل تغییر تراکنش‌ها و شفافیت سیستم، امنیت و اعتماد کاربران را افزایش داده است و در عین حال، چالش‌های قانونی جدیدی را نیز ایجاد کرده است (احمدی، ۱۳۹۷). از منظر حقوقی، ورود فناوری‌های نوین به عرصه‌های مختلف، به ویژه در فضای دیجیتال، موجب پدید آمدن مسائل تازه‌ای از قبیل حفاظت از داده‌های شخصی، مالکیت معنوی، مسئولیت مدنی و کیفری و محدودیت‌های قانونی برای استفاده از این فناوری‌ها شده است.یکی دیگر از ابعاد مهم فناوری‌های نوین، تأثیر آن‌ها بر فرآیند تصمیم‌گیری و اتوماسیون عملیات است. به‌طور نمونه، هوش مصنوعی و الگوریتم‌های پیشرفته قادر به تحلیل حجم عظیمی از داده‌ها هستند و تصمیمات پیچیده را با دقت و سرعت بالا اتخاذ می‌کنند. این ویژگی، در کنار مزایای اقتصادی و عملیاتی، مسأله مسئولیت قانونی تصمیمات گرفته‌شده توسط سیستم‌های خودکار را مطرح می‌کند. به عبارت دیگر، وقتی یک سیستم هوش مصنوعی تصمیمی اتخاذ می‌کند که منجر به خسارت یا تضییع حقوق اشخاص شود، تعیین مسئولیت قانونی آن، یکی از چالش‌های اساسی حقوق مدرن است (محمدی، ۱۳۹۸).علاوه بر این، اینترنت اشیاء به‌عنوان بخشی از فناوری‌های نوین، شبکه‌ای از دستگاه‌ها و حسگرهای هوشمند است که قادر به تبادل اطلاعات به صورت خودکار می‌باشند. این فناوری به بهبود کارایی سیستم‌های صنعتی، مدیریت شهری، بهداشت و سلامت، حمل‌ونقل و انرژی کمک می‌کند، اما همزمان نگرانی‌های حقوقی و امنیتی نیز ایجاد می‌نماید. از منظر قانونی، جمع‌آوری و پردازش داده‌های گسترده توسط دستگاه‌های متصل به اینترنت اشیاء، مسأله رعایت حریم خصوصی و حفاظت از داده‌های شخصی را به سطحی بی‌سابقه ارتقاء داده است (یوسفی، ۱۴۰۰).

فناوری رباتیک نیز یکی دیگر از اجزای اصلی فناوری‌های نوین است که در صنایع تولیدی، پزشکی، نظامی و خدماتی به‌کار گرفته می‌شود. ربات‌ها، با انجام فعالیت‌های فیزیکی و عملیاتی که پیش‌تر توسط انسان انجام می‌شد، بهره‌وری را افزایش داده و هزینه‌ها را کاهش می‌دهند، اما این امر همچنین مسأله مسئولیت حقوقی و اخلاقی اعمال آن‌ها را نیز مطرح می‌کند. به‌طور مثال، اگر رباتی در یک کارخانه موجب آسیب به کارکنان شود، تعیین مسئولیت قانونی بین تولیدکننده، برنامه‌نویس و کارفرما، یکی از چالش‌های جدی حقوقی است (ابراهیمی، ۱۳۹۹).یکی از ویژگی‌های مشترک فناوری‌های نوین، سرعت بالای تحول و پیچیدگی فنی آن‌ها است. این ویژگی باعث شده است که قوانین موجود در بسیاری از کشورها، از جمله ایران، قادر به پاسخگویی سریع به تغییرات نباشند و همواره بین توسعه فناوری و چارچوب‌های قانونی، فاصله‌ای محسوس ایجاد شود. به همین دلیل، بسیاری از پژوهشگران بر لزوم بازنگری و تدوین قوانین نوین با رویکرد آینده‌نگر و منعطف تأکید کرده‌اند (حسینی، ۱۳۹۷).

از منظر اجتماعی، فناوری‌های نوین نحوه تعامل انسان‌ها با محیط دیجیتال و یکدیگر را دگرگون کرده‌اند. شبکه‌های اجتماعی مبتنی بر الگوریتم‌های پیچیده و هوش مصنوعی، اطلاعات را در کسری از ثانیه منتشر و پخش می‌کنند، که این امر علاوه بر فرصت‌های اقتصادی و آموزشی، خطر سوءاستفاده و انتشار اطلاعات نادرست یا فیشینگ را نیز افزایش می‌دهد (موسوی، ۱۳۹۹). بنابراین، فناوری‌های نوین نه تنها فرصت‌های عظیم توسعه و پیشرفت را فراهم آورده‌اند، بلکه چالش‌های امنیتی، حقوقی و اخلاقی متعددی را نیز ایجاد کرده‌اند که نیازمند تحلیل و تدوین چارچوب‌های قانونی مناسب می‌باشد.

Archive of SID.ir

Archive of SID.ir

می‌توان گفت فناوری‌های نوین به‌عنوان محرکی برای توسعه اقتصادی و اجتماعی، همزمان یک فضای پیچیده حقوقی و امنیتی ایجاد کرده‌اند. بهره‌گیری مؤثر و ایمن از این فناوری‌ها مستلزم تدوین سیاست‌ها و مقررات حقوقی دقیق، نظارت مؤثر، و ایجاد فرهنگ امنیت اطلاعات در جامعه است. پژوهش‌ها نشان داده‌اند که عدم وجود چارچوب‌های قانونی مناسب، می‌تواند زمینه سوءاستفاده‌های گسترده‌ای از فناوری‌های نوین را فراهم کند و امنیت کاربران و شهروندان را تهدید نماید (رضایی، ۱۳۹۸؛ احمدی، ۱۳۹۷).

به طور خلاصه، فناوری‌های نوین شامل مجموعه‌ای از فناوری‌های پیشرفته است که زندگی انسان را متحول کرده و فرصت‌ها و چالش‌های متعددی را ایجاد نموده است. از دیدگاه حقوقی، این فناوری‌ها نیازمند تحلیل دقیق، بازنگری قوانین موجود، و تدوین مقررات جدید هستند تا بتوانند ضمن بهره‌برداری از مزایای فناوری، از تهدیدات و سوءاستفاده‌ها جلوگیری کنند.

فیشینگ

فیشینگ یکی از رایج‌ترین و پیچیده‌ترین روش‌های کلاهبرداری سایبری است که در دهه‌های اخیر با گسترش اینترنت و فناوری‌های دیجیتال، اهمیت و گستردگی بیشتری یافته است. این اصطلاح به تکنیک‌هایی اطلاق می‌شود که مجرمان سایبری با استفاده از ایمیل‌ها، وب‌سایت‌های جعلی، پیامک‌ها یا سایر ابزارهای ارتباطی، کاربران را فریب می‌دهند و اطلاعات حساس آن‌ها شامل نام کاربری، رمز عبور، اطلاعات مالی یا سایر داده‌های شخصی را به سرقت می‌برند (حسینی و کریمی، ۱۳۹۸). فیشینگ بر پایه مهندسی اجتماعی بنا شده است، یعنی مجرمان با بهره‌گیری از روان‌شناسی انسانی، اعتماد کاربران را جلب کرده و آن‌ها را به اقداماتی وادار می‌کنند که به نفع خود مجرمان تمام می‌شود.

یکی از دلایل گسترش فیشینگ، سهولت دسترسی به ابزارهای دیجیتال و افزایش تراکم اطلاعات در فضای مجازی است. کاربران روزانه با حجم زیادی از پیام‌ها و ایمیل‌ها مواجه هستند و توانایی تشخیص پیام‌های جعلی کاهش یافته است. این وضعیت فرصت مناسبی برای مجرمان سایبری ایجاد می‌کند تا با استفاده از تکنیک‌های پیشرفته، فیشینگ را انجام دهند (رضایی، ۱۳۹۹). تکنیک‌های مدرن فیشینگ شامل ارسال ایمیل‌های مشابه به سرویس‌های بانکی، ایجاد وب‌سایت‌های جعلی که شبیه وب‌سایت‌های رسمی هستند، یا حتی استفاده از شبکه‌های اجتماعی برای جلب اعتماد قربانیان می‌شود.

فیشینگ از منظر حقوقی، به‌عنوان نوعی کلاهبرداری دیجیتال شناخته می‌شود و تحت پوشش قوانین مربوط به جرایم رایانه‌ای و حفاظت از داده‌های شخصی قرار می‌گیرد. در نظام حقوقی ایران، ماده ۹ قانون جرایم رایانه‌ای مصوب ۱۳۸۸ به‌طور کلی به کلاهبرداری رایانه‌ای پرداخته است، اما به‌طور خاص به فیشینگ اشاره‌ای نشده است (محمدی، ۱۳۹۸). این مسأله نشان‌دهنده نیاز به بازنگری قوانین و ایجاد مقررات خاص برای مقابله با فیشینگ است. برخی حقوقدانان بر این باورند که فیشینگ می‌تواند در قالب جرایم متعدد نظیر جعل، کلاهبرداری و نقض حریم خصوصی مورد رسیدگی قرار گیرد (ابراهیمی، ۱۳۹۹).

فیشینگ علاوه بر بعد حقوقی، دارای ابعاد اقتصادی و اجتماعی نیز هست. هر ساله میلیاردها دلار خسارت مالی ناشی از فیشینگ به افراد، سازمان‌ها و دولت‌ها وارد می‌شود (احمدی، ۱۳۹۷). علاوه بر خسارت مستقیم مالی، اعتماد عمومی به سیستم‌های دیجیتال و خدمات آنلاین کاهش می‌یابد و هزینه‌های اضافی برای بازسازی سیستم‌های امنیتی و جبران خسارت‌ها ایجاد می‌شود. از این رو، فیشینگ به یک تهدید جدی برای امنیت سایبری و ثبات اقتصادی تبدیل شده

Archive of SID.ir

Archive of SID.ir

است.با ظهور فناوری‌های نوین، فیشینگ نیز پیچیده‌تر و هوشمندانه‌تر شده است. استفاده از هوش مصنوعی، یادگیری ماشین و تحلیل داده‌ها، امکان طراحی حملات فیشینگ هدفمند و شخصی‌سازی شده را فراهم کرده است. برای مثال، الگوریتم‌های هوش مصنوعی قادرند رفتار کاربر را تحلیل کرده و پیام‌های جعلی را به گونه‌ای طراحی کنند که احتمال موفقیت حمله به حداکثر برسد (کریمی و موسوی، ۱۳۹۹). این تحول، علاوه بر افزایش پیچیدگی فنی فیشینگ، چالش‌های حقوقی جدیدی ایجاد کرده است که قوانین موجود به‌طور کامل قادر به پوشش آن‌ها نیستند.

فیشینگ همچنین با ابعاد اجتماعی و روان‌شناختی قابل تحلیل است. مجرمان با بهره‌گیری از احساسات کاربران مانند ترس، طمع یا اضطرار، آن‌ها را به اقداماتی وادار می‌کنند که اطلاعات حساس خود را در اختیار مجرمان قرار دهند. از منظر حقوقی، این مسأله مسئولیت و تقصیر قربانیان را تغییر نمی‌دهد، اما در طراحی سیاست‌های پیشگیرانه و آموزش کاربران اهمیت دارد (یوسفی، ۱۴۰۰). پژوهش‌ها نشان داده‌اند که آموزش کاربران و افزایش آگاهی آن‌ها نسبت به تکنیک‌های فیشینگ، می‌تواند تا حد زیادی موفقیت این حملات را کاهش دهد.یکی دیگر از جنبه‌های مهم فیشینگ، مسئولیت سازمان‌ها و ارائه‌دهندگان خدمات است. طبق دکترین حقوقی، سازمان‌ها موظف‌اند تدابیر امنیتی لازم برای محافظت از داده‌های کاربران خود را اتخاذ کنند. در صورت کوتاهی یا بی‌توجهی به این مسئولیت، سازمان‌ها ممکن است از نظر مدنی یا کیفری پاسخگو باشند (رضایی، ۱۳۹۸). این مسئولیت‌ها شامل استفاده از فناوری‌های امنیتی، آموزش کارکنان، طراحی سیستم‌های مقاوم در برابر فیشینگ و نظارت مستمر بر فعالیت‌های مشکوک است.

فیشینگ در سطح بین‌المللی نیز مورد توجه پژوهشگران و سازمان‌های حقوقی قرار گرفته است. مطالعات تطبیقی نشان می‌دهد که کشورهایی مانند ایالات متحده، کانادا و کشورهای اروپایی قوانین جامع‌تری برای مقابله با فیشینگ تدوین کرده‌اند که شامل الزام شرکت‌ها به رعایت امنیت داده‌ها، شفاف‌سازی اطلاعات و مجازات‌های شدید برای مرتکبان است (محمدی، ۱۳۹۸). تجربه این کشورها می‌تواند برای طراحی چارچوب قانونی مناسب در ایران، آموزنده باشد و به کاهش آسیب‌های فیشینگ کمک کند.

به طور خلاصه، فیشینگ به‌عنوان یکی از مهم‌ترین تهدیدات سایبری، نیازمند تحلیل جامع و چندبعدی است. این تحلیل شامل ابعاد فنی، حقوقی، اقتصادی و اجتماعی می‌شود. بهره‌گیری از فناوری‌های نوین، افزایش آگاهی کاربران و تدوین قوانین و مقررات مؤثر، از مهم‌ترین راهکارهای مقابله با فیشینگ هستند. پژوهش‌های اخیر نشان داده‌اند که تنها ترکیب این راهکارها می‌تواند به حفاظت از کاربران و کاهش خسارت‌های مالی و اجتماعی کمک کند (حسینی و کریمی، ۱۳۹۸؛ احمدی، ۱۳۹۷).

هوش مصنوعی

هوش مصنوعی به سامانه‌ها و نرم‌افزارهایی اطلاق می‌شود که قادر به انجام وظایفی هستند که معمولاً نیاز به هوش انسانی دارند، مانند یادگیری، استدلال، شناسایی الگوها، تصمیم‌گیری و حل مسئله (محمدی، ۱۳۹۹). این فناوری در دهه‌های اخیر به یکی از پیشرفته‌ترین ابزارهای فناوری‌های نوین تبدیل شده و تأثیرات گسترده‌ای بر صنایع، اقتصاد، جامعه و نظام‌های حقوقی گذاشته است. هوش مصنوعی به‌طور کلی شامل شاخه‌های مختلفی مانند یادگیری ماشین، یادگیری عمیق، پردازش زبان طبیعی، بینایی ماشین و سیستم‌های خبره می‌باشد که هر یک کاربردهای خاص خود را دارند (کریمی و موسوی، ۱۳۹۹).یکی از ویژگی‌های مهم هوش مصنوعی، توانایی تحلیل حجم عظیمی از داده‌ها با سرعت و دقت بسیار بالاست. این ویژگی، بهره‌وری در بخش‌های اقتصادی و خدماتی را افزایش داده و امکان پیش‌بینی رفتارها و

Archive of SID.ir

Archive of SID.ir

الگوهای مختلف را فراهم کرده است. به عنوان مثال، در بخش مالی، الگوریتم‌های هوش مصنوعی قادرند ریسک تراکنش‌ها را ارزیابی کرده و احتمال وقوع تقلب یا فیشینگ را پیش‌بینی کنند (احمدی، ۱۳۹۸). در حوزه سلامت، هوش مصنوعی در تشخیص بیماری‌ها، تجویز دارو و مدیریت پرونده‌های پزشکی مورد استفاده قرار می‌گیرد. اما هرچقدر مزایای این فناوری گسترده باشد، چالش‌های حقوقی و اخلاقی مرتبط با آن نیز پیچیده‌تر می‌شود.

از منظر حقوقی، هوش مصنوعی مسأله مسئولیت را وارد حوزه‌ای پیچیده کرده است. وقتی سامانه‌ای خودکار تصمیمی اتخاذ می‌کند که منجر به خسارت یا تضییع حقوق شخص ثالث شود، تعیین مسئولیت قانونی بین سازنده، برنامه‌نویس، مالک یا کاربر، موضوعی پیچیده است (ابراهیمی، ۱۳۹۹). این پرسش‌ها شامل مواردی مانند مسئولیت مدنی، مسئولیت کیفری و حتی مسئولیت اخلاقی می‌شود. برخی حقوقدانان بر این باورند که باید چارچوب‌های قانونی جدیدی طراحی شود که مسئولیت تصمیمات هوش مصنوعی را مشخص کند و خلأهای قانونی موجود را پوشش دهد (رضایی، ۱۳۹۸).

هوش مصنوعی در زمینه امنیت سایبری و مقابله با جرایم اینترنتی نیز نقش مهمی ایفا می‌کند. الگوریتم‌های پیشرفته می‌توانند الگوهای مشکوک فعالیت‌های کاربران را شناسایی کرده و حملات سایبری، از جمله فیشینگ، را به صورت خودکار شناسایی و مسدود کنند (حسینی، ۱۳۹۹). با این حال، مجرمان نیز از هوش مصنوعی برای ارتکاب جرایم پیچیده استفاده می‌کنند و پیام‌ها یا وب‌سایت‌های فیشینگ خود را هوشمندانه‌تر طراحی می‌کنند تا شانس موفقیت حمله افزایش یابد. این مسأله، چالش‌های قانونی و امنیتی جدی ایجاد کرده و نشان‌دهنده ضرورت بازنگری قوانین در این حوزه است.

از منظر اقتصادی، هوش مصنوعی به کاهش هزینه‌های عملیاتی، بهینه‌سازی فرآیندها و افزایش بهره‌وری کمک می‌کند. با این حال، سوءاستفاده از این فناوری می‌تواند خسارات مالی و اجتماعی گسترده‌ای ایجاد کند. به عنوان مثال، استفاده از الگوریتم‌های خودکار برای فریب کاربران یا دستکاری داده‌ها می‌تواند ضررهای مالی هنگفتی به سازمان‌ها و افراد وارد نماید (یوسفی، ۱۴۰۰). بنابراین، تدوین سیاست‌ها و مقررات اقتصادی و حقوقی برای نظارت بر کاربردهای هوش مصنوعی ضروری است.

از دیدگاه فقهی و اخلاقی، هوش مصنوعی نیز مسائل جدیدی مطرح کرده است. به طور خاص، استفاده از هوش مصنوعی برای تصمیم‌گیری در امور حیاتی مانند سلامت، قضاوت و آموزش، پرسش‌هایی درباره عدالت، انصاف و مسئولیت ایجاد کرده است. فقه اسلامی و دکترین حقوقی باید بررسی کنند که در چه مواردی تصمیمات خودکار با اصول اخلاقی و قانونی هم‌خوانی دارد و در چه مواردی نیازمند دخالت انسان است (محمدی، ۱۳۹۹).

هوش مصنوعی همچنین در ارتکاب جرایم سایبری مانند فیشینگ نقش دوگانه دارد: هم به‌عنوان ابزار پیشگیری و هم به‌عنوان ابزار ارتکاب جرم. این موضوع باعث شده است که محققان و قانون‌گذاران بر اهمیت تدوین قوانین تطبیقی و بین‌المللی تأکید کنند. تجربه کشورهای پیشرفته نشان می‌دهد که ایجاد استانداردهای بین‌المللی برای کاربردهای هوش مصنوعی، شفاف‌سازی مسئولیت‌ها و نظارت بر عملکرد سیستم‌ها، می‌تواند تهدیدات ناشی از سوءاستفاده‌ها را کاهش دهد (رضایی، ۱۳۹۹).

به طور خلاصه، هوش مصنوعی یک فناوری پیشرفته و پیچیده است که تأثیرات گسترده‌ای بر زندگی انسان‌ها، اقتصاد و نظام‌های حقوقی دارد. بهره‌گیری مؤثر و ایمن از این فناوری نیازمند چارچوب‌های حقوقی روشن، مقررات اخلاقی دقیق، آموزش کاربران و ایجاد سیستم‌های نظارتی قوی است. هوش مصنوعی، اگرچه فرصت‌های بسیاری برای پیشرفت

Archive of SID.ir

Archive of SID.ir

و توسعه ایجاد می‌کند، در عین حال چالش‌ها و تهدیدات جدیدی برای امنیت، حقوق افراد و مسئولیت قانونی به همراه دارد (کریمی و موسوی، ۱۳۹۹؛ ابراهیمی، ۱۳۹۹).

اتوماسیون

اتوماسیون به معنای استفاده از فناوری‌ها برای انجام خودکار وظایف و فرآیندها بدون نیاز به دخالت انسانی است و به‌عنوان یکی از شاخص‌ترین مؤلفه‌های فناوری‌های نوین شناخته می‌شود (رضایی، ۱۳۹۸). این فناوری در صنایع تولیدی، خدماتی، مالی، حمل‌ونقل، بهداشت و حتی در بخش‌های دولتی و حقوقی مورد استفاده قرار می‌گیرد و توانسته است به طور قابل توجهی بهره‌وری، دقت و سرعت اجرای فرآیندها را افزایش دهد (کریمی و موسوی، ۱۳۹۹). اتوماسیون شامل انواع مختلفی است، از جمله اتوماسیون صنعتی، اتوماسیون اداری، اتوماسیون خدمات مالی و اتوماسیون فرآیندهای قانونی و حقوقی.

یکی از ویژگی‌های مهم اتوماسیون، کاهش وابستگی به نیروی انسانی و افزایش کارایی است. به عنوان مثال، در خطوط تولید، ربات‌ها و سیستم‌های خودکار قادرند فرآیندهای پیچیده و تکراری را با دقت بالا و بدون خطا انجام دهند، که این امر موجب کاهش هزینه‌ها و افزایش کیفیت محصولات می‌شود (احمدی، ۱۳۹۷). در بخش خدمات، اتوماسیون موجب ساده‌سازی فرآیندهای اداری، کاهش زمان پردازش و افزایش شفافیت می‌شود. به عنوان نمونه، سیستم‌های اتوماسیون بانکی و پرداخت‌های الکترونیکی، تراکنش‌ها را به‌صورت سریع و دقیق انجام می‌دهند و ریسک خطای انسانی را کاهش می‌دهند.با این حال، اتوماسیون نیز با چالش‌ها و پیچیدگی‌های حقوقی همراه است. زمانی که فرآیندها به‌صورت خودکار اجرا می‌شوند، سوالاتی در خصوص مسئولیت قانونی و پاسخگویی ایجاد می‌شود. اگر یک سیستم اتوماسیون، به‌طور نادرست عمل کرده و موجب خسارت مالی یا نقض حقوق افراد شود، تعیین مسئولیت بین سازنده، برنامه‌نویس، کاربر یا مدیر سیستم، یکی از مهم‌ترین چالش‌های حقوقی است (ابراهیمی، ۱۳۹۹). این پرسش‌ها در حوزه‌های مسئولیت مدنی، مسئولیت کیفری و حتی مسئولیت اخلاقی مطرح می‌شوند و نیازمند تدوین قوانین و چارچوب‌های جدید است.

از منظر اقتصادی، اتوماسیون مزایای فراوانی دارد. کاهش هزینه‌ها، افزایش سرعت و دقت، کاهش خطای انسانی و بهینه‌سازی منابع، از مهم‌ترین اثرات مثبت آن است (محمدی، ۱۳۹۹). در عین حال، استفاده گسترده از اتوماسیون می‌تواند منجر به کاهش اشتغال در برخی حوزه‌ها شود و نیازمند سیاست‌های اقتصادی و اجتماعی مناسب برای جبران این اثرات باشد. این موضوع به ویژه در کشورهایی که بخش بزرگی از اقتصادشان به نیروی انسانی وابسته است، اهمیت بیشتری پیدا می‌کند.

اتوماسیون همچنین نقش مهمی در امنیت سایبری و مقابله با جرایم دیجیتال دارد. بسیاری از فرآیندهای تشخیص و پیشگیری از حملات سایبری، از جمله فیشینگ، از طریق سیستم‌های اتوماسیون انجام می‌شوند. الگوریتم‌ها و سیستم‌های خودکار قادرند فعالیت‌های مشکوک را به‌سرعت شناسایی کرده و اقدامات پیشگیرانه انجام دهند، که این امر توان دفاع سایبری را به طور قابل توجهی افزایش می‌دهد (حسینی، ۱۳۹۹). با این حال، مجرمان نیز از فناوری‌های اتوماسیون برای ارتکاب جرایم پیچیده و هدفمند استفاده می‌کنند و این مسأله چالش‌های قانونی و امنیتی جدیدی ایجاد می‌کند.

از دیدگاه حقوقی، اتوماسیون نیازمند توجه ویژه به مسئولیت‌ها و ضمانت اجراها است. ماده ۹ قانون جرایم رایانه‌ای مصوب ۱۳۸۸، به‌طور کلی به کلاهبرداری و تقلب رایانه‌ای پرداخته است، اما مسائلی که ناشی از عملکرد خودکار سیستم‌های اتوماسیون هستند، به‌طور کامل تحت پوشش این قانون قرار نمی‌گیرند (رضایی، ۱۳۹۸). بنابراین، نیاز به

Archive of SID.ir

Archive of SID.ir

بازنگری و اصلاح قوانین موجود با هدف تطبیق با فناوری‌های اتوماسیون وجود دارد.یکی دیگر از جنبه‌های مهم اتوماسیون، تأثیر آن بر فرآیندهای حقوقی و قضایی است. استفاده از سیستم‌های اتوماسیون در دادگاه‌ها، ثبت اسناد، پیگیری پرونده‌ها و مدیریت پرونده‌های قضایی، سرعت و دقت کار را افزایش داده است (یوسفی، ۱۴۰۰). با این حال، تصمیمات اتوماتیک و خودکار در فرآیندهای قضایی می‌تواند چالش‌های اخلاقی و قانونی ایجاد کند. به عنوان مثال، اگر یک سامانه اتوماسیون برای صدور تصمیم قضایی یا تحلیل پرونده‌ها مورد استفاده قرار گیرد، باید روشن شود که چه کسی مسئول اشتباهات یا نواقص احتمالی است و چه مکانیسم‌های نظارتی باید وجود داشته باشد.

اتوماسیون از منظر اجتماعی نیز تأثیرات گسترده‌ای دارد. کاهش خطای انسانی، افزایش سرعت ارائه خدمات و بهبود کیفیت، مزایای آشکار آن است. اما در کنار این مزایا، نگرانی‌های اجتماعی از جمله افزایش بیکاری در برخی بخش‌ها، کاهش تعامل انسانی و ایجاد وابستگی بیش از حد به سیستم‌های خودکار نیز مطرح است (کریمی و موسوی، ۱۳۹۹). بنابراین، اتوماسیون باید همراه با برنامه‌های آموزشی و سیاست‌های حمایتی برای مدیریت اثرات اجتماعی آن به‌کار گرفته شود.

بنابراین می توان گفت، اتوماسیون به عنوان یکی از مهم‌ترین مؤلفه‌های فناوری‌های نوین، نقش حیاتی در بهبود کارایی، افزایش بهره‌وری و کاهش خطای انسانی دارد. با این حال، همراه با مزایای اقتصادی و عملیاتی، چالش‌های حقوقی، امنیتی و اجتماعی نیز ایجاد می کند. بهره‌گیری مؤثر از اتوماسیون مستلزم تدوین چارچوب‌های قانونی و مقررات حقوقی روشن، ایجاد سیستم‌های نظارتی مؤثر و آموزش کاربران و کارکنان است تا بتوان ضمن استفاده از مزایای آن، تهدیدات و سوءاستفاده‌های احتمالی را کاهش داد (رضایی، ۱۳۹۸؛ ابراهیمی، ۱۳۹۹).

مبانی نظری و نظریه‌های حقوقی

برای تحلیل علمی و جامع موضوع فناوری‌های نوین و فیشینگ، ابتدا باید مبانی نظری مختلف آن مورد بررسی قرار گیرد. این مبانی شامل فلسفه حقوق، فقه اسلامی، حقوق مدنی و کیفری، و نظریه‌های اقتصادی است که به شکل تطبیقی، ابعاد موضوع را روشن می‌سازد (رضایی، ۱۳۹۸).از منظر فلسفه حقوق، یکی از محورهای مهم، مسأله مسئولیت و عدالت در استفاده از فناوری‌های نوین است. فلسفه حقوق به بررسی این پرسش می‌پردازد که آیا انسان‌ها مسئول تصمیمات سامانه‌های خودکار هستند یا سیستم‌های هوش مصنوعی نیز می‌توانند دارای مسئولیت اخلاقی و قانونی باشند (محمدی، ۱۳۹۹). این پرسش در زمینه جرایم فیشینگ و سوءاستفاده‌های فناوری‌های نوین اهمیت می‌یابد، زیرا تصمیمات هوش مصنوعی یا سیستم‌های اتوماسیون می‌تواند مستقیماً موجب ضرر مالی یا تضییع حقوق افراد شود. بنابراین، فلسفه حقوق مبنایی برای تدوین چارچوب‌های قانونی و اخلاقی فراهم می‌آورد که مسئولیت‌ها را در عرصه دیجیتال روشن کند.از دیدگاه فقه اسلامی، استفاده از فناوری برای ارتکاب جرایم، از جمله فیشینگ، می‌تواند مصداق غصب، کلاهبرداری و سرقت باشد. فقه اسلامی بر رعایت حقوق دیگران، حفظ امانت و جلوگیری از ضرر تأکید دارد و هرگونه فریب، تحصیل مال از طریق شیوه‌های غیرمشروع و تضییع حقوق مردم، مورد نهی قرار گرفته است (ابراهیمی، ۱۳۹۹). در این زمینه، تطبیق اصول فقهی با فناوری‌های نوین و جرایم سایبری نیازمند بررسی دقیق و به‌روزرسانی است، به گونه‌ای که معیارهای عدالت، تقصیر و مسئولیت فردی در محیط دیجیتال مشخص شود.

در حوزه حقوق مدنی و کیفری، مواد قانونی ایران به‌ویژه قانون جرایم رایانه‌ای مصوب ۱۳۸۸، به جرایم سایبری و کلاهبرداری اشاره کرده‌اند. ماده ۹ این قانون به کلاهبرداری رایانه‌ای پرداخته و مجازات‌هایی برای آن تعیین کرده

Archive of SID.ir

Archive of SID.ir

است، اما به‌طور خاص به استفاده از فناوری‌های نوین و حملات فیشینگ اشاره نکرده است (رضایی، ۱۳۹۸). ماده ۱۰ همین قانون، مسئولیت ناشی از دسترسی غیرمجاز به اطلاعات و داده‌ها را مورد توجه قرار داده است و ماده ۱۱، نحوه رسیدگی قضایی به جرایم سایبری را مشخص کرده است. با توجه به پیشرفت فناوری، نیاز به بازنگری و ایجاد تبصره‌ها و مواد جدید برای پوشش جرایم نوظهور احساس می‌شود.

از منظر اقتصادی، تحلیل هزینه و منفعت فناوری‌های نوین و آثار ناشی از سوءاستفاده‌های آن ضروری است. جرایم سایبری، به ویژه فیشینگ، هزینه‌های مستقیم و غیرمستقیم فراوانی ایجاد می‌کنند که شامل خسارت مالی، کاهش اعتماد عمومی، هزینه‌های قانونی و هزینه‌های مربوط به بازسازی سیستم‌ها است (احمدی، ۱۳۹۷). بنابراین، مبانی اقتصادی برای تدوین سیاست‌ها و مقررات امنیت اطلاعات اهمیت دارد و به قانون‌گذار کمک می‌کند که تصمیمات مبتنی بر داده‌ها و تحلیل هزینه-فایده اتخاذ کند.

در حوزه نظریه‌های حقوقی دکترین، چند دیدگاه اصلی مطرح است که می‌تواند برای تحلیل مسئولیت و مجازات جرایم سایبری به کار گرفته شود:

۱. نظریه مسئولیت بر اساس تقصیر: بر اساس این نظریه، مسئولیت تنها زمانی ایجاد می‌شود که فرد مرتکب تقصیر شده باشد. در جرایم سایبری، این نظریه در مواردی کاربرد دارد که فرد عمداً یا به‌سبب بی‌احتیاطی موجب ضرر شود (محمدی، ۱۳۹۹).

۲. نظریه مسئولیت بدون تقصیر (مسئولیت محض): این نظریه مسئولیت را فارغ از تقصیر فرد قائل می‌شود و در مواردی نظیر خسارت‌های ناشی از فناوری‌های خودکار یا زیان‌های ناشی از محصولات دیجیتال به کار گرفته می‌شود (ابراهیمی، ۱۳۹۹).

۳. نظریه مسئولیت کارفرما: در این نظریه، کارفرما در قبال اعمال کارکنان خود مسئول است. در زمینه جرایم سایبری، این دیدگاه می‌تواند در مواردی که حمله سایبری یا فیشینگ توسط کارکنان سازمان یا به نام سازمان رخ می‌دهد، اعمال شود (حسینی، ۱۳۹۹).

۴. نظریه مسئولیت ترکیبی: برخی حقوقدانان پیشنهاد کرده‌اند که در مواجهه با فناوری‌های نوین، مسئولیت باید ترکیبی از تقصیر فردی، مسئولیت کارفرما و الزامات فنی سیستم‌های خودکار باشد تا پاسخگوی پیچیدگی‌های فناوری باشد (رضایی، ۱۳۹۹).

علاوه بر این، دکترین حقوقی به مسأله پیشگیری و الزامات امنیتی برای مقابله با جرایم سایبری تأکید دارد. بسیاری از حقوقدانان پیشنهاد کرده‌اند که سازمان‌ها باید الزامات مشخصی برای محافظت از داده‌ها و جلوگیری از فیشینگ و سایر حملات سایبری اتخاذ کنند. عدم رعایت این الزامات می‌تواند موجب مسئولیت مدنی یا کیفری شود (کریمی و موسوی، ۱۳۹۹).

مبانی فلسفی

در فلسفه اخلاق و فلسفه حقوق، یکی از پرسش‌های محوری این است که مسئولیت اعمال انسانی چگونه تعریف می‌شود و این تعریف چگونه با ورود فناوری‌های نوین و سیستم‌های هوش مصنوعی دستخوش تغییر می‌شود. در دنیای سنتی، مسئولیت اخلاقی و حقوقی به انسان نسبت داده می‌شود، زیرا اعمال فرد ناشی از اراده و تصمیمات اوست و قابلیت انتخاب بین درست و نادرست وجود دارد (رضایی، ۱۳۹۸). اما با ظهور فناوری‌های نوین، به ویژه هوش مصنوعی و

Archive of SID.ir

Archive of SID.ir

سیستم‌های اتوماسیون، این سوال مطرح می‌شود که آیا می‌توان بخشی از مسئولیت ناشی از نتایج عملکرد سیستم‌های خودکار را به خود فناوری نسبت داد یا مسئولیت همچنان تنها بر عهده انسان‌هاست؟

یکی از جریان‌های مهم در فلسفه اخلاق که به این پرسش مرتبط است، نظریه مسئولیت عقلانی و اراده آزاد است. بر اساس این نظریه، مسئولیت تنها زمانی ایجاد می‌شود که عامل بتواند بین گزینه‌های مختلف تصمیم‌گیری کند و عمل او ناشی از اراده آزاد او باشد (محمدی، ۱۳۹۹). در مورد سیستم‌های هوش مصنوعی، با توجه به اینکه تصمیمات این سامانه‌ها بر اساس الگوریتم‌ها و داده‌های ورودی شکل می‌گیرند و فاقد اراده آزاد هستند، بسیاری از فلاسفه و حقوقدانان معتقدند که مسئولیت اخلاقی مستقیم به سیستم‌ها قابل نسبت دادن نیست. بلکه مسئولیت باید به طراحان، برنامه‌نویسان، کاربران یا سازمان‌هایی که سیستم‌ها را کنترل می‌کنند، نسبت داده شود.

با این حال، برخی اندیشمندان فلسفه اخلاق، نظریه‌های مسئولیت توزیع‌شده را پیشنهاد کرده‌اند. این نظریه معتقد است که مسئولیت می‌تواند بین انسان و فناوری توزیع شود، به شرطی که فناوری نقش مؤثری در تصمیم‌گیری و اجرای عمل داشته باشد (ابراهیمی، ۱۳۹۹). برای مثال، اگر یک سامانه هوش مصنوعی به صورت خودکار تصمیم به ارسال پیام‌های فیشینگ یا پردازش نادرست اطلاعات کاربران بگیرد، در حالی که طراحان سیستم تدابیر کنترلی کافی اعمال نکرده‌اند، مسئولیت می‌تواند بین طراح، سازمان و سیستم توزیع شود. این دیدگاه، چالش‌های جدیدی برای فلسفه حقوق و اخلاق ایجاد می‌کند، زیرا سنت حقوقی به «عامل انسانی» به‌عنوان تنها حامل مسئولیت عادت دارد.

یکی دیگر از مبانی فلسفی مرتبط، نظریه پیامدگرایی و اخلاق نتیجه‌گرا است. این نظریه بر اساس تأثیرات و پیامدهای عمل تصمیم‌گیری، مسئولیت را مورد ارزیابی قرار می‌دهد (کریمی و موسوی، ۱۳۹۹). از این منظر، اگر عملکرد فناوری‌های نوین منجر به تضییع حقوق دیگران یا ایجاد خسارت شود، فارغ از اینکه عامل انسانی مستقیمی در عمل دخیل بوده یا نه، مسئولیت اخلاقی و حقوقی وجود دارد. این دیدگاه به تدوین چارچوب‌های قانونی جدید برای پوشش جرایم ناشی از فناوری‌های خودکار و هوش مصنوعی کمک می‌کند و می‌تواند مبنایی برای پیشگیری از سوءاستفاده‌های سایبری مانند فیشینگ باشد.

از منظر فلسفه حقوق مدرن، پرسش اصلی این است که چگونه نظام‌های حقوقی می‌توانند با فناوری‌های پیشرفته هماهنگ شوند. برخی فلاسفه حقوق معتقدند که حقوق باید قابلیت تطبیق و انعطاف‌پذیری داشته باشد تا در مواجهه با فناوری‌های نوین، عدالت و امنیت حقوقی حفظ شود (حسینی، ۱۳۹۹). به عبارت دیگر، فلسفه حقوق مدرن تأکید می‌کند که اصول اخلاقی و حقوقی سنتی باید با فناوری‌های جدید بازخوانی شوند، به‌گونه‌ای که هم آزادی‌ها و حقوق فردی حفظ شود و هم از سوءاستفاده‌های فناوری جلوگیری گردد.

یکی دیگر از جنبه‌های فلسفی مرتبط با مسئولیت در فناوری‌های نوین، مسأله شفافیت و قابلیت توضیح تصمیمات فناوری است. سیستم‌های هوش مصنوعی و اتوماسیون پیچیده اغلب به گونه‌ای عمل می‌کنند که حتی طراحان آن‌ها نیز توان توضیح کامل دلایل هر تصمیم را ندارند (رضایی، ۱۳۹۹). این مسأله، از دیدگاه فلسفه اخلاق و حقوق، چالش جدی ایجاد می‌کند، زیرا مسئولیت اخلاقی و قانونی مستلزم شفافیت در چرایی و چگونگی اعمال است. در نتیجه، بسیاری از پژوهشگران پیشنهاد کرده‌اند که طراحی سیستم‌های شفاف و قابل توضیح برای تحقق عدالت و پاسخگویی ضروری است.

Archive of SID.ir

Archive of SID.ir

در فلسفه اخلاق اسلامی نیز مباحث مرتبط با مسئولیت، عدل و امانت مطرح است. اصولی مانند «لزوم رعایت حقوق دیگران» و «تحصیل مال از طریق مشروع» می‌توانند به عنوان مبانی فلسفی برای تحلیل عملکرد فناوری‌های نوین و مسئولیت ناشی از آن‌ها به کار گرفته شوند (ابراهیمی، ۱۳۹۹). به عنوان مثال، هرگونه استفاده از فناوری‌های نوین برای فریب یا سرقت اطلاعات دیگران (مانند فیشینگ) نقض اصول اخلاقی و حقوقی است و مسئولیت آن بر عهده فرد یا سازمانی است که سامانه‌ها را طراحی یا کنترل کرده است.

بنابراین میتوان گفت، مبانی فلسفی مسئولیت در فناوری‌های نوین، هم به تحلیل اخلاقی اعمال و پیامدهای آن می‌پردازد و هم به تدوین چارچوب‌های حقوقی و قانونی کمک می‌کند. این مبانی نشان می‌دهند که فناوری به خودی خود فاقد اراده و مسئولیت اخلاقی است، اما عملکرد آن می‌تواند موجب ضرر شود و مسئولیت ناشی از این عملکرد باید به انسان‌ها، طراحان و سازمان‌های مربوطه نسبت داده شود. همچنین، فلسفه حقوق و فلسفه اخلاق مدرن، بر ضرورت تطبیق قوانین با تحولات فناوری، شفافیت تصمیمات خودکار و طراحی سازوکارهای پاسخگویی تاکید می‌کنند.

مبانی فقهی

در تحلیل حقوقی موضوع فناوری‌های نوین و فیشینگ، بررسی مبانی فقهی و حقوقی اهمیت ویژه‌ای دارد، زیرا این مبانی چارچوب قانونی و اخلاقی لازم برای تعیین مسئولیت‌ها، مجازات‌ها و راهکارهای پیشگیرانه را فراهم می‌کنند. از منظر فقه اسلامی، مسأله اصلی رعایت حقوق دیگران و جلوگیری از ضرر است. اصولی همچون «لزوم رعایت امانت» و «حرمت تحصیل مال به روش غیرمشروع» به‌طور مستقیم با جرایم فیشینگ و سوءاستفاده از فناوری‌های نوین مرتبط هستند (ابراهیمی، ۱۳۹۹).فیشینگ به‌عنوان یک نوع کلاهبرداری دیجیتال، مصداق بارز غصب و تضییع حقوق دیگران است. در فقه اسلامی، غصب مال دیگران، حتی اگر از طریق فناوری انجام شود، از مصادیق محرمات شرعی و واجد ضمانت اجرای قانونی است. از این منظر، هر گونه استفاده از هوش مصنوعی یا سیستم‌های اتوماسیون برای جمع‌آوری اطلاعات حساس کاربران بدون رضایت آن‌ها، خلاف شرع و مصداق امانت‌داری ناقص است و مسئولیت آن بر عهده عامل انسانی است که سامانه را طراحی یا کنترل می‌کند (حسینی، ۱۳۹۹).

از منظر حقوقی مدرن، جرایم فیشینگ و سوءاستفاده‌های فناوری‌های نوین در قالب قوانین مدنی و کیفری قابل بررسی هستند. در نظام حقوقی ایران، قانون جرایم رایانه‌ای مصوب ۱۳۸۸ مواد متعددی دارد که به جرایم دیجیتال می‌پردازد. ماده ۹ این قانون، کلاهبرداری رایانه‌ای را جرم‌انگاری کرده و برای مرتکب مجازات تعیین کرده است، اما اشاره صریحی به فیشینگ نشده است. ماده ۱۰ قانون مذکور به دسترسی غیرمجاز به داده‌ها و اطلاعات اشاره دارد و ماده ۱۱، شیوه رسیدگی قضایی به جرایم سایبری را مشخص می‌کند (رضایی، ۱۳۹۸). با این حال، با پیشرفت فناوری و ظهور هوش مصنوعی و اتوماسیون، این مواد به تنهایی نمی‌توانند تمامی جرایم جدید را پوشش دهند و نیاز به بازنگری و تدوین تبصره‌ها و مواد جدید احساس می‌شود.

یکی از مباحث مهم در مبانی حقوقی، مسئولیت مدنی و کیفری سیستم‌های خودکار است. با ورود فناوری‌های هوشمند، پرسش این است که در صورت ایجاد ضرر یا خسارت توسط یک سامانه خودکار، چه کسی مسئول است؟ دکترین حقوقی معاصر بر چند دیدگاه تاکید دارد:

Archive of SID.ir

Archive of SID.ir

۱. مسئولیت فردی طراح یا برنامه‌نویس: بر اساس این دیدگاه، مسئولیت ناشی از عملکرد سیستم‌های هوشمند بر عهده کسانی است که الگوریتم‌ها و سیستم‌ها را طراحی کرده‌اند، زیرا تصمیمات سیستم بر پایه ورودی‌های طراحی‌شده توسط آن‌ها شکل می‌گیرد (محمدی، ۱۳۹۹).

۲. مسئولیت کارفرما یا سازمان: در این دیدگاه، سازمان‌ها و نهادهایی که سیستم‌ها را به کار می‌گیرند، موظف‌اند تدابیر کنترلی و امنیتی لازم را اعمال کنند و در صورت کوتاهی در انجام این وظایف، مسئول شناخته می‌شوند (ابراهیمی، ۱۳۹۹).

۳. مسئولیت ترکیبی: برخی حقوقدانان معتقدند که در محیط فناوری‌های نوین، مسئولیت باید ترکیبی از مسئولیت فردی، سازمانی و حتی الزامات فنی سیستم‌ها باشد تا پاسخگوی پیچیدگی‌های عملی باشد (کریمی و موسوی، ۱۳۹۹). این دیدگاه می‌تواند در پرونده‌های فیشینگ و سوءاستفاده از هوش مصنوعی کارآمد باشد.

از منظر حقوق کیفری تطبیقی، کشورهای پیشرفته استانداردهایی برای مسئولیت قانونی در استفاده از فناوری‌های خودکار و هوش مصنوعی تدوین کرده‌اند. این استانداردها شامل الزام به رعایت امنیت داده‌ها، آموزش کاربران، شفافیت در طراحی الگوریتم‌ها و مجازات‌های مشخص برای ارتکاب جرایم سایبری است .. تجربه این کشورها می‌تواند به قانون‌گذاران ایران در اصلاح و به‌روزرسانی مواد قانونی کمک کند.

یکی دیگر از مبانی فقهی و حقوقی، لزوم پیشگیری و حفاظت از حقوق کاربران است. مطابق با دکترین حقوقی، سازمان‌ها و نهادها موظف‌اند تدابیر لازم برای محافظت از اطلاعات شخصی و مالی کاربران اتخاذ کنند و در صورت کوتاهی، مسئول شناخته می‌شوند (حسینی، ۱۳۹۹). این اصل حقوقی با مبانی فقهی نیز همخوانی دارد و رعایت آن، هم حفاظت از حقوق دیگران و هم کاهش آسیب‌های مالی و اجتماعی را تضمین می‌کند.از منظر اقتصادی–حقوقی، ضررهای ناشی از فیشینگ و سوءاستفاده‌های فناوری‌های نوین بسیار گسترده است. هزینه‌های مستقیم و غیرمستقیم شامل خسارت مالی، کاهش اعتماد عمومی، هزینه‌های قانونی و بازسازی سیستم‌ها، همگی نشان‌دهنده ضرورت تدوین چارچوب‌های قانونی جامع است (احمدی، ۱۳۹۷). بنابراین، مبانی حقوقی و فقهی، علاوه بر تعیین مسئولیت و مجازات، باید به پیشگیری و کاهش ریسک‌های مالی و اجتماعی نیز توجه داشته باشند.مبانی فقهی و حقوقی، چارچوبی علمی و عملیاتی برای تحلیل جرایم فیشینگ، سوءاستفاده از هوش مصنوعی و اتوماسیون فراهم می‌آورند. این مبانی نشان می‌دهند که مسئولیت اخلاقی و قانونی عملکرد فناوری‌های نوین به خود فناوری نسبت داده نمی‌شود، بلکه به انسان‌ها، طراحان و سازمان‌های کنترل‌کننده بازمی‌گردد. همچنین، ضرورت شفافیت، نظارت، پیشگیری و تدوین مقررات تکمیلی برای انطباق با تحولات فناوری از دیگر اصول مهم این مبانی است.

مبانی حقوقی

در حقوق ایران، قانون جرایم رایانه‌ای مصوب ۱۳۸۸ به‌عنوان اصلی‌ترین مرجع قانونی در حوزه جرایم سایبری شناخته می‌شود و چارچوبی کلی برای مقابله با اقدامات مجرمانه در فضای دیجیتال ارائه می‌دهد. این قانون در بخش‌های مختلف، به جرایم مرتبط با دسترسی غیرمجاز، کلاهبرداری رایانه‌ای، انتشار محتوای مجرمانه و سایر اقدامات سوء در محیط‌های دیجیتال پرداخته است. با این حال، با توجه به تحولات سریع فناوری و ظهور روش‌های نوین کلاهبرداری، از جمله فیشینگ، این قانون نیازمند بازنگری و به‌روزرسانی است تا بتواند پاسخگوی تهدیدات پیچیده و چندجانبه دنیای دیجیتال باشد (رضایی، ۱۳۹۸).

Archive of SID.ir

Archive of SID.ir

ماده ۹ قانون جرایم رایانه‌ای به‌طور خاص به کلاهبرداری رایانه‌ای پرداخته و مجازات‌هایی برای مرتکب تعیین کرده است. این ماده بیان می‌دارد که هر کس به‌وسیله سامانه‌های رایانه‌ای یا مخابراتی، اقدام به فریب افراد و تحصیل مال نامشروع کند، مجرم محسوب می‌شود و به مجازات مقرر محکوم می‌گردد. اگرچه این ماده گستره کلی برای مقابله با جرایم رایانه‌ای فراهم کرده است، اما به‌طور مشخص به شیوه‌های نوین مانند فیشینگ اشاره نکرده است و این امر خلأ قانونی محسوب می‌شود (محمدی، ۱۳۹۹).

فیشینگ به عنوان یک روش پیچیده کلاهبرداری دیجیتال، مبتنی بر فریب روانی کاربران و سرقت اطلاعات حساس مانند نام کاربری، رمز عبور و اطلاعات مالی است. این شیوه می‌تواند از طریق ایمیل‌های جعلی، وب‌سایت‌های تقلیدی یا پیامک‌های غیرمجاز انجام شود. از منظر حقوقی، فیشینگ مصداق کلاهبرداری و تجاوز به حقوق مالکیت داده‌هاست و با اصول کلی قانون مدنی و کیفری ایران همخوانی دارد، اما عدم اشاره صریح در ماده ۹ قانون جرایم رایانه‌ای، امکان ایجاد خلأ در پیگرد قانونی را فراهم کرده است (حسینی، ۱۳۹۹).

یکی از جنبه‌های مهم مبانی حقوقی، مسئولیت اشخاص حقیقی و حقوقی در استفاده و کنترل فناوری‌های نوین است. در مواردی که حملات فیشینگ از طریق سامانه‌های اتوماسیون یا هوش مصنوعی انجام می‌شود، مسئولیت می‌تواند به چند دسته تقسیم شود:

۱. مسئولیت برنامه‌نویس و طراح سیستم: افرادی که الگوریتم‌ها و سامانه‌ها را طراحی می‌کنند، مسئول نتایج عملکرد سیستم هستند، به ویژه اگر نقص‌های امنیتی یا آسیب‌پذیری‌های شناخته‌شده را اصلاح نکرده باشند (ابراهیمی، ۱۳۹۹).

۲. مسئولیت سازمان یا کارفرما: نهادها و سازمان‌هایی که از فناوری‌های نوین استفاده می‌کنند، موظف‌اند الزامات امنیتی و کنترلی لازم را فراهم کنند. در صورت کوتاهی، مسئولیت مدنی و کیفری برای آن‌ها ایجاد می‌شود. این اصل هم در حقوق مدنی و هم در دکترین حقوق کیفری پذیرفته شده است (رضایی، ۱۳۹۹).

۳. مسئولیت ترکیبی: برخی حقوقدانان پیشنهاد کرده‌اند که در مواجهه با فناوری‌های خودکار و هوشمند، مسئولیت باید ترکیبی از مسئولیت فردی، سازمانی و الزامات فنی سیستم‌ها باشد تا پیچیدگی‌های حقوقی ناشی از استفاده از فناوری‌های نوین پوشش داده شود (کریمی و موسوی، ۱۳۹۹).

یکی دیگر از اصول مهم، پیشگیری و الزام به رعایت استانداردهای امنیتی است. بر اساس دکترین حقوقی، سازمان‌ها موظف‌اند تدابیر لازم برای محافظت از داده‌ها و جلوگیری از سوءاستفاده از سامانه‌ها را اتخاذ کنند. عدم رعایت این الزام می‌تواند منجر به مسئولیت مدنی یا کیفری شود و با مواد قانون مدنی مرتبط است، از جمله ماده ۲۸۵ قانون مدنی درباره جبران خسارت ناشی از عدم انجام وظایف قانونی و ماده ۳۵ قانون تجارت الکترونیک درباره تضمین امنیت اطلاعات (حسینی، ۱۳۹۹).

از منظر تطبیقی، تجربه کشورهای پیشرفته نشان می‌دهد که قوانین دیجیتال باید چند ویژگی کلیدی داشته باشند:

شمول کامل برای روش‌های نوین کلاهبرداری: قوانین باید پوشش جامع برای حملات فیشینگ، هک و سوءاستفاده از هوش مصنوعی فراهم کنند.

تعیین مسئولیت دقیق برای اشخاص حقیقی و حقوقی: شامل طراحان، کاربران و سازمان‌ها.

الزام به استانداردهای امنیتی و شفافیت سامانه‌ها: قوانین باید تدوین استانداردهای فنی و نظارتی را الزامی کنند تا پیشگیری از سوءاستفاده تسهیل شود .

Archive of SID.ir

Archive of SID.ir

با توجه به تحولات فناوری و رشد روزافزون حملات سایبری، مبانی حقوقی موجود در ایران نیازمند بازنگری هستند. به طور خاص، تدوین تبصره‌های جدید برای ماده ۹ قانون جرایم رایانه‌ای، شفاف‌سازی مسئولیت‌ها و الزامات امنیتی، و اعمال مقررات پیشگیرانه، ضروری به نظر می‌رسد. این اقدامات می‌تواند خلأ قانونی موجود در حوزه فیشینگ و سوءاستفاده از هوش مصنوعی و اتوماسیون را پر کند و زمینه پیگرد قانونی مؤثر را فراهم نماید (محمدی، ۱۳۹۹).

در مجموع، مبانی حقوقی موضوع نشان می‌دهد که فناوری‌های نوین، اگرچه فرصت‌های اقتصادی و عملیاتی فراوانی ایجاد می‌کنند، اما چالش‌های حقوقی پیچیده‌ای نیز به همراه دارند. مسئولیت قانونی در استفاده و کنترل این فناوری‌ها باید روشن و دقیق تعریف شود، مجازات‌ها و ضمانت اجراها به‌روزرسانی شوند و استانداردهای پیشگیرانه و نظارتی تدوین گردد. تنها با چنین چارچوبی می‌توان بهره‌برداری ایمن و اخلاقی از فناوری‌های نوین را تضمین کرد و حقوق کاربران و جامعه را در برابر تهدیدات دیجیتال حفظ نمود (رضایی، ۱۳۹۸؛ حسینی، ۱۳۹۹).

مبانی اقتصادی

از منظر اقتصادی، جرایم سایبری و به‌ویژه کلاهبرداری‌هایی که با استفاده از فناوری‌های نوین مانند هوش مصنوعی و اتوماسیون انجام می‌شوند، اثرات قابل توجهی بر اقتصاد افراد، سازمان‌ها و حتی دولت‌ها دارند. این اثرات نه تنها شامل خسارات مالی مستقیم، بلکه هزینه‌های غیرمستقیم و بلندمدت نیز می‌شوند که می‌توانند تأثیر جدی بر رشد اقتصادی، سرمایه اجتماعی و اعتماد عمومی داشته باشند (احمدی، ۱۳۹۷).

خسارات مالی مستقیم ناشی از فیشینگ و سایر روش‌های کلاهبرداری دیجیتال شامل سرقت وجه نقد، برداشت غیرمجاز از حساب‌های بانکی و دسترسی به اطلاعات مالی حساس است. به عنوان مثال، حملات فیشینگ موفق می‌توانند میلیون‌ها دلار خسارت مستقیم ایجاد کنند که بازسازی آن مستلزم صرف منابع مالی و انسانی قابل توجهی است. از این منظر، هزینه اقتصادی این جرایم تنها به سطح فرد محدود نمی‌شود و بر سازمان‌ها و شبکه‌های مالی نیز اثرگذار است (محمدی، ۱۳۹۹).هزینه‌های ناشی از کاهش اعتماد عمومی یکی دیگر از اثرات اقتصادی مهم جرایم سایبری است. اعتماد، به ویژه در محیط‌های دیجیتال و معاملات آنلاین، یکی از پایه‌های اساسی توسعه اقتصادی است. هرگونه ضعف امنیتی یا حمله موفق، می‌تواند باعث کاهش اعتماد کاربران به بانک‌ها، پلتفرم‌های پرداخت الکترونیک و حتی دولت شود. کاهش اعتماد عمومی، به نوبه خود، منجر به کاهش تعاملات اقتصادی، کاهش سرمایه‌گذاری و افزایش هزینه‌های نظارتی برای بازگرداندن اعتماد می‌شود (رضایی، ۱۳۹۸).

هزینه‌های حقوقی و قضایی نیز بخش مهم دیگری از آثار اقتصادی جرایم سایبری است. پیگیری قانونی، رسیدگی به شکایات، هزینه‌های وکالت و دفاع قضایی و اجرای مجازات‌ها، همه بار مالی قابل توجهی بر سیستم قضایی و متقاضیان ایجاد می‌کند. علاوه بر این، پیچیدگی‌های فناوری‌های نوین باعث افزایش زمان و هزینه رسیدگی به پرونده‌های سایبری می‌شود. در مواردی که حملات فیشینگ بین‌المللی باشد، این هزینه‌ها می‌تواند شامل تعامل با نهادهای قانونی خارجی و هماهنگی بین‌المللی نیز شود (حسینی، ۱۳۹۹).

هزینه‌های بازسازی و تقویت سیستم‌های امنیتی نیز یکی دیگر از مؤلفه‌های مهم اقتصادی این جرایم است. هرگاه یک سازمان مورد حمله قرار گیرد، لازم است که اقدامات اصلاحی شامل به‌روزرسانی نرم‌افزارها، افزایش امنیت شبکه، آموزش کارکنان و نظارت مستمر بر سامانه‌ها انجام شود. این اقدامات علاوه بر صرف منابع مالی، نیازمند تخصیص نیروی انسانی متخصص و زمان قابل توجهی هستند. از این منظر، هزینه اقتصادی فیشینگ و سایر جرایم سایبری تنها

Archive of SID.ir

Archive of SID.ir

محدود به خسارت مستقیم نیست و شامل هزینه‌های پیشگیری و بازسازی نیز می‌شود (کریمی و موسوی، ۱۳۹۹).از منظر اقتصادی-رفتاری، رفتار کاربران و سازمان‌ها نیز بر میزان خسارت تأثیرگذار است. کمبود آموزش، عدم آگاهی از شیوه‌های حملات سایبری و استفاده ناصحیح از سامانه‌های دیجیتال می‌تواند موجب افزایش ریسک و خسارت شود. بنابراین، سرمایه‌گذاری در آموزش کاربران و کارکنان، طراحی سیستم‌های کاربرپسند و اتخاذ سیاست‌های امنیتی مؤثر، می‌تواند هزینه‌های اقتصادی ناشی از جرایم سایبری را کاهش دهد (ابراهیمی، ۱۳۹۹).

یکی دیگر از جنبه‌های اقتصادی، هزینه‌های فرصت است. منابع مالی، زمانی و انسانی که برای مقابله با جرایم سایبری و بازسازی سیستم‌ها صرف می‌شود، می‌تواند برای توسعه کسب‌وکار، نوآوری یا سایر فعالیت‌های اقتصادی استفاده شود. به عبارت دیگر، جرایم سایبری باعث هدررفت منابع و کاهش بهره‌وری اقتصادی می‌شوند. این مسأله اهمیت تحلیل اقتصادی و تدوین راهکارهای پیشگیرانه را دوچندان می‌کند (رضایی، ۱۳۹۹).

از دیدگاه سیاستگذاری اقتصادی، تحلیل هزینه-فایده پیشگیری از جرایم سایبری اهمیت ویژه‌ای دارد. سرمایه‌گذاری در سامانه‌های امنیتی، آموزش کاربران و طراحی مقررات و استانداردهای پیشگیرانه، اگرچه مستلزم صرف هزینه است، اما در بلندمدت از خسارات مالی و اقتصادی گسترده جلوگیری می‌کند. مطالعات نشان داده‌اند که هزینه پیشگیری معمولاً کمتر از هزینه جبران خسارات است و اتخاذ سیاست‌های پیشگیرانه، بازده اقتصادی مثبت دارد (محمدی، ۱۳۹۹).در چارچوب مبانی اقتصادی، نقش دولت و مقررات‌گذاری نیز بسیار حیاتی است. دولت‌ها می‌توانند با تدوین قوانین شفاف، الزام به رعایت استانداردهای امنیتی و ایجاد نهادهای نظارتی، سطح ریسک و خسارت ناشی از جرایم سایبری را کاهش دهند. همچنین، دولت می‌تواند با ایجاد زیرساخت‌های امنیتی ملی، ارتقای امنیت شبکه‌ها و حمایت از شرکت‌های خصوصی، اثرات اقتصادی این جرایم را به حداقل برساند (احمدی، ۱۳۹۷).

به طور خلاصه، مبانی اقتصادی نشان می‌دهند که جرایم سایبری، به ویژه فیشینگ و سوءاستفاده از هوش مصنوعی و اتوماسیون، آثار گسترده و چندجانبه‌ای دارند که شامل خسارت مالی مستقیم، کاهش اعتماد عمومی، هزینه‌های حقوقی و بازسازی سیستم‌ها و هزینه‌های فرصت است. تحلیل اقتصادی این جرایم، همراه با تدوین سیاست‌ها و مقررات پیشگیرانه، سرمایه‌گذاری در آموزش و ارتقای امنیت، به کاهش هزینه‌ها و افزایش بهره‌وری اقتصادی کمک می‌کند و از این رو یکی از ارکان مهم در تحلیل جامع موضوع فناوری‌های نوین و فیشینگ محسوب می‌شود (رضایی، ۱۳۹۹؛ حسینی، ۱۳۹۹).

نظریه‌های حقوقی

در حقوق ایران، تحلیل مسئولیت در زمینه جرایم سایبری نیازمند توجه به نظریه‌های مختلف حقوقی است که در خصوص مسئولیت مدنی و کیفری تدوین شده‌اند. با ظهور فناوری‌های نوین و ابزارهای هوشمند، تبیین دقیق مسئولیت اشخاص حقیقی و حقوقی و نحوه اعمال مجازات، چالش‌های جدیدی ایجاد کرده است. در این بخش، مهم‌ترین نظریه‌های حقوقی مرتبط با مسئولیت در جرایم سایبری مورد بررسی قرار می‌گیرند و تطبیق آن‌ها با قانون جرایم رایانه‌ای مصوب ۱۳۸۸ تحلیل می‌شود (رضایی، ۱۳۹۸).

۱. نظریه مسئولیت بر اساس تقصیر

بر اساس این نظریه، مسئولیت تنها زمانی برقرار می‌شود که فرد مرتکب تقصیر شده باشد. تقصیر می‌تواند شامل فعل یا ترک فعل عمدی، شبه‌عمد یا بی‌احتیاطی باشد. در زمینه جرایم سایبری، نظریه مسئولیت بر اساس تقصیر به این معناست

Archive of SID.ir

Archive of SID.ir

که فرد تنها در صورتی مسئول شناخته می‌شود که اقدام یا ترک فعل او سبب ایجاد خسارت شده باشد. به عنوان مثال، اگر یک کاربر یا برنامه‌نویس از هشدارهای امنیتی و استانداردهای لازم پیروی نکند و در نتیجه اطلاعات کاربران به سرقت رود، مسئولیت کیفری و مدنی او قابل اثبات است (محمدی، ۱۳۹۹).

مزیت این نظریه، رعایت عدالت و تفکیک میان افراد مقصر و غیرمقصر است، اما محدودیت‌هایی نیز دارد. یکی از چالش‌های مهم در فناوری‌های نوین، تشخیص تقصیر در عملکرد سیستم‌های هوش مصنوعی و اتوماسیون است. از آنجا که تصمیمات سامانه‌ها بر پایه الگوریتم‌ها و داده‌های ورودی شکل می‌گیرد، ممکن است تعیین میزان تقصیر انسان‌ها دشوار شود. بنابراین، اعمال این نظریه در موارد پیچیده جرایم سایبری نیازمند معیارهای دقیق حقوقی و فنی است (حسینی، ۱۳۹۹).

۲. نظریه مسئولیت بدون تقصیر (مسئولیت محض)

نظریه مسئولیت محض بر این اصل استوار است که مسئولیت صرف‌نظر از وجود تقصیر برقرار می‌شود. در برخی سیستم‌های حقوقی، این نوع مسئولیت برای حفاظت از حقوق مصرف‌کنندگان، محیط زیست یا اموال عمومی اعمال می‌شود. در زمینه جرایم سایبری، مسئولیت محض می‌تواند برای سازمان‌ها و نهادهایی که فناوری‌های نوین را به کار می‌گیرند، کاربرد داشته باشد. به عنوان مثال، اگر یک سامانه هوشمند بدون دخالت مستقیم انسان، اطلاعات کاربران را فاش کند، سازمان مسئول آن است حتی اگر هیچ کوتاهی مشخصی در طراحی سیستم وجود نداشته باشد (ابراهیمی، ۱۳۹۹).

مزیت نظریه مسئولیت محض این است که امکان جبران خسارت به قربانیان سریع‌تر و بدون نیاز به اثبات تقصیر فراهم می‌شود. این دیدگاه با اصول پیشگیری و حمایت از حقوق کاربران همخوانی دارد و می‌تواند به عنوان مبنایی برای اصلاح قانون جرایم رایانه‌ای مورد استفاده قرار گیرد. با این حال، محدودیت‌های این نظریه شامل ایجاد بار مالی و قضایی اضافی بر سازمان‌ها و افراد فاقد تقصیر مستقیم است، که باید با سیاست‌گذاری و مقررات شفاف کنترل شود (کریمی و موسوی، ۱۳۹۹).

۳. نظریه مسئولیت کارفرما

بر اساس این نظریه، کارفرما مسئول اعمال کارکنان خود است، حتی اگر کارمند بدون اطلاع یا دستور مستقیم کارفرما مرتکب جرم شود. در محیط فناوری‌های نوین، این نظریه اهمیت ویژه‌ای پیدا می‌کند، زیرا بسیاری از حملات سایبری توسط کارمندان داخلی یا به واسطه سیستم‌های تحت کنترل آن‌ها انجام می‌شود. برای مثال، اگر یک کارمند سامانه‌ای طراحی کند که به طور غیرمستقیم منجر به حمله فیشینگ شود، کارفرما مسئول جبران خسارت است.

این نظریه در حقوق ایران نیز مورد توجه قرار گرفته و با اصول مدنی و کیفری همخوانی دارد. ماده ۹ قانون جرایم رایانه‌ای، هرچند به‌طور مستقیم مسئولیت کارفرما را ذکر نکرده، اما دکترین حقوقی بر این نکته تأکید دارد که سازمان‌ها باید وظایف کنترلی و نظارتی خود را بر کارکنان و سامانه‌ها اعمال کنند، و در صورت کوتاهی، مسئولیت مدنی و کیفری بر عهده آن‌هاست (رضایی، ۱۳۹۹).

نقد و تحلیل نظریه‌ها در چارچوب قانون جرایم رایانه‌ای

ماده ۹ قانون جرایم رایانه‌ای به کلاهبرداری رایانه‌ای اشاره دارد و مجازات‌هایی برای آن تعیین کرده است. این ماده گرچه چارچوب کلی برای مقابله با جرایم دیجیتال فراهم می‌کند، اما با ظهور روش‌های نوین کلاهبرداری مانند

Archive of SID.ir

Archive of SID.ir

فیشینگ و سوءاستفاده از هوش مصنوعی، نیازمند بازنگری و افزودن تبصره‌ها و مواد تکمیلی است. در این زمینه، تلفیق نظریه‌های مسئولیت بر اساس تقصیر، مسئولیت محض و مسئولیت کارفرما می‌تواند پوشش جامع‌تری برای جرایم نوین ایجاد کند. به عنوان مثال:

مسئولیت فردی بر اساس تقصیر می‌تواند در مواردی که کوتاهی مستقیم فرد سبب ایجاد خسارت شده، اعمال شود.

مسئولیت محض می‌تواند برای سازمان‌ها و نهادهایی که فناوری‌های خودکار را به کار می‌گیرند، اعمال شود تا قربانیان بتوانند سریع‌تر جبران خسارت کنند.

نظریه مسئولیت کارفرما می‌تواند در مواردی که کارمندان یا سیستم‌های داخلی سازمان موجب جرم شده‌اند، مبنای اعمال قانون باشد.

با تلفیق این نظریه‌ها، قانون‌گذار می‌تواند چارچوبی منعطف و مؤثر برای مواجهه با جرایم سایبری و فیشینگ ایجاد کند و خلأهای قانونی فعلی را پر نماید (حسینی، ۱۳۹۹).

در مجموع، نظریه‌های حقوقی مسئولیت در جرایم سایبری شامل سه دیدگاه اصلی هستند: مسئولیت بر اساس تقصیر، مسئولیت بدون تقصیر و مسئولیت کارفرما. هر یک از این نظریه‌ها مزایا و محدودیت‌های خود را دارند و در چارچوب فناوری‌های نوین و ظهور روش‌های پیچیده کلاهبرداری، ترکیب و تلفیق آن‌ها می‌تواند چارچوب قانونی مؤثرتری برای حمایت از حقوق قربانیان ایجاد نماید. با توجه به تحولات سریع فناوری، اصلاح و به‌روزرسانی ماده ۹ قانون جرایم رایانه‌ای و تدوین تبصره‌ها و استانداردهای حقوقی مرتبط، ضرورتی انکارناپذیر است. این اقدام هم با اصول عدالت و حمایت از حقوق افراد همخوانی دارد و هم امکان پیشگیری و پاسخگویی مؤثر به جرایم سایبری را فراهم می‌کند.

تحلیل حقوقی فیشینگ و سوءاستفاده از هوش مصنوعی و اتوماسیون در فضای سایبری: بررسی قوانین مدنی، قانون اساسی و حقوق بشر

استفاده از فناوری‌های نوین، به ویژه هوش مصنوعی و اتوماسیون، در فضای سایبری، امکانات گسترده‌ای برای تسهیل امور روزمره و توسعه کسب‌وکارها ایجاد کرده است؛ اما همزمان با تهدیدات جدی همچون فیشینگ و کلاهبرداری‌های دیجیتال همراه است. از منظر حقوقی، این موضوع به صورت مستقیم با حقوق آمره مرتبط است، حقوقی که نقض آن‌ها حتی با توافق طرفین یا قرارداد خصوصی ممکن نیست و شامل حفاظت از امنیت عمومی، اموال و اطلاعات شخصی شهروندان می‌شود (صدقی، ۲۰۱۵). بهره‌گیری از فناوری‌های اتوماسیون برای فیشینگ، نقض آشکار این حقوق است، زیرا موجب ایجاد خسارت مالی و معنوی برای کاربران و تهدید امنیت عمومی در فضای مجازی می‌شود (حسینی، ۲۰۱۸).

قانون اساسی جمهوری اسلامی ایران نیز به صراحت در اصول ۳ و ۴۳ وظیفه دولت را در حفظ حقوق فردی و عمومی و حمایت از اموال مردم مشخص کرده است (قانون اساسی جمهوری اسلامی ایران، ۱۹۷۹). استفاده از هوش مصنوعی برای فیشینگ با این اصول در تضاد است، زیرا با دسترسی غیرمجاز به اطلاعات و سوءاستفاده از آن، حقوق شهروندان در مالکیت و حریم شخصی نقض می‌شود. همچنین اصل ۲۲ قانون اساسی تاکید دارد که هیچ کس نباید از حقوق و آزادی‌های مشروع خود محروم شود و حملات سایبری مبتنی بر هوش مصنوعی می‌تواند این اصل را به طور مستقیم نقض کند.از منظر قانون مدنی ایران، مواد ۳۳۰ و ۳۳۴ تصریح می‌کنند که هر عملی که موجب ضرر به دیگری شود، مسئولیت حقوقی و جبران خسارت دارد (محمدی، ۲۰۱۷). بنابراین، استفاده از فناوری‌های نوین برای انجام فیشینگ و

Archive of SID.ir

Archive of SID.ir

کلاهبرداری دیجیتال، مصداق ایجاد ضرر مادی و معنوی است و مرتکب موظف به جبران آن می‌باشد. تبصره ماده ۲ قانون مدنی نیز اعلام می‌کند هر عملی که برخلاف نظم عمومی و اخلاق حسنه باشد، باطل و قابل پیگرد است؛ استفاده از هوش مصنوعی و اتوماسیون برای سوءاستفاده از اطلاعات دیگران، کاملاً در چارچوب این تبصره قابل پیگرد است و نمی‌توان آن را مشروع دانست.

علاوه بر قوانین داخلی، قوانین و کنوانسیون‌های حقوق بشر نیز حفاظت از حریم خصوصی و امنیت اطلاعات شخصی را به عنوان یک حق بنیادین تضمین می‌کنند (کریمی، ۲۰۱۹). فیشینگ مبتنی بر فناوری‌های نوین نقض آشکار این حقوق است، زیرا بدون رضایت فرد، اطلاعات حساس کاربران جمع‌آوری و مورد سوءاستفاده قرار می‌گیرد. از منظر حقوق بین‌الملل، حق مالکیت و امنیت دیجیتال جزو حقوق اساسی انسان‌ها محسوب می‌شود و دولت‌ها موظفند با تدوین قوانین و مقررات مناسب، شهروندان را در برابر تهدیدات سایبری محافظت کنند.

با توجه به این چارچوب‌ها، می‌توان نتیجه گرفت که هر گونه استفاده از هوش مصنوعی و اتوماسیون در فیشینگ و کلاهبرداری دیجیتال نه تنها خلاف قوانین مدنی و اصول حقوق آمره است، بلکه با قانون اساسی و تعهدات حقوق بشری دولت نیز در تضاد قرار دارد. مقابله با این تهدیدات نیازمند تدوین مقررات خاص سایبری، ایجاد مسئولیت مدنی و کیفری برای مرتکبان و تضمین حمایت قانونی از اطلاعات و مالکیت دیجیتال افراد است. بدون چنین حمایت‌ها و سازوکارهای قانونی، فضای سایبری تبدیل به محیطی پرخطر و غیرامن خواهد شد که نه تنها اعتماد عمومی را کاهش می‌دهد، بلکه زیربنای اقتصادی و اجتماعی کشور را نیز تهدید می‌کند.

پیشینه پژوهش‌ها

موضوع استفاده از فناوری‌های نوین، هوش مصنوعی، اتوماسیون و فیشینگ به‌عنوان یکی از مهم‌ترین مسائل امنیت سایبری و حقوق دیجیتال، طی دو دهه اخیر مورد توجه پژوهشگران و محققان داخلی و بین‌المللی قرار گرفته است. پیشینه پژوهش‌ها نشان می‌دهد که این حوزه، از منظر حقوقی، اقتصادی و فناوری، نیازمند تحلیل جامع و تطبیقی است تا بتوان با توجه به تحولات سریع فناوری، چارچوب‌های قانونی و سیاست‌های پیشگیرانه مناسب را طراحی کرد (رضایی، ۱۳۹۸).

در سطح پژوهش‌های داخلی، چندین مطالعه مهم انجام شده است که هر یک بخشی از ابعاد این موضوع را مورد بررسی قرار داده‌اند. پژوهش «تحلیل جرم‌شناختی فیشینگ در نظام حقوقی ایران» (احمدی، ۱۳۹۷) به بررسی تطبیقی جرایم رایانه‌ای و تکنیک‌های فیشینگ پرداخته و خلأهای قانونی موجود در قانون جرایم رایانه‌ای را شناسایی کرده است. این مطالعه نشان داد که مواد موجود، علی‌رغم تعیین مجازات برای کلاهبرداری رایانه‌ای، به‌طور مشخص حملات مبتنی بر فیشینگ را پوشش نمی‌دهند و لازم است مقررات جدیدی تدوین شود.

پژوهش دیگری تحت عنوان «مسئولیت کیفری در جرایم سایبری» (محمدی، ۱۳۹۹) به بررسی مسئولیت فردی و سازمانی در استفاده از فناوری‌های نوین و ارتکاب جرایم سایبری پرداخته است. نتایج این مطالعه نشان داد که چارچوب قانونی موجود، مسئولیت سیستم‌های خودکار و هوش مصنوعی را به‌طور کامل مشخص نکرده و نیازمند تبیین دقیق مسئولیت‌ها در بستر فناوری‌های دیجیتال است.

همچنین، پژوهش «هوش مصنوعی و امنیت سایبری» (کریمی و موسوی، ۱۳۹۹) به تحلیل نقش هوش مصنوعی در پیشگیری و ارتکاب جرایم سایبری پرداخته است. این مطالعه نشان داد که هوش مصنوعی می‌تواند هم به‌عنوان ابزار

Archive of SID.ir

Archive of SID.ir

پیشگیری و هم به‌عنوان ابزار جرم استفاده شود و در نتیجه چارچوب‌های قانونی باید توان پوشش هردو کاربرد را داشته باشند.

پژوهش «اتوماسیون و حقوق دیجیتال» (ابراهیمی، ۱۳۹۹) بر نقش سیستم‌های خودکار و اتوماسیون در کاهش خطای انسانی و بهبود امنیت داده‌ها تأکید کرده است. نتایج این پژوهش نشان داد که با وجود مزایای اقتصادی و عملیاتی اتوماسیون، عدم تدوین چارچوب‌های قانونی و مسئولیت‌های روشن برای عملکرد سیستم‌های خودکار، می‌تواند زمینه سوءاستفاده و تضییع حقوق کاربران را فراهم کند.

پژوهش «مهندسی اجتماعی و فیشینگ: تحلیل حقوقی و پیشگیرانه» (حسینی و کریمی، ۱۳۹۸) نیز به تحلیل تکنیک‌های روان‌شناختی مورد استفاده در فیشینگ و راهکارهای پیشگیری از آن پرداخته است. این مطالعه بر اهمیت آموزش کاربران و تدوین سیاست‌های پیشگیرانه حقوقی تأکید کرده است و نشان می‌دهد که تنها ترکیب راهکارهای فنی، حقوقی و آموزشی می‌تواند موفقیت حملات فیشینگ را کاهش دهد.

با بررسی پیشینه پژوهشی داخلی ، مشخص می‌شود که علیرغم توجه به ابعاد مختلف فیشینگ و فناوری‌های نوین، خلأهای پژوهشی مهمی وجود دارد:

۱. خلأ قانونی و تطبیقی: قوانین موجود در ایران هنوز پوشش جامع برای جرایم فیشینگ و مسئولیت ناشی از تصمیمات سیستم‌های خودکار و هوش مصنوعی ندارند.

۲. کمبود پژوهش‌های چندبعدی: بسیاری از مطالعات به تحلیل یک بعد (حقوقی یا اقتصادی یا فناوری) پرداخته‌اند، اما کمتر پژوهشی تحلیل جامع و تلفیقی ارائه کرده است.

۳. نقص در تحلیل اثرات اجتماعی و پیشگیری: پژوهش‌های پیشین کمتر به اثرات اجتماعی، آموزش کاربران و راهکارهای پیشگیرانه همه‌جانبه پرداخته‌اند.

۴. کمبود مطالعات تطبیقی: بررسی تطبیقی قوانین و سیاست‌های بین‌المللی برای مقابله با فیشینگ و استفاده از هوش مصنوعی، در پژوهش‌های داخلی به اندازه کافی انجام نشده است.

پژوهش حاضر با هدف پر کردن این خلأهای پژوهشی انجام شده است. این مطالعه به شکل تحلیلی، توصیفی و تطبیقی، ابعاد مختلف فناوری‌های نوین، فیشینگ، هوش مصنوعی و اتوماسیون را بررسی کرده و تحلیل حقوقی، اقتصادی و اجتماعی آن‌ها را ارائه می‌دهد.

مزیت اصلی این پژوهش در موارد زیر خلاصه می‌شود:

۱. تحلیل جامع و تلفیقی: این مقاله تمامی ابعاد حقوقی، فقهی، اقتصادی، اجتماعی و فناوری را یکپارچه بررسی می‌کند.

۲. بررسی قوانین و مقررات: با استناد به مواد و تبصره‌های قانون جرایم رایانه‌ای ایران و مقایسه با قوانین بین‌المللی، نقاط ضعف و قوت قوانین شناسایی شده و پیشنهاداتی برای اصلاح ارائه می‌شود.

۳. تحلیل کاربرد فناوری‌های نوین: نقش هوش مصنوعی و اتوماسیون در ارتکاب و پیشگیری از فیشینگ و سایر جرایم دیجیتال تحلیل شده است.

۴. ارائه راهکارهای پیشگیرانه: این مقاله با توجه به تجارب بین‌المللی و مطالعات داخلی، توصیه‌هایی برای آموزش کاربران، تدوین سیاست‌های پیشگیرانه و طراحی چارچوب‌های حقوقی و امنیتی ارائه می‌دهد.

Archive of SID.ir

Archive of SID.ir

به طور کلی، پژوهش حاضر می‌تواند جایگاه منحصربه‌فردی در ادبیات موضوع داشته باشد، زیرا خلأهای پژوهشی موجود را پوشش می‌دهد و چارچوب علمی و کاربردی برای قانون‌گذاران، سازمان‌ها و محققان فراهم می‌آورد.

با وجود پژوهش‌های انجام‌شده در زمینه جرایم سایبری و فیشینگ، خلأهای پژوهشی متعددی در این حوزه وجود دارد. از جمله این خلأها می‌توان به عدم تحلیل جامع و به‌روز قوانین موجود در زمینه جرایم سایبری، کمبود پژوهش‌های تطبیقی میان نظام‌های حقوقی مختلف و عدم بررسی تأثیر فناوری‌های نوین مانند هوش مصنوعی و اتوماسیون در ارتکاب جرایم سایبری اشاره کرد.

تحلیل و بررسی

از منظر حقوقی، این مسئله به چالش‌های متعددی در قانونگذاری، شناسایی مجرم و تعیین مسئولیت مدنی و کیفری منجر شده است.در بررسی قوانین داخلی ایران، نخستین نقطه توجه قانون‌گذار، قانون مجازات اسلامی و قانون جرایم رایانه‌ای است. بر اساس ماده ۷۴ قانون جرایم رایانه‌ای مصوب ۱۳۸۸، هرگونه دسترسی غیرمجاز به داده‌ها و سیستم‌های رایانه‌ای و استفاده از آن‌ها با قصد کلاهبرداری، جرم محسوب می‌شود. این ماده به‌طور خاص شامل فناوری‌های نوین نیز می‌شود، زیرا تعاریف قانون در بندهای مربوط به «سیستم‌های رایانه‌ای» و «داده‌های الکترونیکی» وسیع بوده و شامل هرگونه ابزار دیجیتال می‌شود. علاوه بر این، ماده ۱ قانون مجازات اسلامی، با تأکید بر قصد مرتکب و نتیجه عمل، می‌تواند زمینه‌ساز پیگرد مجرمان فیشینگ مبتنی بر هوش مصنوعی باشد، زیرا استفاده از الگوریتم‌های اتوماسیون برای جمع‌آوری اطلاعات محرمانه، تلاشی عمدی برای سوءاستفاده مالی و روانی است (محمدی، ۱۴۰۰، ص. ۱۲۳). همچنین، مقررات مربوط به حمایت از اطلاعات شخصی کاربران، مانند قانون حمایت از حریم خصوصی و مصوبات شورای عالی فضای مجازی، به‌طور ضمنی استفاده غیرمجاز از داده‌های شخصی را در حوزه فناوری‌های نوین محدود کرده و متخلفان را تحت تعقیب قرار می‌دهد.

با وجود این، مشکلات عملی در تطبیق قوانین موجود با فناوری‌های نوین آشکار است. قوانین فعلی عمدتاً بر اقدامات سنتی کلاهبرداری تمرکز دارند و فناوری‌هایی که بتوانند رفتار انسانی را تقلید کنند یا حملات خودکار انجام دهند، به‌سختی در چارچوب قانونی موجود جای می‌گیرند. در نتیجه، حقوق‌دانان بر این باورند که برای پوشش خلأ قانونی، باید مفاهیم جرم‌شناسی دیجیتال و مسئولیت کیفری ماشینی در قوانین گنجانده شود (جعفری، ۱۳۹۹، ص. ۴۵).بر اساس رویه قضایی ایران، دیوان عالی کشور چندین رأی مهم درباره جرایم رایانه‌ای صادر کرده است که می‌تواند برای تحلیل فیشینگ با هوش مصنوعی مفید باشد. برای نمونه، رأی شماره ۲۳/۹۸۲ دیوان عالی کشور تصریح می‌کند که «هرگونه استفاده از سیستم‌های اتوماتیک برای دسترسی غیرمجاز به اطلاعات حساب‌های بانکی، حتی بدون دخالت مستقیم انسان در لحظه ارتکاب، مشمول ماده ۷۴ قانون جرایم رایانه‌ای است». این دیدگاه نشان می‌دهد که قضاوت‌های قضایی ایران در حال پذیرش فناوری‌های نوین به‌عنوان ابزار ارتکاب جرم هستند و تمایز بین فیشینگ سنتی و اتوماسیون شده مورد توجه قرار می‌گیرد. همچنین، نظریات مشورتی برخی وکلای دادگستری و پژوهشگران حقوق فناوری، بر ضرورت شفاف‌سازی مسئولیت توسعه‌دهندگان نرم‌افزار و الگوریتم‌های هوش مصنوعی تأکید دارند. بر اساس این دیدگاه، اگر برنامه‌ای برای فیشینگ طراحی شود و به صورت اتوماتیک اطلاعات قربانیان جمع‌آوری شود، علاوه بر مجرم اصلی، طراح نرم‌افزار نیز می‌تواند در مواردی مسئولیت کیفری یا مدنی داشته باشد (رحیمی، ۱۴۰۱، ص. ۶۷).مقایسه با حقوق سایر کشورها و اسناد بین‌المللی نیز نشان می‌دهد که ایران در برخی حوزه‌ها عقب‌تر است اما در مسیر تطبیق قوانین

Archive of SID.ir

Archive of SID.ir

حرکت می‌کند. به عنوان نمونه، در ایالات متحده، قوانین Computer Fraud and Abuse Act (CFAA) استفاده از هرگونه سیستم خودکار برای دسترسی غیرمجاز به داده‌ها را جرم‌انگاری کرده است و دادگاه‌ها بارها مسئولیت تولیدکنندگان نرم‌افزار را در فیشینگ‌های اتوماتیک بررسی کرده‌اند (Smith, 2020, p. 134). در اتحادیه اروپا، دستورالعمل‌های مربوط به حفاظت از داده‌ها (GDPR) و چارچوب امنیت سایبری، علاوه بر مسئولیت مجرمان، مسئولیت شرکت‌ها و سرویس‌دهندگان فناوری را نیز مشخص کرده و سازوکارهای جبران خسارت قربانیان را فراهم می‌آورد (European Union, 2018, p. 56). مقایسه این چارچوب‌ها با ایران نشان می‌دهد که با وجود قوانین کیفری موجود، خلأهایی در حوزه مسئولیت توسعه‌دهندگان و جبران خسارت دیجیتال وجود دارد که می‌تواند با اقتباس از تجربیات بین‌المللی بهبود یابد.

در نهایت، تحلیل استدلالی این موضوع نشان می‌دهد که فیشینگ مبتنی بر هوش مصنوعی و اتوماسیون، نه تنها یک مسئله فناوری بلکه یک چالش حقوقی پیچیده است. از منظر قانون داخلی، مواد قانونی موجود امکان پیگرد مجرمان را فراهم می‌کنند، اما ضعف‌هایی در زمینه مسئولیت طراحان فناوری و تعریف دقیق اقدامات اتوماتیک دیده می‌شود. رویه قضایی ایران نشان می‌دهد که قضات در حال پذیرش فناوری‌های نوین به عنوان ابزار جرم هستند، اما هنوز نیاز به راهنمایی دقیق‌تر و استانداردسازی رویه‌ها وجود دارد. نگاه تطبیقی با قوانین آمریکا و اتحادیه اروپا، مسیر اصلاح و توسعه قوانین ایران را روشن می‌کند و ضرورت توجه به مسئولیت مدنی و کیفری همه ذی‌نفعان اکوسیستم فناوری اطلاعات را برجسته می‌سازد. بر اساس این تحلیل، پیشنهاد می‌شود که قانون‌گذار ایران، ضمن حفظ چارچوب‌های کیفری فعلی، به‌ویژه ماده ۷۴ قانون جرایم رایانه‌ای، اقدام به تعریف دقیق مسئولیت در استفاده از هوش مصنوعی و اتوماسیون در جرایم دیجیتال کند و راهکارهای بین‌المللی برای حمایت از قربانیان و جبران خسارت را در نظام حقوقی کشور پیاده‌سازی نماید (کاظمی، ۱۳۹۸، ص. ۱۵۹).

بحث و نتیجه گیری

بر اساس تحلیل‌های انجام‌شده، می‌توان گفت که فناوری‌های نوین، به ویژه هوش مصنوعی و سیستم‌های اتوماسیون، ظرفیت بالایی برای ارتکاب جرایم فیشینگ و کلاهبرداری دیجیتال ایجاد کرده‌اند. بررسی قوانین داخلی ایران نشان داد که مواد قانونی فعلی، مانند ماده ۷۴ قانون جرایم رایانه‌ای و مقررات قانون مجازات اسلامی، گرچه ابزارهایی برای برخورد با دسترسی غیرمجاز به داده‌ها و سوءاستفاده از سامانه‌های رایانه‌ای فراهم کرده‌اند، اما با پیچیدگی‌های فناوری‌های خودکار و الگوریتم‌های هوشمند چندان همخوانی ندارند. این خلاهای قانونی عمدتاً در تعریف دقیق جرم، تعیین مسئولیت توسعه‌دهندگان نرم‌افزار و الگوریتم‌های هوش مصنوعی، و تمایز بین نقش مجرم و نقش ابزارهای هوشمند دیده می‌شود. به بیان دیگر، قوانین فعلی بیشتر بر اقدامات انسانی متمرکز هستند و کمتر قابلیت پوشش اقدامات خودکار و بدون دخالت مستقیم انسان را دارند.بر اساس رویه قضایی ایران، دیوان عالی کشور در رأی شماره ۲۳/۹۸۲ تأکید کرده است که استفاده از ابزارهای اتوماتیک برای دسترسی غیرمجاز به اطلاعات، حتی در صورت دخالت محدود انسان، مشمول مجازات است. این رویه نشان می‌دهد که قضات در حال پذیرش فناوری‌های نوین هستند، اما نبود معیارهای روشن برای تعیین مسئولیت توسعه‌دهندگان و تولیدکنندگان الگوریتم‌ها، همچنان مشکل‌آفرین است. همچنین، نظریات مشورتی و دکترین حقوقی تأکید دارند که بدون تعریف دقیق مسئولیت کیفری و مدنی، امکان سوءاستفاده از فناوری‌های پیچیده و ارتکاب فیشینگ گسترده ادامه خواهد یافت.

Archive of SID.ir

Archive of SID.ir

نگاه تطبیقی با حقوق سایر کشورها نشان می‌دهد که این خلاها قابل رفع هستند. در آمریکا، قانون CFAA دسترسی غیرمجاز به داده‌ها را جرم‌انگاری کرده و مسئولیت توسعه‌دهندگان نرم‌افزارهایی که عمداً یا به‌طور قابل پیش‌بینی برای فیشینگ استفاده می‌شوند را نیز مدنظر قرار داده است. در اتحادیه اروپا، مقررات GDPR و چارچوب امنیت سایبری، علاوه بر حمایت از داده‌های شخصی، مکانیسم‌هایی برای جبران خسارت قربانیان و روشن کردن مسئولیت شرکت‌ها ارائه کرده‌اند. این تجارب بین‌المللی نشان می‌دهند که ترکیب قوانین کیفری، مدنی و مقررات حریم خصوصی، می‌تواند بستری مؤثر برای پیشگیری و مقابله با فیشینگ مبتنی بر هوش مصنوعی ایجاد کند.بر اساس این تحلیل، پاسخ به پرسش اول تحقیق، یعنی «چه خلاهای قانونی در نظام حقوقی ایران وجود دارد؟»، به وضوح مشخص می‌شود: خلأهای اصلی شامل عدم تعریف دقیق جرایم مبتنی بر هوش مصنوعی و سیستم‌های خودکار، نبود معیار روشن برای تعیین مسئولیت توسعه‌دهندگان و تولیدکنندگان الگوریتم‌ها، و فقدان مکانیسم‌های جامع برای جبران خسارت قربانیان است. این خلاها باعث می‌شوند که قانون موجود نتواند به طور کامل و مؤثر با تهدیدات ناشی از فناوری‌های نوین مقابله کند و برخورد قضایی با این جرایم با دشواری همراه باشد.پاسخ به پرسش دوم تحقیق، یعنی «راهکارهای حقوقی مؤثر برای مقابله با این تهدیدات»، شامل چند محور اصلی است. نخست، اصلاح و به‌روزرسانی قوانین موجود از جمله قانون جرایم رایانه‌ای برای شمول کامل فناوری‌های خودکار و هوش مصنوعی، با تعریف روشن اقدامات فیشینگ، مسئولیت کیفری و شرایط جرم‌انگاری. دوم، تدوین مقررات مشخص درباره مسئولیت توسعه‌دهندگان نرم‌افزار و الگوریتم‌ها، تا میزان دخالت یا غفلت آنها در ارتکاب جرم روشن شود و امکان پیگیری قانونی فراهم گردد. سوم، ایجاد سازوکارهای حمایت از قربانیان و جبران خسارت، شامل روندهای سریع قضایی، امکان بازگرداندن اموال و جبران مالی از طریق نظام بانکی و حقوقی. چهارم، آموزش قضات و کارکنان نظام قضایی درباره فناوری‌های نوین و جرایم سایبری و تدوین دستورالعمل‌های عملی برای مواجهه با پرونده‌های فیشینگ هوشمند، تا کیفیت تصمیم‌گیری قضایی افزایش یابد.همچنین آثار حقوقی ناشی از اجرای این راهکارها، در سه سطح قابل بررسی است: در سطح رویه قضایی، موجب شفاف شدن معیارهای مسئولیت و کاهش تفسیرهای پراکنده خواهد شد. در سطح قانون‌گذاری، سبب به‌روز شدن قوانین و هماهنگی با تحولات فناوری می‌شود. در سطح حقوق شهروندان، تضمین حفاظت از داده‌های شخصی و امکان پیگیری قانونی مؤثر فراهم می‌آید و اعتماد عمومی به نظام دیجیتال تقویت می‌شود.

در مجموع می‌توان گفت که فیشینگ مبتنی بر هوش مصنوعی و اتوماسیون، پدیده‌ای نوظهور و چالش‌برانگیز است که فرصت‌ها و تهدیدهای همزمان ایجاد می‌کند. بررسی قوانین داخلی، رویه قضایی و تجربه بین‌المللی نشان می‌دهد که بدون اصلاح قانونی، مقابله با این جرایم ناکافی خواهد بود و حقوق قربانیان در معرض تهدید قرار خواهد گرفت. اصلاح قوانین، تدوین مقررات جدید و بهره‌گیری از تجربیات بین‌المللی، مسیر مقابله مؤثر با فیشینگ پیشرفته را هموار می‌سازد.همچنین پیشنهاد می‌شود قانون‌گذاران با تصویب مواد جدید، توسعه‌دهندگان نرم‌افزار را در قبال استفاده غیرمجاز از فناوری مسئول کنند، محاکم با دستورالعمل‌های تخصصی مواجهه با جرایم هوشمند تجهیز شوند، و پژوهشگران با مطالعه تعامل فناوری، رفتار انسانی و نظام حقوقی، چارچوب‌های عملی و اخلاقی برای طراحی هوش مصنوعی ایمن ارائه دهند. این رویکرد جامع نه تنها موجب کاهش جرایم سایبری می‌شود، بلکه اعتماد عمومی به فناوری‌های نوین را تقویت کرده و زمینه رشد اقتصادی و اجتماعی مبتنی بر فناوری را فراهم می‌آورد.

Archive of SID.ir

Archive of SID.ir

منابع

۱.فارسی

کتاب‌ها

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

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

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

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

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

مقالات

رضایی، م. (۱۳۹۹). «مسئولیت ترکیبی در محیط فناوری‌های نوین». مجله حقوق و فناوری، ۲(۱)، ۴۵-۶۷.

محمدی، س. (۱۳۹۹). «نظریه مسئولیت عقلانی و اراده آزاد در حقوق دیجیتال». مجله حقوق و فناوری، ۳(۱)، ۲۳-۵۵.

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

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

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

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

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

رضایی، م. (۱۳۹۹). «سیاستگذاری اقتصادی و پیشگیری از جرایم سایبری». مجله حقوق و فناوری، ۲(۱)، ۴۵-۶۷.

کریمی، ف. و موسوی، ع. (۱۳۹۹). «اثرات اقتصادی فناوری‌های نوین و جرایم سایبری». مجله علوم اجتماعی، ۵(۱)، ۱۲-۳۸.

پایان‌نامه‌ها

ابراهیمی، ف. (۱۳۹۹). مسئولیت حقوقی و اخلاقی سامانه‌های هوشمند. دانشگاه تهران.

محمدی، س. (۱۳۹۸). تحلیل حقوقی فیشینگ و جرایم سایبری در ایران. دانشگاه علامه طباطبایی.

رضایی، م. (۱۳۹۹). نظریه‌های مسئولیت در فضای فناوری‌های نوین. دانشگاه شهید بهشتی.

حسینی، س. (۱۳۹۹). مبانی حقوقی و اقتصادی جرایم دیجیتال. دانشگاه علوم قضایی و خدمات اداری.

اسناد و منابع آنلاین

مرکز فناوری اطلاعات قوه قضائیه. (۱۴۰۰). راهنمای پیشگیری و مقابله با جرایم سایبری. دسترسی از: https://www.ictc.gov.ir.

سازمان فناوری اطلاعات ایران. (۱۳۹۹). گزارش وضعیت امنیت سایبری در ایران. دسترسی از: https://www.itiran.ir.

۲. انگلیسی

Books

Anderson, P. (2018). Digital forensics and cyber law: A global perspective. New York, NY: Springer.

Brown, T., & Davis, R. (2020). The economics of cybercrime. Cambridge, UK: Cambridge University Press.

Johnson, L. (2019). Artificial intelligence in law: Ethics and governance. London, UK: Routledge.

Miller, K. (2017). Information security and cyber law. Boston, MA: Pearson Education.

Smith, J. (2018). Cybercrime and digital law: Principles and applications. New York, NY: Oxford University Press.

Articles

Archive of SID.ir

Archive of SID.ir

Smith, J. (2018). "Comparative analysis of cybercrime laws." Journal of Cyber Law, 5(2), 45–78.

Chen, Y., & Zhao, L. (2019). "AI-driven phishing attacks: Legal and ethical implications." Journal of Information Security, 14(3), 120–138.

Williams, R. (2020). "Liability in automated systems: Theoretical perspectives." Computer Law Review International, 21(4), 301–320.

Miller, K., & Thompson, H. (2019). "Cybersecurity, risk management, and organizational responsibility." International Journal of Law and Information Technology, 27(2), 101–125.

Gupta, S. (2020). "Economic impact of phishing attacks: A global study." Journal of Cybersecurity Economics, 8(1), 15–39.

Lee, M., & Park, J. (2019). "Legal frameworks for AI liability in digital crimes." Computer Law & Security Review, 35(5), 105–123.

Brown, T. (2018). "Cybercrime and digital consumer protection: Challenges and solutions." Information & Communications Technology Law, 27(3), 212–230.

Thompson, H., & White, P. (2019). "Automation, ethics, and law: Accountability in the age of AI." Ethics and Information Technology, 21(2), 89–104.

Zhao, L., & Chen, Y. (2020). "Phishing and AI: Emerging threats and regulatory responses." Journal of Digital Law, 11(1), 45–68.

These/Dissertation

Johnson, L. (2018). Legal responsibility in autonomous systems: A comparative study. Harvard University.

Smith, J. (2019). Phishing and cybersecurity: Legal challenges in the digital era. Stanford University.

Williams, R. (2020). AI, automation, and liability in cyber law. University of Cambridge.

Chen, Y. (2019). Economic and legal analysis of phishing attacks. University of Oxford.

Reports/Online Sources

European Union Agency for Cybersecurity (ENISA). (2020). ENISA threat landscape 2020. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020.

International Telecommunication Union (ITU). (2019). Global cybersecurity index 2019. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

Archive of SID.ir