Jurisprudence and Legal Studies of Media Journal
VOL. 7 / Autumn 2025 and Winter 2026 / NO. 2 (Serial 14)

Legal Challenges of Cyber Insurance in International Contracts

Mahzad Saffarinia[1] 0000-0002-7818-0262

Abstract

With the expansion of digital technologies and the increase in cyber attacks, insurance has emerged as an important tool for managing risks related to cyberspace. Cyber insurance in international contracts faces numerous legal challenges that arise from differences in national laws, varying definitions of cyber incidents, and the complexities of determining liability. This article shows that the legal challenges of cyber insurance in international contracts are divided into two parts: substantive and formal. Determining jurisdiction, conflict of laws, interpretation of contract provisions, and enforcement of arbitration awards are among the most important challenges facing activists in this field. With the expansion of digital technologies and the increase in cyber attacks, insurance has emerged as an important tool for managing risks related to cyberspace. Cyber insurance in international contracts faces numerous legal challenges that arise from differences in national laws, varying definitions of cyber incidents, and the complexities of determining liability. This article shows that the legal challenges of cyber insurance in international contracts are divided into two parts: substantive and formal. Determining jurisdiction, conflict of laws, interpretation of contract provisions, and enforcement of arbitration awards are among the most important challenges facing activists in this field.

Keyword: Cyber insurance, Contract Law, Internationa, Contracts, Legal Challenges, Cyberspace

1- Assistant Professor of law, Refah university, Tehran, Iran saffarinia@refah.ac.ir

دوفصلنامه
مطالعات فقه و حقوق رسانه
دانشکده غیردولتی – غیرانتفاعی رفاه

دوره ۷، شماره ۲(پیاپی ۱٤)
پاییز و زمستان ۱٤۰٤
صص: ۷۳-۹۲

چالش‌های حقوقی بیمه سایبری در قراردادهای بین‌المللی

نوع مقاله: پژوهشی
تاریخ دریافت: ۱٤۰٤/۰٤/۱۷
تاریخ پذیرش: ۱٤۰٤/۰۷/۰۵

مهزاد صفاری‌نیا[۱]

چکیده

با گسترش فناوری‌های دیجیتال و افزایش حملات سایبری، بیمه به‌عنوان یکی از ابزارهای مهم برای مدیریت ریسک‌های مرتبط با فضای مجازی مطرح شده است. بیمه سایبری که به‌مثابه پوششی در برابر زیان‌های ناشی از نقض امنیت اطلاعات، حملات بدافزاری و اختلال در سیستم‌های دیجیتالی ارائه می‌شود در قراردادهای بین‌المللی با چالش‌های حقوقی متعددی مواجه است و این چالش‌ها ناشی از تفاوت‌های قوانین ملی، تعریف‌های متغیر از حوادث سایبری و پیچیدگی‌های تعیین مسئولیت است. این پژوهش با روش تحلیل موردی و بررسی آرای قضایی بین‌المللی، چالش‌های حقوقی بیمه سایبری در قراردادهای بین‌المللی را در دو محور کلی بررسی کرده و مشخص می‌کند؛ چالش‌های حقوقی بیمه سایبری در قراردادهای بین‌المللی به دو بخش ماهوی و شکلی تقسیم می‌شود. تعیین صلاحیت قضایی، تعارض قوانین، تفسیر مفاد قرارداد و اجرای آرای داوری از مهم‌ترین چالش‌های پیش‌روی ذی‌نفعان این حوزه هستند. همچنین تعیین مرجع صالح برای رسیدگی به دعاوی، به‌ویژه در مواردی که طرفین در حوزه قضایی مختلف مستقر هستند یا اینکه حمله از یک کشور و خسارت در کشور دیگر رخ داده نیز از مسائل مورد توجه در این حوزه است. اختلاف در تفسیر بندهای قراردادی مانند استثنای حملات تحت حمایت دولت‌ها که در پرونده‌های مهم نظیر مندلز، نورسک و هیدور مشاهده شده است، نیاز به تدوین مقررات شفاف‌تر و هماهنگ‌تر را برجسته می‌کند. در نهایت، مقاله ضمن ارائه نمونه‌های عملی از دعاوی مطرح شده در این حوزه به بررسی چالش‌های موجود در کشورهایی که طرف کنوانسیون نیویورک نیستند، می پردازد و راهکارهایی برای افزایش کارآمدی و انسجام در مقررات بیمه سایبری در سطح بین‌المللی پیشنهاد می‌کند.

واژگان کلیدی

بیمه سایبری، حقوق قراردادها، قردادهای بین‌المللی، چالش‌های حقوقی، فضای سایبری.

۱. استادیار گروه حقوق، دانشکده غیرانتفاعی رفاه، تهران، ایران saffarinia@refah.ac.ir

مقدمه

در عصر تحول دیجیتال، گسترش فناوری‌های ارتباطی و وابستگی روزافزون صنایع و کسب‌وکارها به زیرساخت‌های سایبری، زمینه‌ساز افزایش تهدیدات و مخاطرات سایبری شده است. این تهدیدات که از نفوذهای غیرمجاز و حملات باج‌افزاری تا جاسوسی سایبری و ازکاراندازی زیرساخت‌های حیاتی را شامل می‌شود، ضرورت اتخاذ تدابیر حمایتی و خسارت‌های احتمالی را بیش‌ازپیش ساخته است. آنتونیو گوترش[1]، دبیرکل سازمان ملل، در اولین سخنرانی خود در افتتاحیه نشست سران مجمع عمومی سازمان ملل متحد در سال ۲۰۱۷، تشدید تهدیدات امنیت سایبری را به‌عنوان یک تهدید اصلی برای امنیت بین‌المللی برجسته کرد *(فرجزاده، ۱٤۰۱، ص. ۱)*. دراین‌میان، بیمه سایبری به‌عنوان ابزاری کارآمد برای مدیریت ریسک وکاهش پیامدهای مالی حملات سایبری، جایگاه ویژه‌ای در نظام حقوقی و تجاری بین‌المللی یافته است. بااین‌حال، بهره‌گیری از بیمه سایبری در قراردادهای بین‌المللی با چالش‌های حقوقی متعددی همراه است که عمدتاً از ماهیت فراملی فضای سایبری، تنوع مقررات ملی و پیچیدگی‌های فنی ناشی می‌شود؛ به‌عنوان‌مثال، حمله سایبری که در یک کشور طراحی شده و داده‌های متعلق به شرکتی در کشور دیگر را هدف قرار می‌دهد، می‌تواند در چندین نظام حقوقی بررسی و منجر به بروز اختلاف در تعیین مرجع صالح و قانون حاکم شود. علاوه‌براین، نبود یک چهارچوب واحد و جامع بین‌المللی برای تنظیم و تفسیر قراردادهای بیمه سایبری، اجرای این قراردادها را در سطح بین‌المللی با دشواری‌هایی مواجه ساخته است. پرسش اصلی مقاله این است که مهم‌ترین چالش‌های حقوقی در این زمینه کدام موارد هستند و در عرصه بین‌الملل دادگاه‌های بین‌المللی چه نتایج حقوقی برای حل دعاوی ارائه داده‌اند.

۱- حملات سایبری

سایبر مخفف واژه سایبرنتیک واژه‌ای است برگرفته از لغت یونانی به‌معنای حاکمیت و یا حکومت می‌باشد *(السان، کلانتری و سجادی، ۱۳۹۵، ص. ۸٤)*. عموماً واژه سایبر به اختصار

1. Antonio Guterres

به‌جای واژه فضای سایبری به‌کار می‌رود. فضای سایبری، دامنه‌ای جهانی درون محیط اطلاعاتی که دربردارنده شبکه به هم متصل زیرساختاری سیستم اطلاعاتی است که خود شامل اینترنت، شبکه‌های ارتباط راه دور، سیستم‌های رایانه‌ای و کنترل‌گرها و پردازشگرهای آن است. این فضا محیطی است مجازی و غیرملموس که در فضای شبکه‌های مختلف که از طریق اینترنت به‌هم وصل می‌شوند، وجود دارد. در این محیط، تمام اطلاعات مربوط به افراد، ملت، فرهنگ‌ها، کشورها، به‌صورت ملموس و فیزیکی مانند نوشته، تصویر، صوت و اسناد در یک فضای مجازی و به شکل دیجیتالی وجود داشته و قابل استفاده و در دسترس استفاده کنندگان و کاربران می‌باشد *(میرزایی ورزنه، ۱۳۹۵، ص. ۱۱)*. امنیت فناوری اطلاعات، به هر آن چیزی که اطلاعات را مورد تهدید قرار می‌دهد اطلاق می‌شود. ذیل این مفهوم، امنیت سایبری قرار دارد که به حملاتی که به واحدهای اپلیکیشن‌ها، نرم‌افزارها، سخت‌افزارها و مراکز اطلاعات می‌پردازد. اکثر رویدادهایی که در رایانه‌ها یا شبکه‌ها اتفاق می‌افتد، عادی و مجاز هستند و بنابراین برای متخصصان امنیتی نگران‌کننده نیستند، بااین‌حال گاهی اوقات یک رویداد بخشی از یک حمله است، یا به دلایل دیگری یک نگرانی امنیتی به حساب می‌آید *(Howard & Longstaff, 1998, 16)*؛ بنابراین می‌توان گفت: رویداد سایبری طیف گسترده‌ای از فعالیت‌ها، ازجمله رویدادهای بی‌خطر و مخرب را در برمی‌گیرد. رویدادهای سایبری می‌توانند شامل فعالیت‌های معمولی مانند به‌روزرسانی نرم‌افزار، تعمیر و نگهداری سیستم، یا نوسانات ترافیک شبکه و همچنین فعالیت‌های غیرعادی یا مخرب مانند حملات سایبری باشند. حملات سایبری درواقع زیرمجموعه‌ای از رویدادهای سایبری می‌باشند و به‌طور خاص یک اقدام عمدی و مخرب انجام شده برای تخریب، سرقت، مختل کردن، یا آسیب رساندن به سیستم‌های اطلاعاتی، شبکه‌های رایانه‌ای یا دارایی‌های دیجیتال و همچنین هرگونه تلاش برای افشا، تغییر، غیرفعال کردن، تخریب، سرقت یا دستیابی به دسترسی غیرمجاز یا استفاده غیرمجاز از یک دارایی تعریف می‌شود. حمله سایبری هر نوع مانور تهاجمی است که سامانه‌های اطلاعات رایانه‌ای، زیرساخت‌ها، شبکه‌های رایانه‌ای یا دستگاه‌های رایانه شخصی را هدف قرار می‌دهد. مهاجم یک شخص یا فرایندی است که سعی در دسترسی به داده‌ها، کارکردها یا سایر مناطق محدود سامانه

بدون مجوز به‌طور بالقوه با قصد مخرب دارد *(ادیبی، دریایی و زهدی، ۱۳۹۶، ص. ۱۵)*.

حمله سایبری ممکن است با هک کردن یک سامانه مستعد، هدف مشخص شده را دزدیده، تغییر داده یا از بین ببرد. حملات سایبری می‌تواند از نصب جاسوس‌افزارها بر روی رایانه شخصی تا تلاش برای تخریب زیرساخت کشورها را دربرگیرد. دستورالعمل کمیته سامانه‌های امنیت ملی[1](CNSS) شماره ٤٠٠٩ مورخ ٢٦ آوریل ٢٠١٠، حمله را چنین تعریف می‌کند: هرنوع فعالیت مخرب که سعی در جمع‌آوری، مختل کردن، انکار، تخریب یا نابودی منابع سامانه اطلاعات یا خود اطلاعات را دارد. همچنین این دستورالعمل حمله سایبری را بدین‌شرح تعریف می‌کند: حمله از طریق فضای مجازی، به‌معنای هدف قرار دادن استفاده سازمانی از فضای سایبر به منظور اخلال، غیرفعال‌سازی، تخریب یا کنترل، سوءاستفاده از محیط زیرساخت‌های محاسباتی، یا از بین بردن یکپارچگی داده‌ها یا سرقت اطلاعات کنترل شده، می‌باشد *(پژوهشکده بیمه، ١٤٠٢، ص. ٧٨)*.

۲- چالش‌های حقوقی حملات سایبری

همان‌طور که گفته شد بیمه سایبری یکی از حوزه‌های نوظهور در صنعت بیمه است که به‌دنبال کاهش خسارات مالی ناشی از حملات سایبری و نقص داده‌ها می‌باشد. با گسترش فناوری دیجیتال و افزایش تهدیدات سایبری، نیاز به ایجاد چهارچوب‌های حقوقی مناسب برای تنظیم و اجرای قراردادهای بیمه سایبری بیش‌ازپیش احساس می‌شود. بااین‌حال، این حوزه با چالش‌های حقوقی پیچیده‌ای مواجه است که می‌توان آن راها به دودسته کلی تقسیم کرد: چالش‌های شکلی و چالش‌های ماهوی.

چالش‌های شکلی شامل مسائل مرتبط با تعیین قانون حاکم و تعارض قوانین، تعیین صلاحیت قضایی و حل‌وفصل اختلافات می‌باشد؛ زیرا بیشتر به جنبه‌های اجرایی و فرایندی رسیدگی به دعاوی مرتبط می‌شود. چالش‌های ماهوی بیشتر به مباحث اساسی و بنیادی حقوق بیمه سایبری مربوط می‌شوند.

1. Comitte on National Security System

۲-۱. تعیین قانون حاکم و تعارض قوانین[1]

یکی از چالش‌های اساسی در قراردادهای بین‌المللی بیمه سایبری، تعیین قانون حاکم است. اختلاف در مقررات حریم خصوصی و استانداردهای امنیت سایبری بین نظام‌های حقوقی مختلف می‌تواند منجر به تعارضات قانونی شود *(Eneken Tikk & Kardi kaska, 2017, p. 106)*. بسیاری از کشورها در جرایم سایبری فاقد جرم‌انگاری بوده و هیچ قانونی برای آن ندارند و از طرفی، برخی از کشورها نیز بسیاری از مواردی را که توسط بسیاری از کشورها جرم‌انگاری شده را جرم‌انگاری نکرده‌اند. برخی از کشورها همانند کشور جمهوری اسلامی ایران فاقد قانون جامع و کامل در این خصوص است. موارد فوق موجب شده است که چالش پیش‌رو در حوزهٔ تعارض قوانین، بسیار عمیق‌تر از موارد تعارض قوانین سنتی در حقوق بین الملل محسوب شود *(صبح‌خیر، ۱۳۹٤، ص. ۱۳۷)*. در قراردادهای بیمه، طرفین معمولاً شرط تعیین قانون حاکم را مشخص می‌کنند. این شرط بیان می‌کند که اگر اختلافی پیش بیاید، قوانین کدام کشور باید اعمال شود؛ اما درصورتی‌که چنین شرطی در قرارداد وجود نداشته باشد، عوامل مختلفی مانند، محل اقامت بیمه‌گذار و بیمه‌گر، محل اجرای تعهدات بیمه‌ای مبنای تعیین قانون حاکم قرار می‌گیرد *(نوشادی و باقری، ۱۳۹۲، ص. ۲۲۸)*.

همچنین یکی از مهم‌ترین چالش‌ها در دعاوی بیمه سایبری بین‌المللی، مسئله تعارض قوانین است. هنگامی که طرفین قرارداد از کشورهای مختلف هستند، تعیین اینکه کدام قانون حاکم بر قرارداد بیمه سایبری اعمال می‌شود، می‌تواند پیچیده باشد. به‌ویژه زمانی که قوانین داخلی کشورها در حوزه حفاظت از داده‌ها یا مقررات امنیت سایبری تفاوت‌های اساسی دارند *(Gareht, 2018, p. 21)*؛ به‌طورمثال در دعاوی مرتبط با نقض داده‌های شخصی، ممکن است هم قوانین حفاظت از داده‌های[2] اتحادیه اروپا و هم قوانین محلی کشوری دیگر مانند قانون حریم خصوصی مصرف‌کننده در آمریکا[3] اعمال شوند که منجر به تضاد در تعهدات قانونی می‌شود *(Kuner, 2020, p. 250)*. این تضاد می‌تواند منجر به پیچیدگی در تعیین مسئولیت بیمه‌گر و بیمه‌گذار شود و همچنین روند حل‌وفصل اختلافات را طولانی‌تر کند. با

1. conflict of law
2. General Data Protection Regulation
3. California Consumer Privacy Act

توجه به پیچیدگی‌های فضای سایبری و تعارض‌های قانونی موجود، تدوین قوانین بین‌المللی هماهنگ و ایجاد سازوکارهای همکاری بین‌المللی می‌تواند به کاهش این تعارض‌ها و تسهیل در حل‌وفصل اختلافات در حوزه سایبری کمک کند. اتحادیه بین‌المللی مخابرات[1]، سازمان همکاری و توسعه اقتصادی[2]، گروه کارشناسان دولتی سازمان ملل متحد[3]، مرکز عالی دفاع سایبری ناتو[4]، مجمع جهانی اقتصاد[5] و کارگروه باز بررسی تحولات در زمینه اطلاعات و ارتباطات[6] نقش مهمی در مقابله با تهدیدات سایبری و تدوین قوانین بین‌المللی دارند.

۲-۲. تعیین صلاحیت قضایی[7]

تعیین اینکه کدام دادگاه یا نهاد داوری صلاحیت رسیدگی به دعاوی بیمه سایبری را دارد، یکی از مسائل پیچیده در قراردادهای بین‌المللی است. حملات سایبری ماهیت فرامرزی دارند و ممکن است چندین حوزه قضایی و کشور را درگیر کنند.

چالش اصلی این است که دعاوی مربوط به بیمه سایبری می‌توانند در دادگاه‌های ملی، مراجع داوری بین‌المللی، یا حتی در چندین کشور به صورت همزمان مطرح شوند (*Ridi & Schultz, 2020, p. 33*).

در پرونده نورسک هیدرو علیه شرکت بیمه اختلاف بر سر صلاحیت قضایی بین دادگاه‌های نروژ و مراجع داوری بین‌المللی وجود داشت که روند دادرسی را پیچیده کرد. برای حل این چالش چندین راهکار ارائه شده است. یکی از راهکارها صلاحیت مبتنی بر قلمرو است که به محل وقوع خسارت سایبری یا محل اقامت طرفین قرارداد بیمه وابسته است. همچنین در بسیاری از قراردادهای بیمه سایبری، یک بند اختصاصی برای تعیین صلاحیت گنجانده می‌شود. طبق این بند، طرفین توافق می‌کنند که در صورت بروز اختلاف،

1. ITU
2. OECD
3. UNGGE
4. CCDCOE
5. WEF
6. OEWG
7. Jurisdictional Challenges

کدام دادگاه صلاحیت رسیدگی را خواهد داشت. صلاحیت مبتنی بر محل اجرای تعهد نیز که می‌تواند شامل محل ذخیره داده‌ها یا محل ارائه خدمات سایبری باشد، ازجمله راهکارهاست *(باغبان و دیگران، ۱۴۰۲، ص. ۱۸)*.

۲-۳. روش‌های حل‌وفصل اختلافات

حل‌وفصل اختلافات در حوزه بیمه سایبری به‌دلیل پیچیدگی‌های فنی و حقوقی نیازمند سازوکارهایی است که بتواند منافع طرفین را حفظ کرده واز اتلاف منابع جلوگیری کند. ازجمله روش‌های مهم برای حل اختلافات دراین زمینه می‌توان به مذاکره، میانجی‌گری، داوری و رسیدگی قضایی اشاره کرد *(Carver, 2020, pp. 345-367)*. انتخاب بین روش‌های حل اختلاف مانند داوری بین‌المللی، میانجیگری یا دادرسی قضایی از چالش‌های دیگر است. در پرونده‌های بیمه سایبری از ترکیب داوری و میانجی‌گری با هم استفاده می‌کنند تا روند حل اختلاف سریع‌تر و کم‌هزینه‌تر باشد. همین‌طور استفاده از هوش مصنوعی در پرونده‌های داوری نیز از فناوری‌های نوینی است که در دعوای لاپاگلیا[۱] از این فناوری استفاده شد *(Silicon Valley Arbitration & Mediation center, 2020)*. داوری به‌دلیل محرمانگی و انعطاف‌پذیری بیشتر در دعاوی مرتبط با بیمه سایبری ترجیح داده می‌شود. عدم آشنایی قضات سنتی با دانش فنی لازم نسبت به فضای سایبری از دیگر چالش‌های بزرگ است. همچنین اجرای آرای داوری اگر این کشورها عضو کنوانسیون‌هایی مانند کنوانسیون نیویورک نباشند؛ دشوار است؛ زیرا این کنوانسیون چهارچوبی استاندارد و کارآمد برای شناسایی و اجرای آرای داوری خارجی فراهم می‌کند، در غیاب این کنوانسیون اجرای آرا تابع قوانین داخلی کشورهاست که ممکن است زمان بر و غیرقابل‌پیش‌بینی باشد. در پرونده شرکت ایکس وای زد در مقابل شرکت ای بی سی۲۰۱۸ در دادگاه امارات متحده عربی، بررسی اعتبار شرط داوری در قراردادهای تجاری بررسی شد. در این پرونده بین دو شرکت قرارداد ساخت‌وساز منعقد شد که در آن شرط داوری گنجانده شده بود. پس از بروز اختلاف، شرکت ال تی دی تصمیم گرفت که به دادگاه مراجعه کند؛ اما شرکت مقابل

3- Lapaglia

استدلال کرد که طبق قرارداد اختلاف باید از طریق داوری حل شود. ازجمله مسائل حقوقی مطرح شده در این پرونده الزام‌آوری شرط داوری و اولویت روش‌های حل اختلاف بوده است. دادگاه درنهایت حکم داد که شرط داوری معتبر است و طرفین باید اختلاف خود را از طریق داوری حل کنند. این پرونده نشان داد که انتخاب روش حل اختلاف باید به‌طور دقیق در قرارداد مشخص شود تا از بروز اختلافات بعدی جلوگیری شود. در این پرونده تأکید شد که طرفین قرارداد باید در هنگام تنظیم قرارداد، روش‌های حل اختلاف را به‌طور شفاف مشخص کنند. همچنین، دادگاه‌ها معمولاً به شرط‌های داوری احترام می‌گذارند، مگر اینکه دلایل قانونی برای بی‌اعتباری آن وجود داشته باشد *(Generis one online, 2024)*.

۲-۴. دعاوی مرتبط با تأخیر در پرداخت خسارت توسط بیمه‌گر

یکی دیگر از موضوعات متداول در دعاوی بیمه سایبری، تأخیر بیمه‌گران در پرداخت خسارت به‌دلیل نیاز به بررسی‌های پیچیده فنی و حقوقی است. اگر این فرایند بیش از حد طولانی شود یا بیمه‌گذار احساس کند که بیمه‌گر عمدا فرایند را کند کرده است، می‌تواند از بیمه‌گر شکایت کند و درخواست تسریع در پرداخت خسارت را داشته باشد. اگر تأخیر بیمه‌گر باعث زیان مالی بیشتر بیمه گذار شده باشد؛ بیمه‌گذار می‌تواند علاوه بر دریافت مبلغ بیمه، درخواست جبران خسارت ناشی از تأخیر را نیز مطرح کند *(Harrington, 2020, p. 215)*.

در پرونده نقض داده‌های شرکت تارگت[1] مسئله تأخیر در پرداخت خسارت توسط بیمه‌گر نیز مطرح شد. تارگت تحت پوشش بیمه‌ای برای حوادث سایبری قرار داشت. این موضوع در جریان دعاوی بین تارگت و بیمه‌گرهایش، به‌ویژه درخصوص تفسیر مفاد بیمه‌نامه و تعهدات پرداخت خسارت، مورد اختلاف قرار گرفت. شرکت بیمه در پرداخت خسارت به دلیل ابهامات مربوط به میزان پوشش بیمه‌ای و هزینه‌های حقوقی مرتبط با دعاوی مشتریان تأخیر داشت. این پرونده نشان داد که بیمه‌گران باید فرایندهای سریع‌تری برای ارزیابی و پرداخت خسارات ناشی از حملات سایبری اتخاذ کند و دادگاه تأکید کرد بیمه‌گر باید پس از تکمیل مدارک و ارزیابی خسارت، در یک بازه زمانی معقول خسارت را

1. Target

پرداخت کند. همچنین در قوانین داخلی کشورهایی نظیر ایالات متحده آمریکا، طبق مقررات یو سی سی [1] شرکت‌های بیمه موظفند خسارت را در مدت زمان معقول پرداخت کنند. در اتحادیه اروپا نیز بند ٤١ از دستورالعمل بیمه EC/2009/138 به لزوم پرداخت به‌موقع خسارت اشاره کرده و تأخیر غیرموجه را تخلف می‌داند *(EIOPA, 2020)*.

۳- چالش‌های ماهوی

بیمه‌های سایبری علاوه بر چالش‌های حقوقی شکلی با چالش‌های حقوقی ماهوی نیز مواجه هستند. یکی از مهم‌ترین مسائل، عدم تعریف واحد و مشخص از خطرهای سایبری و پوشش‌های بیمه‌ای مرتبط است، به‌گونه‌ای که هر شرکت بیمه ممکن است معیارهای متفاوتی برای ارزیابی و جبران خسارت داشته باشد. علاوه‌براین اصل سببیت در بیمه سایبری با پیچیدگی‌های زیادی همراه است؛ زیرا شناسایی عامل حمله و تعیین مسئولیت آن در بسیاری از موارد دشوار است. همچنین، اختلافات حقوقی ناشی از هماهنگ نبودن قوانین حفاظت از داده‌ها میان کشورها، اجرای تعهدات بیمه‌گران را با چالش مواجه کرده است.

۳-۱. دعاوی مربوط به اثبات وقوع حمله سایبری [2] و پرداخت‌های احتمالی غیرقانونی

یکی از چالش‌های اصلی در دعاوی بیمه سایبری، بار اثبات منشأ حمله سایبری [3] است. بسیاری از بیمه‌گران برای اثبات اینکه یک حمله سایبری ناشی از یک دولت یا گروه تحت حمایت دولت است، نیاز به مدارک قوی دارند. در دعاوی بیمه سایبری، تعیین منشأ حمله می‌تواند تأثیر زیادی بر نتیجه پرونده داشته باشد. بیمه‌گران اغلب برای پرداخت خسارت نیاز به شواهدی دارند که نشان دهد حمله چگونه و توسط چه کسی انجام شده است. حملات سایبری به‌راحتی می‌توانند ردپای جعلی ایجاد کنند و شناسایی دقیق مهاجمان بسیار دشوار است *(Buchanan & Rid, 2015, p. 27)*.

1. Uniform Commercial Code
2. Attribution Challenges
3. Burden of Proof

چالش‌هایی مانند تغییرپذیری داده‌ها، حذف شواهد و ناشناس بودن مهاجمان می‌تواند روند اثبات را پیچیده کند. در تغییرپذیری داده‌ها مهاجمان سایبری می‌توانند داده‌ها را تغییر دهند یا دستکاری کنند تا مسیر حمله را پنهان کنند، این تغییرات ممکن است شامل حذف یا تغییر لاگ‌های سیستم، رمزگذاری داده‌ها یا جایگزینی اطلاعات واقعی یا داده‌های جعلی باشد. در بسیاری از حملات سایبری به‌گونه‌ای طراحی شده‌اند که پس از اجرا، شواهد خود را از بین ببرند، مهاجمان ممکن است از روش‌هایی مانند پاک کردن لاگ‌ها، استفاده از بدافزارهای خود تخریب‌کننده یا تغییر مسیرهای ارتباطی برای جلوگیری ازردیابی استفاده کنند. همچنین ناشناس بودن که در آن معمولاً از ابزارهایی مانند شبکه‌های خصوصی مجازی، پروکسی‌ها و روش‌های جعل هویت استفاده می‌کنند. پرونده شرکت سی ان ای[1] که یکی از بزرگ‌ترین شرکت‌های بیمه در ایالات متحده است، در سال ۲۰۲۱ مورد حمله باج‌افزاری[2] قرار گرفت.[3] مهاجمان از گروه‌های هکری پیشرفته که مرتبط با حملات سازمان‌یافته بین‌المللی بودند. چندین مشتری علیه سی ان ای شکایت کردند و مدعی شدند این شرکت نتوانسته است اقدامات مناسبی برای حفاظت از داده‌های حساس اتخاذ کند. یکی از چالش‌های این پرونده آن بود که آیا حمله توسط یک دولت خارجی هدایت‌شده (که مشمول استثناء می‌شود) یا توسط مجرمان سایبری مستقل انجام شده است. همچنین یکی از مسائل بحث‌برانگیز، مشروعیت حقوقی پرداخت مبلغ هنگفت به مهاجمان بود. برخی از قوانین بین‌المللی و داخلی[4] پرداخت به گروه‌های تحریم شده را ممنوع می‌کنند. چندین مشتری و سهام‌دار علیه شرکت یاد شده دعوا مطرح کرده و مدعی شدند که این شرکت نتوانسته است اقدامات امنیتی مناسبی برای حفاظت از داده‌های حساس اتخاذ کند. برهمین‌اساس دادگاه در این پرونده به نظرهای کارشناسان امنیت اطلاعات برای تحلیل حمله و شناسایی مهاجمان احتمالی تکیه کرد. درحال‌حاضر برای

1. CAN Financial Cyber Attack
2. Ransomware attack

۳. پرونده در دادگاه فدرال ایالات متحده آمریکا مطرح شده است.

٤. قطعنامه ۱۳۷۳ شورای امنیت، کنوانسیون بین‌المللی مبارزه با تأمین مالی تروریسم، قوانین اداره کنترل دارایی‌های خارجی آمریکا.

مقابله با این چالش‌ها، متخصصان امنیت سایبری از روش‌هایی مانند تحلیل رفتار شبکه، استفاده از هوش مصنوعی برای شناسایی الگوهای غیرعادی و همکاری بین‌المللی برای ردیابی مهاجمان استفاده می‌کنند *(رومانوسکی و دیگران، ۱۴۰۱، ص. ۲۷)*.

۳-۲- همپوشانی بیمه‌نامه‌ها[1]

نهادهای متولی بیمه اجتماعی در قبال بعضی خطراتی که بیمه‌شدگان را تهدید می‌کند، تعهداتی دارند که همه انواع آن را حمایت‌گری بیمه‌ای نامیده‌اند *(کاویانی، ۱۳۸۷، ص. ۲۹۵)*؛ اما این حمایت ممکن است موجب هم‌پوشانی بیمه‌ای شود که یک ریسک یا دارایی مشخص توسط بیش از یک بیمه‌نامه تحت پوشش قرار گرفته باشد *(طالب احمدی و رحمانی، ۱۳۹۲، ص. ۳۲)*. دعاوی مربوط به هم‌پوشانی بیمه‌ها می‌تواند هم جنبه شکلی و هم ماهوی داشته باشند؛ اما در بیشتر موارد این موضوع ماهوی محسوب می‌شود. در بسیاری از موارد، شرکت‌های چندملیتی دارای بیمه‌نامه‌های مختلفی برای پوشش ریسک‌های متفاوت هستند. این مسئله می‌تواند منجر به تداخل پوشش‌ها شود و مشخص نباشد کدام بیمه‌نامه مسئول جبران خسارت است. ابهام در پوشش بیمه‌ای به این معناست که کدام بیمه‌نامه مسئول پرداخت خسارت است و این مسئله نیاز به تفسیر قراردادها و تعریف پوشش‌های بیمه‌ای آن دارد. شرکت‌های بیمه ممکن است حمله سایبری را متفاوت تعریف کنند؛ به‌عنوان‌مثال یک بیمه‌نامه ممکن است حملات ناشی از بدافزار را پوشش دهد، درحالی‌که دیگری آن را استثناء کرده باشد. این موضوع به تفسیر ماهوی شرایط بیمه‌نامه‌ها برمی‌گردد. همچنین شرکتی دارای دو بیمه‌نامه است یکی برای حوادث سایبری و دیگری برای اختلال در کسب‌وکار می‌باشد. اگر حمله باج‌افزاری باعث اختلال در کسب‌وکار شود ممکن است هر دو بیمه‌نامه خسارت را پوشش دهند. تعیین اینکه کدام بیمه مسئول پرداخت است مستلزم بررسی شرایط ماهوی قرارداد است. درج شرط مشارکت، استفاده از اصل تقدم و تقسیم بیمه‌نامه‌ها به بیمه‌نامه اولیه و بیمه‌نامه مازاد که اگر خسارت بیش از سقف تعهد آن باشد، بیمه مازاد وارد عمل می‌شود *(Jelmini, 2021, p. 17)* و استفاده از استانداردهای بین‌المللی

5. Overlap of insurance policies

مانند اصول اینکوترمز،[۱] مقررات لندن[۲] و راهنمایی‌های سازمان‌های بیمه‌ای می‌تواند در شفاف‌سازی و هماهنگ‌سازی پوشش بیمه‌ای مؤثر باشد. در برخی شرایط، هم‌پوشانی بیمه‌ها جنبه شکلی پیدا می‌کند؛ مانند تعارض صلاحیت قضایی که اگر بیمه‌نامه‌ها تحت قوانین کشورهای مختلف تنظیم شده باشد، چالش شکلی در تعیین دادگاه یا مرجع صالح برای رسیدگی به اختلاف به‌وجود می‌آید؛ برای‌مثال دو بیمه‌نامه از دو شرکت در دو کشور مختلف صادر شده‌اند حالا برای تعیین مسئولیت هرکدام باید مشخص شود کدام کشور صلاحیت رسیدگی دارد و این یک چالش شکلی است. همچنین سایلنت سایبر که ریسک‌های سایبری پنهان در بیمه‌نامه‌هایی است که به‌طور خاص برای پوشش تهدیدات سایبری طراحی نشده‌اند و در بیمه‌نامه‌های سنتی همانند بیمه اموال، بیمه مسئولیت یا بیمه اختلال در کسب‌وکار وجود دارند، ممکن است باعث ابهام در پرداخت خسارت شود؛ زیرا بیمه‌گر ممکن است ادعا کند که خسارت ناشی از حمله سایبری تحت پوشش بیمه نیست؛ بنابراین بسیاری از شرکت‌های بیمه برای کاهش ریسک‌های سایلنت سایبر، درحال بازنگری بیمه‌نامه‌های خود هستند تا شرایط پوشش سایبری را شفاف‌تر کنند و از ابهامات جلوگیری کند. همچنین، برخی از بیمه‌گران بیمه‌نامه‌های ترکیبی ارائه می‌دهند که شامل پوشش‌های سنتی و سایبری به‌طور همزمان است. این بیمه‌نامه‌های ترکیبی و یا سایلنت سایبر بدون اینکه به‌طور مشخص پوشش سایبری را رد کنند، ممکن است خسارات ناشی از حملات سایبری را جبران کنند و این وضعیت باعث ابهام در پرداخت خسارت و عدم قطعیت برای بیمه‌گران و بیمه‌گذاران می‌شود *(Marsh, 2020, p. 15)*.

---

۱. اینکوترمز مجموعه‌ای از اصطلاحات و قوانین بین‌المللی تجارت است که توسط اتاق بازرگانی بین‌المللی تدوین شده‌اند. این قوانین برای تعیین مسئولیت‌ها، هزینه‌ها و ریسک‌های مرتبط با حمل‌ونقل کالا بین خریدار و فروشنده در معاملات بین‌المللی استفاده می‌شوند. اینکوترمز به شفاف‌سازی قراردادهای تجاری کمک و مشخص می‌کند که چه کسی مسئول بیمه، حمل‌ونقل و تشریفات گمرکی است.

۲. مقررات لندن به مجموعه‌ای از قوانین و استانداردهای بیمه‌ای اشاره دارد که در صنعت بیمه بین‌المللی مورد استفاده قرار می‌گیرند. این مقررات شامل اصول و رویه‌هایی هستند که توسط نهادهای بیمه‌ای مستقر در لندن، مانند بیمه لویدز تدوین شده‌اند. این قوانین به هماهنگ‌سازی پوشش بیمه‌ای و تعیین مسئولیت‌های بیمه‌گران در قراردادهای بین‌المللی کمک می‌کنند. LIOYD S Market Rules

۳-۳. دعاوی مربوط به محدوده پوشش بیمه‌ای

محدوده پوشش بیمه‌ای یکی از بحث‌برانگیزترین مسائل در دعاوی بیمه‌ای است، به‌ویژه در بیمه‌های سایبری که پیچیدگی‌های خاصی دارند. در بسیاری از موارد، اختلافات بین بیمه‌گر و بیمه‌گذار درباره میزان تعهدات بیمه‌گر در قبال خسارات وارده به‌دلیل ابهامات موجود در شرایط قراردادی به‌وجود می‌آید. در پرونده‌های محدوده پوشش بیمه‌ای پرسش مهم این است که آیا حمله سایبری که منجر به نشت داده‌ها می‌شود، تحت پوشش سایبری قرار می‌گیرد یا خیر؟ و اینکه آیا شرکت بیمه باید خسارات ناشی از نشت داده‌ها را به‌دلیل حمله سایبری به شرکت‌هایی تحت پوشش بیمه هستند، پرداخت کند؟

در سال ۲۰۱۷، شرکت اکوئیفاکس یکی از بزرگ‌ترین مؤسسات گزارش‌دهی اعتباری در ایالات متحده، هدف یک حمله سایبری گسترده قرار گرفت که منجر به نشت اطلاعات شخصی حدود ۱۴۷ میلیون نفر شد. این حادثه یکی از بزرگ‌ترین نقض‌های داده‌ای[1] در تاریخ بود و باعث شد که دعاوی حقوقی متعددی علیه شرکت مطرح شود.[2] پرونده اکوئیفاکس به‌دلیل پیچیدگی‌های حقوقی در حوزه امنیت سایبری، مسئولیت مدنی و بیمه سایبری اهمیت ویژه‌ای دارد. در ماه مارس ۲۰۱۷، مهاجمان از یک آسیب‌پذیری در نرم‌افزار آپاچی استراتس که برای مدیریت تارنماهای اکوئیفاکس استفاده می‌شد، بهره‌برداری کردند. این آسیب‌پذیری به مهاجمان اجازه داد که به سرورهای حاوی داده‌های حساس کاربران دسترسی پیدا کنند. اطلاعات فاش‌شده شامل نام، شماره تأمین اجتماعی، تاریخ تولد، آدرس و برخی اطلاعات مربوط به کارت‌های اعتباری بود. با وجود هشدارهای امنیتی، شرکت این آسیب‌پذیری را تا اواخر جولای ۲۰۱۷ برطرف نکرد که باعث شد حمله به مدت چند ماه ادامه داشته باشد.

پس از افشای این حمله در سپتامبر ۲۰۱۷، دعاوی متعددی علیه اکوئیفاکس[3] در دادگاه‌های ایالات متحده مطرح شد. این دعاوی عمدتاً شامل دعاوی مصرف‌کنندگان، دعوای کمیسیون تجارت فدرال و سایر نهادهای نظارتی بود. چندین شکایت گروهی

1. Data Breach

۲. این پرونده در دادگاه جورجیا در ایالات متحده آمریکا مطرح شد.

3. Equifax

توسط مصرف‌کنندگانی که اطلاعات شخصی‌شان فاش شده بود، مطرح شد. شاکیان ادعا کردند که شرکت در حفاظت از داده‌های آنها سهل‌انگاری کرده و منجر به سرقت هویت و خسارات مالی شده است. دادگاه استدلال کرد که عدم رعایت استانداردهای امنیتی شرکت باعث این نقض داده‌ها شده است. کمیسیون تجارت فدرال[1]، کمیسیون بورس و اوراق بهادار[2] و دفتر حمایت از مصرف‌کنندگان مالی[3] نیز از شرکت به‌دلیل نقض قوانین حفظ حریم خصوصی و عدم رعایت استانداردهای امنیت سایبری شکایت کردند (*Geltman & Craig, 2021, p. 22*).

کمیسیون تجارت فدرال استدلال کرد که این شرکت اقدامات مناسبی برای جلوگیری از این حمله انجام نداده و پس از وقوع حمله نیز به‌درستی کاربران را مطلع نکرده است. اکوئیفاکس دارای بیمه سایبری بود؛ اما بیمه‌نامه شرکت نتوانست تمامی خسارات ناشی از این حمله را پوشش دهد. شرکت بیمه مبلغی در حدود ۱۲۵ میلیون دلار را تحت پوشش بیمه سایبری پرداخت کرد؛ اما این مبلغ در مقایسه با خسارت کلی (۷۰۰ میلیون دلار) بسیار کمتر بود. برخی از خسارات مانند جریمه‌های قانونی و جبران خسارت سهام‌داران تحت پوشش بیمه قرار نگرفتند؛ زیرا بسیاری از بیمه‌نامه‌های سایبری جریمه‌های قانونی و دعاوی ناشی از نقض مقررات را پوشش نمی‌دهند.

پرونده اکوئیفاکس نشان داد که بیمه سایبری نمی‌تواند جایگزین کامل تدابیر امنیتی قوی باشد. چالش‌های اصلی بیمه سایبری در این پرونده عدم شفافیت در مفاد بیمه‌نامه بود. بسیاری از پوشش‌های بیمه‌ای استثناهای زیادی داشتند که باعث شد بخشی از خسارات تحت پوشش قرار نگیرد. محدودیت سقف پوشش بیمه‌ای نیز موجب شد حتی با وجود بیمه سایبری، خسارات مالی شرکت بسیار بیشتر از مبلغی باشد که بیمه جبران کرد. برخی بیمه‌گران معتقد بودند که شرکت به‌دلیل عدم رعایت استانداردهای امنیتی اولیه مانند به‌روزرسانی نرم‌افزارها خود در این حادثه مقصر است و نباید تحت پوشش بیمه قرار گیرد. این امر به‌دلیل عدم شفافیت در مفاد بیمه‌نامه بود. همچنین بسیاری از پوشش‌های

1. FTC
2. SEC
3. CFPB

بیمه‌ای استثناهای زیادی داشتند که باعث شد بخشی از خسارات تحت پوشش قرار نگیرد. محدودیت سقف پوشش بیمه‌ای نیز موجب شد حتی با وجود بیمه سایبری، خسارات مالی شرکت بسیار بیشتر از مبلغی باشد که بیمه جبران کرد. برخی بیمه‌گران معتقد بودند که شرکت به‌دلیل عدم رعایت استانداردهای امنیتی اولیه مانند به‌روزرسانی نرم‌افزارها خود در این حادثه مقصر است و نباید تحت پوشش بیمه قرار گیرد *(Brown, 2020, p. 45)*.

۳-۴. دعاوی مرتبط با استثنائات بیمه‌نامه[1]

بسیاری از بیمه‌نامه‌های سایبری شامل استثنائاتی هستند که خسارات خاصی را از پوشش بیمه‌ای خارج می‌کنند. مهم‌ترین استثنائات شامل:

- حملات سایبری ناشی از دولت‌ها یا گروه‌های تحت حمایت دولتی؛
- خسارات ناشی از ضعف در دستورالعمل‌های امنیتی شرکت بیمه‌شده؛
- حوادثی که بیمه‌گذار از آنها آگاه بوده؛ اما اقدامات پیشگیرانه انجام نداده است.

یکی از پرونده‌ها، پرونده مرک علیه شرکت بیمه آمریکایی اس‌سی‌ای در سال ۲۰۲۳ است.[2] شرکت داروسازی مرک نیز در سال ۲۰۱۷ قربانی حمله سایبری نوت پتیا شد و از شرکت بیمه برای جبران ۱.٤ میلیارد دلار خسارت شکایت کرد. بیمه‌گر استناد کرد که این حمله سایبری توسط روسیه علیه اوکراین انجام شده و مشمول استثنای «عمل جنگی» در بیمه‌نامه می‌شود. دادگاه حکم داد که بیمه‌گر باید خسارت را بپردازد؛ زیرا بیمه‌نامه به‌طور مشخص حملات سایبری را از تعریف «جنگ» مستثنی نکرده بود. این رأی تأکید کرد که شرکت‌های بیمه باید در تدوین بندهای استثنایی شفاف‌تر عمل کنند.

دعوای شرکت بین‌المللی موندلز علیه شرکت بیمه سوئیس نیز یکی از مهم‌ترین دعاوی حقوقی در حوزه بیمه سایبری است که چالش‌های مربوط به استثنائات بیمه‌ای در حملات سایبری را نشان می‌دهد.[3] این پرونده پس از حمله سایبری نوت پتیا[4] در سال ۲۰۱۷ مطرح

1. Interpretation of Exclusions
2. Merk v ACE American Insurance
۳. پرونده در دادگاه ایالتی ایلینوی آمریکا مطرح شد و تمرکز دادگاه برتفسیر بندهای استثناء در بیمه‌نامه‌های سایبری بود.
4. Not Petya

شد و تأثیر مهمی بر تفسیر استثنای «جنگ سایبری» در بیمه‌نامه‌های سایبری داشت. در ژوئن ۲۰۱۷، یک حمله سایبری گسترده با استفاده از بدافزار نوت پدیا رخ داد که بسیاری از شرکت‌های جهانی، ازجمله شرکت بین‌المللی موندلز، را تحت تأثیر قرار داد. این شرکت یکی از بزرگ‌ترین شرکت‌های تولیدکننده مواد غذایی و شکلات در جهان در این حمله دچار اختلال در سیستم‌های IT و از بین رفتن داده‌ها شد. حمله منجر به خسارت ۱۰۰ میلیون دلاری به شرکت z شد که شامل هزینه‌های بازیابی داده‌ها، خسارت به تجهیزات IT و تأخیر در عملیات تولید و توزیع بود *(Jones, 2020, p. 56)*.

موندلز برای جبران خسارت خود، به بیمه‌نامه سایبری خود با شرکت بیمه زوریخ استناد کرد واعلام نمود این حمله یک حمله گسترده جهانی بود که شرکت‌های متعددی را در سراسر جهان تحت تأثیر قرار داده است؛ اما هیچ شواهد قطعی قانونی یا تأییدیه رسمی از سوی دولت ایالات متحده یا سازمان ملل مبنی بر اینکه این حمله به‌طور رسمی «جنگ سایبری» محسوب می‌شود، وجود نداشت. همچنین استثنای «جنگ» باید محدود به درگیری‌های نظامی سنتی باشد، نه حملات سایبری که شرکت‌های خصوصی را هدف قرار می‌دهند. اگر شرکت‌های بیمه بتوانند هر حمله سایبری بزرگی را به‌عنوان «جنگ سایبری» طبقه‌بندی کنند، بسیاری از بیمه‌نامه‌های سایبری عملاً بی‌ارزش خواهند شد *(Farell & Newman, 2019, p. 38)*.

بیمه‌نامه شرکت شامل پوشش خسارات ناشی از حملات سایبری، از جمله بدافزارها و حملات باج‌افزاری بود؛ اما شرکت بیمه زوریخ از پرداخت خسارت خودداری کرد و استدلال کرد که حمله نوت پدیا یک اقدام جنگی[1] توسط یک دولت علیه دولت دیگر (روسیه علیه اوکراین) بوده است و تحت استثنای «جنگ و خصومت‌های نظامی» در بیمه‌نامه قرار می‌گیرد.

این پرونده برای چندین سال در دادگاه‌های ایالات متحده جریان داشت و یکی از اولین پرونده‌هایی بود که به‌طور جدی به موضوع «استثنای جنگ در بیمه سایبری» پرداخت. سرانجام در سال ۲۰۲۲، این دو شرکت به توافق خارج از دادگاه رسیدند و شرکت زوریخ موافقت کرد که بخشی از خسارت موندلز را جبران کند. جزئیات توافق محرمانه باقی ماند؛

1. Act of War

اما این پرونده به یک نقطه عطف در صنعت بیمه سایبری تبدیل شد.

این پرونده نشان داد تفسیر استثنائات بیمه‌ای در حملات سایبری می‌تواند بسیار پیچیده باشد و شرکت‌های بیمه و بیمه‌گذاران باید تعاریف روشن‌تری در قراردادهای خود داشته باشند. نیاز به اصلاح و استانداردسازی بیمه‌نامه‌های سایبری برای جلوگیری از اختلافات حقوقی در آینده وجود دارد و دولت‌ها و نهادهای بین‌المللی باید تعریف مشخصی از «جنگ سایبری» ارائه دهند تا از سردرگمی در پرونده‌های مشابه جلوگیری شود. این پرونده همچنین به سایر صنایع، از جمله صنعت انرژی و نفت و گاز، هشدار داد که باید در انتخاب بیمه سایبری دقت بیشتری داشته باشند و مفاد قراردادهای بیمه‌ای خود را با دقت بررسی کنند تا در برابر حملات سایبری محافظت شوند *(Kesan & Hayes, 2021,p. 68)*.

نتیجه‌گیری

از محدودیت‌های این پژوهش عدم وجود داده‌های کافی وکمبود اطلاعات دقیق و جامع درباره بیمه‌های سایبری است؛ زیرا بسیاری از شرکت‌های بیمه اطلاعات مربوط به خسارات سایبری را منتشر نمی کنند. همچنین چالش‌های حقوقی به دلیل تفاوت درقوانین ومقررات بیمه‌های سایبری کشورها مقایسه دقیق بین نظام‌های حقوقی را با مشکل مواجه می‌کند. بیمه سایبری در قراردادهای بین‌المللی با چالش‌های متعددی مواجه است که می‌توان آن‌ها را از منظر ماهوی و شکلی تفکیک کرد. بررسی دقیق این چالش‌ها نشان می‌دهد که عدم هماهنگی میان نظام‌های حقوقی مختلف و پیچیدگی‌های خاص فضای سایبری، موجب اختلافات گسترده بین بیمه‌گر و بیمه‌گذار شده است. از دیدگاه ماهوی یکی از مهم‌ترین مسائل در بیمه سایبری، عدم وجود یک تعریف جامع و واحد از خطرهای تحت پوشش بیمه‌ای است. فقدان استانداردهای یکپارچه موجب شده است که هر شرکت بیمه، معیارهای متفاوتی را در ارزیابی و جبران خسارت‌های سایبری اعمال کند. همچنین، سببیت در بیمه سایبری به‌دلیل دشواری در شناسایی مهاجمان و تعیین مسئولیت حقوقی آن ها، یکی از چالش‌های اساسی محسوب می‌شود. علاوه‌براین، تفاوت‌های میان قوانین حفاظت از داده‌ها در کشورها بر تعیین میزان تعهدات بیمه‌گران تأثیرگذار بوده و موجب

پیچیدگی دعاوی بیمه‌ای شده است. از منظر شکلی، اجرای قراردادهای بیمه سایبری در سطح بین‌المللی با مشکلات حقوقی متعددی همراه است. مسئله تعیین صلاحیت قضایی در دعاوی مرتبط با بیمه‌های سایبری به‌دلیل ماهیت فرامرزی این خسارت‌ها و تفاوت‌های موجود در نظام‌های قضایی کشورها، موجب دشواری در حل‌وفصل اختلاف شده است. همچنین، تفسیر استثنائات بیمه‌ای و میزان تعهدات بیمه‌گر، از جمله مباحث مورد اختلاف در دعاوی بیمه سایبری است که در برخی پرونده‌ها به تفاسیر متفاوت در محاکم قضایی منجر شده است. درنهایت، برای کاهش این چالش‌ها، تدوین مقررات بین‌المللی هماهنگ و شفاف‌سازی مفاهیم و تعهدات بیمه‌ای ضروری به نظر می‌رشد. اصلاح قوانین مرتبط با بیمه سایبری و توسعه استانداردهای مشترک نه‌تنها موجب افزایش شفافیت قراردادهای بیمه‌ای می‌شود بلکه اعتماد بیمه‌گذاران را نیز تقویت خواهد کرد.

منابع

ادیبی، مهدی؛ دریایی، علی و زهدی، امیر (۱۳۹٦). مروری برمخاطرات اینترنتی و نقش بیمه سایبری در مدیریت آنها، *دومین کنفرانس بین‌المللی مدیریت و حسابداری*.

السان، م.؛ مصطفی کلانتری، رضا و سجادی، هادی (۱۳۹۷). *بیمه مسئولیت و خسارت‌های وارده در فضای مجازی*. پژوهشکده بیمه، نسخه ۱۲۵،

باغبان، اسماعیل؛ پورقهرمانی، بابک و احدی، فاطمه (۱٤۰۲). چالش تعارض صلاحیت کیفری در جرایم سایبری و راهکار آن در رویه قضایی ایالات متحده آمریکا، *مطالعات حقوقی فضای مجازی*، سال سوم، شماره سوم.

پژوهشکده بیمه (۱٤۰۲). طرح پژوهشی شماره ۱۷٤ *مطالعه و بررسی مقدماتی تجربیات سایر کشورها در حوزه ریسک‌ها و بیمه‌های سایبری*.

صبح‌خیز، رضا (۱۳۹٤). چالش‌های حقوقی جرایم سایبری در نظام حقوق بین‌الملل و نظام حقوقی ایران، *پژوهش‌های اطلاعاتی و جنایی*، دوره دهم، شماره سوم.

رومانوسکی، ساشا؛ لیلیان آیلون، اندریاس و کوئن، تیریزجونزف (۱٤۰۱). *تحلیل محتوایی بیمه‌نامه‌ها*؛ یاسمین احمدیان، *انجمن حرفه‌ای صنعت بیمه*، بازیابی شده در ۱٤۰۱/۱۲/۱۵

تارنمای انجمن حرفه‌ای صنعت بیمه.

طالب احمدی، حبیب و رحمانی، عبدالله (۱۳۹۶). بیمه مضاعف، *مطالعات حقوقی دانشگاه شیراز*، دوره نهم، شماره چهارم.

فرج‌زاده، حبیبه (۱۴۰۱). امنیت سایبری؛ ظرفیت‌های حقوق بین‌الملل، *تالار گفتگوی انجمن ایرانی مطالعات سازمان ملل متحد*.

کاویانی، کوروش (۱۳۸۸). مبانی و آثار منع همپوشانی تعهدات بیمه‌های اجتماعی، *پژوهش‌های حقوق عمومی*، سال یازدهم، شماره ۲۶.

میرزایی ورزنه، محمدرضا (۱۳۹۵). امنیت فضای سایبری و چالش‌های پیش‌رو. *کنفرانس ملی پدافند غیرعامل در قلمرو فضای سایبری*.

Brown, K. (2020). Cyber insurance coverage disputes: A legal analysis *journal of law and technology*. Vol 12, N.1.45-67.

Carver, R. (2020). Negotiation strategies in cyber insurance claims. *Cambridge law Journal*. Vol 55, N.3. 345-367.

European insurance and occupational pensions authority (2020). (EIOPA) *Eiopa strategy on cyber underwriting*.

Gareht, Peters, Pavel V, (2018), *Understanding syber risk and syber insurance*, Macquarie university, faculty of business and economics research paper.

Geltman, s. s, & Craig s. (2021) *The insurance disputes law review: united states chapter*. simpson thacher & Bartlett llp.

Generis one oneline. (2024). *The case of xyz v .ABC: implications for contract law in the UAE*.

Harrington, S. E. (2020). Legal issues in delayed insurance claim payments: policy holder protections and insurer obligations. *Journal of insurance law and regulation*. Vol.38, N.2. 215-240.

Howard, J. & Longstaff, T. (1998). *A common language for computer security incidents* (SAND98-8667, 751004; pp. SAND98-8667, 751004).

Jelmini jelmii & james Finucane (2021). Swiss Re institute. managing Insurance overlaps in global contracts.

Jones (2022). Interpretation of insurance policy exclusion: judicial approaches and case studies, *international law review*, Vol.19, N.1.34-56.

Kesan, J. P & .Hayes, C. (2021) .Cybersecurity *insurance and the interpretation of war exclusions in the digital age*. *Journal of Law and Cyber Warfare*, Vol 9, N.2. 45-68.

Kuner, C. (2020). *Transborder data flows and data privacy law*. Oxford University Press.

Marsh (2020). *silent cyber: managing cyber coverage within a changing insurance market*.

Eneken Tikk, Kardi kaska, (2017). International Cyber Incidents Legal Consideration, ccdcoe

Schultz, T. & Ridi, N. (2020). Mapping and navigating the landscape of international

commercial courts .*International Journal of Procedural Law*, Vol.10, N.1.
Rid, T. & .Buchanan, B. (2015). Attributing cyberattacks. Journal of Strategic Studies, Vol38, N.1.
Silicon Valley and mediation center 2020