Iran. J. Insur. Res., **(*): *-*, ****** ***

Iranian Journal of Insurance Research
(IJIR)
Homepage: https://ijir.irc.ac.ir/?lang=en

Legal and Criminological Analysis of Cybercrimes in the Digital Insurance Ecosystem

Mostafa Pakniat [1,*], khadijeh Mozafari [2]

[1] *Assistant Professor,Department of Law, Faculty of Social Sciences and Economics, Alzahra University, Tehran, Iran*

[2] *Assistant Professor,Department of Law, Faculty of Social Sciences and Economics, Alzahra University, Tehran, Iran*

ARTICLE INFO

***KEYWORDS*:**
Blockchain, Cybercrimes, Digital insurance, Regulatory technologies, Public trust

ABSTRACT

BACKGROUND AND OBJECTIVES: The rapid digital transformation of the insurance industry has fundamentally reshaped contemporary insurance systems and altered traditional mechanisms of risk assessment, policy issuance, claims management, and customer interaction.Technologies such as artificial intelligence (AI), machine learning, blockchain, cloud computing, big data analytics, and Internet of Things (IoT) infrastructures have enabled insurers to automate operational processes, improve efficiency, reduce costs, and provide highly personalized insurance services. At the same time, however, the growing dependence on digital platforms and automated systems has generated complex legal, regulatory, cybersecurity, and criminological challenges that traditional insurance law and conventional liability doctrines are not fully equipped to address. The increasing use of electronic and smart insurance contracts, AI-assisted decision-making systems, and large-scale data-processing mechanisms has raised important questions concerning the validity and enforceability of digital contracts, the legal status of electronic signatures and AI-generated outputs, the attribution of liability in automated systems, and the protection of sensitive personal data. In parallel, the digital insurance ecosystem has become a highly attractive target for cybercriminal activities because of the concentration of valuable financial, medical, behavioral, and personal information within interconnected digital infrastructures. Insurance companies, policyholders, online insurance intermediaries, cloud-service providers, software developers, and third-party data processors are all exposed to sophisticated forms of cybercrime, including ransomware attacks, phishing operations, identity theft, manipulation of digital evidence, unauthorized access to databases, and algorithmic fraud. These developments challenge traditional criminal justice mechanisms and require integrated approaches combining legal regulation, cybersecurity governance, and criminological prevention strategies. Accordingly, this study seeks to analyze the legal and criminological dimensions of cybercrimes within the digital insurance ecosystem through an interdisciplinary framework. The research examines the validity and legal nature of electronic and smart insurance contracts, the implications of AI-based insurance systems and algorithmic governance, the vulnerabilities associated with data-driven insurance practices, and the typology of cyber threats targeting insurance infrastructures.

METHODS: This study adopts a descriptive–analytical methodology grounded in interdisciplinary legal and criminological inquiry. The analytical framework combines doctrinal legal analysis, comparative regulatory evaluation, and criminological assessment in order to provide a comprehensive understanding of cyber threats

within the digital insurance environment. The research draws upon principles derived from insurance law, information technology law, cyber law, electronic commerce regulations, data-protection frameworks, and contemporary theories of cyber criminology. A comparative approach was employed to examine domestic legal norms alongside selected international regulatory frameworks governing electronic contracts, digital signatures, AI-based systems, cybersecurity obligations, and data governance in the insurance sector. Data collection relied on the examination of legislative instruments, judicial doctrines, academic literature, policy papers, cybersecurity reports, and supervisory guidelines issued by insurance institutions and cybersecurity agencies. In addition, documented case studies involving cyberattacks against insurance and financial infrastructures were analyzed in order to identify patterns of vulnerability and emerging forms of digital insurance fraud. The study also incorporates insights from previous scholarship concerning fintech regulation, algorithmic governance, regulatory technologies (RegTech), automated contracting systems, and AI-assisted compliance mechanisms. The analytical process integrates conceptual analysis, comparative legal evaluation, criminological classification of cyber threats, and normative assessment of liability-allocation mechanisms within partially autonomous technological systems.

FINDINGS: The findings demonstrate that electronic and smart insurance contracts possess distinctive characteristics that significantly challenge traditional legal doctrines governing contract formation, interpretation, performance, and liability. Automated contractual execution through blockchain-based smart contracts, algorithmic processing of claims, real-time data dependency, and delegation of decision-making functions to AI systems complicate the determination of genuine consent, contractual intent, and mutual understanding between parties. The research further reveals that existing legal frameworks, particularly within Iranian law, continue to face significant gaps regarding the evidentiary validity of digital data, the authentication of electronic signatures, the legal recognition of AI-generated decisions, and the attribution of civil liability arising from coding defects, cybersecurity breaches, or unpredictable behavior of autonomous systems. From a criminological perspective, the study confirms that the digital insurance ecosystem constitutes a highly vulnerable environment exposed to a broad spectrum of cyber threats. The typology of cybercrimes identified in this research includes unauthorized access to insurance databases, theft of personal and financial data, ransomware attacks, phishing schemes, identity theft, manipulation of algorithmic systems, distributed denial-of-service (DDoS) attacks, and fraudulent claims supported by fabricated digital evidence. The findings also indicate that algorithmic opacity and excessive reliance on automated systems may generate discriminatory outcomes, inaccurate risk classifications, and unjustified denial of insurance benefits, thereby raising concerns regarding transparency, accountability, and procedural fairness. At the same time, the study demonstrates that advanced technologies can strengthen predictive and preventive capacities through anomaly-detection systems, automated fraud-detection mechanisms, blockchain verification tools, and AI-assisted cybersecurity management.

CONCLUSION: The study concludes that effective governance of the digital insurance ecosystem and meaningful prevention of cybercrimes require a multidimensional strategy integrating legal reform, regulatory modernization, institutional coordination, cybersecurity resilience, and technological innovation. The findings underscore the necessity of adopting specialized legal frameworks governing smart insurance contracts and automated insurance operations, clarifying the legal status of AI-generated outputs, establishing coherent liability regimes for autonomous systems, and developing cybersecurity standards proportionate to the sensitivity of insurance-related data. The research further highlights the importance of strengthening supervisory technologies, promoting algorithmic transparency and accountability, enhancing digital literacy among stakeholders, and expanding international cooperation in combating cybercrime. Ultimately, the sustainability of digital insurance systems depends upon achieving an appropriate balance between

technological innovation, operational efficiency, cybersecurity protection, legal certainty, and protection of policyholders' rights.

Iran. J. Insur. Res., **(*): *-*, ****** ***

Iranian Journal of Insurance Research
(IJIR)
Homepage: https://ijir.irc.ac.ir/?lang=fa

تحلیل حقوقی و جرم‌شناختی جرایم سایبری در اکوسیستم بیمه دیجیتال

مصطفی پاک نیت*[۱]، خدیجه مظفری[۲]

[۱] استادیار، گروه حقوق، دانشکده علوم اجتماعی و اقتصادی، دانشگاه الزهرا، تهران، ایران.
[۲] استادیار، گروه حقوق، دانشکده علوم اجتماعی و اقتصادی، دانشگاه الزهرا، تهران، ایران.

چکیده

پیشینه و اهداف: تحول دیجیتال در صنعت بیمه با گسترش فناوری‌هایی مانند هوش مصنوعی، کلان‌داده، اینترنت اشیا و سامانه‌های ابری، ساختار سنتی روابط بیمه‌ای را دگرگون ساخته و چالش‌های نوینی را در حوزه حقوق قراردادها، مسئولیت مدنی و امنیت سایبری ایجاد کرده است. پژوهش حاضر با تمرکز بر قراردادهای الکترونیکی و هوشمند بیمه، به بررسی اعتبار، ماهیت و آثار حقوقی این قراردادها و نیز تحلیل جرم‌شناختی تهدیدهای سایبری در اکوسیستم بیمه دیجیتال می‌پردازد. همچنین چالش‌های مربوط به احراز اراده و رضایت طرفین، انتساب تعهدات به سامانه‌های خودکار و آثار ناشی از تصمیم‌گیری الگوریتمی مورد مطالعه قرار گرفته است.

روش‌شناسی: این پژوهش با رویکرد توصیفی ـ تحلیلی و با بهره‌گیری از مبانی حقوق فناوری اطلاعات، حقوق بیمه و نظریه‌های جرم‌شناسی سایبری انجام شده است. داده‌ها از طریق بررسی قوانین و مقررات داخلی و بین‌المللی، گزارش‌های تخصصی نهادهای بیمه‌ای و امنیتی، مطالعات تطبیقی و تحلیل نمونه‌های موردی جرایم سایبری در صنعت بیمه گردآوری شده‌اند. روش تحلیل نیز مبتنی بر تلفیق تحلیل مفهومی، بررسی تطبیقی و ارزیابی کارکردی فرصت‌ها و تهدیدهای ناشی از فناوری‌های نوین است.

یافته‌ها: نتایج پژوهش نشان می‌دهد قراردادهای هوشمند بیمه به دلیل خوداجرا بودن، وابستگی به داده‌های بلادرنگ و استفاده از الگوریتم‌های تصمیم‌گیر، چالش‌هایی جدی در زمینه احراز اراده واقعی طرفین، تفسیر شروط قراردادی، اثبات تعهدات و تعیین حدود مسئولیت ایجاد می‌کنند. بررسی تطبیقی نشان داد حقوق ایران در زمینه اعتبار اسناد دیجیتال، جایگاه حقوقی خروجی‌های هوش مصنوعی و تعیین مسئولیت ناشی از خطا یا رفتار غیرقابل پیش‌بینی سامانه‌های هوشمند با خلأهای تقنینی مواجه است. همچنین اکوسیستم بیمه دیجیتال در معرض تهدیدهایی نظیر جعل و دستکاری داده‌ها، حملات باج‌افزاری، سرقت اطلاعات، نفوذ به سامانه‌ها و دستکاری الگوریتم‌های ارزیابی ریسک قرار دارد. در عین حال، فناوری‌های هوشمند می‌توانند از طریق تحلیل رفتاری، نظارت پیشگیرانه و کشف الگوهای مجرمانه، ظرفیت‌های مؤثری برای پیشگیری و مقابله با جرایم سایبری فراهم کنند.

نتیجه‌گیری: مقابله مؤثر با جرایم سایبری در صنعت بیمه مستلزم اتخاذ رویکردی جامع و چندبعدی است که اصلاحات حقوقی، توسعه زیرساخت‌های فنی، ارتقای استانداردهای امنیت سایبری و تقویت نظارت بر سامانه‌های هوشمند را به‌صورت همزمان دنبال کند. نتایج تحقیق بر ضرورت تدوین مقررات ویژه برای قراردادهای هوشمند، تبیین وضعیت حقوقی تصمیمات مبتنی بر هوش مصنوعی و طراحی نظام مسئولیت‌پذیری متناسب با فناوری‌های نوین تأکید دارد. آینده حکمرانی داده و مدیریت ریسک در صنعت بیمه وابسته به ایجاد تعادل میان نوآوری فناورانه، امنیت و حمایت مؤثر از حقوق ذی‌نفعان خواهد بود.

کلمات کلیدی:
اعتماد عمومی، بلاکچین، بیمه دیجیتال، جرایم سایبری، فناوری های نظارتی،

مقدمه

با دگرگون‌سازی ساختارها و فرآیندهای صنعت بیمه، بستر جدیدی تحت عنوان «بیمه دیجیتال» پدید آمده است؛ بستری که در آن قراردادهای الکترونیکی، بیمه‌نامه‌های مبتنی بر بلاک‌چین و الگوریتم‌های هوش مصنوعی نقش محوری در ارائه خدمات ایفا می‌کنند. این تغییرات هرچند موجب افزایش کارآمدی، کاهش هزینه‌ها و ارتقای کیفیت خدمات شده، اما هم‌زمان الگوهای نوینی از جرایم سایبری را نیز در اکوسیستم بیمه ایجاد کرده است (Zucca, 2025; Zucca & Fiorinelli, 2025)؛ جرایمی که از نفوذ به سامانه‌ها و سرقت داده‌ها تا جعل بیمه‌نامه‌های دیجیتال، دستکاری ارزیابی خسارات و سوءاستفاده از داده‌های حساس را در بر می‌گیرد. این وضعیت، پرسش‌های بنیادینی را درباره حدود اعتبار حقوقی ابزارهای نوین بیمه‌ای، مسئولیت ناشی از نقض امنیت داده‌ها و ماهیت جرم‌شناختی تهدیدهای سایبری در صنعت بیمه مطرح می‌سازد.

مسئله اصلی پژوهش آن است که مقررات موجود در حقوق ایران — از جمله قانون تجارت الکترونیکی و قانون جرایم رایانه‌ای — پاسخگوی پیچیدگی‌های قراردادهای هوشمند، عملکرد الگوریتم‌های خودکار و جرایم سایبری ساختاریافته در حوزه بیمه نیستند.

بر همین اساس، هدف پژوهش تحلیل جامع چالش‌های حقوقی و جرم‌شناختی جرایم سایبری در بیمه دیجیتال است.

ضرورت انجام پژوهش از آن‌روست که بیمه دیجیتال در ایران با سرعتی فزاینده در حال گسترش است، اما چارچوب حقوقی و جرم‌شناختی موجود توان پاسخ‌گویی به تهدیدات نوظهور را ندارد؛ تهدیداتی که در صورت بی‌توجهی می‌توانند اعتماد عمومی به صنعت بیمه، ثبات مالی و امنیت داده‌های شهروندان را با خطر مواجه سازند. نوآوری این تحقیق نیز در پیوند دادن سه حوزه حقوق، جرم‌شناسی و فناوری‌های نظارتی و ارائه الگویی یکپارچه برای مواجهه با مخاطرات بیمه دیجیتال است.

مبانی نظری پژوهش

تحلیل جرایم سایبری در بیمه دیجیتال مستلزم بهره‌گیری از چارچوب‌های نظری چندرشته‌ای است که بتواند ابعاد حقوقی، فنی و جرم‌شناختی این پدیده را تبیین کند.

این پژوهش بر مجموعه‌ای از رویکردها و تئوری‌های حقوقی و جرم‌شناختی استوار است. در حوزه جرم‌شناسی، نظریه‌های فرصت، انتخاب عقلانی و فعالیت‌های روزمره توضیح می‌دهند که چگونه ساختارهای فناورانه، دسترسی آسان، اختفای هویت و امکان ارتکاب کم‌هزینه، شرایط مساعدی برای وقوع جرایم سایبری فراهم می‌سازد.

بر اساس نظریه فعالیتهای روزمره جرم زمانی رخ می‌دهد که ۳ ضلع یک مثلث در زمان و مکانی واحد با یکدیگر تلاقی کنند. در فضای بیمه دیجیتال، مکان فیزیکی به فضای سایبر تبدیل می‌شود (Cohen & Felson, 1979 ; Felson, 2008)

الف) هدف مناسب : داده‌های هویتی و مالی در پورتال‌های بیمه :کاربرانی که برای تمدید سریع بیمه شخص ثالث یا بدنه به سایت‌ها مراجعه می‌کنند. **بیمه‌گذاران منتظر دریافت خسارت،** افرادی که به تازگی تصادف کرده یا خسارت درمانی داشته‌اند و منتظر واریز پول هستند، به شدت در برابر پیامک‌های جعلی («خسارت شما تایید شد، جهت دریافت وارد لینک شوید») آسیب‌پذیرند.

ب) نبود نگهبان توانمند : نگهبانان انسانی :ضعف آگاهی عمومی کاربران و عدم آموزش آن‌ها توسط شرکت‌های بیمه درباره نحوه تشخیص دامنه‌های رسمی. **نگهبانان تکنولوژیک :**نبود فیلترینگ هوشمند پیامک‌های جعلی در اپراتورها، عدم استفاده شرکت‌های بیمه از پروتکل‌های امنیتی پیشرفته برای ایمیل‌ها یا سرشماره‌های پیامکی ماسک‌شده و اختصاصی و نبود سیستم‌های پایش مداوم برای شناسایی دامنه‌های فیشینگ کلون‌شده

ج) مجرم باانگیزه:فیشرهایی که می‌دانند صنعت بیمه با جریان مالی کلان سروکار دارد و با ساخت یک صفحه درگاه پرداخت جعلی به نام سامانه یکپارچه تخفیف بیمه مرکزی، می‌توانند اطلاعات کارت بانکی صدها نفر را در چند ساعت سرقت کنند.

نظریه فرصت نیز بر این باور است که فرصت، ایجادکننده جرم است. طراحی زیرساخت پلتفرم‌های بیمه دیجیتال اگر بدون پیوست امنیتی باشد، خود مولد فرصت مجرمانه است؛ پلتفرم‌های بیمه‌ای برای جلب رضایت مشتری، فرآیند صدور و پرداخت خسارت را بسیار سریع و با حداقل نظارت انسانی طراحی می‌کنند. این سرعت و سهولت، فرصتی طلایی برای فیشرهاست تا پلتفرم‌های فرعی یا صفحات واسط جعلی ایجاد کنند و از تمایل مشتری به «خرید ۲ دقیقه‌ای بیمه» سوءاستفاده کنند. همچنین رشد قارچ‌گونه سایت‌های مقایسه قیمت بیمه، بازاری آشفته ایجاد می‌کند که در آن کاربران به راحتی تفاوت میان یک پلتفرم قانونی جدید و یک سایت فیشینگ را تشخیص نمی‌دهند.

رویکردهای بزه‌دیده‌شناسی دیجیتال نیز بیان می‌کنند که **سبک زندگی دیجیتال** کاربر است که احتمال قربانی شدن او را تعیین می‌کند. کاربران با آگاهی فنی پایین، کارکنان بیمه و حتی شرکت‌های بیمه، به دلیل وابستگی شدید به سامانه‌های دیجیتال و ناآگاهی نسبت به تهدیدات، چگونه در معرض بزه‌دیدگی سایبری قرار می‌گیرند. بزه‌دیدگان فیشینگ بیمه‌ای معمولاً افرادی هستند که بدون چک کردن آدرس بار(URL) ، صرفاً به دلیل وجود لوگوی رسمی شرکت بیمه یا «بیمه مرکزی» روی صفحه، اطلاعات حساس خود را وارد می‌کنند. پاشنه آشیل بزه‌دیدگان، رفتارهای اقتصادی آن‌ها در فضای مجازی است. فیشرها با کلیدواژه‌هایی مثل «٪۷۰ تخفیف بیمه شخص ثالث فقط تا پایان امشب»، سد دفاع عقلانی کاربر (بزه‌دیده بالقوه) را می‌شکنند.

نکته حائز اهمیت اینکه **در بیشتر موارد** پلتفرم بیمه پس از لو رفتن اطلاعات کاربران در اثر فیشینگ یا هک، مسئولیت را به گردن خود کاربر می‌اندازد («خودت رمزت را دادی») و با عدم پشتیبانی حقوقی و فنی، بزه دیدگی او را تشدید می‌کند.

مروری بر پیشینه پژوهش

۱. پیشینه نظری

پیشینه نظری این پژوهش بر مجموعه‌ای از رویکردها و تئوری‌های حقوقی و جرم‌شناختی استوار است که ابعاد مختلف جرایم سایبری در اکوسیستم بیمه دیجیتال را تبیین می‌کنند. در حوزه جرم‌شناسی، نظریه‌های فرصت، انتخاب عقلانی و فعالیت‌های روزمره توضیح می‌دهند که چگونه ساختارهای فناورانه، دسترسی آسان، اختفای هویت و امکان ارتکاب کم‌هزینه، شرایط مساعدی برای وقوع جرایم سایبری فراهم می‌سازد.

رویکردهای بزه‌دیده‌شناسی دیجیتال نیز بیان می‌کنند که کاربران با آگاهی فنی پایین، کارکنان بیمه و حتی شرکت‌های بیمه، به دلیل وابستگی شدید به سامانه‌های دیجیتال و ناآگاهی نسبت به تهدیدات، چگونه در معرض بزه‌دیدگی سایبری قرار می‌گیرند.

از منظر حقوقی، نظریه‌های مرتبط با اعتبار اسناد الکترونیکی، ماهیت قراردادهای هوشمند و مسئولیت مدنی و کیفری ناشی از عملکرد سیستم‌های خودکار بنیان اصلی تحلیل را تشکیل می‌دهد. این رویکردها نشان می‌دهند که چگونه توسعه بیمه دیجیتال ـ از بیمه‌نامه‌های الکترونیکی تا قراردادهای هوشمند مبتنی بر بلاک‌چین ـــ مرزهای سنتی قرارداد بیمه را تغییر داده و پرسش‌های جدیدی درباره اعتبار امضاهای دیجیتال، تفسیر شروط خوداجرا و مسئولیت ناشی از خطای الگوریتم ایجاد کرده است.

نظریه‌های حکمرانی داده و حریم خصوصی دیجیتال نیز اهمیت حفاظت از داده‌های حساس بیمه‌گذاران را تبیین می‌کنند و بر ضرورت وجود نظام حقوقی شفاف برای پردازش، ذخیره و تبادل داده‌ها تأکید دارند. مجموعه این رویکردها چارچوب نظری لازم برای تحلیل حقوقی و جرم‌شناختی جرایم سایبری در بیمه دیجیتال را فراهم می‌سازد.

۲. پیشینه تجربی

پژوهش‌های تجربی داخلی و خارجی درباره جرایم سایبری در صنعت بیمه عمدتاً بر سه محور تمرکز داشته‌اند: تهدیدشناسی سایبری در بیمه، تحلیل بزه‌دیدگی دیجیتال و ارزیابی اثربخشی فناوری‌های نظارتی.

مطالعات خارجی در سال‌های اخیر با استفاده از روش‌های مطالعه موردی، تحلیل داده‌های بزرگ، پیمایش‌های تخصصی و آزمایش‌های الگوریتمی به بررسی موضوعاتی مانند نفوذ به سامانه‌های بیمه‌ای، حملات باج‌افزاری، جعل بیمه‌نامه، انحراف الگوریتمی، سوءاستفاده از داده‌های پزشکی و عملکرد قراردادهای هوشمند پرداخته‌اند. این پژوهش‌ها نشان داده‌اند که ضعف احراز هویت دیجیتال، نقص در معماری امنیتی سامانه‌ها و نبود استانداردهای مشترک، مهم‌ترین عوامل مؤثر بر گسترش جرایم سایبری هستند.

در مطالعات داخلی نیز بخش عمده پژوهش‌ها با روش اسنادی–تحلیلی یا پیمایش محدود انجام شده و بیشتر بر موضوعاتی چون «چالش‌های حقوقی شناسایی امضای الکترونیکی»، «تهدیدهای سایبری در بیمه‌های آنلاین»، «آسیب‌پذیری داده‌های مشتریان»، «خلأهای قانون جرایم رایانه‌ای در پوشش پدیده‌های نوین» و «مشکلات امنیتی شرکت‌های بیمه» متمرکز بوده‌اند. با این حال، اغلب این تحقیقات فاقد رویکرد تلفیقی میان حقوق، جرم‌شناسی و فناوری بوده و کمتر به نقش فناوری‌های نظارتی و کارکردهای آن‌ها در پیشگیری از جرایم پرداخته‌اند.

بررسی مجموع پیشینه تجربی نشان می‌دهد که شکاف پژوهشی اصلی در دو حوزه قرار دارد:

الف: نبود پژوهش جامع درباره پیوند سه‌گانه حقوق – جرم‌شناسی – فناوری نظارتی در زمینه بیمه دیجیتال؛

ب: فقدان مدل عملیاتی برای تبیین رابطه میان جرایم سایبری، آسیب‌پذیری داده‌ها، نقش فناوری نظارتی و سطح امنیت بیمه دیجیتال.

پژوهش حاضر با تمرکز بر این خلأها، تلاش می‌کند تصویری یکپارچه و مبتنی بر شواهد از نقش فناوری‌های نظارتی در مواجهه با جرایم سایبری بیمه دیجیتال ارائه کند.

روش‌شناسی پژوهش

پژوهش حاضر از نوع کیفی و با رویکرد توصیفی ـ تحلیلی انجام شده است. داده‌های پژوهش از طریق مطالعه اسناد حقوقی، منابع کتابخانه‌ای و تحلیل متون تخصصی گردآوری شده‌اند. جامعه اسنادی پژوهش شامل: الف) قوانین و مقررات ایران از جمله قانون بیمه (۱۳۱۶)، قانون تجارت الکترونیکی (۱۳۸۲)، قانون جرایم رایانه‌ای (۱۳۸۸)، آیین‌نامه‌های بیمه مرکزی و دستورالعمل‌های مرتبط با خدمات الکترونیکی بیمه؛ ب) اسناد بین‌المللی شامل مقررات جی دی آر[۱]، مقررات ای‌داس[۲] و کنوانسیون بوداپست درباره جرایم سایبری؛ و ج) گزارش‌های تخصصی انیسا [۳] و مطالعات علمی منتشرشده در فاصله زمانی ۲۰۱۸ تا ۲۰۲۵ بوده است.

در بخش تطبیقی، سه محور «حفاظت از داده‌های بیمه‌ای»، «اعتبار امضای الکترونیکی در قراردادهای بیمه» و «مسئولیت ناشی از نقض امنیت سایبری» به عنوان واحد تحلیل انتخاب شدند. معیار انتخاب این محورها، بیشترین ارتباط آن‌ها با فرایند انعقاد، اجرای و نظارت بر قراردادهای بیمه دیجیتال بوده است.

چارچوب تحلیلی پژوهش بر تلفیق سه حوزه حقوق بیمه، جرم‌شناسی سایبری و حکمرانی فناوری استوار است. در بعد حقوقی، اعتبار قراردادهای الکترونیکی، مسئولیت ناشی از پردازش داده‌ها و الزامات حمایت از اطلاعات بیمه‌ای بررسی شده است. در بعد جرم‌شناختی، از نظریه‌های فعالیت‌های روزمره، انتخاب عقلانی و بزه‌دیده‌شناسی دیجیتال برای تبیین زمینه‌های وقوع جرایم سایبری در بیمه دیجیتال استفاده شده است. در بعد فناوری نیز نقش فناوری‌های نظارتی، سامانه‌های احراز هویت دیجیتال و ابزارهای تحلیل داده در پیشگیری و کشف جرایم مورد ارزیابی قرار گرفته است..

نتایج و بحث

۱- تحلیل حقوقی جرایم سایبری در اکوسیستم بیمه دیجیتال

---

[۱] - مقررات عمومی حفاظت از داده اتحادیه اروپا (The General Data Protection Regulation (GDPR) (EU) 2016/679)

[۲] - چارچوب قانونی اتحادیه اروپا برای شناسایی الکترونیکی و خدمات اعتماد دیجیتال eIDAS (Electronic Identification, Authentication and Trust Services)

[۳] -آژانس امنیت سایبری اتحادیه اروپا (The European Union Agency for Cybersecurity, ENISA)

بررسی منابع نشان می‌دهد یکی از مهم‌ترین چالش‌های حقوقی در ایران، فقدان قانون جامع حفاظت از داده‌های شخصی است. بیمه به‌عنوان یکی از مهم‌ترین نهادهای حقوق خصوصی و ابزار مدیریت ریسک، همواره متکی بر قرارداد بوده است. قرارداد بیمه سنتی معمولاً به‌صورت حضوری، با ارائه فرم‌های کاغذی و امضای طرفین منعقد می‌شد. با گسترش فناوری‌های اطلاعاتی، بیمه به تدریج به فضای دیجیتال منتقل شد و امروز پدیده‌ای به نام بیمه دیجیتال[1] شکل گرفته است. پرسش اساسی این است که از منظر حقوقی، ماهیت بیمه دیجیتال چیست؟ آیا همان قرارداد بیمه سنتی است که صرفاً در بستر الکترونیکی انجام می‌شود، یا نهادی جدید با ماهیت متفاوت است؟

۲-۱- ماهیت حقوقی بیمه دیجیتال

بیمه دیجیتال به مجموعه فرایندها و خدمات بیمه‌ای گفته می‌شود که به‌طور کامل یا عمده در بستر فناوری دیجیتال ارائه می‌شوند. این شامل مراحل مختلف از بازاریابی و انعقاد قرارداد تا مدیریت خسارت و پرداخت غرامت است. بیمه دیجیتال می‌تواند در سه سطح ظهور کند:

سطح اول: بیمه‌نامه‌های سنتی که صرفاً به‌صورت الکترونیکی صادر و نگهداری می‌شوند (مانند صدور آنلاین بیمه شخص ثالث).

سطح دوم: استفاده از فناوری‌های نوین مانند اپلیکیشن‌های موبایلی، هوش مصنوعی و تحلیل داده برای ارائه خدمات (مانند محاسبه آنلاین حق بیمه بر اساس داده‌های رانندگی واقعی).

سطح سوم: بیمه‌نامه‌های مبتنی بر قراردادهای هوشمند و بلاک‌چین که بدون دخالت مستقیم انسان و به‌طور خودکار اجرا می‌شوند.

بیمه دیجیتال با بهره‌گیری از فناوری‌های اطلاعاتی، قراردادهای بیمه‌ای را در قالب الکترونیک یا حتی قراردادهای هوشمند بلاک‌چین منعقد می‌سازد. بیمه دیجیتال از منظر حقوقی یک عقد بیمه است که در بستر دیجیتال منعقد می‌شود. ماهیت آن همچنان مبتنی بر اصول سنتی بیمه است، اما شکل و سازوکارهای آن تحول یافته‌اند. چالش‌هایی چون اعتبار امضاهای دیجیتال، مسئولیت در قراردادهای هوشمند و حمایت از داده‌های شخصی ایجاب می‌کند که قانون‌گذار با وضع مقررات ویژه، چارچوبی روشن برای بیمه دیجیتال فراهم کند. در غیر این صورت، هم بیمه‌گذاران و هم شرکت‌های بیمه با ناامنی حقوقی مواجه خواهند بود.

پرسش بنیادین در اینجا اعتبار حقوقی چنین قراردادهایی است. در حقوق ایران، قانون تجارت الکترونیکی (۱۳۸۲) و قانون جرایم رایانه‌ای (۱۳۸۸) بستر حداقلی را برای شناسایی اسناد و امضای الکترونیکی فراهم ساخته‌اند، اما همچنان ابهامات جدی درخصوص بیمه‌نامه‌های هوشمند و اعتبار تعهدات خودکار وجود دارد؛ مطابق ماده ٦ قانون تجارت الکترونیکی مصوب ۱۳۸۲، هرگاه وجود یک نوشته از نظر قانون لازم باشد، داده‌پیام در حکم نوشته است.(به استثنای اسناد مالکیت اموال غیرمنقول). همچنین ماده ۷ همین قانون امضای الکترونیکی را معتبر دانسته است. در این چارچوب بیمه دیجیتال از نظر ماهیت حقوقی، عقد بیمه سنتی است که در بستر الکترونیکی منعقد و اجرا می‌شود، اما این تحول شکلی، چالش‌های جدیدی در اعتبار اسناد، مسئولیت و حفاظت از داده‌ها ایجاد کرده است.

۲-۲- چالش های حقوقی بیمه دیجیتال

۲-۲-۱- اعتبار امضاهای دیجیتال

یکی از نخستین و مهم‌ترین چالش‌های حقوقی در بیمه دیجیتال، موضوع اعتبار امضاهای دیجیتال است. در قراردادهای سنتی بیمه، امضای طرفین بر روی نسخه کاغذی بیمه‌نامه نشانه‌ای از قصد و رضای آنان برای انعقاد عقد محسوب می‌شد. اما در فضای دیجیتال، قرارداد بیمه معمولاً به‌صورت فایل الکترونیکی یا حتی یک قرارداد هوشمند در بستر بلاک‌چین شکل می‌گیرد و به‌جای امضای دستی، از امضای دیجیتال یا رمزنگاری‌شده استفاده می‌شود. پرسش بنیادین این است که آیا این نوع امضا در حقوق ایران همان ارزش و اعتباری را دارد که امضای سنتی کاغذی داشت یا خیر؟

[1] - Digital insurance

مواد ٦ و ١٠ قانون تجارت الکترونیکی ایران (١٣٨٢) ، داده‌پیام‌ها و امضاهای الکترونیکی را معتبر دانسته و آن‌ها را در حکم نوشته و امضا معرفی کرده است. این گام مهمی در شناسایی اسناد دیجیتال بوده است. با این حال، در عمل مشکلاتی جدی وجود دارد. نخست، زیرساخت‌های صدور گواهی امضای دیجیتال در ایران هنوز به‌طور کامل توسعه نیافته و بسیاری از شرکت‌های بیمه یا بیمه‌گذاران از آن استفاده نمی‌کنند. دوم، برخی مراجع قضایی و اداری همچنان در پذیرش امضای دیجیتال دچار تردید هستند و ترجیح می‌دهند نسخه چاپی یا کاغذی قرارداد را ملاک قرار دهند.

قانون تجارت الکترونیک ایران (١٣٨٢) سطوح امضای الکترونیکی را به‌صورت سه‌گانه ایداس اتحادیه اروپا (European Union Regulation, Artes 25-26,2014/910)(ساده، پیشرفته و واجد شرایط) تفکیک نکرده است. (در ایداس، تنها امضای واجد شرایط[1] معادل کامل امضای دستی است و انگاشتِ قانونی دارد. در ایران، پذیرش قضایی امضای دیجیتال هنوز ناهمگون است و در بسیاری از موارد (مانند بیمه شخص ثالث خودرو) نسخه چاپی نیز مطالبه می‌شود. این فاصله میان قانون و اجرا، ناامنی حقوقی ایجاد کرده است.

٢-٢-٢- قراردادهای هوشمند بیمه‌ای

پرسش اصلی آن است که آیا قرارداد هوشمند خود یک قرارداد مستقل محسوب می‌شود یا صرفاً ابزار اجرای تعهدات قراردادی است؟

مطابق ماده ١٨٣ قانون مدنی، عقد عبارت است از توافق اراده دو یا چند شخص بر ایجاد اثر حقوقی. از این منظر، کد رایانه‌ای به تنهایی فاقد اراده مستقل بوده و نمی‌تواند جایگزین قصد و رضای طرفین شود. بنابراین به نظر می‌رسد قرارداد هوشمند در حقوق ایران بیش از آنکه یک عقد مستقل باشد، سازوکار فناورانه اجرای تعهدات ناشی از قرارداد بیمه است.

این تحلیل در صنعت بیمه اهمیت مضاعف دارد؛ زیرا قرارداد بیمه مبتنی بر اصل حسن نیت نهایتی و افشای کامل اطلاعات خطر است. چنانچه الگوریتم‌های خودکار صرفاً بر داده‌های ورودی متکی باشند، امکان دارد وضعیت واقعی ریسک بیمه‌گذار را منعکس نکنند. افزون بر این، در صورت بروز خطا در کدنویسی یا حمله سایبری به قرارداد هوشمند، تعیین شخص مسئول با دشواری مواجه خواهد شد(Abramowicz, 2019; Regazzoni,2022).

حقوق ایران در این زمینه فاقد مقررات خاص است و روشن نیست در صورت پرداخت اشتباه خسارت یا عدم اجرای تعهدات بیمه‌ای ناشی از خطای الگوریتم، مسئولیت متوجه بیمه‌گر، طراح نرم‌افزار، پیمانکار فناوری یا بهره‌بردار سامانه خواهد بود. این خلأ تقنینی یکی از مهم‌ترین موانع توسعه بیمه هوشمند در ایران محسوب می‌شود.

مثال روشن آن، بیمه پرواز است: مسافر پروازی بیمه‌نامه‌ای مبتنی بر قرارداد هوشمند خریداری می‌کند که در صورت تأخیر بیش از دو ساعت پرواز، سامانه به‌طور خودکار خسارت را به حساب او واریز می‌کند. در این حالت، نیازی به ارائه مدارک یا پیگیری از سوی مسافر وجود ندارد.

اما این پدیده از منظر حقوقی پرسش‌های متعددی ایجاد می‌کند. نخست، آیا قرارداد هوشمند همان قرارداد بیمه به معنای سنتی است؟ اگرچه از لحاظ ماهوی، موضوع عقد همان تأمین خطر و جبران خسارت است، اما شکل انعقاد و اجرای آن کاملاً متفاوت است. عنصر «قصد و رضا» در قرارداد سنتی به‌طور مستقیم میان طرفین ابراز می‌شود، اما در قرارداد هوشمند، کدهای رایانه‌ای به‌جای اراده انسانی عمل می‌کنند. این امر موجب شده است که برخی حقوقدانان قراردادهای هوشمند را صرفاً «ابزارهای فنی اجرای قرارداد» بدانند و نه خودِ قرارداد.

اگرچه اصل اعتبار بیمه‌نامه‌های الکترونیکی در قالب قواعد عمومی قراردادها در نظام حقوقی ایران قابل پذیرش است و صرف الکترونیکی بودن قرارداد مانع نفوذ و اعتبار آن نیست. با این حال، چالش اصلی در بیمه دیجیتال صرفاً اعتبار شکلی سند نیست، بلکه احراز اراده واقعی طرفین در محیط‌های کاملاً خودکار است. در بسیاری از سامانه‌های بیمه‌ای، فرآیند انعقاد قرارداد از طریق کلیک

[1]-Qualified Electronic Signature

کاربر بر گزینه‌های از پیش طراحی شده انجام می‌شود. در چنین وضعیتی، اثبات اطلاع بیمه‌گذار از شروط قراردادی، استثنائات پوشش بیمه و آثار حقوقی رضایت الکترونیکی اهمیت ویژه‌ای پیدا می‌کند.

۲-۲-۳- حریم خصوصی داده‌ها در بیمه دیجیتال

حمایت از حریم خصوصی در بیمه دیجیتال با سه چالش اساسی مواجه است: نخست، فقدان نظام جامع حمایت از داده‌های شخصی؛ دوم، دشواری تحقق رضایت آگاهانه بیمه‌گذار در فرآیندهای دیجیتال؛ و سوم، تضمین امنیت داده‌های شخصی در برابر مخاطرات سایبری.

بیمه دیجیتال ذاتاً مبتنی بر جمع‌آوری، پردازش و تحلیل داده‌های شخصی است. بیمه‌گر برای ارزیابی ریسک و محاسبه حق بیمه نیازمند دسترسی به اطلاعات دقیق بیمه‌گذار است؛ از جمله داده‌های مالی، سوابق پزشکی، وضعیت رانندگی، عادات زندگی و حتی داده‌های رفتاری جمع‌آوری‌شده از دستگاه‌های هوشمند. این حجم گسترده از داده‌ها بیمه دیجیتال را به یکی از حساس‌ترین حوزه‌ها در زمینه حریم خصوصی بدل ساخته است (Bartholic et al.,2021).

در حقوق ایران، ماده ۵۸ قانون تجارت الکترونیکی (۱۳۸۲) بر ضرورت حفظ اسرار تجاری و اطلاعات خصوصی تأکید کرده است. همچنین مواد ۱۶ و ۱۷ قانون جرایم رایانه‌ای (۱۳۸۸) انتشار یا افشای غیرمجاز داده‌های خصوصی اشخاص را جرم‌انگاری کرده‌اند. با وجود این، مقررات موجود بیشتر ناظر بر مرحله افشا یا انتشار اطلاعات است و درباره نحوه جمع‌آوری، پردازش، نگهداری، انتقال و اشتراک‌گذاری داده‌های شخصی مقررات جامعی وجود ندارد.

در مقابل، مقررات جی دی آر پی اتحادیه اروپا بر اصولی همچون رضایت آگاهانه، محدودیت هدف، حداقل‌گرایی داده، حق دسترسی، حق اصلاح و حق حذف اطلاعات استوار است(European Union Regulation, Artes 15-17, 5-7, 2016/679). مقایسه این مقررات با نظام حقوقی ایران نشان می‌دهد که مهم‌ترین خلأ موجود، فقدان قانون جامع حمایت از داده‌های شخصی در حوزه بیمه دیجیتال است.

این خلأ زمانی اهمیت بیشتری می‌یابد که شرکت‌های بیمه از سامانه‌های هوش مصنوعی برای تحلیل رفتار مشتریان و تعیین ریسک استفاده می‌کنند؛ زیرا امکان تبعیض الگوریتمی، پردازش فراتر از رضایت اولیه و بهره‌برداری ثانویه از داده‌ها را افزایش می‌دهد (Aleksandrova et al.,2023; European Union. European Parliament and Council, 2016). چنین مواردی الزاماً جرم نیستند، اما می‌توانند موجب مسئولیت مدنی یا تخلف حرفه‌ای شوند.

چالش دوم مربوط به رضایت آگاهانه بیمه‌گذار است. بسیاری از افراد هنگام تکمیل فرم‌های آنلاین بیمه، بدون مطالعه دقیق شرایط، اجازه پردازش داده‌های خود را به شرکت بیمه می‌دهند. در نتیجه، بیمه‌گر می‌تواند داده‌های حساس پزشکی یا مالی افراد را در اختیار داشته باشد و حتی در مواردی از آن برای اهداف غیر بیمه‌ای استفاده کند. مثلا در بیمه‌های مبتنی بر استفاده از وسیله نقلیه ، بیمه‌گر از طریق نصب دستگاه یا اپلیکیشن، داده‌های مربوط به سرعت، ترمز، مسیر حرکت و زمان رانندگی فرد را جمع‌آوری می‌کند. این داده‌ها علاوه بر محاسبه حق بیمه، می‌تواند الگوهای رفتاری فرد را آشکار کند و در صورت افشا یا فروش به اشخاص ثالث، پیامدهای جدی برای حریم خصوصی به همراه داشته باشد (Bartholic et al., 2021).

چالش سوم، امنیت داده‌ها است. حتی اگر بیمه‌گر تعهد به محرمانگی داشته باشد، در صورت ضعف سامانه‌های امنیتی، داده‌های بیمه‌گذاران می‌تواند هدف حملات سایبری قرار گیرد. سرقت اطلاعات پزشکی یا مالی بیمه‌گذاران نه‌تنها به خسارت شخصی منجر می‌شود، بلکه می‌تواند اعتماد عمومی به صنعت بیمه را متزلزل کند.

از منظر حقوقی، لازم است نظام جامع حمایت از داده‌های شخصی در ایران تصویب شود که شامل اصولی همچون رضایت آگاهانه، حداقل‌گرایی در گردآوری داده‌ها، مسئولیت بیمه‌گر در قبال نقض داده‌ها و ضمانت اجراهای کیفری و مدنی باشد. تا زمانی که چنین نظامی ایجاد نشود، بیمه دیجیتال همواره با خطر نقض حریم خصوصی و بی‌اعتمادی عمومی مواجه خواهد بود.

۲-۲-٤- تأثیر جرایم سایبری بر اصول بنیادین حقوق بیمه

۲-۲-٤-۱- اصل حسن نیت و چالش‌های ناشی از محیط دیجیتال

قرارداد بیمه بیش از هر قرارداد دیگری بر اصل حسن نیت مبتنی است. در حقوق بیمه، بیمه‌گذار مکلف است تمامی اطلاعات مؤثر بر ارزیابی خطر را به‌طور صحیح و کامل در اختیار بیمه‌گر قرار دهد و بیمه‌گر نیز موظف است شرایط، استثنائات و حدود پوشش بیمه‌ای را به‌صورت شفاف اعلام کند. دیجیتالی‌شدن فرایندهای بیمه‌ای اگرچه موجب تسهیل انعقاد قرارداد شده است، اما زمینه‌های جدیدی برای نقض اصل حسن نیت ایجاد کرده است.

در بیمه‌های دیجیتال، امکان ارائه اطلاعات نادرست از طریق سامانه‌های برخط، استفاده از هویت‌های جعلی، دستکاری سوابق پزشکی یا مالی و بهره‌گیری از ابزارهای هوش مصنوعی برای پنهان‌سازی واقعیت‌های مؤثر بر خطر افزایش یافته است. از سوی دیگر، استفاده شرکت‌های بیمه از الگوریتم‌های غیرشفاف در ارزیابی ریسک می‌تواند موجب نقض تعهد اطلاع‌رسانی و تضعیف اعتماد متقابل میان طرفین شود. بنابراین جرایم سایبری صرفاً یک تهدید امنیتی نیستند، بلکه می‌توانند مبنای شکل‌گیری روابط بیمه‌ای را که بر حسن نیت استوار است، متزلزل سازند(Nurse et al., 2020).

۲-۲-٤-۲- تکلیف افشای اطلاعات و مخاطرات داده‌های دیجیتال

یکی از مهم‌ترین تعهدات بیمه‌گذار، افشای اطلاعات مرتبط با موضوع بیمه است. در بیمه دیجیتال، بخش عمده این اطلاعات از طریق فرم‌های الکترونیکی، پایگاه‌های داده و سامانه‌های هوشمند جمع‌آوری می‌شود. هرگونه دستکاری داده‌ها، جعل اطلاعات یا نفوذ به سامانه‌های اطلاعاتی می‌تواند فرآیند ارزیابی خطر را مختل کند.

برای مثال، اگر متقاضی بیمه درمان با استفاده از ابزارهای دیجیتال بخشی از سوابق بیماری خود را حذف یا تغییر دهد، بیمه‌گر بر مبنای اطلاعات نادرست اقدام به تعیین حق بیمه خواهد کرد. در چنین وضعیتی، مسئله صرفاً یک تخلف قراردادی نیست، بلکه ممکن است رفتار مزبور واجد وصف کیفری نیز باشد. به همین دلیل، اعتبار و صحت داده‌های ورودی در بیمه دیجیتال اهمیت بسیار بیشتری نسبت به نظام سنتی پیدا می‌کند.

۲-۲-٤-۳- ارزیابی ریسک و دستکاری الگوریتم‌های بیمه‌ای

ارزیابی ریسک هسته اصلی فعالیت بیمه‌ای است. در اکوسیستم بیمه دیجیتال، این فرایند به‌طور فزاینده‌ای به الگوریتم‌های هوش مصنوعی، تحلیل کلان‌داده‌ها و سامانه‌های خودکار واگذار شده است. هرگونه نفوذ سایبری، دستکاری داده‌ها یا تغییر در مدل‌های تصمیم‌گیری می‌تواند بر نتایج ارزیابی ریسک اثر مستقیم بگذارد.

برای نمونه، مهاجمان ممکن است با دستکاری داده‌های ورودی، ریسک واقعی بیمه‌گذار را کمتر از میزان واقعی نشان دهند یا از طریق حملات سایبری، سامانه‌های ارزیابی خسارت را فریب دهند. در چنین شرایطی، نه تنها تعادل اقتصادی قرارداد بیمه برهم می‌خورد، بلکه اصل برابری بیمه‌گذاران و عدالت بیمه‌ای نیز آسیب می‌بیند.

۲-۲-٤-٤- رابطه سببیت در خسارت‌های سایبری

احراز رابطه سببیت میان فعل زیان‌بار و خسارت وارده از مهم‌ترین ارکان مسئولیت در حقوق بیمه است. در محیط دیجیتال، تعیین منشأ خسارت با پیچیدگی‌های فراوانی روبه‌رو است. در بسیاری از موارد مشخص نیست خسارت ناشی از حمله سایبری، نقص نرم‌افزار، خطای کاربر، تقصیر پیمانکار فناوری یا ضعف زیرساخت‌های شرکت بیمه بوده است (Kesan & Hayes, 2017).

برای مثال، اگر سامانه پرداخت خسارت یک شرکت بیمه در اثر حمله باج‌افزاری از کار بیفتد، تعیین اینکه زیان وارده نتیجه مستقیم اقدام مهاجم بوده یا ناشی از قصور شرکت بیمه در رعایت استانداردهای امنیتی است، اهمیت اساسی پیدا می‌کند. دشواری اثبات رابطه سببیت در چنین مواردی یکی از چالش‌های نوظهور حقوق بیمه دیجیتال محسوب می‌شود.

۲-۲-٤-٥- تعهدات بیمه‌گر و مسئولیت ناشی از نقض امنیت سایبری

شرکت‌های بیمه در عصر دیجیتال صرفاً ارائه‌دهنده پوشش بیمه‌ای نیستند، بلکه متولی نگهداری حجم گسترده‌ای از داده‌های شخصی، مالی و پزشکی بیمه‌گذاران نیز محسوب می‌شونداز این رو، رعایت استانداردهای امنیت سایبری بخشی از تعهدات حرفه‌ای و قراردادی آنان تلقی می‌شود.

چنانچه نشت اطلاعات یا افشای داده‌های بیمه‌گذاران ناشی از ضعف تدابیر امنیتی شرکت بیمه باشد، مسئولیت مدنی بیمه‌گر قابل طرح خواهد بود. همچنین در برخی موارد، قصور در حفاظت از داده‌ها می‌تواند زمینه اعمال ضمانت اجراهای انتظامی و نظارتی را فراهم کند. از این منظر، امنیت سایبری دیگر صرفاً یک مسئله فنی نیست، بلکه به یکی از اجزای تعهدات حرفه‌ای بیمه‌گر تبدیل شده است.

۲-۲-٤-٦- جایگاه نمایندگان و کارگزاران بیمه در محیط دیجیتال

نمایندگان و کارگزاران بیمه یکی از مهم‌ترین حلقه‌های زنجیره خدمات بیمه‌ای هستند. با گسترش فروش برخط بیمه‌نامه‌ها، بخش قابل توجهی از اطلاعات بیمه‌گذاران از طریق سامانه‌های دیجیتال نمایندگان و کارگزاران جمع‌آوری و پردازش می‌شود. بنابراین ضعف امنیتی در این سامانه‌ها می‌تواند منجر به افشای اطلاعات، جعل هویت یا ارتکاب جرایم سایبری شود.

در چنین شرایطی، تعیین حدود مسئولیت نماینده، کارگزار، شرکت بیمه و پیمانکار فناوری اهمیت ویژه‌ای پیدا می‌کند. یکی از خلأهای حقوقی موجود در نظام بیمه‌ای ایران، فقدان قواعد روشن درباره تقسیم مسئولیت میان این اشخاص در موارد وقوع جرایم سایبری است.

۲-۲-٤-۷- نقش بیمه مرکزی در حکمرانی و نظارت بر بیمه دیجیتال

گسترش بیمه دیجیتال ضرورت تحول در الگوهای نظارتی را نیز افزایش داده است. بیمه مرکزی به عنوان نهاد ناظر بر بازار بیمه، علاوه بر وظایف سنتی خود، باید بر امنیت سایبری، حفاظت از داده‌های بیمه‌ای، استانداردهای فناوری و مدیریت ریسک‌های دیجیتال نیز نظارت مؤثر داشته باشد. در خصوص شزکت های فناور بیمه ای، مواد ۱۷ و ۱۸ آیین نامه شماره ۱۰۵ مصوب شورای عالی بیمه (۱٤۰۲) صراحتا مسئولیت نظارت را بر عهده بیمه مرکزی قرار داده و رعایت قانون مدیریت داده ها و اطلاعات ملی و حفظ حریم خصوصی اشخاص را نیز مورد توجه قرار داده است.

در این چارچوب، بهره‌گیری از فناوری‌های نظارتی و فناوری‌های نظارت هوشمند می‌تواند امکان پایش مستمر فعالیت شرکت‌های بیمه، شناسایی رفتارهای مشکوک، کشف تقلب و مدیریت ریسک‌های سایبری را فراهم کند (Aleksandrova et al.,2023). از این رو، مقابله با جرایم سایبری در صنعت بیمه تنها از طریق ضمانت اجراهای کیفری امکان‌پذیر نیست، بلکه نیازمند حکمرانی داده‌محور و نظارت فناورانه مستمر است.

۲-۳- گونه های جرایم سایبری

یکی از پیچیده‌ترین مسائل حقوقی بیمه دیجیتال، تعیین مسئولیت در صورت وقوع حملات سایبری است. مطابق مواد ۱ و ۲ قانون جرایم رایانه‌ای، دسترسی غیرمجاز و شنود غیرمجاز داده‌ها جرم محسوب می‌شوند. همچنین ماده ۱۳ این قانون تحصیل مال از طریق دستکاری داده‌ها یا سامانه‌های رایانه‌ای را تحت عنوان کلاهبرداری رایانه‌ای جرم‌انگاری کرده است.

بر این اساس، تغییر سوابق خسارت، جعل بیمه‌نامه دیجیتال، دستکاری سامانه ارزیابی ریسک یا تحصیل خسارت از طریق تغییر داده‌های بیمه‌ای می‌تواند مشمول عنوان کلاهبرداری رایانه‌ای باشد. با این حال، تمامی مخاطرات فناورانه موجود در صنعت بیمه وصف کیفری ندارند.

برای مثال، تبعیض الگوریتمی در تعیین حق بیمه، خطای سامانه هوش مصنوعی در ارزیابی خسارت یا نقص فنی قرارداد هوشمند، در اغلب موارد جرم تلقی نمی‌شوند، بلکه در قلمرو مسئولیت مدنی قرار می‌گیرند.

در خصوص مسئولیت ناشی از نشت داده‌ها نیز ابهام قابل توجهی وجود دارد. اگر اطلاعات بیمه‌گذاران در نتیجه حمله سایبری افشا شود، مسئولیت ممکن است میان شرکت بیمه، ارائه‌دهنده خدمات ابری، پیمانکار فناوری یا حتی کارکنان داخلی توزیع شود. فقدان مقررات اختصاصی در زمینه مسئولیت ناشی از نقض داده‌ها موجب شده است که تعیین حدود مسئولیت هر یک از این اشخاص در نظام حقوقی ایران با دشواری همراه باشد.

از منظر حقوق بیمه نیز حملات سایبری می‌توانند اصول بنیادینی همچون حسن نیت، افشای اطلاعات و ارزیابی صحیح ریسک را تحت تأثیر قرار دهند. بنابراین تحلیل مسئولیت در بیمه دیجیتال نباید صرفاً بر مبنای قواعد عمومی جرایم رایانه‌ای انجام شود، بلکه باید ویژگی‌های خاص رابطه بیمه‌گر و بیمه‌گذار نیز مورد توجه قرار گیرد.

۲-۳-۱ کلاهبرداری‌های دیجیتال در بیمه

کلاهبرداری بیمه‌ای یکی از قدیمی‌ترین جرایم مرتبط با صنعت بیمه است، اما با دیجیتالی‌شدن این صنعت، شکل و ابعاد آن دگرگون شده است. در بیمه سنتی، متقلبان معمولاً با ارائه اطلاعات نادرست یا صحنه‌سازی برای وقوع حادثه، سعی در دریافت غرامت غیرقانونی داشتند. اما در بیمه دیجیتال، ابزارهای سایبری فرصت‌های جدیدی برای ارتکاب کلاهبرداری فراهم کرده‌اند. (Novak, 2025)

یکی از مهم‌ترین اشکال کلاهبرداری دیجیتال، ثبت هویت جعلی یا هویت‌سازی دیجیتال است. متخلف می‌تواند با استفاده از مدارک هویتی سرقتی یا جعل‌شده، به‌طور آنلاین بیمه‌نامه دریافت کند و سپس با صحنه‌سازی یا حتی بدون وقوع حادثه، خسارت مطالبه نماید. ضعف در سامانه‌های احراز هویت دیجیتال این خطر را تشدید می‌کند.

نوع دیگر کلاهبرداری دیجیتال، استفاده از بدافزار یا حملات سایبری برای تغییر داده‌ها است. در برخی موارد، هکرها وارد سامانه شرکت بیمه شده و داده‌های مربوط به سوابق بیمه‌ای فرد را تغییر می‌دهند. برای مثال، ممکن است فردی بدون داشتن بیمه بدنه خودرو، با کمک هکرها داده‌های سامانه را دستکاری کرده و خود را بیمه‌شده معرفی کند تا پس از تصادف خسارت دریافت کند.

جرم با اثرگذاری مستقیم بر روی داده‌ها یا فرآیند خودکار سامانه (بدون دخالت ذهن انسان) رخ می دهد که در قانون جرایم رایانه‌ای ایران جرم‌انگاری شده است. ماده ۱۳ قانون جرایم رایانه‌ای(۱۳۸۸) مقرر داشته است هرکس به طور غیرمجاز از سامانه های رایانه ای یا مخابراتی با ارتکاب اعمالی از قبیل وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده ها یا مختل کردن سامانه، وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری تحصیل کند علاوه بر رد مال به صاحب آن به حبس از یک تا پنج سال یا جزای نقدی از ۱۶۵.۰۰۰.۰۰۰ تا۸۲۵.۰۰۰.۰۰۰ ریال یا هر دو مجازات محکوم خواهد شد. . در حوزه بیمه دیجیتال، با توجه به اینکه تمام فرایندها از صدور بیمه‌نامه تا ارزیابی خسارت و پرداخت آن به صورت دیجیتالی و مبتنی بر سامانه‌ها انجام می‌شود، این ماده کاربرد بسیار گسترده‌ای دارد. مثلا چنانچه کاربر در سامانه بیمه بدنه آنلاین، تاریخ وقوع تصادف را به روزی تغییر دهد که بیمه‌نامه معتبر داشته است (در حالی که تصادف قبل از خرید بیمه رخ داده) از آنجا که اطلاعات دروغین در سامانه برای کاهش حق بیمه یا دریافت خسارت غیرواقعی صورت گرفته است، مصداق کلاهبرداری رایانه ای است؛ یا چنانچه شخصی با نفوذ غیرمجاز به سامانه شرکت بیمه، اطلاعات مربوط به میزان خسارت یا وضعیت پوشش بیمه‌ای را تغییر دهد و از این طریق وجوهی بیش از استحقاق واقعی دریافت کند، رفتار وی نیز با توجه به ماده ۱۳ قانون جرایم رایلنه‌ای می‌تولند مصداق کلاهبرداری رایانه‌ای باشد؛ زیرا تحصیل مال از طریق تغییر یا دستکاری داده‌ها و سامانه‌های رایانه‌ای صورت گرفته است. بنابراین، عنصر مادی این جرم در بستر بیمه دیجیتال نه صرف ارائه اطلاعات خلاف واقع، بلکه مداخله غیرمجاز در داده‌ها یا فرآیندهای الکترونیکی مؤثر بر تصمیم‌گیری بیمه‌گر است.

با این حال، اثبات چنین جرایمی در عمل دشوار است؛ چراکه نیازمند تخصص فنی بالا و همکاری میان بیمه‌گران، نهادهای نظارتی و پلیس فتا است.

چالش اصلی در برخورد با کلاهبرداری دیجیتال بیمه‌ای، فقدان مقررات اختصاصی و کمبود سازوکارهای پیشگیرانه است. قوانین فعلی به‌طور کلی جرایم رایانه‌ای را جرم‌انگاری کرده‌اند، اما ویژگی‌های خاص صنعت بیمه دیجیتال، از جمله وابستگی شدید به داده‌های حساس و الگوریتم‌های پیچیده، اقتضا می‌کند که مقررات ویژه‌ای تدوین شود.

برای مقابله با این پدیده، علاوه بر راهکارهای فنی مانند استفاده از بلاک‌چین برای جلوگیری از تغییر داده‌ها و تقویت سامانه‌های احراز هویت دیجیتال، باید قوانین ویژه‌ای برای مسئولیت بیمه‌گر، بیمه‌گذار و اشخاص ثالث در کلاهبرداری‌های سایبری بیمه‌ای تدوین شود.

۲-۳-۲ نفوذ و حملات سایبری علیه سامانه‌های بیمه

صنعت بیمه دیجیتال به‌شدت متکی بر زیرساخت‌های فناوری اطلاعات است. تمامی مراحل از ثبت‌نام و انعقاد قرارداد تا مدیریت خسارت و پرداخت، در بستر سامانه‌های آنلاین صورت می‌گیرد. این وابستگی، شرکت‌های بیمه را به یکی از اهداف اصلی حملات سایبری بدل کرده است.

ماده ۱ قانون جرایم رایانه ای مقرر داشته است: هر کس به طور غیرمجاز به داده ها یا سامانه های رایانه ای یا مخابراتی که به وسیله تدابیر امنیتی حفاظت شده است دسترسی یابد به حبس از نود و یک روز تا یک سال یا جزای نقدی ... یا هر دو مجازات محکوم خواهد شد. این ماده نقشی کلیدی در حفاظت از دو دارایی حیاتی ایفا می‌کند: داده‌های حساس کاربران (حریم خصوصی) و پایداری زیرساخت‌های مالی. در این ماده، نیازی نیست که متهم حتماً اطلاعاتی را ربوده یا پولی جابجا کرده باشد؛ صرف ورود غیرمجاز جرم است. شرکت‌های بیمه دیجیتال حجم عظیمی از داده‌های هویتی، پزشکی، مالی و موقعیت مکانی کاربران را ذخیره می‌کنند. حملات مرتبط در این صنعت معمولاً به اشکال زیر رخ می‌دهد:

نوع دسترسی غیرمجاز	شرح در بستر بیمه دیجیتال	هدف مهاجم
نفوذ به پایگاه داده (Database Breach)	دسترسی به سرورهای مرکزی حاوی سوابق پزشکی و مالی بیمه‌گذاران.	سرقت اطلاعات لو رفته جهت فروش در دارک‌وب یا باج‌گیری.
حمله به APIها	سوءاستفاده از ضعف‌های امنیتی در پل‌های ارتباطی بین اپلیکیشن بیمه و بانک یا ثبت احوال.	استخراج فله‌ای اطلاعات کاربران یا دستکاری فرآیند استعلام قیمت.
سرقت حساب کاربری (Account Takeover)	ورود غیرمجاز به پنل کاربری یک بیمه‌گذار خاص از طریق حملات بروت‌فورس یا فیشینگ.	مشاهده جزئیات بیمه‌نامه یا ثبت درخواست‌های خسارت جعلی به نام او.

راهکار مقابله با این چالش، ترکیبی از تدابیر فنی و حقوقی است: الزام شرکت‌های بیمه به رعایت استانداردهای امنیت سایبری، تدوین دستورالعمل‌های نظارتی توسط بیمه مرکزی، و پیش‌بینی ضمانت‌اجراهای مدنی و کیفری در صورت قصور بیمه‌گران. همچنین می‌توان از تجربیات بین‌المللی مانند استانداردهای مؤسسه ملی استاندارد و فناوری ایالات متحده یا چارچوب‌های امنیت سایبری اتحادیه اروپا بهره گرفت.

۲-۳-۳ سوءاستفاده از داده‌های شخصی بیمه‌گذاران

در بیمه دیجیتال، داده‌ها دارایی اصلی محسوب می‌شوند. بیمه‌گر برای محاسبه ریسک و تعیین حق بیمه، به داده‌های دقیق بیمه‌گذار نیاز دارد..(European Union Agency for Cybersecurity [ENISA], 2024) یکی از اشکال سوءاستفاده، فروش غیرمجاز داده‌های بیمه‌ای است. کارمندان یا پیمانکاران شرکت‌های بیمه ممکن است داده‌های بیمه‌گذاران را به اشخاص ثالث، مانند شرکت‌های تبلیغاتی یا باندهای مجرمانه، بفروشند. این اقدام نه‌تنها نقض حریم خصوصی است، بلکه می‌تواند امنیت فردی و اجتماعی افراد را به خطر اندازد.

نوع دیگر سوءاستفاده، سرقت هویت دیجیتال است. با دسترسی به داده‌های بیمه‌ای، متخلفان می‌توانند هویت بیمه‌گذار را جعل کنند و از آن برای دریافت بیمه‌نامه یا مطالبه خسارت استفاده کنند. این امر هم به زیان شرکت بیمه است و هم می‌تواند آثار کیفری و مدنی برای بیمه‌گذار واقعی ایجاد کند.

همچنین، داده‌های بیمه‌ای می‌توانند برای تبعیض الگوریتمی به کار روند. برای مثال، اگر بیمه‌گر داده‌های پزشکی یا رفتاری فرد را بدون چارچوب قانونی استفاده کند، ممکن است حق بیمه او را به‌طور ناعادلانه افزایش دهد یا حتی از بیمه‌کردنش خودداری کند. این مسئله جنبه‌ای تازه از جرایم یا سوءاستفاده‌های سایبری را نشان می‌دهد که در مرز میان نقض حریم خصوصی و تبعیض قرار دارد (Weber et al. 2024,)در سطح بین‌المللی، مقرراتی مانند مقررات مقررات عمومی حفاظت از داده‌ها اتحادیه اروپا به‌طور سختگیرانه این رفتارها را ممنوع کرده و برای نقض داده‌ها جریمه‌های سنگین تعیین کرده است. در ایران اما، به دلیل فقدان قانون جامع حفاظت از داده‌های شخصی، نظارت کافی بر نحوه استفاده از داده‌های بیمه‌گذاران وجود ندارد. در نتیجه، سوءاستفاده از داده‌ها در بیمه دیجیتال می‌تواند به‌راحتی رخ دهد، بدون آنکه بیمه‌گذار امکان پیگیری حقوقی مؤثر داشته باشد.

افشا یا فروش غیرمجاز داده‌ها تحت مواد مربوط به نقض محرمانگی در فصل اول قانون جرایم رایانه ای قابل تعقیب است، اما خلأ در تعریف «سوءاستفاده تجاری» و تبعیض الگوریتمی وجود دارد. چالش اصلی اینجاست که مسئولیت کیفری و مدنی سوءاستفاده از داده‌ها شفاف نیست. آیا صرف فروش داده جرم است یا نیازمند تحقق نتیجه زیان‌بار است؟ آیا شرکت بیمه مسئول رفتار کارکنان خود است یا تنها کارمند خاطی باید پاسخگو باشد؟ این ابهامات موجب می‌شود که راه برای سوءاستفاده باز بماند.

در حقوق ایران، مسئولیت سوءاستفاده از داده‌ها در قراردادهای هوشمند بیمه، یک مسئولیت چندلایه است و نمی‌توان آن را صرفاً بر دوش کارمند یا صرفاً بر دوش شرکت گذاشت . با عنایت به ماده ۱۹ و ۲۰ قانون جرایم رایانه ای (۱۳۸۸) قواعد موجود نشان می‌دهد که *اصل* بر مسئولیت شرکت بیمه است، اما کارمند خاطی نیز مسئولیت مستقل دارد. کارمند خاطی که داده را افشا یا منتقل کرده، مسئولیت کیفری مستقیم دارد. شرکت بیمه فقط در صورتی مسئولیت کیفری دارد که: مدیر آن شرکت دستور داده باشد،یا از وقوع جرم آگاه بوده و جلوگیری نکرده باشد، یا ساختار سازمانی آن به‌گونه‌ای باشد که جرم را تسهیل کند.در غیر این صورت، شرکت به‌طور مستقیم مسئولیت کیفری ندارد.

فروش داده نیز در بسیاری از موارد صرفاً با وقوع فعل جرم‌انگاری می‌شود و نیازمند تحقق نتیجه زیان‌بار نیست برای مسئولیت مدنی، تحقق ضرر لازم است؛ اما برای مسئولیت کیفری، در جرایم مطلق، نتیجه شرط نیست. بنابراین **:فروش داده بیمه‌گذاران—در بسیاری از موارد جرم است.** ماده ۱ و ۵ قانون جرائم رایانه ای (۱۳۸۸)، «دسترسی غیرمجاز»، «افشا»، «انتشار» و «در دسترس قرار دادن داده‌های شخصی» را جرم می‌داند.

۳- تحلیل جرم‌شناختی جرایم سایبری در اکوسیستم بیمه دیجیتال

۳-۱- ویژگی‌های جرم‌شناختی بزهکاران در اکوسیستم بیمه دیجیتال

بزهکاران جرایم سایبری در حوزه بیمه دیجیتال طیف متنوعی را دربرمی‌گیرند؛ از هکرهای حرفه‌ای گرفته تا کارکنان ناراضی شرکت‌های بیمه. برخلاف جرایم سنتی، مرتکبان این دسته از جرایم لزوماً در صحنه فیزیکی حضور ندارند و همین امر شناسایی آن‌ها را دشوار می‌کند.

ویژگی نخست، دانش فنی بالا است. بسیاری از مرتکبان جرایم سایبری در بیمه دیجیتال متخصصان فناوری اطلاعات یا افرادی با مهارت در زمینه برنامه‌نویسی و شبکه هستند. این توانایی فنی به آن‌ها امکان می‌دهد به سامانه‌های بیمه نفوذ کنند، داده‌ها را دستکاری کنند یا الگوریتم‌های قراردادهای هوشمند را فریب دهند. نمونه بارز آن، حملات سایبری به بانک‌های اطلاعاتی بیمه‌ای در کشورهای مختلف است که توسط گروه‌های سازمان‌یافته هکری انجام شده است.

ویژگی دوم، ناشناس‌ماندن و پنهان‌کاری است. مجرمان سایبری اغلب از ابزارهایی مانند شبکه‌های خصوصی مجازی یا مرورگرهای ناشناس‌ساز استفاده می‌کنند تا هویت خود را مخفی نگه دارند. این امر ردیابی و تعقیب آن‌ها را بسیار دشوار می‌سازد و موجب می‌شود احتمال کشف جرم کاهش یابد.

ویژگی سوم، ماهیت فراملی بزهکاران است. بسیاری از حملات سایبری علیه شرکت‌های بیمه در ایران یا سایر کشورها توسط هکرهایی انجام می‌شود که در کشورهای دیگر مستقرند. این ویژگی فراملی، نه تنها روند شناسایی بزهکاران را پیچیده می‌کند، بلکه همکاری‌های بین‌المللی قضایی و پلیسی را نیز ضروری می‌سازد.

ویژگی چهارم، انگیزه‌های متنوع است. برخی بزهکاران صرفاً انگیزه مالی دارند و به دنبال کسب سود از طریق کلاهبرداری بیمه‌ای یا فروش داده‌های بیمه‌گذاران در بازار سیاه‌اند. گروهی دیگر انگیزه‌های انتقامجویانه یا ایدئولوژیک دارند و ممکن است با هدف ضربه زدن به اعتبار شرکت بیمه یا حتی نظام اقتصادی یک کشور، حمله سایبری ترتیب دهند.

بنابراین، بزهکاران جرایم سایبری در بیمه دیجیتال از مجرمان سنتی متمایزند؛ آنان متخصص، ناشناس، اغلب فراملی و گاه سازمان‌یافته‌اند. این ویژگی‌ها موجب می‌شود راهبردهای مقابله با آنان نیز باید متفاوت، فناورانه و بین‌المللی باشد.

۳-۲- ویژگی بزه‌دیدگان جرایم سایبری در بیمه دیجیتال

بزه‌دیدگان جرایم سایبری در بیمه دیجیتال به دو دسته کلی تقسیم می‌شوند: بیمه‌گذاران (افراد حقیقی یا حقوقی) و شرکت‌های بیمه. هرکدام ویژگی‌هایی دارند که آن‌ها را در معرض بزه‌دیدگی سایبری قرار می‌دهد.

بیمه‌گذاران، به‌ویژه افراد عادی، معمولاً دانش فنی پایینی درباره امنیت دیجیتال دارند. بسیاری از آنان بدون توجه به خطرات، داده‌های حساس خود مانند اطلاعات هویتی، مالی یا پزشکی را در سامانه‌های آنلاین بیمه وارد می‌کنند. همین ناآگاهی، آن‌ها را به هدفی آسان برای سرقت هویت و سوءاستفاده از داده‌ها تبدیل می‌کند. برای نمونه، در حملات فیشینگ تمرکز مجرمان بیش از آنکه بر نفوذ فنی به سامانه‌ها باشد، بر فریب روانی کاربران است؛ ازاین‌رو بیمه‌گذاران عادی بیش از سایر گروه‌ها در معرض این نوع بزه‌دیدگی قرار دارند. (Gupta et al., 2017)

بزه‌دیدگان اصلی در این حوزه معمولاً بیمه‌گذاران عادی هستند، اما شرکت‌های بیمه نیز به‌طور غیرمستقیم متحمل خسارت می‌شوند. بیمه‌گذاران به دلیل سطح پایین آگاهی امنیتی، بیش از سایرین در معرض آسیب قرار دارند. بسیاری از آن‌ها بدون بررسی اعتبار لینک‌های دریافتی، روی ایمیل‌ها یا پیامک‌های جعلی کلیک می‌کنند و اطلاعات ورود به سامانه بیمه یا داده‌های هویتی خود را افشا می‌نمایند. ویژگی روانی این بزه‌دیدگان اعتماد ساده‌دلانه به برند بیمه یا عدم درک تهدیدهای دیجیتال است.

شرکت‌های بیمه دومین بزه‌دیدگان اصلی‌اند. هنگامی که الگوریتم‌ها دستکاری می‌شوند، زیان مالی مستقیم بر دوش شرکت‌ها می‌افتد. افزون بر آن، افشای عمومی یک مورد از دستکاری هوش مصنوعی می‌تواند اعتبار شرکت بیمه را نابود کند، زیرا مشتریان اعتماد خود را به سلامت فرآیندهای دیجیتال از دست می‌دهند.

گروه دیگری از بزه‌دیدگان نظام حقوقی و قضایی است. دادگاه‌ها برای رسیدگی به دعاوی مرتبط با سوءاستفاده از هوش مصنوعی با چالش‌های عظیم مواجه می‌شوند، چرا که اثبات دستکاری الگوریتم‌ها و تعیین مسئولیت حقوقی بسیار دشوار است. (Aleksandrova et al., 2023) از منظر جرم‌شناسی، بیمه‌گذاران و شرکت‌های بیمه در یک چرخه بزه‌دیدگی قرار دارند. ناآگاهی بیمه‌گذاران و ضعف امنیتی شرکت‌های بیمه هر دو موجب افزایش احتمال وقوع جرم می‌شود. به بیان دیگر، بزه‌دیدگی در بیمه دیجیتال نه‌تنها نتیجه اقدامات مجرمان است، بلکه تا حدی ناشی از ساختارهای ضعیف حمایتی و آموزشی نیز هست.

۳-۳- پیشگیری وضعی از جرایم سایبری در بیمه دیجیتال

پیشگیری وضعی رویکردی است که بر کاهش فرصت‌های ارتکاب جرم تمرکز دارد. در زمینه جرایم سایبری علیه بیمه دیجیتال، این شیوه از پیشگیری به معنای طراحی و اجرای تدابیری است که دسترسی مجرمان به سامانه‌های بیمه‌ای را دشوارتر، پرهزینه‌تر و پرریسک‌تر می‌کند.

نخستین ابزار پیشگیری وضعی، تقویت سامانه‌های امنیتی است. بیمه دیجیتال بر بستر داده‌های حساس کار می‌کند؛ داده‌هایی شامل اطلاعات هویتی بیمه‌گذاران، تراکنش‌های مالی و سوابق پزشکی. ضعف امنیتی در زیرساخت‌های بیمه‌ای می‌تواند به افشای این داده‌ها و کلاهبرداری‌های گسترده منجر شود. (Kothandapani, 2024)استفاده از دیواره‌های آتش چندلایه، سامانه‌های تشخیص نفوذ و مانیتورینگ بلادرنگ شبکه می‌تواند احتمال نفوذ را کاهش دهد. برای نمونه، در یکی از شرکت‌های بیمه اروپایی حمله باج‌افزاری تنها به دلیل عدم به‌روزرسانی منظم سیستم‌ها رخ داد و میلیون‌ها دلار خسارت به همراه داشت؛ حال آن‌که یک سیاست امنیتی مبتنی بر پیشگیری وضعی می‌توانست این آسیب‌پذیری را رفع کند.

ابزار دوم، احراز هویت چندمرحله‌ای است. بسیاری از حملات سایبری با سرقت رمز عبور ساده آغاز می‌شود. در بیمه دیجیتال، دسترسی غیرمجاز به حساب کاربری یک بیمه‌گذار می‌تواند به تغییر در سوابق بیمه‌ای یا صدور بیمه‌نامه‌های جعلی منجر شود. استفاده از احراز هویت چندعاملی، شامل رمز یک‌بارمصرف، تأیید بیومتریک یا تأیید از طریق دستگاه ثانویه، امنیت حساب‌ها را به‌طور چشمگیری افزایش می‌دهد. (Nurse et al. 2020)

سومین رکن پیشگیری وضعی، رمزنگاری داده‌ها است. حتی اگر مهاجمان موفق به نفوذ شوند، رمزگذاری پیشرفته یا رمزنگاری کلید عمومی مانع از بهره‌برداری عملی از داده‌ها می‌شود. رمزنگاری نه‌تنها در ذخیره‌سازی اطلاعات، بلکه در انتقال داده‌ها میان سرورها و پایگاه‌های بیمه‌ای نیز ضروری است. (Papantoniou, 2022)

پیشگیری وضعی در بیمه دیجیتال همچنین شامل اقداماتی مانند کاهش جذابیت هدف مثلاً ذخیره‌سازی داده‌ها به‌صورت توزیع‌شده به‌جای یک نقطه مرکزی، افزایش ریسک کشف (استفاده از سیستم‌های هشدار هوشمند در صورت فعالیت غیرعادی) و ایجاد مانع در مسیر مهاجم (به‌کارگیری کپچا یا محدودیت‌های دسترسی جغرافیایی) است. (Jeyasingh 2023, 24) نکته مهم آن است که پیشگیری وضعی هرچند نمی‌تواند جرایم سایبری را به صفر برساند، اما با دشوار کردن فرایند حمله، انگیزه بسیاری از مهاجمان فرصت‌طلب را کاهش می‌دهد. در واقع، هزینه–فایده ارتکاب جرم برای مجرم برهم می‌خورد و او به‌جای حمله به سامانه‌ای ایمن، هدف دیگری را انتخاب می‌کند.(Onabowale, 2025)

جمع‌بندی و پیشنهادها

این پژوهش با عبور از تحلیل‌های منفک فقهی–حقوقی و فرضیات انتزاعی جرم‌شناختی، به یک **الگوی سه–بعدی هم‌افزا** دست یافته است. دستاورد تفسیری و ساختاری این تحقیق در پاسخ به پرسش‌های بنیادین پژوهش، به صورت گزاره‌های کاربردی زیر استنتاج می‌شود:

.دستاورد تفسیری در تفکیک مرزهای حقوقی (ماده‌محور)

تحلیل حقوقی این پژوهش اثبات می‌کند که در اکوسیستم بیمه دیجیتال، بخش عمده‌ای از رفتارهای مجرمانه به اشتباه در محاکم ذیل کلاهبرداری سنتی دسته‌بندی می‌شوند. یافته استنتاجی این تحقیق مرزهای قانونی را بدین شرح تفکیک می‌کند:

- **اصالت فریب سیستم در ماده ۱۳ :**چنانچه مجرم با آپلود مدرک پزشکی جعلی، اپراتور انسانی شرکت بیمه را فریب دهد، جرم «کلاهبرداری سنتی» است. اما اگر با دستکاری لایه‌های فنی، نفوذ به API یا تغییر فرآیند خودکار الگوریتم ارزیابی

خسارت (بدون دخالت ذهن انسان)، سامانه را به پرداخت غرامت یا صدور بیمه‌نامه رایگان وادار کند، رفتار کاملاً از قلمرو کلاهبرداری سنتی خارج و منحصراً مشمول **ماده ۱۳ قانون جرایم رایانه‌ای** است.

- **تعدد معنوی فیشینگ بیمه‌ای :**فیشینگ در حوزه بیمه دیجیتال صرفاً یک جرم مالی نیست؛ این رفتار واجد وصف تعدد معنوی میان **ماده ۱** (دسترسی غیرمجاز از طریق دور زدن تدابیر امنیتی پورتال) و **ماده ۱۳** (تحصیل امتیاز مالی نامشروع) قانون جرایم رایانه‌ای است.

- **مسئولیت ساختاری پلتفرم :**بر اساس انطباق با **ماده ۷۴۷ قانون مجازات اسلامی**، در صورت وقوع نشت داده یا تسهیل فیشینگ به دلیل ضعف در معماری امنیتی، شرکت InsurTech به عنوان شخص حقوقی دارای مسئولیت کیفری و مدنی مستقل از کارمند خاطی است.

۲ .مدل فرآیندی مهار جرم (پیوند جرم‌شناسی و فناوری نظارتی)

پژوهش حاضر ادعای پیوند میان نظریه‌ها و ابزارهای نظارتی را در قالب یک **»سازوکار عملیاتی چهارمرحله‌ای «**مدل‌سازی کرده است. این مدل، تئوری‌های جرم‌شناسی را از حالت وصفی به ابزار پیشگیری وضعی تبدیل می‌کند:

{۱ .تحلیل بستر (جرم‌شناسی)] <—— [۲ .پایش پیش‌دستانه }

شناسایی هدف مناسب و بزه‌دیده اسکن آنومالی‌ها و رفتارهای مشکوک

بر اساس ویژگی‌های سبک زندگی دیجیتال تراکنشی به صورت برخط و ۲٤ ساعته

| |

▼ ▼

{٤ .بهینه‌سازی و بازخورد] ——> [۳ .مستندسازی (حقوقی)}

تزریق شگردهای جدید به هسته سیستم تبدیل لاگ‌های فنی به ادله الکترونیکی

جهت کاهش عقلانی سود مجرم تخدیش‌ناپذیر بر بستر بلاک‌چین (ماده ٦٨٥)

پیشنهادهای ساختاری و تقنینی (مبتنی بر یافته‌ها)

جهت اصلاح فرآیندها در صنعت بیمه دیجیتال، راهکارهای زیر پیشنهاد می‌گردد:

اصلاح رویه قضایی :صدور رأی وحدت رویه از سوی دیوان عالی کشور جهت تبیین مرز «فریب سیستم» (ماده ۱۳ جرایم رایانه‌ای) و «فریب انسان» در پلتفرم‌های خودکار بیمه‌ای.

الزام به پی‌بست فناوری نظارتی: وضع مقررات تکلیفی از سوی بیمه مرکزی جهت اجبار شرکت‌های بیمه دیجیتال به پیاده‌سازی پورتال‌های نظارت هوشمند تراکنش‌ها و سیستم‌های احراز هویت بیومتریک زنده در لایه‌های واریز خسارت.

تدوین ضوابط اختصاصی صیانت از داده :طراحی دستورالعمل بومی حریم خصوصی داده‌های بیمه‌ای با الگوبرداری کارکردی از جی دی آر پی تا زمان تصویب قانون جامع حفاظت از داده‌های شخصی در کشور.

-جدول ماتریس یافته‌های نهایی تحقیق (پیوست خلاصه نتیجه‌گیری)

راهکار عملیاتی و ساختاری	مستند و ضمانت‌اجرای حقوقی	یافته مادی و تحلیلی پژوهش	پرسش پژوهش
ارتقای سیستم‌های لاگ‌گیری استاندارد پلتفرم جهت تولید ادله دیجیتال تخدیش‌ناپذیر.	مواد ۱ و ۱۳ قانون جرایم رایانه‌ای و ماده ۷۴۷ ق.م.ا	دستکاری داده‌های خسارت و فیشینگ، کلاهبرداری رایانه‌ای و دسترسی غیرمجاز است، نه کلاهبرداری سنتی.	**۱ .چگونگی انطباق حقوقی جرایم؟**
پیاده‌سازی فرآیندهای احراز هویت چندعاملی و توزیع هشدار در زنجیره کارگزاری‌ها.	نظریه فعالیت‌های روزمره و انتخاب عقلانی	حذف ناظر انسانی، سرعت صدور و اشتیاق بزه‌دیده به تخفیف، فرصت مجرمانه و هدف مناسب ایجاد می‌کند.	**۲ .تبیین جرم‌شناختی بزه؟**
بکارگیری فناوری نظارتی هوش مصنوعی جهت آنومالی‌سنجی تراکنش‌ها به صورت پیش‌دستانه.	ماده ٦٨٥ قانون آیین دادرسی کیفری (۱۳۹۲) (اعتبار ادله)	حقوق بدون ابزار نظارتی آنلاین توان کشف ندارد؛ RegTech حلقه وصل حقوق و جرم‌شناسی است.	**۳ .الگوی مهار و نوآوری؟**

تعارض منافع

"نویسنده اعلام می‌کند که هیچ تضاد منافعی در مورد انتشار پژوهش ثبت شده وجود ندارد. علاوه بر این، موارد اخلاقی از جمله سرقت ادبی، رضایت آگاهانه، رفتار نادرست، جعل و/یا جعل داده ها، انتشار مضاعف و یا سوء رفتار به طور کامل توسط نویسندگان رعایت شده است."

References

Abramowicz, M. B. (2019). Blockchain-based insurance. In P. Hacker, I. Lianos, G. Dimitropoulos, & S. Eich (Eds.), Regulating blockchain: Techno-social and legal challenges (pp. 195–212). Oxford University Press. https://doi.org/10.1093/oso/9780198842187.003.0011

Aleksandrova, A., Ninova, V., & Zhelev, Z. (2023). A survey on AI implementation in finance, (cyber) insurance and financial controlling. *Risks*, 11(5), 91. https://doi.org/10.3390/risks11050091

Bartholic, M., Gu, Z., Su, J., Goldstein, J., & Matsuo, S. (2021). Smart auto insurance: High resolution, dynamic, privacy-driven, telematic insurance. *arXiv*. https://doi.org/10.48550/arXiv.2102.03410

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4), 588–608. https://doi.org/10.2307/2094589

Computer Crimes Act. (2009).[Computer Crimes Act] . The Islamic Consultative Assembly (Iranian Parliament). [In persian] https://qavanin.ir/Law/TreeText/?IDS=١٦٢٨٠٩٥٧٨٢٦٨٧٧٢٥٢٣٤٩

Electronic Commerce Act. (2003).[Electronic Commerce Act]. The Islamic Consultative Assembly (Iranian Parliament). [In persian] https://qavanin.ir/Law/TreeText/?IDS=15700719202226051269

European Parliament and Council. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). *Official Journal of the European Union*, L 119, 1–88 https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Union Agency for Cybersecurity (ENISA). (2024). *Cyber insurance—Models and methods and the use of AI*. https://www.enisa.europa.eu/publications/cyber-insurance-models-and-methods-and-the-use-of-ai

European Union. European Parliament and Council. (2014). Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market. *Official Journal of the European Union*, L 257, 73–114. https://eur-lex.europa.eu/eli/reg/2014/910/oj

Felson, M. (2008). Routine activity approach. In R. Wortley & L. Mazerolle (Eds.), Environmental criminology and crime analysis (pp. 70–77). Willan Publishing. https://books.google.com/books?id=٨U٨ObTP٨١QsC

Gupta, B. B., Arachchilage, N. A., & Psannis, K. E. (2018). Defending against phishing attacks: taxonomy of methods, current issues and future directions. *Telecommunication Systems*, 67(2), 247-267. https://doi.org/10.1007/s11235-017-0334-z

Jeyasingh, B. B. F. (2023). Impact of RegTech on compliance risk due to financial misconduct in the United States banking industry. *Digital Economy and Sustainable Development*, 1, Article 24. https://doi.org/10.1007/s44265-023-00024-z

Kesan, J. P., & Hayes, C. M. (2017). Strengthening cybersecurity with cyberinsurance markets and better risk assessment. *Minnesota Law Review*, 102(1), 191–276. https://doi.org/10.24926/265535.985

Kothandapani, H. P. (2024). Automating financial compliance with AI: A new era in Regulatory Technology (RegTech). *International Journal of Science and Research Archive*, 11(1), 2646–2659. https://doi.org/10.30574/ijsra.2024.11.1.0040

National Association of Insurance Commissioners. (2024). Cybersecurity. https://content.naic.org/insurance-topics/cybersecurity

Novak, W. (2025). Reg-tech, open banking, and AI-based fraud defense in fintech. SSRN. https://doi.org/10.2139/ssrn.5386290

Nurse, J. R. C., Axon, L., Erola, A., Agrafiotis, I., Goldsmith, M., & Creese, S. (2020). The data that drives cyber insurance: A study into the underwriting and claims processes. In 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA) (pp. 1–8). IEEE. https://doi.org/10.1109/CyberSA49311.2020.9139703

Onabowale, O. (2025). Navigating the Fintech landscape: The impact of RegTech and InsurTech on financial services. *International Journal of Computer Applications Technology and Research*, 14(2), 99–112. https://doi.org/10.7753/IJCATR1402.1007

Papantoniou, A. A. (2022). Regtech: Steering the regulatory spaceship in the right direction?. *Journal of Banking and Financial Technology*, 6, 1–16. https://doi.org/10.1007/s42786-022-00038-9

Regazzoni, L. (2022). Some issues about insurance smart contracts, between technological innovation and mandatory legal principles. *Osservatorio del diritto civile e commerciale*, 119–134. https://doi.org/10.4478/106703

Regulation No. 105 on the establishment and operation of insurance technology companies (InsurTech). (2024). [Regulation No. 105 on the establishment and operation of insurance technology companies (InsurTech)] .*Supreme Council of Insurance*. [In persian] https://qavanin.ir/Law/TreeText/?IDS=1391210946680348158

The Iranian Civil Code.(1928). [The Iranian Civil Code]. National Consultative Assembly of Iran .[In persian] https://qavanin.ir/Law/TreeText/?IDS=12021850837713548188

The Iranian Code of Criminal Procedure. (2013). [The Iranian Code of Criminal Procedure]. The Islamic Consultative Assembly (Iranian Parliament). [In persian] https://qavanin.ir/Law/TreeText/?IDS=2433638803151753757

The Iranian Insurance Act. (1937). [The Iranian Insurance Act]. National Consultative Assembly of Iran. [In persian] https://qavanin.ir/Law/TreeText?IDS=4693937366938194803

The Islamic Penal Code.(2013). [The Islamic Penal Code]. The Islamic Consultative Assembly (Iranian Parliament). [In persian] https://qavanin.ir/Law/TreeText?IDS=4693937366938194803

Weber, S., Scherer, M., Pascu, C., & Lourenco, M. B. (2024). Cyber insurance: Models and methods and the use of AI. *European Union Agency for Cybersecurity* (ENISA). https://doi.org/10.2824/464473

Zucca, M. V. (2025). Mappare il Crime-as-a-Service: Analisi delle strutture, dei ruoli e dei servizi nell'offerta criminale digitale. *Rivista Italiana di Informatica e Diritto*, 7(2), 159–169. https://doi.org/10.32091/RIID0249

Zucca, M. V., & Fiorinelli, G. (2025). Regulating AI to combat tech-crimes: Fighting the misuse of generative AI for cyber attacks and digital offenses. *Technology and Regulation*, 2025, 247–262. https://doi.org/10.71265/23nqtq40