

Legal Assessment of Cyber Insurance in Iran with Emphasis on Challenges and Problems

1. Mohammad Bahrami: Department of Private Law, Ra.C., Islamic Azad University, Rasht, Iran
2. Mohammadreza Dadashi Niaki*: Department of Private Law, Ra.C., Islamic Azad University, Rasht, Iran.
Email: dadashi@iau.ac.ir (Corresponding Author)
3. Mahdi Haghighatjoo: Department of Private Law, Ra.C., Islamic Azad University, Rasht, Iran

ABSTRACT

The rapid expansion of information technology and the development of economic activities in cyberspace have given rise to new forms of risks and losses for which traditional compensation mechanisms alone are inadequate. Cyber insurance, as a modern instrument for risk management and risk transfer, can play an effective role in compensating losses arising from cyberattacks, data breaches, disruptions to information systems, and in enhancing economic security and public trust. The present study aims to assess the capacity and effectiveness of Iran's legal system in relation to insurance coverage for losses arising from cyberspace and to identify the principal challenges and obstacles to its development. The study employs a descriptive-analytical method based on library research and a comparative approach. The findings indicate that, although the general rules governing insurance contracts, including the principles of good faith, insurable interest, indemnity, and subrogation, possess the necessary theoretical capacity to accommodate and regulate cyber insurance, the absence of comprehensive and specialized regulations, ambiguity concerning the legal nature of data and digital assets, difficulties in assessing and proving non-pecuniary losses, the lack of clearly defined limits of liability for persons and entities operating in cyberspace, and the absence of specialized risk-assessment standards constitute some of the most significant barriers to the development of this field in Iran. Furthermore, international sanctions have adversely affected the capacity to transfer and manage cyber risks by restricting access to reinsurance markets, global data resources, and the updating of technological infrastructure. Accordingly, the effectiveness of Iran's legal system in the field of cyber insurance may be characterized as "conditional and transitional." The enactment of comprehensive and specialized regulations, the establishment of technical standards for risk and loss assessment, the strengthening of supervision by the Central Insurance of Iran, the expansion of cooperation among legal, insurance, and technology institutions, and the development of specialized informational and expert infrastructures are among the principal requirements for establishing an efficient cyber insurance market in Iran.

Keywords: *cyber insurance, cyberspace, cyber losses, insurance contract, cyber risk, economic security.*

How to cite: Bahrami, M., Dadashi Niaki, M., & Haghighatjoo, M. (2027). Legal Assessment of Cyber Insurance in Iran with Emphasis on Challenges and Problems. *Comparative Studies in Jurisprudence, Law, and Politics*, 9(6), 1-21.

© 2027 the authors. This is an open access article under the terms of the Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

Submit Date: 10 May 2026
Revise Date: 11 September 2026
Accept Date: 18 September 2026
Initial Publish Date: 02 October 2026
Final Publish Date: 20 February 2028



پژوهش‌ها و تطبیق فقه،

حقوق و سیاست

ارزیابی حقوقی بیمه فضای مجازی در ایران با تأکید بر چالش‌ها و مشکلات

۱. محمد بهرامی: گروه حقوق خصوصی، واحد رشت، دانشگاه آزاد اسلامی، رشت، ایران

۲. محمد رضا داداشی نیاکی*: گروه حقوق خصوصی، واحد رشت، دانشگاه آزاد اسلامی، رشت، ایران.

پست الکترونیک: dadashi@iau.ac.ir (نویسنده مسئول)

۳. مهدی حقیقت جو: گروه حقوق خصوصی، واحد رشت، دانشگاه آزاد اسلامی، رشت، ایران

چکیده

گسترش روزافزون فناوری اطلاعات و توسعه فعالیت‌های اقتصادی در فضای مجازی، زمینه ظهور مخاطرات و خسارات نوینی را فراهم ساخته است که سازوکارهای سنتی جبران خسارت به‌تنهایی پاسخگوی آن‌ها نیستند. بیمه سایبری به عنوان یکی از ابزارهای نوین مدیریت و انتقال ریسک، می‌تواند در جبران خسارات ناشی از حملات سایبری، نقض داده‌ها، اختلال در سامانه‌های اطلاعاتی و تقویت امنیت اقتصادی و اعتماد عمومی نقش مؤثری ایفا کند. پژوهش حاضر با هدف ارزیابی ظرفیت و کارآمدی نظام حقوقی ایران در زمینه بیمه خسارت‌های ناشی از فضای مجازی و شناسایی مهم‌ترین چالش‌ها و موانع توسعه آن انجام شده است. روش پژوهش توصیفی - تحلیلی و با بهره‌گیری از مطالعات کتابخانه‌ای و رویکرد تطبیقی انجام گرفته است. یافته‌های پژوهش نشان می‌دهد که اگرچه قواعد عمومی قرارداد بیمه، از جمله اصول حسن نیت، نفع بیمه‌پذیر، غرامت و قائم مقامی، ظرفیت نظری لازم برای پذیرش و تنظیم بیمه‌های سایبری را دارا هستند، اما فقدان مقررات جامع و تخصصی، ابهام در ماهیت حقوقی داده‌ها و دارایی‌های دیجیتال، دشواری ارزیابی و اثبات خسارات غیرمادی، عدم تعیین روشن حدود مسئولیت اشخاص فعال در فضای مجازی و نبود استانداردهای تخصصی ارزیابی ریسک، از مهم‌ترین موانع توسعه این حوزه در ایران محسوب می‌شوند. افزون بر این، تحریم‌های بین‌المللی با ایجاد محدودیت در بازار اتکایی، دسترسی به داده‌های جهانی و به‌روزرسانی زیرساخت‌های فناورانه، بر ظرفیت انتقال و مدیریت ریسک‌های سایبری تأثیر منفی گذاشته‌اند. بر این اساس، کارآمدی نظام حقوقی ایران در حوزه بیمه سایبری را می‌توان «مشروط و در حال گذار» ارزیابی کرد. تدوین مقررات تخصصی و جامع، تعیین استانداردهای فنی ارزیابی ریسک و خسارت، تقویت نظارت بیمه مرکزی، توسعه همکاری میان نهادهای حقوقی، بیمه‌ای و فناوری و ایجاد زیرساخت‌های اطلاعاتی و کارشناسی تخصصی، از مهم‌ترین الزامات شکل‌گیری بازار کارآمد بیمه سایبری در ایران است.

واژگان کلیدی: بیمه سایبری، فضای مجازی، خسارات سایبری، قرارداد بیمه، ریسک سایبری، امنیت اقتصادی.

نحوه استناددهی: بهرامی، محمد، داداشی نیاکی، محمد رضا، و حقیقت جو، مهدی. (۱۴۰۶). ارزیابی حقوقی بیمه فضای مجازی در ایران با تأکید بر چالش‌ها و مشکلات. پژوهش‌های تطبیقی فقه، حقوق و سیاست، ۹(۶)، ۲۱-۱.

© ۱۴۰۶ تمامی حقوق انتشار این مقاله متعلق به نویسنده است. انتشار این مقاله به‌صورت دسترسی آزاد مطابق با گواهی (CC BY-NC 4.0) صورت گرفته است.

تاریخ ارسال: ۲۰ اردیبهشت ۱۴۰۵

تاریخ بازنگری: ۲۰ شهریور ۱۴۰۵

تاریخ پذیرش: ۲۷ شهریور ۱۴۰۵

تاریخ چاپ اولیه: ۱۰ مهر ۱۴۰۵

تاریخ چاپ نهایی: ۱ اسفند ۱۴۰۶



گسترش شتابان فناوری اطلاعات و توسعه روزافزون فعالیت‌های اقتصادی، تجاری و اجتماعی در فضای مجازی، تحولات بنیادینی را در شیوه تعامل اشخاص و انجام فعالیت‌های اقتصادی ایجاد کرده است. در کنار مزایای گسترده این تحولات، وابستگی فزاینده اشخاص و بنگاه‌های اقتصادی به سامانه‌های اطلاعاتی و خدمات دیجیتال، زمینه بروز مخاطرات و خسارت‌های جدیدی همچون حملات سایبری، نفوذ غیرمجاز، از بین رفتن یا افشای داده‌ها، اختلال در سامانه‌های اطلاعاتی و توقف فعالیت‌های اقتصادی را فراهم ساخته است. ویژگی‌های خاص این مخاطرات، از جمله ماهیت ناملموس، پیچیدگی فنی، فرامرزی بودن و دشواری تعیین میزان خسارت، موجب شده است سازوکارهای سنتی جبران خسارت به‌تنهایی پاسخگوی تمامی آثار ناشی از حوادث سایبری نباشند. (Pourkavian & Bozorgi, 2025)

در چنین شرایطی، بیمه سایبری به‌عنوان یکی از ابزارهای نوین مدیریت و انتقال ریسک، اهمیت ویژه‌ای یافته است. این نوع بیمه می‌تواند با پوشش بخشی از خسارت‌های ناشی از حوادث سایبری، آثار مالی این حوادث را برای اشخاص و بنگاه‌های اقتصادی کاهش داده و در افزایش تاب‌آوری اقتصادی و اعتماد عمومی به فعالیت‌های دیجیتال مؤثر باشد. افزون بر کارکرد جبرانی، بیمه سایبری می‌تواند از طریق الزام بیمه‌گذاران به رعایت استانداردهای امنیتی و اتخاذ تدابیر پیشگیرانه، در ارتقای سطح امنیت اطلاعات و کاهش احتمال وقوع خسارت نیز نقش داشته باشد. با وجود اهمیت روزافزون بیمه سایبری، توسعه این حوزه در نظام حقوقی ایران با چالش‌های متعدد حقوقی، فنی و نهادی مواجه است. اگرچه قواعد عمومی قرارداد بیمه، از جمله اصل حسن نیت، نفع بیمه‌پذیر، اصل غرامت و قائم‌مقامی، از ظرفیت نظری لازم برای پذیرش مخاطرات سایبری برخوردارند، اما فقدان مقررات تخصصی و جامع، ابهام در ماهیت حقوقی داده‌ها و دارایی‌های دیجیتال، دشواری ارزیابی و اثبات خسارت‌های غیرمادی، پیچیدگی تعیین رابطه سببیت و مسئولیت اشخاص فعال در زنجیره خدمات دیجیتال، از مهم‌ترین موانع شکل‌گیری یک نظام منسجم بیمه سایبری در ایران به شمار می‌روند. از سوی دیگر، ماهیت فراملی بسیاری از مخاطرات سایبری و وابستگی صنعت بیمه به داده‌های تخصصی، فناوری‌های نوین و بازارهای بیمه اتکایی، موجب شده است محدودیت‌های بین‌المللی و تحریم‌ها نیز بر ظرفیت توسعه این حوزه در ایران اثرگذار باشد. محدودیت دسترسی به بازارهای اتکایی، داده‌های آماری و اطلاعات تخصصی بین‌المللی و همچنین دشواری به‌روزرسانی برخی زیرساخت‌های فناورانه، می‌تواند فرآیند ارزیابی و نرخ‌گذاری ریسک‌های سایبری را با چالش مواجه سازد.

بر این اساس، مسئله اساسی پژوهش حاضر آن است که نظام حقوقی ایران تا چه اندازه ظرفیت لازم برای شناسایی، تنظیم و پوشش بیمه‌ای خسارت‌های ناشی از فضای مجازی را داراست و مهم‌ترین موانع حقوقی، فنی و نهادی توسعه بیمه سایبری در ایران کدام‌اند. در این راستا، ضمن بررسی جایگاه بیمه سایبری در چارچوب قواعد عمومی قرارداد بیمه، نقش نهادهای ناظر، به‌ویژه بیمه مرکزی، در تنظیم و توسعه این حوزه مورد توجه قرار می‌گیرد و چالش‌های مربوط به شناسایی خطر، تعیین مسئولیت، ارزیابی و اثبات خسارت و نیز خلأهای تقنینی بررسی می‌شود. همچنین، آثار محدودیت‌های بین‌المللی بر انتقال و مدیریت ریسک‌های سایبری مورد تحلیل قرار خواهد گرفت. هدف اصلی این پژوهش، ارزیابی ظرفیت و کارآمدی نظام حقوقی ایران در مواجهه با مخاطرات سایبری از طریق سازوکار بیمه و شناسایی مهم‌ترین چالش‌ها و الزامات توسعه بیمه سایبری است. بر این اساس، پژوهش حاضر با رویکرد توصیفی - تحلیلی و با بهره‌گیری از مطالعات کتابخانه‌ای و رویکرد تطبیقی، تلاش می‌کند ضمن تبیین وضعیت موجود، راهکارهایی برای ایجاد چارچوبی شفاف، تخصصی و کارآمد در زمینه بیمه خسارت‌های ناشی از فضای مجازی در ایران ارائه دهد.

نقش بیمه سایبری در تضمین امنیت اقتصادی در فضای مجازی

در عصر حاضر، امنیت اقتصادی در فضای مجازی به یکی از مهم‌ترین دغدغه‌های نظام‌های حقوقی تبدیل شده است. گسترش تجارت الکترونیکی، بانکداری دیجیتال و فعالیت‌های اقتصادی مبتنی بر داده موجب شده است که هرگونه اختلال در زیرساخت‌های سایبری، آثار مستقیم و قابل توجهی بر ثبات اقتصادی داشته باشد. در چنین شرایطی، بیمه سایبری می‌تواند به‌عنوان یکی از ابزارهای مهم مدیریت ریسک، نقش مؤثری در تضمین امنیت اقتصادی ایفا کند. (Elsan, 2023)

بیمه سایبری با جبران خسارات ناشی از حملات سایبری، نقض داده‌ها و سایر مخاطرات مرتبط با فناوری اطلاعات، موجب کاهش آثار مالی این حوادث بر اشخاص و بنگاه‌های اقتصادی می‌شود. در واقع، این نوع بیمه با توزیع ریسک میان بیمه‌گذاران و شرکت‌های بیمه، امکان مدیریت بهتر خسارات و جلوگیری از ورشکستگی یا تضعیف شدید بنگاه‌های اقتصادی را فراهم می‌آورد. چنین کارکردی می‌تواند به حفظ ثبات اقتصادی و افزایش اعتماد فعالان اقتصادی در فضای مجازی کمک کند.

یکی از مهم‌ترین آثار اقتصادی توسعه بیمه‌های سایبری، افزایش اعتماد عمومی به فعالیت‌های دیجیتال است. هنگامی که اشخاص حقیقی و حقوقی بدانند در صورت وقوع حوادث سایبری امکان جبران خسارت وجود دارد، با اطمینان بیشتری از خدمات الکترونیکی استفاده خواهند کرد. این امر به توسعه تجارت الکترونیکی و گسترش اقتصاد دیجیتال منجر می‌شود و زمینه رشد اقتصادی را فراهم می‌سازد.

از سوی دیگر، بیمه سایبری می‌تواند شرکت‌ها و سازمان‌ها را به ارتقای سطح امنیت اطلاعات خود ترغیب کند. شرکت‌های بیمه معمولاً برای ارائه پوشش بیمه‌ای، رعایت حداقل استانداردهای امنیتی را از بیمه‌گذاران مطالبه می‌کنند. این امر موجب می‌شود سازمان‌ها برای کاهش حق بیمه و بهره‌مندی از پوشش‌های مناسب، سرمایه‌گذاری بیشتری در حوزه امنیت سایبری انجام دهند. در نتیجه، سطح کلی امنیت در فضای مجازی ارتقا می‌یابد و احتمال وقوع خسارات گسترده کاهش پیدا می‌کند.

نقش بیمه سایبری در حمایت از مصرف‌کنندگان نیز قابل توجه است. در صورت افشای اطلاعات شخصی یا مالی کاربران، بیمه مسئولیت سایبری می‌تواند هزینه‌های جبران خسارت و نیز هزینه‌های اطلاع‌رسانی و حمایت از زیان‌دیدگان را پوشش دهد. این امر موجب افزایش حمایت از حقوق مصرف‌کنندگان و تقویت اعتماد آنان به خدمات دیجیتال می‌شود.

در نظام حقوقی ایران، با توجه به رشد سریع خدمات الکترونیکی و افزایش وابستگی فعالیت‌های اقتصادی به فناوری اطلاعات، توجه به نقش بیمه سایبری در تضمین امنیت اقتصادی از اهمیت ویژه‌ای برخوردار است. توسعه این نوع بیمه می‌تواند به کاهش آثار مالی جرایم سایبری، حمایت از کسب‌وکارهای نوپا و افزایش تاب‌آوری اقتصادی در برابر مخاطرات نوین کمک کند.

بر این اساس، به نظر می‌رسد که سیاست‌گذاران و قانون‌گذاران باید با نگاهی راهبردی به توسعه بیمه‌های سایبری، زمینه استفاده گسترده از این ابزار را فراهم سازند. حمایت تقنینی، ارائه مشوق‌های اقتصادی و تدوین مقررات شفاف می‌تواند به گسترش این نوع بیمه و در نتیجه تقویت امنیت اقتصادی در فضای مجازی منجر شود.

نقش نهادهای ناظر و ساختار حاکمیتی در توسعه بیمه‌های سایبری

نقش بیمه مرکزی به‌عنوان نهاد ناظر و تفکیک از شورای عالی بیمه

در تحلیل ساختار حاکم بر صنعت بیمه ایران، برای درک صحیح فرآیند نظارت بر بیمه‌های سایبری، ابتدا باید میان دو نهاد اصلی تفکیک قائل شد:

الف) شورای عالی بیمه (نهاد سیاست‌گذار): این شورا وظیفه تعیین جهت‌گیری‌های کلان و تصویب سیاست‌های کلی صنعت را بر عهده دارد. در حوزه بیمه‌های سایبری، وظیفه این شورا می‌تواند شامل تصویب برنامه‌های توسعه‌ای برای ورود شرکت‌های بیمه به بازار دیجیتال و تعیین اولویت‌های ملی در پوشش ریسک‌های تکنولوژیک باشد.

ب) بیمه مرکزی ایران (نهاد ناظر و اجرایی): برخلاف شورای عالی، بیمه مرکزی به‌عنوان «نهاد ناظر» (Regulator) دارای وظایف عملیاتی و تخصصی است که مستقیماً بر توسعه بیمه سایبری اثر می‌گذارد. نقش‌های کلیدی این نهاد شامل موارد زیر است:

۱. تدوین مقررات و استانداردهای فنی: بیمه مرکزی مسئولیت دارد دستورالعمل‌های مشخصی برای «نحوه ارزیابی ریسک سایبری» و «استانداردهای ممیزی امنیت اطلاعات» تدوین کند تا شرکت‌های بیمه نتوانند بدون دانش فنی کافی، وارد این بازار شوند.

۲. نظارت بر توانگری مالی و مدیریت ریسک: با توجه به ماهیت «ریسک سیستماتیک» در حملات سایبری (که ممکن است هم‌زمان هزاران شرکت را آسیب بزند)، بیمه مرکزی موظف است از نظر میزان ذخایر قانونی و توانگری مالی شرکت‌ها برای پوشش این نوع خسارات خاص، نظارت سخت‌گیرانه‌ای اعمال کند. (Katouzian, 2018)

۳. نظارت بر محصولات و قراردادهای: این نهاد مسئول تأیید طرح‌های بیمه‌ای و جلوگیری از استفاده شرکت‌ها از «استثنائات غیرمنطقی» در قراردادهای سایبری است تا از حقوق بیمه‌گیرنده حمایت شود.

چالش‌های نظارتی و ضرورت همکاری بین‌سازمانی

در حال حاضر، بزرگ‌ترین چالش در توسعه بیمه سایبری، عدم وجود «مقررات جامع و تخصصی» از سوی بیمه مرکزی است. فعالیت شرکت‌های بیمه در این حوزه، عمدتاً بر پایه «ابتکار عمل فردی» و بدون چارچوب‌های استاندارد ارزیابی ریسک استوار است که این امر موجب عدم یکپارچگی در بازار و افزایش ریسک ناشی از عدم تقارن اطلاعاتی می‌گردد.

علاوه بر این، از آنجا که مخاطرات سایبری فراتر از مرزهای صنعت بیمه است، توسعه این بازار مستلزم گذار از «نظارت تک‌بعدی» به سمت «نظارت چندجانبه» است. همکاری میان بیمه مرکزی، مرکز ملی امنیت زیرساخت‌های حیاتی و نهادهای امنیت سایبری برای تبادل داده‌های تهدید (Threat Intelligence) و ایجاد بانک‌های اطلاعاتی خسارت، ضرورتی اجتناب‌ناپذیر است تا بتوان از مدل‌های نرخ‌گذاری سنتی عبور و به سمت مدل‌های دقیق مبتنی بر داده حرکت کرد.

توسعه بیمه خسارت‌های ناشی از فضای مجازی در هر نظام حقوقی، علاوه بر وجود مقررات قانونی مناسب، مستلزم فراهم بودن زیرساخت‌های نهادی و نظارتی در صنعت بیمه است. در ایران، صنعت بیمه تحت نظارت نهاد ناظر تخصصی قرار دارد که وظیفه تنظیم بازار، صدور مجوز فعالیت شرکت‌های بیمه، تدوین آیین‌نامه‌ها و نظارت بر عملکرد آن‌ها را بر عهده دارد. نقش این نهاد در توسعه بیمه‌های نوین، از جمله بیمه‌های سایبری، بسیار تعیین‌کننده است.

یکی از مهم‌ترین وظایف نهاد ناظر در حوزه بیمه، تدوین مقررات و آیین‌نامه‌های لازم برای فعالیت شرکت‌های بیمه در رشته‌های مختلف بیمه‌ای است. در خصوص بیمه‌های سایبری، تدوین دستورالعمل‌های تخصصی می‌تواند چارچوب مشخصی برای ارزیابی ریسک، تعیین شرایط بیمه‌نامه، نحوه محاسبه حق بیمه و حدود تعهدات بیمه‌گر فراهم سازد. در حال حاضر، فقدان مقررات صریح در این زمینه موجب شده است که شرکت‌های بیمه با احتیاط وارد حوزه بیمه‌های سایبری شوند و محصولات محدودی در این زمینه ارائه گردد.

از سوی دیگر، توسعه بیمه‌های سایبری نیازمند ارتقای دانش فنی و تخصصی در صنعت بیمه است. ارزیابی ریسک‌های سایبری با ریسک‌های سنتی تفاوت اساسی دارد و مستلزم شناخت دقیق تهدیدات فضای مجازی، روش‌های حملات سایبری و پیامدهای اقتصادی آن‌هاست. شرکت‌های بیمه برای ارائه پوشش‌های مناسب باید از کارشناسان متخصص در حوزه فناوری اطلاعات، امنیت سایبری و حقوق فناوری بهره‌مند شوند. نهاد ناظر می‌تواند با برگزاری دوره‌های آموزشی تخصصی و حمایت از توسعه دانش فنی در صنعت بیمه، زمینه ارتقای توانمندی شرکت‌ها را فراهم سازد.

همچنین ایجاد بانک‌های اطلاعاتی جامع درباره حوادث سایبری و خسارات ناشی از آن‌ها از جمله اقداماتی است که می‌تواند به توسعه بیمه‌های سایبری کمک کند. دسترسی به داده‌های آماری دقیق درباره میزان وقوع حملات سایبری، نوع خسارات و هزینه‌های جبران آن‌ها، امکان ارزیابی دقیق‌تر ریسک و تعیین حق بیمه متناسب را فراهم می‌سازد. در بسیاری از کشورها، نهادهای ناظر با همکاری شرکت‌های بیمه و نهادهای دولتی، سامانه‌های ثبت و تحلیل حوادث سایبری را ایجاد کرده‌اند که نقش مهمی در توسعه بازار بیمه‌های سایبری ایفا می‌کند.

از منظر نظارتی، حمایت از نوآوری در صنعت بیمه نیز اهمیت ویژه‌ای دارد. بیمه‌های سایبری به‌عنوان یکی از محصولات نوین بیمه‌ای نیازمند رویکردی منعطف و حمایتی از سوی نهاد ناظر هستند. تسهیل فرایند صدور مجوز برای ارائه محصولات جدید، تشویق شرکت‌های بیمه به طراحی پوشش‌های نوآورانه و ایجاد فضای رقابتی سالم می‌تواند به گسترش این نوع بیمه کمک کند. در مقابل، اعمال محدودیت‌های بیش از حد یا عدم شفافیت مقررات ممکن است انگیزه شرکت‌های بیمه برای ورود به این حوزه را کاهش دهد. (Abdi & Kalantari, 2024)

افزون بر این، همکاری میان نهادهای مختلف دولتی و خصوصی در حوزه امنیت سایبری و بیمه اهمیت زیادی دارد. وزارتخانه‌ها، سازمان‌های مسئول در حوزه فناوری اطلاعات، نهادهای امنیتی و شرکت‌های بیمه می‌توانند با تبادل اطلاعات و تجربیات، چارچوب جامع‌تری برای مدیریت ریسک‌های سایبری ایجاد کنند. چنین همکاری‌هایی می‌تواند به تدوین سیاست‌های کلان در زمینه بیمه‌های سایبری و حمایت از کاربران فضای مجازی منجر شود.

در مجموع، می‌توان گفت که نقش نهاد ناظر و ساختار صنعت بیمه در توسعه بیمه خسارت‌های ناشی از فضای مجازی بسیار اساسی است. بدون وجود چارچوب‌های نظارتی شفاف، دانش فنی کافی و حمایت از نوآوری، گسترش بیمه‌های سایبری با کندی مواجه خواهد شد. ازاین‌رو، اتخاذ رویکردی فعال و آینده‌نگر در سیاست‌گذاری بیمه‌ای می‌تواند زمینه‌ساز شکل‌گیری بازار کارآمد بیمه‌های سایبری در ایران باشد.

نسبت بیمه سایبری با اصول حاکم بر قراردادهای بیمه

بیمه سایبری، اگرچه پدیده‌ای نوظهور در نظام‌های حقوقی محسوب می‌شود، اما از حیث ساختار قراردادی تابع اصول کلی حاکم بر قراردادهای بیمه است. بررسی نسبت این نوع بیمه با اصول سنتی بیمه می‌تواند به درک دقیق‌تر جایگاه آن در نظام حقوقی ایران کمک کند.

نخستین اصل بنیادین در قراردادهای بیمه، اصل حسن نیت است. در بیمه سایبری، این اصل اهمیت دوچندان دارد؛ زیرا ارزیابی ریسک سایبری به میزان زیادی وابسته به اطلاعاتی است که بیمه‌گذار در اختیار بیمه‌گر قرار می‌دهد. اگر بیمه‌گذار اطلاعات ناقص یا نادرستی درباره وضعیت امنیتی سامانه‌های خود ارائه دهد، تعادل قراردادی برهم می‌خورد و محاسبه حق بیمه بر مبنای واقعی انجام نمی‌شود. ازاین‌رو، رعایت کامل اصل حسن نیت در این نوع بیمه از اهمیت اساسی برخوردار است.

اصل دوم، اصل نفع بیمه‌پذیر است. در بیمه سایبری، بیمه‌گذار باید دارای نفع مشروع در حفظ داده‌ها، سامانه‌های اطلاعاتی یا اعتبار تجاری خود باشد. این نفع ممکن است مالی، قراردادی یا حتی اعتباری باشد. با توجه به اینکه در بسیاری از موارد خسارات سایبری به اعتبار و شهرت تجاری لطمه می‌زند، مفهوم نفع بیمه‌پذیر در این حوزه می‌تواند گسترده‌تر از بیمه‌های سنتی تفسیر شود.

اصل غرامت نیز از اصول مهم بیمه‌های خسارت است. بر اساس این اصل، بیمه نباید موجب انتفاع بیمه‌گذار شود، بلکه صرفاً باید زیان وارده را جبران کند. در بیمه‌های سایبری، تعیین میزان واقعی خسارت ممکن است پیچیده باشد، به‌ویژه در مواردی که خسارات غیرمادی مانند لطمه به اعتبار تجاری مطرح است. بنابراین، رعایت دقیق اصل غرامت مستلزم تدوین معیارهای مشخص برای ارزیابی خسارات سایبری است.

اصل جانشینی یا قائم‌مقامی بیمه‌گر نیز در بیمه سایبری قابل اعمال است. در صورتی که خسارت ناشی از فعل شخص ثالث باشد، بیمه‌گر پس از جبران خسارت می‌تواند به قائم‌مقامی از بیمه‌گذار علیه عامل ورود زیان اقدام کند. با این حال، در فضای سایبری شناسایی عامل اصلی حمله ممکن است با دشواری همراه باشد، که این امر اجرای عملی اصل جانشینی را پیچیده‌تر می‌کند.

از منظر تطبیقی، در نظام حقوقی ایالات متحده آمریکا نیز بیمه سایبری تابع همین اصول بنیادین است، اما به دلیل پیچیدگی‌های فنی، بیمه‌نامه‌های سایبری غالباً دارای شروط تفصیلی‌تری هستند که حدود و ثغور این اصول را روشن‌تر می‌سازد. این تجربه نشان می‌دهد که برای اجرای مؤثر اصول سنتی بیمه در حوزه سایبری، نیاز به تنظیم دقیق‌تر شرایط قراردادی وجود دارد.

در حقوق ایران، اجرای این اصول در حوزه بیمه سایبری مستلزم تفسیر پویا و انطباق‌پذیر از قواعد موجود است. اصول کلی عقد بیمه ظرفیت لازم برای پوشش مخاطرات نوین را دارند، اما بدون تدوین مقررات تکمیلی و دستورالعمل‌های تخصصی، ممکن است در عمل با ابهاماتی مواجه شوند. بنابراین، نسبت بیمه سایبری با اصول حاکم بر قراردادهای بیمه را می‌توان نسبتی تبعی اما نیازمند توسعه تفسیری دانست.

(Nikouei, 2024)

در مجموع، بیمه سایبری در چارچوب اصول سنتی بیمه قابل تحلیل است، اما ویژگی‌های خاص مخاطرات دیجیتال ایجاب می‌کند که این اصول با رویکردی نوین و متناسب با تحولات فناوری تفسیر و اجرا شوند. چنین رویکردی می‌تواند به انسجام بیشتر نظام حقوقی و افزایش کارآمدی بیمه‌های سایبری در ایران کمک کند.

ارزیابی کارآمدی نظام حقوقی ایران در پاسخ به مخاطرات سایبری

در ارزیابی نهایی، پرسش اساسی آن است که آیا نظام حقوقی ایران از ظرفیت کافی برای مواجهه با مخاطرات نوین سایبری در قالب سازوکار بیمه‌ای برخوردار است یا خیر. پاسخ به این پرسش مستلزم تحلیل هم‌زمان سه مؤلفه اساسی است: کفایت قواعد عمومی بیمه، انسجام مقررات مسئولیت مدنی و میزان انطباق نظام تقنینی با تحولات فناوری.

از حیث قواعد عمومی بیمه، می‌توان گفت چارچوب موجود ظرفیت نظری لازم برای پذیرش بیمه سایبری را دارد. مفاهیمی همچون خطر، نفع بیمه‌پذیر، اصل غرامت و قائم‌مقامی قابلیت تفسیر در بستر دیجیتال را دارند. با این حال، این ظرفیت بیشتر جنبه بالقوه دارد و در عمل به دلیل فقدان مقررات تفصیلی و استانداردهای تخصصی، اجرای منسجم آن با دشواری روبه‌روست.

از منظر مسئولیت مدنی، چالش اصلی در تعیین رابطه سببیت و میزان تقصیر در حوادث سایبری بروز می‌کند. ساختار سنتی مسئولیت که عمدتاً بر مبنای تقصیر شخصی بنا شده، در برابر حملات پیچیده و چندلایه سایبری ممکن است پاسخ کامل ارائه نکند. این امر بر کارآمدی بیمه‌های مسئولیت سایبری نیز تأثیر می‌گذارد، زیرا دامنه تعهد بیمه‌گر تابع حدود مسئولیت بیمه‌گذار است.

از حیث انطباق تقنینی با تحولات فناوری، نظام حقوقی ایران هنوز فاقد قانون جامع در زمینه حمایت از داده‌ها و مسئولیت ناشی از نقض امنیت اطلاعات است. این خلأ موجب می‌شود که بیمه سایبری در فضایی از ابهام حقوقی فعالیت کند. در چنین شرایطی، بیمه‌گران ناگزیرند از شروط قراردادی گسترده برای تحدید مسئولیت استفاده کنند که ممکن است تعادل قراردادی را بر هم زند.

با وجود این کاستی‌ها، نمی‌توان نظام حقوقی ایران را فاقد ظرفیت توسعه دانست. قواعد عمومی موجود، در صورت تکمیل با مقررات تخصصی و تدوین دستورالعمل‌های نظارتی، می‌توانند زمینه‌ساز شکل‌گیری بازار منسجم بیمه سایبری شوند. آنچه بیش از هر چیز ضروری به نظر می‌رسد، رویکردی فعال در سیاست‌گذاری تقنینی و پذیرش ماهیت فراملی مخاطرات سایبری است.

در نتیجه، کارآمدی نظام حقوقی ایران در حوزه بیمه سایبری را باید «مشروط و در حال گذار» ارزیابی کرد؛ ظرفیتی که نیازمند تکمیل، شفاف‌سازی و هماهنگی بیشتر میان قانون‌گذار، نهادهای نظارتی و صنعت بیمه است.

ضرورت شناسایی خطرات سایبری به‌عنوان خطر قابل بیمه در حقوق ایران

یکی از مهم‌ترین پیش‌نیازهای توسعه بیمه‌های سایبری در نظام حقوقی ایران، شناسایی رسمی خطرات سایبری به‌عنوان خطرات قابل بیمه است. در حقوق بیمه، اصل قابلیت بیمه‌شدن خطر، مبتنی بر امکان ارزیابی ریسک، احتمال وقوع و قابلیت محاسبه خسارت است. در صورتی که خطری از این ویژگی‌ها برخوردار باشد، می‌توان آن را موضوع قرارداد بیمه قرار داد. با این حال، در خصوص خطرات سایبری، هنوز تردیدهایی در برخی نظام‌های حقوقی در خصوص قابلیت بیمه‌پذیری این خطرات وجود دارد.

در نظام‌های حقوقی پیشرفته، از جمله ایالات متحده آمریکا، خطرات سایبری به‌عنوان خطراتی واقعی و قابل ارزیابی شناسایی شده‌اند. شرکت‌های بیمه با استفاده از داده‌های آماری، تحلیل‌های فنی و ارزیابی‌های امنیتی، امکان سنجش احتمال وقوع حملات سایبری و میزان خسارات ناشی از آن را فراهم کرده‌اند. این امر موجب شده است که بیمه‌نامه‌های متنوعی برای پوشش این خطرات طراحی و عرضه شود.

(Mahmoudi & Miri Balajorshari, 2022)

در مقابل، در حقوق ایران هنوز شناسایی صریح و قانونی خطرات سایبری به‌عنوان خطرات قابل بیمه صورت نگرفته است. هرچند بر اساس اصول کلی حقوق بیمه، منع قانونی برای بیمه کردن این خطرات وجود ندارد، اما نبود مقررات صریح و دستورالعمل‌های تخصصی موجب شده است که شرکت‌های بیمه با احتیاط بیشتری در این حوزه فعالیت کنند. این وضعیت باعث شده است که بازار بیمه‌های سایبری در ایران رشد کندی داشته باشد.

از منظر حقوقی، می‌توان استدلال کرد که خطرات سایبری تمامی ویژگی‌های لازم برای بیمه‌پذیری را دارا هستند. این خطرات دارای احتمال وقوع مشخص، قابلیت ارزیابی نسبی و امکان برآورد خسارت هستند. علاوه بر این، توسعه ابزارهای فنی و نرم‌افزاری موجب شده است که ارزیابی ریسک‌های سایبری با دقت بیشتری انجام شود. بنابراین، از نظر نظری مانعی برای شناسایی این خطرات به‌عنوان موضوع بیمه وجود ندارد.

یکی از اقدامات ضروری در این زمینه، تدوین مقرراتی از سوی نهادهای قانون‌گذار و تنظیم‌گر است که به‌طور صریح خطرات سایبری را در زمره خطرات قابل بیمه قرار دهد. چنین اقدامی می‌تواند موجب رفع ابهامات موجود و افزایش اطمینان شرکت‌های بیمه برای ورود به این حوزه شود. همچنین تعیین معیارهای مشخص برای ارزیابی ریسک سایبری و نحوه محاسبه حق بیمه می‌تواند به توسعه این بازار کمک کند.

از سوی دیگر، شناسایی رسمی خطرات سایبری به عنوان خطرات قابل بیمه می‌تواند به افزایش آگاهی عمومی نسبت به این مخاطرات نیز منجر شود. هنگامی که اشخاص حقیقی و حقوقی بدانند این خطرات به طور رسمی مورد توجه نظام بیمه‌ای قرار گرفته است، اهمیت بیشتری برای مدیریت ریسک‌های سایبری قائل خواهند شد و به استفاده از پوشش‌های بیمه‌ای مرتبط با آن تمایل بیشتری نشان خواهند داد. در نهایت، می‌توان گفت که شناسایی خطرات سایبری به عنوان خطرات قابل بیمه، یکی از مهم‌ترین گام‌ها در مسیر توسعه بیمه‌های سایبری در ایران محسوب می‌شود. تحقق این امر مستلزم همکاری میان قانون‌گذاران، شرکت‌های بیمه و متخصصان فناوری اطلاعات است و می‌تواند زمینه‌ساز شکل‌گیری بازاری پویا و کارآمد در این حوزه باشد.

ضرورت فرهنگ‌سازی و افزایش تقاضا برای بیمه سایبری

یکی دیگر از عوامل مؤثر در توسعه بیمه خسارت‌های فضای مجازی، میزان آگاهی و تقاضای بازار است. بسیاری از سازمان‌ها و کسب‌وکارها در ایران هنوز نسبت به اهمیت مدیریت ریسک‌های سایبری و نقش بیمه در این زمینه آگاهی کافی ندارند. در نتیجه، تقاضا برای بیمه سایبری محدود است و شرکت‌های بیمه نیز انگیزه کمتری برای سرمایه‌گذاری در این حوزه دارند. افزایش حملات سایبری و خسارت‌های ناشی از آن می‌تواند به تدریج توجه سازمان‌ها را به ضرورت استفاده از پوشش‌های بیمه‌ای جلب کند. فرهنگ‌سازی در این زمینه از طریق آموزش، اطلاع‌رسانی و ارائه نمونه‌های موفق بیمه سایبری در سایر کشورها، می‌تواند نقش مهمی در توسعه این بازار ایفا کند.

دکترین حقوقی درباره بیمه سایبری

با گسترش فضای مجازی و افزایش مخاطرات ناشی از فعالیت در این فضا، موضوع بیمه سایبری به تدریج مورد توجه اندیشمندان و صاحب‌نظران حقوقی قرار گرفته است. بسیاری از حقوقدانان بر این باورند که ابزارهای سنتی جبران خسارت، به‌تنهایی پاسخگوی پیچیدگی‌های ناشی از خسارات سایبری نیست و لازم است سازوکارهای نوینی همچون بیمه سایبری در نظام‌های حقوقی مورد توجه قرار گیرد. (Safarinia, 2025)

از دیدگاه برخی صاحب‌نظران، بیمه سایبری را می‌توان ادامه منطقی تحول نهاد بیمه در مواجهه با خطرات نوین دانست. همان‌گونه که در گذشته با ظهور صنایع جدید، بیمه‌های تخصصی در حوزه‌هایی مانند حمل‌ونقل، انرژی و مسئولیت حرفه‌ای شکل گرفت، در عصر دیجیتال نیز بیمه سایبری به عنوان پاسخی به مخاطرات ناشی از فناوری‌های نوین مطرح شده است. این دیدگاه بر نقش تطبیقی و تحول‌پذیر نهاد بیمه تأکید دارد و آن را ابزاری برای انطباق نظام حقوقی با تحولات اجتماعی و اقتصادی می‌داند.

گروهی دیگر از حقوقدانان بر جنبه اقتصادی بیمه سایبری تمرکز کرده‌اند. از منظر آنان، توسعه این نوع بیمه می‌تواند به افزایش اعتماد فعالان اقتصادی در فضای مجازی منجر شود و زمینه رشد اقتصاد دیجیتال را فراهم آورد. هنگامی که اشخاص حقیقی و حقوقی اطمینان داشته باشند که در صورت وقوع حوادث سایبری امکان جبران خسارت وجود دارد، با اطمینان بیشتری به فعالیت‌های مبتنی بر فناوری اطلاعات روی خواهند آورد. این امر می‌تواند به افزایش سرمایه‌گذاری در حوزه فناوری و توسعه کسب‌وکارهای دیجیتال کمک کند.

در مقابل، برخی حقوقدانان به چالش‌های حقوقی و فنی بیمه سایبری اشاره کرده‌اند. از جمله این چالش‌ها می‌توان به دشواری ارزیابی ریسک‌های سایبری، پیچیدگی تعیین میزان خسارت و احتمال سوءاستفاده از پوشش‌های بیمه‌ای اشاره کرد. به اعتقاد این گروه، بدون تدوین

مقررات دقیق و ایجاد زیرساخت‌های فنی مناسب، توسعه بیمه‌های سایبری ممکن است با مشکلاتی همراه باشد. از این رو، آنان بر ضرورت تدوین مقررات شفاف و ایجاد سازوکارهای نظارتی مؤثر تأکید دارند.

برخی دیگر از اندیشمندان حقوقی، بیمه سایبری را نه تنها ابزاری برای جبران خسارت، بلکه وسیله‌ای برای پیشگیری از وقوع خسارات می‌دانند. از این منظر، شرکت‌های بیمه با تعیین استانداردهای امنیتی برای بیمه‌گذاران می‌توانند نقش مهمی در ارتقای سطح امنیت اطلاعات ایفا کنند. الزام بیمه‌گذاران به رعایت تدابیر امنیتی مناسب، موجب کاهش احتمال وقوع حملات سایبری و در نتیجه کاهش خسارات می‌شود. این رویکرد نشان می‌دهد که بیمه می‌تواند در کنار کارکرد جبرانی، نقش پیشگیرانه نیز داشته باشد.

در نظام‌های حقوقی پیشرفته از جمله ایالات متحده آمریکا، دکترین حقوقی نقش مهمی در شکل‌گیری مقررات بیمه سایبری داشته است. مقالات علمی، پژوهش‌های دانشگاهی و تحلیل‌های حقوقی ارائه‌شده از سوی صاحب‌نظران، به تدریج زمینه تدوین مقررات تخصصی و توسعه محصولات بیمه‌ای را فراهم کرده است. این تجربه نشان می‌دهد که تعامل میان دانشگاه و صنعت بیمه می‌تواند به توسعه چارچوب‌های حقوقی کارآمد کمک کند.

در حقوق ایران نیز توجه به دکترین حقوقی در این حوزه از اهمیت بالایی برخوردار است. پژوهش‌های علمی می‌تواند با شناسایی خلأهای قانونی، ارائه راهکارهای تقنینی و تحلیل تجربیات سایر کشورها، نقش مهمی در توسعه بیمه‌های سایبری ایفا کند. تقویت ارتباط میان مراکز علمی، نهادهای قانون‌گذار و صنعت بیمه می‌تواند زمینه‌ساز شکل‌گیری چارچوبی منسجم و کارآمد در این حوزه باشد. (Moghadamfar & Seifkar, 2026)

در مجموع، بررسی دکترین حقوقی نشان می‌دهد که بیمه سایبری به‌عنوان یکی از ابزارهای نوین مدیریت ریسک، مورد توجه فزاینده اندیشمندان حقوقی قرار گرفته است. هرچند چالش‌هایی در مسیر توسعه این نوع بیمه وجود دارد، اما مزایای آن در جبران خسارات، افزایش امنیت اقتصادی و ارتقای اعتماد عمومی موجب شده است که بسیاری از صاحب‌نظران بر ضرورت توسعه آن تأکید کنند.

تحلیل ساختاری تأثیر تحریم‌های بین‌المللی و محدودیت‌های نظام بین‌المللی بر توسعه بیمه سایبری در ایران

توسعه بازار بیمه سایبری در ایران تنها با چالش‌های حاکمیتی یا تقنینی محدود نمی‌شود، بلکه با یک «بحران ساختاری در زنجیره انتقال ریسک» مواجه است. تحریم‌های بین‌المللی، نه تنها بر جریان سرمایه، بلکه بر زیرساخت‌های معرفتی و فنی که رکن اصلی «تعیین نرخ» (Pricing) در بیمه هستند، اثر گذاشته‌اند. این تحلیل را می‌توان در چهار لایه ساختاری تبیین نمود:

انزوای اتکایی و اختلال در مدیریت ریسک‌های تجمعی (Reinsurance Isolation)

بیمه سایبری به دلیل ماهیت «ریسک‌های سیستماتیک» و احتمال وقوع خسارات تجمعی (Accumulation Risk) ناشی از حملات گسترده، به شدت به بازار اتکایی جهانی متکی است. در یک نظام بیمه‌ای استاندارد، شرکت‌های داخلی با انتقال بخشی از ریسک‌های بزرگ به بازارهای بین‌المللی، از فروپاشی مالی در صورت وقوع بحران‌های سایبری بزرگ جلوگیری می‌کنند.

در ایران، تحریم‌ها منجر به نوعی «انزوای اتکایی» شده است. این انزوا باعث می‌شود که شرکت‌های بیمه داخلی در مواجهه با ریسک‌های سایبری، با «محدودیت ظرفیت پذیرش» (Capacity Constraint) مواجه شوند. از منظر ساختاری، این امر منجر به افزایش «ریسک ناتوانی در پرداخت» (Insolvency Risk) در صورت وقوع حملات تجمعی می‌گردد، زیرا بیمه‌گر داخلی قادر به توزیع ریسک در بازارهای فرامرزی نیست و ناچار به نگه داشتن ریسک‌های سنگین در ترازنامه خود است.

بحران عدم تقارن اطلاعاتی و فرآیند نرخ‌گذاری (Information Asymmetry)

دقت در نرخ‌گذاری بیمه سایبری، مستلزم دسترسی به «بزرگ‌داده‌های (Big Data) جهانی» در حوزه تهدیدات سایبری است. مدل‌های ریاضیاتی نرخ‌گذاری (مانند مدل‌های توزیع احتمالی خسارت)، بر پایه آمارهای دقیق از فراوانی و شدت حملات در سطح جهان بنا می‌شوند. (Sharkey, 2022)

محدودیت‌های بین‌المللی، دسترسی به این جریان‌های اطلاعاتی و پایگاه‌های داده امنیتی را مختل کرده است. این مسئله منجر به ایجاد «عدم تقارن اطلاعاتی» میان بیمه‌گر و بیمه‌گذار می‌شود؛ به گونه‌ای که بیمه‌گر بدون دسترسی به معیارهای استاندارد جهانی (Benchmark)، قادر به ارزیابی دقیق «احتمال وقوع» (Probability of Occurrence) نیست. در نتیجه، نرخ‌های صادرشده یا بسیار محافظه‌کارانه و بالا هستند (که مانع از توسعه بازار می‌شود) و یا با ریسک‌های پنهان همراه‌اند.

فرسایش تکنولوژیک و افزایش ریسک سیستماتیک (Technological Obsolescence)

بیمه سایبری، نوعی «بیمه مبتنی بر فناوری» است که کیفیت خود را از کیفیت زیرساخت‌های فناورانه بیمه‌گذار می‌گیرد. تحریم‌ها، فرآیند به‌روزرسانی تجهیزات و نرم‌افزارهای امنیتی را در ایران با تأخیر مواجه کرده است.

از منظر تحلیل ریسک، این امر منجر به پدیده «فرسایش تکنولوژیک» می‌شود که مستقیماً «ریسک سیستماتیک» (Systemic Risk) را افزایش می‌دهد. زمانی که زیرساخت‌های حیاتی کشور (مانند شبکه برق یا آب) به دلیل محدودیت‌های تأمین، از آخرین لایه‌های حفاظتی محروم بمانند، احتمال وقوع یک حادثه سایبری که کل شبکه را فلج کند، افزایش می‌یابد. این وضعیت، محیطی را برای بیمه‌گر ایجاد می‌کند که در آن، «پیش‌بینی‌پذیری ریسک» به شدت کاهش یافته و ریسک‌های غیرقابل کنترل (Uncontrollable Risks) غالب شده‌اند. (Elsan, 2016)

پیامدهای ساختاری بر مدل‌های قراردادهای بیمه‌ای

این محدودیت‌های فرامرزی، مدل‌های قراردادی بیمه در ایران را از حالت «پوشش جامع» به حالت «پوشش‌های محدود و استثنا محور» سوق داده است. شرکت‌های بیمه برای مدیریت عدم قطعیت ناشی از تحریم‌ها، به جای ارائه پوشش‌های استاندارد، بر روی «استثنائات گسترده» (Broad Exclusions) تمرکز می‌کنند تا مسئولیت‌های خود را در قبال ریسک‌های ناشی از عدم دسترسی به تکنولوژی یا ناشی از حملات دولتی (War/Cyber War) به حداقل برسانند. این امر، ماهیت «انتقال ریسک» را که هدف اصلی بیمه است، تضعیف کرده و بیمه را به یک ابزار پوششی بسیار محدود تبدیل می‌کند.

تحلیل خلأهای تقنینی و چالش‌های حقوقی توسعه بیمه سایبری در نظام حقوقی ایران

با وجود گذار اقتصاد ملی به سوی دیجیتال‌شدن، نظام حقوقی ایران در مواجهه با مخاطرات فضای مجازی دچار نوعی «ناهمخوانی ساختاری» (Structural Mismatch) است. در حالی که ریسک‌های سایبری ماهیتی پویا و غیرمادی دارند، چارچوب‌های حقوقی فعلی همچنان بر مفاهیم سنتی «خسارت مادی-فیزیکی» استوارند. این خلأها و چالش‌ها را می‌توان در سطوح تحلیل کرد:

خلأهای ماهوی و شناسایی (Ontological Gaps)

نخستین و بنیادین‌ترین مانع، عدم تعین ماهیت حقوقی موضوع بیمه است.

ابهام در ماهیت دارایی‌های دیجیتال: در نظام حقوقی ایران، هنوز تعریف واحد و صریحی از «داده‌ها» (Data) یا «دارایی‌های دیجیتال» به عنوان یک مال یا حق قابل معامله وجود ندارد. از آنجا که اصل بر «معین بودن موضوع بیمه» در قراردادهای بیمه است، ابهام در ماهیت حقوقی

داده‌ها (آیا داده یک «مال» است یا یک «حق» یا یک «خدمت»؟) موجب می‌شود که تعیین «موضوع بیمه» (Subject Matter) در قراردادهای سایبری با تردید حقوقی مواجه شود. این امر مستقیماً بر قابلیت اجراپذیری تعهدات بیمه‌گر اثر می‌گذارد.

تضاد میان مفهوم خسارت مادی و غیرمادی

قوانین فعلی بیمه در ایران عمدتاً بر «خسارت فیزیکی» (Physical Damage) متمرکز هستند. اما خسارات سایبری غالباً از نوع «خسارات غیرمادی» (Non-physical Loss) مانند از بین رفتن اعتبار تجاری، از دست رفتن فرصت‌های اقتصادی یا نقض حریم خصوصی هستند. فقدان تعریف قانونی از «خسارت سایبری» باعث شده است که شرکت‌های بیمه برای پرهیز از ریسک‌های مجهول، پوشش‌های خود را محدود به خسارات فیزیکی ناشی از حملات (مانند آسیب به سرورها) کنند و از پوشش خسارات ماهوی (مانند نشت اطلاعات) اجتناب ورزند.

خلأهای فرآیندی و ارزیابی (Procedural & Assessment Gaps)

حتی در صورت وجود قرارداد، فرآیند اجرایی آن با بن‌بست‌های فنی-حقوقی روبه‌روست:

بحران تقویم خسارت (Quantification Challenge)

ارزیابی میزان زیان در حملات سایبری بسیار پیچیده‌تر از حوادث سنتی است. تعیین ارزش اقتصادی «داده‌های از دست‌رفته» یا محاسبه «هزینه توقف فعالیت اقتصادی» (Business Interruption) مستلزم مدل‌های ریاضیاتی و استانداردهای حسابداری نوین است که در دستورالعمل‌های جاری بیمه ایران تعریف نشده‌اند. (Markopoulou, 2021)

عدم قطعیت در تعیین مسئولیت (Liability Uncertainty)

در دعاوی ناشی از حملات سایبری، تفکیک میان «خطای سیستم»، «تقصیر کاربر» و «مسئولیت تأمین‌کننده زیرساخت» بسیار دشوار است. نبود رویه قضایی منسجم و مستند در زمینه «مسئولیت مدنی در فضای مجازی»، باعث می‌شود که بیمه‌گران نتوانند «احتمال وقوع مسئولیت» را به‌درستی پیش‌بینی کنند و در نتیجه، از ورود به این بازار خودداری می‌کنند. (Adabi et al., 2024)

خلأهای نظارتی و حاکمیتی (Regulatory & Governance Gaps)

توسعه این بازار مستلزم حرکت از «قواعد عمومی» به سمت «قواعد تخصصی» است:

فقدان تقنین تخصصی در صنعت بیمه

در حال حاضر، بیمه سایبری به‌عنوان یک شاخه مستقل در ساختار نظارتی بیمه ایران شناخته نشده است. این فقدان «تقنین تخصصی» منجر به این شده که شرکت‌های بیمه به‌جای طراحی محصولات استاندارد، به سمت استفاده از «استثنائات گسترده» (Broad Exclusions) در قراردادهای خود روی آورند تا از ریسک‌های ناشی از ابهام قانونی بگریزند.

نیاز به تدوین دستورالعمل‌های ممیزی فنی

از آنجا که بیمه سایبری با «ریسک فنی» گره خورده است، نهاد ناظر (بیمه مرکزی) نیازمند تدوین آیین‌نامه‌هایی است که چارچوب‌های مشخصی برای «ممیزی امنیت اطلاعات» (Cyber Audit) پیش از صدور بیمه‌نامه تعیین کند.

پراکندگی مقررات و فقدان چارچوب حقوقی منسجم در تعیین حدود مسئولیت اشخاص دخیل در فضای مجازی، به‌ویژه ارائه‌دهندگان خدمات دیجیتال، در قبال خسارت‌های ناشی از مخاطرات سایبری است. هرچند در نظام حقوقی ایران، قواعد عمومی مسئولیت مدنی و برخی مقررات، از جمله قانون تجارت الکترونیکی، قانون جرایم رایانه‌ای و آیین‌نامه‌های مرتبط، حسب مورد در تحلیل مسئولیت اشخاص فعال در فضای

مجازی قابل استناد هستند، اما این مقررات به صورت پراکنده تدوین شده‌اند و هر یک تنها بخشی از مسائل حقوقی این حوزه را تنظیم می‌کنند. برای نمونه، قانون تجارت الکترونیکی عمدتاً ناظر بر اعتبار داده‌پیام، معاملات و قراردادهای الکترونیکی و برخی قواعد مربوط به جمع‌آوری، پردازش و حفظ اطلاعات شخصی در بستر تجارت الکترونیکی است، لیکن موضوعاتی همچون تعیین حدود مسئولیت متولیان داده، تکالیف قانونی در قبال نشت و افشای داده‌ها، الزامات امنیت اطلاعات، مسئولیت ارائه‌دهندگان خدمات ابری، و نیز بسیاری از حقوق نوین مرتبط با داده‌های شخصی، از جمله حق فراموش شدن، حق حذف داده و حق انتقال داده را به صورت جامع و منسجم تنظیم نکرده است. همچنین، قانون جرایم رایانه‌ای عمدتاً بر جرم‌انگاری رفتارهایی مانند دسترسی غیرمجاز، شنود غیرمجاز، تخریب داده‌ها و سایر جرایم سایبری تمرکز دارد و قانون مسئولیت مدنی نیز صرفاً قواعد عام جبران خسارت را بیان می‌کند. افزون بر این، آیین‌نامه واحدهای ارائه‌کننده خدمات اطلاع‌رسانی با محوریت فعالیت پایگاه‌های اطلاع‌رسانی و ارائه‌دهندگان محتوا تدوین شده و عمدتاً ناظر بر تکالیف این اشخاص در حوزه انتشار اطلاعات است؛ از این رو، قلمرو آن بسیاری از بازیگران نوین فضای مجازی، از جمله متولیان پایگاه‌های داده، ارائه‌دهندگان خدمات ابری، پردازشگران داده، بهره‌برداران مراکز داده و سایر ارائه‌دهندگان خدمات دیجیتال را در بر نمی‌گیرد.

این وضعیت آثار مستقیمی بر صنعت بیمه دارد؛ زیرا ارزیابی ریسک، تعیین حق بیمه، طراحی پوشش‌های بیمه‌ای و حدود تعهدات بیمه‌گر، تا حد زیادی تابع قلمرو مسئولیت قانونی اشخاص دخیل در حادثه سایبری است. هر اندازه حدود این مسئولیت‌ها مبهم‌تر یا پراکنده‌تر باشد، ارزیابی دقیق ریسک و طراحی بیمه‌نامه‌های تخصصی نیز با دشواری بیشتری مواجه خواهد شد.

بر این اساس، آنچه در نظام حقوقی ایران مورد نیاز است، صرفاً تصویب مقررات جدید در حوزه مسئولیت مدنی نیست، بلکه تدوین قانونی جامع و منسجم در زمینه مسئولیت اشخاص دخیل در فضای مجازی متناسب با ویژگی‌های مخاطرات سایبری است؛ قانونی که ضمن تعیین دقیق جایگاه، حدود مسئولیت و تکالیف هر یک از بازیگران اصلی فضای مجازی، از جمله متولیان داده، ارائه‌دهندگان خدمات اینترنتی، ارائه‌دهندگان خدمات ابری، مدیران سامانه‌ها و سایر ارائه‌دهندگان خدمات دیجیتال، آثار حقوقی نقض تعهدات امنیتی، مسئولیت ناشی از نشت و افشای داده‌ها، حدود جبران خسارت و ارتباط این مسئولیت‌ها با نظام بیمه سایبری را نیز به طور شفاف تبیین کند.

همچنین نبود دستورالعمل‌های تخصصی برای ارزیابی ریسک سایبری از دیگر موانع توسعه بیمه‌های سایبری محسوب می‌شود. شرکت‌های بیمه برای ارائه پوشش مناسب نیازمند معیارهای مشخصی برای سنجش سطح ریسک هستند. در غیاب چنین معیارهایی، تعیین حق بیمه و شرایط پوشش با عدم قطعیت همراه خواهد بود. تدوین دستورالعمل‌های فنی و حقوقی در این زمینه می‌تواند به ایجاد وحدت رویه در صنعت بیمه کمک کند. (Esfidani et al., 2011)

در مقابل، در نظام حقوقی ایالات متحده آمریکا با تدوین مقررات تخصصی و ایجاد رویه‌های قضایی، بسیاری از این خلأها تا حد زیادی برطرف شده است. وجود بیمه‌نامه‌های استاندارد، دستورالعمل‌های نظارتی و همکاری میان نهادهای بیمه‌ای و فناوری اطلاعات موجب شده است که بازار بیمه‌های سایبری در این کشور رشد قابل توجهی داشته باشد. مقایسه این وضعیت با حقوق ایران نشان می‌دهد که اصلاح و تکمیل مقررات موجود تا چه اندازه ضروری است. (Lim & Morgan, 2024)

برای رفع خلأهای قانونی موجود، می‌توان مجموعه‌ای از اقدامات تقنینی و نهادی را پیشنهاد کرد. تدوین مقررات مستقل در حوزه بیمه سایبری، اصلاح قوانین موجود در زمینه مسئولیت مدنی و تجارت الکترونیکی، تعیین استانداردهای امنیت اطلاعات و ایجاد سازوکارهای نظارتی مؤثر

از جمله اقداماتی است که می‌تواند به توسعه این حوزه کمک کند. همچنین ایجاد تعامل میان نهادهای قانون‌گذار، شرکت‌های بیمه و متخصصان فناوری اطلاعات می‌تواند زمینه تدوین مقررات کارآمد را فراهم سازد.

در نهایت، می‌توان گفت که رفع خلأهای قانونی موجود در حوزه بیمه سایبری، شرط اساسی توسعه این نوع بیمه در نظام حقوقی ایران است. بدون ایجاد چارچوب‌های حقوقی شفاف و کارآمد، امکان گسترش پوشش‌های بیمه‌ای و حمایت مؤثر از فعالان اقتصادی در برابر مخاطرات سایبری فراهم نخواهد شد. از این‌رو، توجه جدی قانون‌گذاران و نهادهای مرتبط به این موضوع ضروری به نظر می‌رسد.

چالش‌های اثبات خسارت در بیمه‌های سایبری

یکی از مهم‌ترین مسائل حقوقی در حوزه بیمه‌های سایبری، نحوه اثبات خسارات ناشی از حوادث سایبری است. برخلاف بسیاری از خسارات سنتی که آثار فیزیکی و ملموسی دارند، خسارات سایبری غالباً ماهیتی غیرمادی و نامحسوس دارند و همین امر اثبات آن‌ها را با دشواری‌هایی مواجه می‌سازد. از این‌رو، بررسی چالش‌های اثبات خسارت در بیمه‌های سایبری از منظر حقوقی و عملی اهمیت ویژه‌ای دارد.

در بسیاری از موارد، حملات سایبری موجب از بین رفتن داده‌ها، اختلال در سامانه‌های اطلاعاتی یا افشای اطلاعات محرمانه می‌شود. این نوع خسارات ممکن است آثار مالی مستقیم و غیرمستقیم به همراه داشته باشد، اما تعیین دقیق میزان زیان وارد شده نیازمند بررسی‌های فنی پیچیده است. برای مثال، در صورت از بین رفتن داده‌های یک شرکت، ارزش اقتصادی این داده‌ها و هزینه‌های بازیابی آن‌ها باید توسط کارشناسان متخصص ارزیابی شود. چنین ارزیابی‌هایی مستلزم همکاری میان متخصصان حقوقی و کارشناسان فناوری اطلاعات است. (Herr, 2021)

(2021)

از سوی دیگر، در برخی موارد خسارات سایبری به صورت غیرمستقیم و تدریجی ظاهر می‌شود. کاهش اعتبار تجاری، از دست رفتن اعتماد مشتریان و کاهش درآمد ناشی از توقف فعالیت‌های دیجیتال از جمله خساراتی است که اندازه‌گیری دقیق آن‌ها با دشواری همراه است. در این شرایط، تعیین رابطه سببیت میان حادثه سایبری و خسارات وارده نیز ممکن است محل اختلاف قرار گیرد و موجب طرح دعاوی پیچیده میان بیمه‌گر و بیمه‌گذار شود.

در نظام‌های حقوقی پیشرفته، از جمله ایالات متحده آمریکا، برای حل این چالش‌ها از روش‌های تخصصی ارزیابی خسارت استفاده می‌شود. شرکت‌های بیمه و دادگاه‌ها با بهره‌گیری از کارشناسان فنی و مالی، تلاش می‌کنند میزان واقعی خسارات را برآورد کنند. همچنین در بسیاری از بیمه‌نامه‌های سایبری، روش‌های مشخصی برای ارزیابی خسارت پیش‌بینی شده است تا از بروز اختلافات جدی میان طرفین جلوگیری شود.

در حقوق ایران نیز با گسترش استفاده از فناوری‌های دیجیتال، به تدریج دعاوی مرتبط با خسارات سایبری افزایش خواهد یافت. در چنین شرایطی، نبود دستورالعمل‌های مشخص برای ارزیابی این خسارات می‌تواند موجب بروز اختلافات حقوقی و طولانی شدن روند رسیدگی قضایی شود. از این‌رو، تدوین مقررات و دستورالعمل‌های تخصصی در خصوص نحوه اثبات و ارزیابی خسارات سایبری ضروری به نظر می‌رسد. (Singh et al., 2025)

نقش بیمه در این میان بسیار مهم است. شرکت‌های بیمه می‌توانند با پیش‌بینی سازوکارهای دقیق برای ارزیابی خسارت در قراردادهای بیمه سایبری، از بروز اختلافات بعدی جلوگیری کنند. تعیین معیارهای مشخص برای محاسبه خسارات، استفاده از کارشناسان مستقل و پیش‌بینی روش‌های حل اختلاف از جمله اقداماتی است که می‌تواند به شفافیت بیشتر روابط قراردادی کمک کند.

علاوه بر این، توسعه رویه‌های کارشناسی تخصصی در حوزه جرایم و خسارات سایبری می‌تواند نقش مهمی در تسهیل اثبات خسارت ایفا کند. تربیت کارشناسان رسمی با تخصص در حوزه فناوری اطلاعات و بیمه، ایجاد بانک‌های اطلاعاتی مربوط به خسارات سایبری و استفاده از فناوری‌های نوین در تحلیل داده‌ها از جمله اقداماتی است که می‌تواند به بهبود فرایند اثبات خسارت کمک کند.

در مجموع، می‌توان گفت که اثبات خسارت در بیمه‌های سایبری یکی از چالش‌های اساسی این حوزه است که نیازمند توجه جدی قانون‌گذاران، شرکت‌های بیمه و نهادهای قضایی است. ایجاد چارچوب‌های حقوقی و فنی مناسب برای ارزیابی دقیق خسارات می‌تواند به افزایش کارآمدی بیمه‌های سایبری و تقویت اعتماد عمومی به این ابزار حقوقی منجر شود.

با توسعه تعاملات دیجیتال و گسترش فعالیت‌های اقتصادی در بسترهای الکترونیکی، بیمه سایبری به‌عنوان ابزار پوشش ریسک‌های نوین مطرح شده است. با این حال، اجرای عملی این نوع بیمه در نظام حقوقی ایران با چالش‌های تفسیری متعددی روبه‌رو است که ناشی از فقدان مقررات اختصاصی و اتکای صرف به قواعد سنتی بیمه می‌باشد.

نخستین تعارض، در تفسیر مفهوم «خطر» بروز می‌کند. در بیمه‌های سنتی، خطر غالباً ماهیتی فیزیکی و عینی دارد؛ حال آنکه در فضای سایبری، خطر ممکن است ناملموس، تدریجی و چندلایه باشد. پرسش اساسی آن است که آیا نفوذ غیرمجاز به سامانه، بدون تحقق خسارت مالی فوری، مصداق خطر بیمه‌پذیر محسوب می‌شود یا خیر؟ در فقدان تصریح قانونی، پاسخ به این پرسش وابسته به تفسیر قضایی خواهد بود.

تعارض دوم در تعیین زمان تحقق خسارت است. در بسیاری از حملات سایبری، فاصله زمانی میان نفوذ اولیه و کشف آن ممکن است طولانی باشد. این امر تعیین زمان شروع تعهد بیمه‌گر و شمول یا عدم شمول پوشش بیمه‌ای را با ابهام مواجه می‌سازد. اگر قرارداد بیمه در فاصله میان نفوذ و کشف آن منعقد شده باشد، تعیین اینکه خسارت در چه زمانی واقع شده، می‌تواند محل اختلاف جدی باشد. ([European Court of Justice](#), 2024)

(of, 2024)

تعارض سوم ناظر بر رابطه سببیت است. در فضای دیجیتال، وقوع خسارت ممکن است ناشی از مجموعه‌ای از عوامل باشد؛ از جمله ضعف امنیتی بیمه‌گذار، فعل شخص ثالث، یا حتی نقص نرم‌افزاری. تعیین اینکه کدام عامل سبب اصلی ورود زیان بوده است، نقش تعیین‌کننده‌ای در مسئولیت بیمه‌گر دارد. قواعد سنتی سببیت ممکن است در مواجهه با این پیچیدگی‌ها کارآمدی کامل نداشته باشند.

همچنین، ابهام در حدود تعهدات پیشگیرانه بیمه‌گذار از دیگر مسائل تفسیری است. آیا عدم به‌روزرسانی نرم‌افزارها یا رعایت نکردن استانداردهای امنیتی، مصداق تقصیر مؤثر در سقوط یا کاهش تعهد بیمه‌گر است؟ در نبود ضوابط روشن، پاسخ به این پرسش‌ها می‌تواند موجب صدور آرای متعارض شود.

در مقایسه با تجربه نظام حقوقی ایالات متحده آمریکا، مشاهده می‌شود که بسیاری از این تعارضات از طریق تنظیم دقیق شروط بیمه‌نامه و تدوین رویه‌های قضایی تخصصی تا حد زیادی مدیریت شده‌اند. این تجربه نشان می‌دهد که اتکا به قواعد کلی بدون توسعه تفسیری متناسب با ویژگی‌های فناوری، نمی‌تواند پاسخگوی پیچیدگی‌های بیمه سایبری باشد.

در نتیجه، می‌توان گفت که مهم‌ترین چالش اجرای بیمه سایبری در حقوق ایران، نه فقدان کامل ظرفیت حقوقی، بلکه نبود چارچوب تفسیری منسجم و تخصصی است. تا زمانی که این چارچوب تدوین نشود، اختلافات قراردادی در این حوزه محتمل خواهد بود و امنیت حقوقی فعالان اقتصادی به‌طور کامل تأمین نخواهد شد.

نتیجه‌گیری

گسترش روزافزون فناوری اطلاعات و وابستگی فزاینده فعالیت‌های اقتصادی، تجاری و اجتماعی به فضای مجازی، موجب ظهور و توسعه انواع جدیدی از خطرات و خسارت‌های سایبری شده است؛ خطراتی که از حیث ماهیت، گستره و شیوه تحقق، با بسیاری از ریسک‌های سنتی تفاوت دارند. در چنین شرایطی، بیمه سایبری می‌تواند به عنوان یکی از ابزارهای مهم مدیریت و انتقال ریسک، نقش قابل توجهی در جبران خسارت‌های ناشی از حملات سایبری، نقض امنیت اطلاعات، افشای داده‌ها و اختلال در فعالیت‌های الکترونیکی ایفا کند. با این حال، بررسی وضعیت حقوقی و بیمه‌ای ایران نشان می‌دهد که ظرفیت موجود برای توسعه این نوع بیمه هنوز با چالش‌ها و کاستی‌های متعددی مواجه است.

نتایج این پژوهش نشان می‌دهد که اگرچه اصول کلی حاکم بر قراردادهای بیمه، از جمله اصل حسن نیت، وجود نفع بیمه‌ای، اصل جبران خسارت و قائم مقامی، قابلیت انطباق با بیمه سایبری را دارند، اما ویژگی‌های خاص خطرات فضای مجازی موجب می‌شود اجرای این اصول با مسائل جدیدی مواجه شود. ابهام در ماهیت حقوقی داده‌ها و دارایی‌های دیجیتال، دشواری تشخیص و ارزیابی خسارت‌های غیرمادی، پیچیدگی اثبات وقوع خسارت و رابطه سببیت، تعیین مسئولیت اشخاص مختلف در زنجیره خدمات دیجیتال و نبود معیارهای روشن برای تعیین میزان خسارت، از مهم‌ترین چالش‌های حقوقی این حوزه به شمار می‌روند.

از سوی دیگر، خلأهای تقنینی و فقدان مقررات تخصصی و منسجم درباره بیمه سایبری، در کنار پراکندگی قواعد مربوط به مسئولیت مدنی و حمایت از داده‌ها، موجب شده است چارچوب حقوقی موجود پاسخ کاملاً روشنی به بسیاری از مسائل نوظهور این حوزه ارائه نکند. همچنین، محدودیت‌های ناشی از تحریم‌های بین‌المللی، دشواری دسترسی به بازارهای بیمه و اتکایی بین‌المللی، ضعف دسترسی به اطلاعات و داده‌های تخصصی و نیز سرعت بالای تحول فناوری، بر امکان توسعه و ارزیابی صحیح بیمه‌های سایبری در ایران تأثیر گذاشته است. در نهایت، می‌توان گفت کارآمدی بیمه سایبری در ایران صرفاً با توسعه محصولات بیمه‌ای محقق نخواهد شد، بلکه نیازمند ایجاد یک بستر حقوقی، فنی و نهادی هماهنگ است. تدوین مقررات تخصصی و شفاف در زمینه بیمه سایبری، تعیین دقیق حقوق و تکالیف بیمه‌گر و بیمه‌گذار، ایجاد استانداردهای فنی و حرفه‌ای برای ارزیابی و حسابرسی امنیت سایبری، تقویت سازوکارهای اثبات و ارزیابی خسارت، افزایش همکاری میان نهادهای بیمه‌ای، قضایی و تخصصی و ارتقای آگاهی عمومی و حرفه‌ای از جمله اقداماتی است که می‌تواند زمینه توسعه این بیمه را فراهم سازد. بنابراین، توسعه بیمه سایبری در ایران را باید فرایندی تدریجی و چندبعدی دانست که تحقق آن مستلزم هماهنگی میان تحولات فناوری و الزامات حقوقی و بیمه‌ای است.

تعارض منافع

در انجام مطالعه حاضر، هیچ‌گونه تضاد منفعی وجود ندارد.

مشارکت نویسندگان

در نگارش این مقاله تمامی نویسندگان نقش یکسانی ایفا کردند.

حامی مالی

این پژوهش حامی مالی نداشته است.

EXTENDED SUMMARY

The rapid expansion of information technology and the growing dependence of economic, commercial, administrative, and social activities on digital infrastructures have fundamentally

transformed the structure of modern risks and the mechanisms required for their management. Alongside the benefits of digitalization, including increased efficiency, lower transaction costs, broader market access, and accelerated communication, individuals, corporations, financial institutions, and public bodies have become increasingly exposed to cyberattacks, unauthorized access, data breaches, system failures, ransomware incidents, business interruption, and other forms of digital loss. These risks differ substantially from conventional insurable risks because they are often intangible, technically complex, transboundary, interconnected, and difficult to quantify with conventional actuarial methods. Consequently, traditional mechanisms of civil liability and compensation may not be sufficient to address the full economic consequences of cyber incidents. Cyber insurance has therefore emerged as an important instrument of contemporary risk management, enabling policyholders to transfer part of the financial consequences associated with cyber incidents to insurers while simultaneously encouraging preventive investment in cybersecurity. The development of such insurance may also contribute to the resilience of digital markets by reducing uncertainty and providing businesses with greater confidence in the continuity of their operations. In the Iranian legal context, however, the emergence of cyber insurance has not yet been accompanied by a comprehensive and specialized regulatory framework, notwithstanding the increasing exposure of economic actors to digital threats. Existing insurance law principles provide a general contractual foundation for insuring new forms of risk, but the effective incorporation of cyber risks requires further regulatory development, technical standardization, and institutional coordination. These challenges are particularly significant because cyber insurance depends not merely on contractual risk transfer but also on accurate risk identification, access to reliable information, technical security assessments, and clearly defined legal liabilities. Accordingly, the legal recognition and development of cyber insurance should be viewed as an integral component of broader strategies for strengthening digital economic security and managing emerging technological risks in Iran (Pourkavian & Bozorgi, 2025; Singh et al., 2025).

From the perspective of economic security, cyber insurance performs both compensatory and preventive functions. Its compensatory function consists primarily in covering financial losses arising from cyberattacks, data breaches, information-system disruptions, digital fraud, costs of data recovery, business interruption, and, depending on the policy, third-party liabilities resulting from failures in cybersecurity. By transferring part of these losses to insurers, cyber insurance may reduce the probability that a severe cyber event will cause financial instability, insolvency, or the complete interruption of business operations. This function is especially important for small and medium-sized enterprises, technology-dependent companies, online businesses, and start-ups whose financial capacity to absorb major cyber losses may be limited. At the same time, cyber insurance may strengthen public and commercial confidence in digital services because users and businesses are more likely to engage in online transactions when they perceive that adequate mechanisms for financial recovery exist. In addition, cyber insurance has a preventive dimension because insurers typically assess the security posture of prospective policyholders and may require compliance with minimum cybersecurity standards as a condition of coverage. Such requirements can incentivize organizations to improve access controls, information-security governance, software updating practices, incident-response plans, data-backup systems, and other preventive measures. The insurer therefore functions not only as a compensating institution but also as a private actor that may influence cybersecurity practices through contractual conditions, risk-based pricing, and underwriting requirements. This regulatory potential is increasingly recognized in discussions of cyber insurance as a mechanism of private governance capable of encouraging more responsible

cybersecurity behavior (Herr, 2021). In Iran, the effectiveness of this function depends heavily on the development of sufficient technical expertise within insurance companies, the availability of standardized cyber-risk assessment models, and clearer supervisory policies. The digitalization of insurance services and the emergence of innovative financial technologies further reinforce the need for specialized supervisory mechanisms capable of responding to the new risks associated with digital economic activity (Abdi & Kalantari, 2024; Adabi et al., 2024).

The institutional framework governing cyber insurance is another critical dimension of its development. Within the Iranian insurance system, a distinction must be maintained between institutions responsible for general insurance policy-making and those responsible for regulatory supervision and implementation. The Central Insurance of Iran, as the principal supervisory institution, has a particularly important role in the development of cyber insurance through the formulation of technical regulations, approval and supervision of insurance products, oversight of insurers' solvency, and establishment of risk-management requirements. Cyber risks raise distinctive supervisory problems because a single large-scale attack may simultaneously affect hundreds or thousands of insured entities, producing an accumulation of correlated losses rather than isolated claims. This feature distinguishes systemic cyber events from many conventional risks and requires regulators to consider insurers' capital adequacy, reinsurance arrangements, catastrophe exposure, and concentration of cyber risk. At the contractual level, regulatory oversight is also necessary to prevent excessive reliance on broad exclusions that could undermine the practical value of cyber insurance coverage. Furthermore, the complexity of cyber threats means that effective supervision cannot be undertaken solely within the conventional boundaries of the insurance industry. It requires institutional cooperation between insurance regulators, cybersecurity authorities, digital infrastructure organizations, technology experts, financial institutions, and data-protection bodies. The establishment of cyber-incident databases, threat-intelligence systems, and standardized loss-reporting mechanisms could significantly improve underwriting accuracy and contribute to more reliable premium determination. At present, one of the principal difficulties in Iran is the absence of a comprehensive and unified regulatory framework specifically addressing cyber insurance, which may result in differences between insurers in underwriting standards, contractual conditions, and risk-assessment procedures. The development of specialized regulations could reduce informational asymmetry and facilitate more consistent market practices. General principles of insurance law, including good faith, insurable interest, indemnity, and subrogation, remain relevant to cyber insurance, but they require adaptive interpretation in response to the particular characteristics of digital risks (Katouzian, 2018; Nikouei, 2024). These principles therefore provide a legal foundation, but their effective application depends on specialized regulatory and contractual clarification.

A central legal challenge concerns the recognition and characterization of cyber risks and digital assets within the existing framework of insurance law. In conventional insurance, the subject matter of insurance and the insured risk are usually identifiable in relatively concrete economic terms, whereas cyber insurance may concern data, digital assets, confidential information, network availability, reputational interests, or liabilities arising from unauthorized access and disclosure. The legal characterization of data is particularly important because uncertainty as to whether data constitute property, an economic interest, a legally protected right, or another form of intangible asset can influence the identification of insurable interest and the assessment of compensable loss. Related difficulties arise when cyber incidents produce non-physical losses, such as reputational damage, loss of customer confidence, missed business opportunities, privacy violations, and

financial losses caused by business interruption. Unlike physical property damage, such losses may be difficult to quantify and may depend on complex economic and evidentiary assessments. Nevertheless, the increasing importance of digital assets and technologically mediated economic relations demonstrates that insurance law cannot remain confined to conventional concepts of tangible property and physical damage. The possibility of insuring digital assets and technologically generated economic interests has already attracted scholarly attention in relation to new forms of digital property and non-fungible tokens, illustrating the broader transformation of the concept of insurable assets ([Mahmoudi & Miri Balajorshari, 2022](#)). Furthermore, the legal framework governing liability in electronic transactions and cyberspace affects the viability of cyber liability insurance because an insurer's exposure depends directly on the legal obligations imposed on insured actors. Iranian electronic commerce law and general principles of civil liability provide certain legal foundations for addressing digital harms, but they do not comprehensively regulate the responsibilities of data controllers, cloud service providers, processors, digital platforms, infrastructure operators, and other actors involved in complex digital service chains ([Elsan, 2016, 2023](#)). Comparative developments similarly demonstrate that the allocation of liability among online intermediaries and digital platforms is a central issue in determining the scope of technology-related risk and insurance coverage ([European Court of, 2024; Lim & Morgan, 2024](#)).

Another major challenge lies in the assessment, proof, and pricing of cyber losses. Cyber incidents frequently generate a combination of direct and indirect losses, including the costs of technical investigation, system restoration, data recovery, notification of affected parties, interruption of business activities, loss of revenue, reputational harm, legal claims, and regulatory consequences. Establishing a causal connection between the cyber event and the claimed loss may be difficult where multiple factors contribute to the incident, such as inadequate cybersecurity measures, third-party misconduct, software vulnerabilities, failures by service providers, or delayed detection of unauthorized access. The temporal dimension of cyber incidents also creates difficulties because the initial intrusion into a system may occur long before the attack is detected, raising questions concerning when the insured event legally occurred and which insurance period applies. Such complexities require detailed contractual provisions and specialized technical and financial expertise in loss adjustment. Comparative experience indicates that cyber insurance markets have responded to these problems through increasingly specific policy wording, technical underwriting standards, and specialized claims procedures, although significant market and regulatory challenges remain even in more developed jurisdictions ([Markopoulou, 2021](#)). The difficulty of cyber-risk pricing is compounded by informational asymmetry, limited historical loss data, and the rapidly evolving nature of cyber threats. Insurers require access to extensive datasets concerning the frequency, severity, and characteristics of cyber incidents in order to estimate expected losses and establish actuarially appropriate premiums. International sanctions create an additional structural constraint for Iranian insurers by restricting access to foreign reinsurance markets, global cybersecurity databases, specialized analytical technologies, and certain forms of technical cooperation. These limitations may reduce the ability of insurers to diversify large cyber risks internationally and may increase their exposure to accumulated losses. They may also contribute to technological obsolescence, which can increase the vulnerability of insured entities and thereby exacerbate systemic cyber risk. In response to uncertainty, insurers may adopt highly conservative pricing strategies or extensive contractual exclusions, potentially reducing the attractiveness and economic effectiveness of cyber insurance. These difficulties demonstrate that sustainable development of the Iranian cyber insurance market requires specialized loss-assessment standards, cyber-risk

databases, expert training, appropriate reinsurance strategies, and stronger technical cooperation between insurance, legal, and cybersecurity institutions (Esfidani et al., 2011; Moghadamfar & Seifikar, 2026; Safarinia, 2025; Sharkey, 2022).

In conclusion, the Iranian legal system possesses a basic theoretical capacity to accommodate cyber insurance through the general principles governing insurance contracts and civil liability, but this capacity remains incomplete and transitional in practical terms. The principal challenge is not the total absence of legal foundations, but the lack of an integrated framework capable of adapting those foundations to the technical, intangible, interconnected, and transnational characteristics of cyber risks. Effective development of cyber insurance therefore requires coordinated reforms at several levels. Specialized legislation should clarify the legal status of digital assets, the scope of compensable cyber losses, the responsibilities of different actors in digital service chains, and the legal consequences of failures to comply with cybersecurity obligations. Regulatory authorities should establish standardized procedures for cyber-risk assessment, security auditing, premium calculation, claims evaluation, and insurer solvency management in relation to systemic cyber events. At the same time, insurers must expand their technical capacity through the employment of cybersecurity specialists, legal experts, financial analysts, and qualified loss assessors. Greater institutional cooperation is also necessary for the creation of reliable databases on cyber incidents and losses, which would improve actuarial calculations and reduce informational asymmetry. Finally, public awareness and professional understanding of cyber insurance should be strengthened so that businesses view such coverage not merely as an optional financial product but as part of a broader strategy of digital risk governance. Accordingly, the future of cyber insurance in Iran depends on the coordinated evolution of law, insurance regulation, technological infrastructure, risk-management practices, and institutional expertise, and its successful development should be understood as a gradual and multidimensional process rather than as the simple introduction of a new insurance product.

References

- Abdi, J., & Kalantari, R. (2024). Creating a Cyber Insurance Market in Iran: The Institutional Role of Government and Its Effects on Businesses. *Social Business Journal*, 1(1).
- Adabi, M., Haji Heydari, N., & Vares, S. H. (2024). Developing a Digital Insurance Model Using a Grounded Theory Approach. *Journal of Business Management*, 16(2). <https://doi.org/10.22059/jibm.2022.336731.4284>
- Elsan, M. (2016). Liability Insurance and Damages Arising in Cyberspace. *Insurance Research Journal (Insurance Industry)*, 96(1).
- Elsan, M. (2023). *Electronic Commerce Law* (10 ed.). SAMT.
- Esfidani, M. R., Daghighi Asl, A., & Esmaeili Ahangar Kalabi, E. (2011). The Effect of the Internet on Life Insurance Marketing Performance. *Insurance Research Journal*(102).
- European Court of, J. (2024). *Case Law on Platform Intermediaries: From Uber to Airbnb*.
- Herr, T. (2021). Cyber Insurance and Private Governance: The Enforcement Power of Markets. *Regulation & Governance*, 15(1). <https://doi.org/10.1111/rego.12266>
- Katouzian, N. (2018). *Liability Arising from Product Defects: A Critical and Comparative Study of the Balance between Producer and Consumer Rights* (1 ed.). University of Tehran Press.
- Lim, E., & Morgan, P. (2024). *The Cambridge Handbook of Private Law and Artificial Intelligence*. Cambridge University Press.
- Mahmoudi, A., & Miri Balajorshari, S. M. (2022). An Analysis of Insurance Mechanisms for Non-Fungible Tokens. *Quarterly Journal of Cyberspace Legal Studies*, 1(1).
- Markopoulou, D. (2021). Cyber-Insurance in EU Policy-Making: Regulatory Options, the Market's Challenges and the US Example. *Computer Law & Security Review*, 43. <https://doi.org/10.1016/j.clsr.2021.105627>
- Moghadamfar, A., & Seifikar, M. (2026). Civil Liability for Damages Arising from Cyberspace in Imamiyyah Jurisprudence and the Role of Insurance in Compensation. *Insurance Research Journal*.
- Nikouei, M. (2024). The Basis of Civil Liability Arising from Breach of Electronic Contracts. *Journal of Financial and Economic Law Research*, 1(2).

- Pourkavian, S., & Bozorgi, M. S. (2025). Examining the Effects of Emerging Financial Technologies on Transparency and Insurance Supervisory Requirements in Iran.
- Safarinia, M. (2025). Legal Challenges of Cyber Insurance in International Contracts. *Biannual Scientific Journal of Media Jurisprudence and Law*, 7(2).
- Sharkey, C. M. (2022). Products Liability in the Digital Age: Online Platforms as 'Cheapest Cost Avoiders'. *UC Law Journal*, 73(5).
- Singh, K., Chatterjee, S., Mariani, M., & Wamba, S. F. (2025). Cybersecurity Resilience and Innovation Ecosystems for Sustainable Business Excellence: Examining the Dramatic Changes in the Macroeconomic Business Environment. *Technovation*, 143. <https://doi.org/10.1016/j.technovation.2025.103219>