*Jurisprudence and Legal Studies of Media Journal*
*VOL. 8 / Autumn 2026 and Winter 2027 / NO. 2 (Serial 16)*

# Cyber Insurance in the Light of Governmental Jurisprudence

Maryam Seifikar[1] 0009-0005-4361-7865
Atiyeh Moghadamfar[2] 0009-0005-3858-8297

## Abstract

This research analyzes the Islamic government's responsibility and legitimacy in intervening in cyber insurance, based on governmental jurisprudence and Imam Khomeini's theory of Absolute Velayat-e Faqih. A descriptive-analytical method with library-based data collection from jurisprudential, legal, and cybersecurity risk management sources was employed. Ensuring cybersecurity is an inherent duty of the Islamic government under "preservation of the Islamic system." Cyber risks were classified into four categories (technical, security, legal-regulatory, reputational), and their insurability was analyzed. Digital assets' legal personality was established based on Imam Khomeini and Shahid Sadr's opinions. Cyber insurance's legitimacy as an independent contract was affirmed using Imam Khomeini's theory, Quranic evidence, and narrative evidence. Five jurisprudential challenges were addressed: ransomware payment, compensation for lost profits, liability for AI errors, policy overlap in cyber-physical attacks, and insurer subrogation when the hacker is unknown. Government intervention's legitimacy was substantiated across four dimensions: expediency, security-defense, economic, and social. A comparative study indicated a combined model including gradual mandatory coverage for vital sectors, a dual conventional/Takaful model, technical risk assessment standards, and a government guarantee fund suits Iran. Relying on Absolute Velayat-e Faqih, the Islamic government is obligated to adopt an active, multi-level approach (legislation, regulation, supervision, empowerment) to organize cyber insurance. Imami jurisprudence can respond to emerging issues through dynamic ijtihad.

**Keywords:** Cyber Insurance, Governmental Jurisprudence, Absolute Velayat-e Faqih, Cybersecurity, Legitimacy of Intervention.

1- Master's Student, Department of Islamic Jurisprudence and Law, Refah Faculty, Tehran, Iran
seifmaryam401@gmail.com
2- Assistant Professor, Department of Islamic Jurisprudence and Law, Refah Faculty, Tehran, Iran
(corresponding author of the article) farokhi@refah.ac.ir

دوفصلنامه دوره ۸، شماره ۲ (پیاپی ۱۶)
مطالعات فقه و حقوق رسانه پاییز و زمستان ۱۴۰۵
دانشکده غیردولتی – غیرانتفاعی رفاه صص: ۳۹-۹۳

# بیمه سایبری در پرتو فقه حکومتی

نوع مقاله: پژوهشی DOI: 10.22034/jlsm.2026.2081065.1079
تاریخ دریافت: ۱۴۰۴/۱۰/۱۱ تاریخ بازنگری: ۱۴۰۵/۰۳/۲۲ تاریخ پذیرش: ۱۴۰۵/۰۴/۲۸

مریم صیفی کار[۱] عطیه مقدم‌فر[۲]

## چکیده

***این پژوهش با روش توصیفی-تحلیلی با گردآوری کتابخانه‌ای از منابع فقهی، حقوقی و مطالعات مدیریت ریسک سایبری انجام شده است. تأمین امنیت سایبری ذیل تکلیف «حفظ نظام»، مسئولیتی ذاتی برای حکومت اسلامی است. ریسک‌های سایبری در چهار دسته (فنی، امنیتی، قانونی-نظارتی، اعتباری) طبقه‌بندی شده و قابلیت بیمه‌پذیری هر دسته تحلیل گردید. مالیت دارایی‌های دیجیتال با استناد به آرای امام خمینی و شهید صدر اثبات شد. مشروعیت عقد بیمه سایبری با تأکید بر نظریه «عقد مستقل» امام خمینی و ادله قرآنی (أوفوا بالعقود، تعاونوا علی البر) و روایی (المؤمنون عند شروطهم) احراز گردید و به شبهات غرر، جهالت، تعلیق و ربا پاسخ داده شد. پنج چالش فقهی خاص شامل حکم پرداخت باج‌افزار (تزاحم قاعده نفی سبیل و اضطرار)، جبران سود منتفی (تمایز سود قطعی و احتمالی)، مسئولیت ناشی از خطای هوش مصنوعی، تداخل بیمه‌نامه‌ها در حملات سایبری-فیزیکی و قائم‌مقامی بیمه‌گر در فرض ناشناس بودن هکر، بررسی و راهکارهای میانی ارائه گردید. مشروعیت مداخله حکومت در چهار بُعد مصلحتی (حفظ نظام اقتصادی دیجیتال)، امنیتی-دفاعی (صیانت از مرزهای سایبری)، اقتصادی (نفی ضرر نوعی بر اساس قاعده لاضرر) و اجتماعی (تحقق عدالت و تنظیم بازار بر اساس آیه تعاون) مستند شد. مطالعه تطبیقی نشان داد که الگوی ترکیبی شامل الزام تدریجی بخش‌های حیاتی، مدل دوگانه بیمه متعارف و تکافل سایبری، استانداردهای فنی ارزیابی ریسک و صندوق تضمین دولتی برای ایران مناسب است. حکومت اسلامی با اتکا به نظریه ولایت مطلقه فقیه، نه تنها مجاز بلکه مکلف است رویکردی فعال و چندسطحی (تقنین، تنظیم‌گری، نظارت و توانمندسازی) برای ساماندهی بیمه سایبری در پیش گیرد. فقه امامیه با مبانی مستحکم و ظرفیت اجتهاد پویا، توانایی پاسخگویی به مسائل مستحدثه را دارد.***

## واژگان کلیدی

***امنیت سایبری، بیمه سایبری، فقه حکومتی، مشروعیت مداخله، ولایت مطلقه فقیه.***

---

۱. دانشجوی کارشناسی ارشد، گروه فقه و حقوق اسلامی دانشکده رفاه، تهران، ایران seifmaryam401@gmail.com
۲. استادیار، گروه فقه و حقوق اسلامی، دانشکده رفاه، تهران، ایران (نویسنده مسئول) a.moghadam10@gmail.com

## مقدمه

گسترش فضای سایبری و اقتصاد دیجیتال، ریسک‌های نوینی را پدید آورده است که امنیت ملی و ثبات اقتصادی را با چالش مواجه کرده‌اند . بیمه سایبری به‌عنوان ابزاری برای انتقال این ریسک‌ها مطرح شده، اما در نظام جمهوری اسلامی ایران، تنظیم آن نیازمند تبیین مبانی مشروعیت و حدود مسئولیت حکومت بر اساس فقه اسلامی است. این امر بهره‌گیری از چهارچوب فقه حکومتی را ضروری می‌سازد. پرسش اصلی پژوهش آن است که حکومت اسلامی بر اساس فقه حکومتی چه مسئولیتی در قبال توسعه و تنظیم بیمه سایبری دارد؟ پرسش‌های فرعی شامل اثبات مالیت دارایی‌های دیجیتال، مشروعیت عقد بیمه سایبری، چالش‌های فقهی خاص (باج‌افزار، سود منتفی، خطای هوش مصنوعی) است. فرضیه آن است که تأمین امنیت سایبری ذیل تکلیف حفظ نظام، مسئولیتی ذاتی برای حکومت است و مداخله آن در ساماندهی بیمه سایبری مشروع و ضروری می‌باشد.

مرور پیشینه پژوهش نشان می دهد که مطالعات پیشین به چند دسته تقسیم می‌شوند. بهمن‌پوری و همکاران (۱۳۹۳) با رویکرد فقهی فردمحور به تحلیل بیمه و اثبات مالیت داده‌های رایانه‌ای پرداخته‌اند. السان و همکاران (۱۳۹۵) و نیز آدریکو و نرس (۲۰۲٤)، بیمه سایبری را صرفاً ابزاری برای مدیریت ریسک معرفی کرده‌اند. محمد (۲۰۲۱) از منظر مقاصد شریعت بر ضرورت امنیت سایبری تأکید داشته است. همچنین ایزدهی و صدیق‌پور (۱۳۹۹) در ادبیات فقه حکومتی به تبیین مبانی این دانش پرداخته‌اند. بااین‌حال، هیچ‌یک از این پژوهش‌ها به تحلیل مسئولیت حکومت در قبال بیمه سایبری بر اساس نظریه ولایت مطلقه فقیه نپرداخته‌اند و شکاف اصلی در همین نقطه باقی است. پژوهش حاضر با آگاهی از اینکه صرف اثبات مشروعیت کلی کافی نیست بلکه تحلیل فقه حکومتی نیازمند فهم دقیق انواع ریسک‌ها، ساختار پوشش‌ها، شرایط بیمه‌نامه‌ها، مطالعه تطبیقی و وضعیت حقوق ایران است. ازاین‌رو، ابتدا این لایه‌های تخصصی تبیین شده و سپس مسئولیت حکومت تحلیل می‌گردد. روش پژوهش توصیفی-تحلیلی با گردآوری کتابخانه‌ای است. نوآوری این مقاله در پر کردن این شکاف و ارائه تحلیلی سه سطحه است؛ نخست سطح نظری که عبارت است از استفاده از مبانی فقه حکومتی برای استنتاج مسئولیت ذاتی حکومت در

تأمین امنیت سایبری، دوم؛ سطح میانی که تحلیل حدود و اختیارات حکومت در این عرصه است و درنهایت سطح کاربردی به معنای طراحی الگویی برای مداخله مشروع حکومت در زمینه بیمه سایبری است.

## ۱. مفهوم‌شناسی بیمه سایبری

پیش از تحلیل مبانی مشروعیت مداخله حکومت اسلامی در عرصه بیمه سایبری، تبیین روشن مفاهیم پایه‌ای مرتبط با موضوع ضروری است. درک دقیق این مفهوم که به‌عنوان پوششی در برابر ریسک‌ها و خسارات ناشی از تهدیدات فضای مجازی طراحی شده، پیش‌نیاز ضروری برای بررسی مبانی فقهی و حقوقی مسئولیت حکومت در تنظیم، نظارت و حمایت از این حوزه نوین بیمه‌ای محسوب می‌شود.

### ۱-۱. مفهوم بیمه سایبری، کارکرد و سیر تحول

بیمه سایبری، به‌عنوان پاسخی حقوقی و اقتصادی به چالش‌های پیچیده فضای مجازی، نهادی نوظهور و ابزاری کلیدی در مدیریت ریسک‌های عصر دیجیتال است. این سازوکار فراتر از یک قرارداد جبران خسارت ساده، به‌مثابه یک سامانه جامع مدیریت ریسک عمل می‌کند که ضمن ارائه پوشش مالی، خدمات مشاوره‌ای پیشگیرانه و مدیریت بحران را نیز عرضه می‌دارد و درنهایت به افزایش تاب‌آوری سایبری بنگاه‌ها و نهادهای اقتصادی می‌انجامد *(السان، ۱۳۹۱؛ پژوهشکده بیمه، ۱۴۰۲)*.

از منظر تعریف، بیمه سایبری به پوشش‌هایی اطلاق می‌شود که با هدف محافظت در برابر خسارات مالی ناشی از حوادثی چون سرقت اطلاعات، نقض حریم خصوصی، اختلال در سرویس‌ها و عملیات بازیابی داده‌ها طراحی شده‌اند *(پورقصاب امیری و حسنی کاخ، ۱۳۹۷)*. به بیان دقیق‌تر، این بیمه به‌طور خاص جهت جبران هزینه‌های مرتبط با حوادث امنیتی نظیر سرقت اطلاعات، نقض حریم خصوصی، اختلال در سرویس‌های برخط و عملیات بازگردانی داده‌ها ارائه می‌گردد. سازوکار اصلی آن، تبدیل ریسک‌های غیرقطعی و فاجعه‌بار سایبری به هزینه‌های قابل پیش‌بینی و مدیریت‌شده است که به ایجاد یک تنظیم‌گر غیرمستقیم بازار و تسهیل توسعه امن دیجیتال منجر می‌شود *(Adricko & Ners, 2024)*.

لارنس گوردون[5]، بیمه سایبری را یک روش و سیاست و همچنین ابزاری راهبردی برای مدیریت ریسک‌های سایبری عنوان می‌نماید *(Böhme, 2015)*. با افزایش وابستگی روزافزون سازمان‌ها به فناوری‌های دیجیتال، به‌ویژه در صنایع حساسی مانند بانکداری، سلامت و تجارت الکترونیک، نیاز به این نوع بیمه شدت یافته است. مطالعات نشان می‌دهد کسب‌وکارها با بهره‌گیری از بیمه سایبری نه‌تنها می‌توانند خسارات مالی ناشی از حملات را مدیریت کنند بلکه از طریق مشاوره‌های پیشگیرانه و ارائه راه‌حل‌های امنیتی که برخی بیمه‌گران ارائه می‌دهند، ابزارهایی برای بهبود زیرساخت‌های امنیتی خود نیز به‌دست می‌آورند. این امر به ایجاد یک پیامد خارجی مثبت و ارتقای کلی امنیت فضای مجازی می‌انجامد *(پورقصاب امیری و حسنی کاخ، ۱۳۹۷)*.

به‌بیان‌دیگر، بیمه فضای مجازی به‌عنوان یک پوشش بیمه‌ای، از فعالیت‌های تجارت الکترونیک در برابر خسارت‌های ناشی از دسترسی‌های غیرمجاز، دزدی داده‌ها، اختلال در سرویس (مانند حملات انکار سرویس)[6]، ویروس‌های یارانه‌تری و تراکنش‌های الکترونیکی غیرقانونی محافظت می‌کند. درحقیقت، این بیمه‌نامه‌ها هم از خسارات وارده به شخص اول (بیمه‌گذار) و هم از مسئولیت‌های وی در قبال اشخاص ثالث حمایت می‌کنند و از سوی بیمه‌گران با هدف هماهنگی انگیزه‌های بازار برای بهبود امنیت اینترنتی ارائه می‌شوند *(Majuca, Yurcik & Kesan, 2016)*.

شرکت‌های ارائه‌دهنده این خدمت می‌توانند در قالب سازمان‌های دولتی، ارائه‌دهندگان خدمات اینترنتی یا شرکت‌های بیمه خصوصی/عمومی فعالیت نمایند. به‌طور کلی، بیمه‌های سایبری به‌عنوان یکی از راهبردهای کلیدی کسب‌وکارها، نقش مهمی در مدیریت ریسک سازمانی ایفا کرده و مزایایی چون ارتقای آگاهی از تهدیدات، کمک به بهبود سیستم‌های امنیتی، تشویق به سرمایه‌گذاری در کاهش ریسک و ارائه پشتیبانی تخصصی برای پاسخ به حوادث را به همراه دارند. رشد چشمگیر و تطبیق مستمر این بیمه‌نامه‌ها با ریسک‌های پویای سایبری، گواه اهمیت فزاینده آن در مدیریت ریسک دنیای دیجیتال است *(پژوهشکده بیمه، ۱۴۰۲، صص. ۷۱-۶۹)*.

---

5. Lawrence Gordon
6. Denial of Service (DoS)

سیر تحول تاریخی بیمه سایبری نیز نشان‌دهنده تعامل پویای فناوری، تهدیدات و مقررات است. ظهور اولیه آن در دهه ۱۹۹۰ همزمان با گسترش اینترنت تجاری بود *(Springer, 2015)*. در دهه ۲۰۰۰ حوادثی مانند حمله به یاهو [۷] و پیامدهای یازدهم سپتامبر، و در دهه ۲۰۱۰ تصویب قوانینی مانند آیین‌نامه حفاظت از داده‌های عمومی اتحادیه اروپا[۸] (GDPR)و حملات بزرگی مانند نقض داده در فروشگاه تارگت[۹]، تقاضا برای این بیمه را افزایش داد *(Fitch Ratings, 2022)*. در دهه اخیر نیز همه‌گیری حملات باج‌افزاری[۱۰] به محرک اصلی رشد بازار تبدیل شده است.

در جهان اسلام، کشورهایی مانند امارات و عربستان با تدوین چهارچوب‌های قانونی زودهنگام پیشتاز بوده‌اند، درحالی‌که مدل اسلامی «تکافل سایبری» نیز در کشورهایی مانند مالزی و بحرین در حال گسترش است. در ایران، فعالیت رسمی از دهه ۱۳۹۰ آغاز شده؛ اما توسعه بازار نیازمند تقویت چهارچوب‌های قانونی و افزایش آگاهی عمومی است *(کنفرانس ملی امنیت سایبری، ۱۴۰۰)*.

## ۱-۲. گونه‌شناسی و دسته‌بندی ریسک‌های سایبری: از واقعیت عینی تا چهارچوب تحلیلی (فنی، امنیتی، قانونی، اعتباری)

گسترش فضای سایبری و اقتصاد دیجیتال، گونه‌های جدیدی از ریسک را پدید آورده که حیات اقتصادی، اجتماعی و امنیت ملی را تهدید می‌کنند. این ریسک‌ها در قالب تهدیدات متنوعی ظاهر می‌شوند که برای تحلیل دقیق موضوع و طراحی پوشش‌های بیمه‌ای مناسب، نیازمند یک چهارچوب تحلیلی جامع و در عین حال توجه به واقعیت‌های عینی در سطوح جهانی و ملی است.

آمارهای جهانی و داخلی نشان‌دهنده روند افزایشی و تأثیرات ویرانگر تهدیدات سایبری در سطوح مختلف، از کسب‌وکارهای کوچک تا امنیت ملی است. بر اساس گزارش بارومتر

7. Yahoo
8. General Data Protection Regulation
9. Target Data Breach
10. Ransomware

ریسک آلیانز [11]۲۰۲٤، ریسک‌های سایبری برای چهارمین سال متوالی بزرگترین نگرانی جهانی کسب‌وکارها باقی مانده است، به‌طوری‌که ۳٦درصد از پاسخ‌دهندگان آن را مهم‌ترین ریسک دانسته‌اند *(Allianz Risk Barometer, 2024)*. گزارش هزینه نقض داده آی بی ام در سال ۲۰۲۳ میانگین هزینه جهانی یک نقض داده را ٤.٤٥ میلیون دلار اعلام کرده که نسبت به سال قبل ٪۱۵ افزایش یافته است *(IBM, 2023)*[12]. همچنین گزارش کروداسترایک نشان می‌دهد که حملات به زنجیره تأمین در سال ۲۰۲۳ چهل درصد افزایش یافته و مهاجمان به طور فزاینده‌ای از روش‌های پیچیده‌تری برای هدف قرار دادن تأمین‌کنندگان استفاده می‌کنند *(CrowdStrike, 2024)*. در حوزه جنگ سایبری نیز گزارش دفاع دیجیتال مایکروسافت[13] ۲۰۲۳ نشان می‌دهد که ۵۸درصد از حملات سایبری شناسایی‌شده توسط دولت‌ها انجام شده و ٤۰درصد از این حملات زیرساخت‌های حیاتی را هدف قرار داده‌اند *(Microsoft, 2023)*. این آمارها بیانگر دغدغه مداوم و رو به رشد در مواجهه با تهدیدات سایبری است.

ایران نیز به‌عنوان یک بازیگر فعال در عرصه دیجیتال و با موقعیت ژئوپلیتیک خاص خود، با حجم قابل‌توجهی از تهدیدات سایبری مواجه است. بر اساس گزارش مرکز ملی فضای مجازی، در سال ۱٤۰۲ بیش از ۹۵۰۰ حمله سایبری دفع شده و رشد ۱۸ درصدی جرائم سایبری نسبت به سال قبل گزارش شده است *(مرکز ملی فضای مجازی، ۱٤۰۲)*. کلاهبرداری اینترنتی با افزایش ٤۲ درصدی نسبت به سال ۱٤۰۱، همچنان صدرنشین جرایم سایبری در ایران بوده است *(پلیس فتا، ۱٤۰۲)*. سهم حملات فیشینگ یا مهندسی اجتماعی در ایران بین ٦۵ تا ۷۰ درصد از کل حملات برآورد می‌شود که رقمی بسیار بالاتر از میانگین جهانی است. هزینه حملات سایبری در ایران دو برابر عربستان و چهار برابر امارات تخمین زده شده است *(پژوهشکده بیمه، ۱٤۰۲)*. بااین‌حال، ضریب نفوذ بیمه سایبری در کشور کمتر از ۲ درصد برآورد می‌شود *(فتاحی زفرقندی و کلانتری، ۱٤۰۳)*. فقدان یک نظام شفاف و جامع برای ثبت و پایش حملات سایبری، مانع از دستیابی به تصویری دقیق از

11. Allianz Risk Barometer
12. IBM Cost of a Data Breach Report
13. Microsoft Digital Defense Report

دامنه و هزینه‌های واقعی این تهدیدات شده است. عواملی همچون محدودیت‌های ناشی از تحریم‌های بین‌المللی، استفاده از نرم‌افزارهای غیررسمی و فاقد پشتیبانی امنیتی، فرسودگی تجهیزات زیرساختی، و ضعف در همکاری‌های فرامرزی، نه‌تنها آسیب‌پذیری‌های امنیتی را تشدید کرده، بلکه بر پیچیدگی و هزینه‌های پنهان مقابله با آن‌ها افزوده است. از سوی‌دیگر، بازار بیمه‌های سایبری در ایران، علیرغم رشد چشمگیر این صنعت در سطح جهانی، هنوز در مراحل اولیه و غیرفعال باقی مانده است. این رکود را می‌توان حاصل یک دور باطل دانست: از یک‌سو، نبود داده‌های شفاف و قابل اتکا درباره خسارات، شرکت‌های بیمه را در طراحی و قیمت‌گذاری محصولات مناسب دچار تردید می‌کند و از سوی‌دیگر، همین نبود محصولات بیمه‌ای استاندارد و فرهنگ‌سازی نشدن در میان بنگاه‌ها، موجب شده تا تقاضای مؤثری در بازار شکل نگیرد.

پیش از دسته‌بندی ریسک‌ها، تبیین سلسله‌مراتب مفاهیم پایه ضروری است. بر اساس استاندارد بین‌المللی ISO/IEC 27000:2011، مفاهیم کلیدی امنیت اطلاعات در یک سلسله‌مراتب منطقی قرار می‌گیرند که در حوزه سایبری نیز قابل‌تعمیم است. تهدید سایبری به هر اقدام بالقوه یا بالفعل گفته می‌شود که با سوءاستفاده از آسیب‌پذیری‌های سیستم‌های اطلاعاتی، قصد وارد آوردن آسیب به دارایی‌های دیجیتال (داده‌ها، سیستم‌ها، شبکه‌ها) یا اختلال در خدمات را دارد. خالقی‌دخت تهدید سایبری را به‌عنوان «هر عامل داخلی یا خارجی که دارای قابلیت و نیت برای نقض خط‌مشی امنیتی یک دارایی سایبری باشد» تعریف می‌کند *(خالقی‌دخت، ۱۴۰۱، صص. ۵۱-۵۰)*. حادثه سایبری تحقق عملی یک تهدید است؛ رویدادی که منجر به نقض امنیت اطلاعات، اختلال در دسترسی یا عملکرد، یا آسیب به یک سیستم اطلاعاتی می‌شود *(NIST, 2018)*[14]. ریسک سایبری نیز ترکیبی از احتمال وقوع یک حادثه سایبری و شدت پیامدهای مالی، عملیاتی، اعتباری یا قانونی ناشی از آن است. الینگ و اشنل در مطالعه خود بر روی ریسک‌های سایبری در صنعت بیمه، تأکید می‌کنند که ریسک سایبری دارای ویژگی‌های منحصربه‌فردی از جمله وابستگی متقابل سیستم‌ها، سرعت انتشار و دشواری در ارزیابی خسارت است *(Eling & Schnell, 2016)*.

14. NIST (National Institute of Standards and Technology)

برای درک عمیق‌تر ماهیت تهدیدات و فراهم آوردن بستر لازم برای دسته‌بندی ریسک‌ها، می‌توان تهدیدات را بر اساس سه معیار اصلی طبقه‌بندی کرد:

نخست، بر اساس سطح پیچیدگی و توان مهاجم: تهدیدهای گزنده با پیچیدگی پایین و انگیزه فرصت‌طلبی (مانند اسکریپت‌کیدی، اسپم و اسکن خودکار) که تأثیر مالی آن‌ها معمولاً زیر ۱۰,۰۰۰ دلار است؛ تهدیدهای مجرمانه با پیچیدگی متوسط تا بالا و انگیزه منفعت مالی (مانند باج‌افزار، بدافزارهای بانکی و فیشینگ هدفمند) که تأثیر مالی آن‌ها بین ۱۰,۰۰۰ تا یک میلیون دلار است؛ و تهدیدهای پیشرفته پایدار با پیچیدگی بسیار بالا و اهداف راهبردی (مانند حملات به زیرساخت‌های حیاتی و سرقت مالکیت فکری) که تأثیر مالی آن‌ها میلیون‌ها تا میلیاردها دلار برآورد می‌شود *(McAfee, 2024; Verizon DBIR, 2024)*.

دوم، بر اساس منشأ تهدید: تهدیدهای داخلی ناشی از افراد دارای دسترسی مجاز به سیستم‌ها (کارکنان، پیمانکاران، شرکا) که به دو دسته عمدی (با سوءنیت) و غیرعمدی (ناشی از بی‌دقتی یا خطا) تقسیم می‌شوند؛ و تهدیدهای خارجی از سوی عوامل خارج از سازمان (هکرها، گروه‌های مجرمانه، دولت–ملت‌ها) که معمولاً پیچیده‌تر و با انگیزه‌های متنوع‌تری همراه هستند. برک در تحلیل خود از تهدیدات سایبری علیه زیرساخت‌های حیاتی، نشان می‌دهد که تهدیدات خارجی سازمان‌یافته بیشترین آسیب‌پذیری را برای سیستم‌های کنترل صنعتی ایجاد می‌کنند *(Cremer et al., 2022)*.

سوم، بر اساس عامل تهدید: این طبقه‌بندی که توسط پژوهشکده بیمه در گزارش تحلیل ریسک‌های سایبری ارائه شده، بر اساس ماهیت و انگیزه عامل تهدید انجام می‌شود و شامل هکرهای کلاه سفید (با انگیزه آزمون امنیت)، هکرهای کلاه سیاه (با انگیزه منفعت مالی یا تخریب)، هکتیویست‌ها (با انگیزه ایدئولوژی یا اعتراض سیاسی)، مجرمان سایبری سازمان‌یافته (با هدف درآمدزایی در مقیاس بزرگ)، و دولت–ملت‌ها (با اهداف جاسوسی یا برهم‌زدن ثبات) است. این طبقه‌بندی برای صنعت بیمه حیاتی است؛ زیرا بیمه‌پذیری هر یک متفاوت است؛ برای‌نمونه، حملات دولت–ملت‌ها معمولاً مستثنی از پوشش بیمه‌ای است *(پژوهشکده بیمه، ۱۴۰۲)*.

اکنون با اتکا بر واقعیت‌های عینی، چهارچوب مفهومی و گونه‌شناسی تحلیلی پیش‌گفته، می‌توان ریسک‌های سایبری را که مبنای طراحی پوشش‌های بیمه‌ای قرار می‌گیرند، در

چهار دسته اصلی طبقه‌بندی کرد:

دسته اول: ریسک‌های فنی. این دسته شامل ریسک‌های ناشی از خرابی زیرساخت، از دست‌دادن داده‌ها، اختلال در سرویس (مانند حملات انکار سرویس)، ویروس‌های رایانه‌ای، کرم‌های اینترنتی، و تزریق اس کیو ال[۱۵] است. همچنین تهدیدات مبتنی بر هوش مصنوعی که برای تولید فیشینگ پیشرفته، دور زدن سیستم‌های تشخیص و بهینه‌سازی حملات به کار می‌روند، در این دسته جای می‌گیرند. این ریسک‌ها عمدتاً با معیارهای فنی قابل ارزیابی هستند و قابلیت اندازه‌گیری خسارت در آن‌ها بالاست.

دسته دوم: ریسک‌های امنیتی. این دسته شامل حملات باج‌افزاری (رمزارگذاری داده‌ها و درخواست باج برای بازگردانی)، نقض گسترده داده‌ها، دسترسی‌های غیرمجاز، جاسوس‌افزار، تروجان، و حملات پیشرفته پایدار می‌شود. بر اساس گزارش‌ها، حدود ۲٤ درصد از حوادث امنیتی مرتبط با بدافزار با باج‌خواهی همراه است. همچنین جرائم سایبری به‌عنوان سرویس که در آن ابزارها و خدمات هک در بازار سیاه به مجرمان کم‌تجربه فروخته می‌شود، از مصادیق نوظهور این دسته است. حملات به زنجیره تأمین مانند حادثه سولار ویندز ۲۰۲۰[۱۶] که از طریق به‌روزرسانی نرم‌افزار قانونی صورت گرفت، نیز در این دسته قرار می‌گیرد.

دسته سوم: ریسک‌های قانونی و نظارتی. این ریسک‌ها ناشی از نقض قوانین حفاظت از داده، مسئولیت در قبال اشخاص ثالث، و الزامات قانونی پس از وقوع حادثه است. تصویب قوانینی مانند آیین‌نامه حفاظت از داده‌های عمومی اتحادیه اروپا (GDPR)[17] نمونه بارزی از چهارچوب‌های قانونی است که عدم رعایت آن‌ها می‌تواند به جریمه‌های سنگین منجر شود. در ایران نیز خلأ چهارچوب‌های قانونی مشخص در حوزه بیمه سایبری، خود یک ریسک نظارتی محسوب می‌شود.

دسته چهارم: ریسک‌های اعتباری. این ریسک‌ها به آسیب به شهرت، برند و اعتماد عمومی نسبت به یک مؤسسه پس از وقوع حادثه امنیتی مربوط می‌شود؛ برای‌نمونه، حملات

15. SQL Injection
16. SolarWinds
17. General Data Protection Regulation (GDPR)

هکتیویست‌ها با هدف افشای اطلاعات یا اختلال در سرویس می‌تواند اعتماد مشتریان را به شدت خدشه‌دار کند. این ریسک‌ها اگرچه غیرملموس‌تر از سایر ریسک‌ها هستند؛ اما تأثیر بلندمدت آن‌ها بر ارزش بازار و جایگاه رقابتی بنگاه‌ها قابل توجه است.

بیمه‌پذیری این ریسک‌های نوظهور منوط به احراز معیارهای مشخص حقوقی و فنی است. از منظر حقوق بیمه، ریسک باید دارای ویژگی‌هایی چون اتفاقی بودن، قابلیت ارزیابی و سنجش، و امکان پراکندگی در جامعه باشد تا از حالت سوداگری خارج شود. از نگاه فقهی نیز مشروعیت موضوع بیمه، شرط اولیه محسوب می‌شود *(بابایی، ۱۴۰۱)*. ریسک‌های سایبری با وجود پویایی ذاتی، به مدد پیشرفت مدل‌های ارزیابی کمی و کیفی (مانند تحلیل آمارهای تاریخی و بررسی‌های تخصصی امنیتی) به‌تدریج در حال عبور از ابهام مطلق و واجد شرایط بیمه‌پذیری شدن هستند.

معیارهای عینی نیز در تصمیم بیمه‌گر برای پذیرش یا قیمت‌گذاری این ریسک‌ها تأثیر مستقیم دارند. بر اساس پژوهش‌های داخلی، عواملی مانند میزان آمادگی امنیتی سازمان، رعایت استانداردهایی چون رمزنگاری و فایروال[18]، و قابلیت اندازه‌گیری خسارت، ازجمله این معیارها هستند. به‌عبارت‌دیگر، شرکت‌هایی که سطح حفاظتی بالاتری دارند، ریسک کمتری محسوب شده و شانس بیشتری برای دریافت پوشش بیمه‌ای با شرایط مطلوب خواهند داشت *(صابری، ۱۳۹۹؛ حسن‌پور و اولوخانی، ۱۴۰۰)*. این ارزیابی علمی، پایه شکل‌گیری قرارداد بیمه سایبری را تشکیل می‌دهد.

درک دقیق از گونه‌شناسی تهدیدات برای دو حوزه حیاتی است: در مدیریت ریسک سازمانی، طبقه‌بندی تهدیدات کمک می‌کند تا احتمال وقوع و شدت تأثیر هر نوع حادثه برآورد شود. فتاحی زفرقندی و کلانتری نشان داده‌اند که طبقه‌بندی دقیق تهدیدات دقت ارزیابی ریسک را تا ۴۰درصد افزایش می‌دهد *(فتاحی زفرقندی و کلانتری، ۱۴۰۳)*. در صنعت بیمه سایبری نیز شرکت‌های بیمه‌گر با درک انواع تهدیدات می‌توانند پوشش‌های اختصاصی طراحی کنند و محدودیت‌ها و استثنائات پوشش بیمه‌ای را بر اساس نوع تهدید تعریف نمایند.

18. Firewall

نکته کلیدی آنکه فقدان داده‌های شفاف درباره توزیع انواع تهدیدات و الگوی خسارات ناشی از آن‌ها در ایران دقیقاً بر همین نقطه تأثیر می‌گذارد: بیمه‌گران نمی‌توانند بر اساس طبقه‌بندی دقیق تهدیدات، محصولات متناسب طراحی کنند و بیمه‌گذاران نیز درک درستی از ریسک‌های واقعی خود ندارند. پژوهشکده بیمه در گزارش اولیه خود درباره بیمه سایبری در ایران، به این چالش به‌عنوان یکی از موانع اصلی توسعه این بیمه‌نامه اشاره کرده است *(پژوهشکده بیمه، ۱۳۹۳)*. درنهایت، شناخت دقیق این تهدیدات و تحلیل معیارهای بیمه‌پذیری آن‌ها، مقدمه‌ای ضروری برای بررسی فقهی ماهیت مسئولیت‌های مدنی نوین و حدود ضمان در فضای سایبر است. این درک، شالوده‌ای برای تعیین تکلیف حکومت در قبال ساماندهی این عرصه فراهم می‌آورد.

### ۱-۳. پوشش‌های بیمه‌ای (شخص اوّل، شخص ثالث، وقفه کسب‌وکار)

پیش از ورود به جزئیات پوشش‌های بیمه سایبری، ذکر این نکته ضروری است که طراحی این پوشش‌ها مستلزم شناخت معیارهای بیمه‌پذیری ریسک‌های سایبری است. در حقوق بیمه، ریسک واقعه‌ای است اتفاقی و احتمالی که در آینده ممکن است رخ دهد و منشأ ایراد خسارت خواهد بود. موضوع عقد بیمه، همین خطر یا ریسک تحقق حادثه خسارت‌بار است. برای آنکه یک ریسک قابل بیمه شدن باشد، باید واجد شرایطی چون اتفاقی بودن، واقعی بودن، مشروع بودن، و قابلیت سنجش و ارزیابی باشد *(بابایی، ۱۴۰۱)*. ریسک‌های سایبری با ماهیت پویا و پیچیده خود، چالش‌های منحصربه‌فردی را برای اعمال این معیارهای سنتی ایجاد می‌کنند. مهم‌ترین چالش، ارزیابی دقیق احتمال وقوع و شدت خسارات است. پویایی سریع فناوری، ظهور مداوم تهدیدات جدید، و کمبود داده‌های تاریخی قابل‌اتکا به دلیل نوظهور بودن پدیده و تمایل قربانیان به عدم افشای کامل حوادث، این ارزیابی را دشوار می‌سازد *(Biener, Eling & Wirfs, 2015)*. بر اساس گزارش آژانس اتحادیه اروپا برای امنیت سایبری (۲۰۲۳)[۱۹]، یکی از موانع اصلی توسعه بازار بیمه سایبری در اروپا، فقدان پایگاه داده‌های استاندارد برای مدل‌سازی ریسک است. این چالش به‌ویژه در مقایسه با

19. European Union Agency for Cybersecurity (ENISA)

ریسک‌های سنتی مانند بلایای طبیعی که داده‌های تاریخی قرن‌ها از آن‌ها موجود است، برجسته‌تر می‌شود *(Boehme & Schwartz, 2010)*.

همچنین مرز بین حادثه اتفاقی و قصور یا سهل‌انگاری بیمه‌گذار در رعایت دستورالعمل‌های امنیتی، در حوزه سایبری بسیار مبهم است. بسیاری از حملات سایبری از طریق خطای انسانی یا ضعف‌های امنیتی داخلی رخ می‌دهند که می‌تواند ناشی از عدم رعایت استانداردهای حداقلی باشد. بر اساس گزارش مؤسسه پونمون و امنیت آی‌بی‌ام (۲۰۲۳)[۲۰]، خطای انسانی عامل اصلی در ۷٤ درصد از نقض‌های امنیتی است. شرکت‌های بیمه با درج شروط امنیتی مشخص در قراردادها و ارزیابی اقدامات احتیاطی بیمه‌گذاران، این چالش را مدیریت می‌کنند *(Kesan & Hayes, 2019)*. بازار لویدز لندن (۲۰۲۱)[۲۱] در دستورالعمل‌های بازار خود تصریح کرده که نقض شروط امنیتی می‌تواند منجر به تعلیق پوشش یا کاهش تعهد بیمه‌گر شود. وودز و بومه (۲۰۲۱) [۲۲]نشان دادند که بیمه‌گران سایبری پیشرو به‌طور فزاینده‌ای از ابزارهای ارزیابی فنی مستمر برای پایش وضعیت امنیتی بیمه‌گذار در طول دوره بیمه استفاده می‌کنند.

در زمینه قابلیت اندازه‌گیری خسارت نیز خسارات مستقیم ناشی از حملات سایبری مانند هزینه‌های بازیابی اطلاعات، پرداخت باج‌افزاری، یا تعمیر سیستم‌ها نسبتاً قابل اندازه‌گیری هستند؛ اما کمّی‌سازی خسارات غیرمستقیم مانند آسیب به شهرت، از دست دادن مزیت رقابتی، یا تأثیر بر ارزش سهام، با ابهامات حقوقی قابل توجهی مواجه است *(Camillo, 2017)*. بر اساس گزارش مؤسسه پونمون و امنیت آی‌بی‌ام (۲۰۲۳)، میانگین هزینه کلی یک نقض داده در سال ۲۰۲۳ به ٤.٤٥ میلیون دلار رسیده که بخش قابل‌توجهی از آن را خسارات غیرمستقیم تشکیل می‌دهد. مجمع جهانی اقتصاد (۲۰۲۳)[۲۳] تخمین می‌زند که خسارات ناشی از جرایم سایبری در سطح جهان تا سال ۲۰۲۵ به ۱۰.۵ تریلیون دلار سالانه خواهد رسید. قراردادهای بیمه سایبری با تعریف دقیق انواع خسارات تحت پوشش، تعیین سقف جبران خسارت برای هر نوع، و استفاده از روش‌های ارزیابی تخصصی مانند

20. Ponemon Institute and IBM Security
21. Lloyd's Market Association
22. Woods & Bome
23. World Economic Forum

کارشناسی‌های مستقل به کاهش این ابهام کمک می‌کنند *(Merkin & Steele, 2013)*. برخی قراردادها نیز خسارات غیرمستقیم را به طور صریح مستثنی می‌کنند یا پوشش محدودی برای آن‌ها در نظر می‌گیرند *(Swiss Re, 2020)*.

علاوه‌براین، ریسک سایبری دارای ظرفیت بالایی برای تبدیل شدن به ریسک نظام‌مند است. یک حمله سایبری واحد مانند حمله به زیرساخت‌های حیاتی یا یک سکو پرداخت گسترده می‌تواند به طور همزمان هزاران بیمه‌گذار در صنایع مختلف را تحت تأثیر قرار دهد که مدیریت ریسک انباشت را برای بیمه‌گران دشوار می‌سازد *(Cummins & Mahul, 2009)*. گزارش بازار لویدز لندن و مرکز مطالعات ریسک دانشگاه کمبریج (۲۰۱۷)[۲۴] نشان داد که یک حمله سایبری بزرگ به زیرساخت‌های ابری می‌تواند خسارات بیمه‌شده‌ای بین ٤.٦ تا ۵۳ میلیارد دلار ایجاد کند. مؤسسه سوئیس ری (۲۰۲۰)[۲۵] این نوع ریسک را به‌عنوان «ریسک انباشت سایبری» معرفی کرده و آن را یکی از بزرگ‌ترین چالش‌های صنعت بیمه در دهه آینده می‌داند. بیمه‌گران از طریق محدودیت‌های پوشش جمعی، بیمه‌گذاری مجدد، و ایجاد کنسرسیوم‌های تخصصی این ریسک را مدیریت می‌کنند *(Munich Re, 2023)*.

از منظر فقهی نیز برای اینکه خطری قابل بیمه شدن باشد، باید شرایطی چون اتفاقی بودن، مشروعیت موضوع، و معلوم بودن حدود تعهد احراز شود. در ریسک‌های سایبری، غرر می‌تواند در دو سطح ماهیت خطر و میزان خسارت بررسی شود. با این حال، فقهای قائل به صحت بیمه، با تغییر نگرش نسبت به موضوع اصلی معامله، اشکال غرر را رد می‌کنند: موضوع معامله، خود ریسک مجهول نیست، بلکه تعهد معلوم بیمه‌گر به جبران خسارت در صورت وقوع ریسک است. این تعهد، کالایی ارزشمند است که در برابر حق بیمه معلوم مبادله می‌شود. برای کاهش غرر و افزایش قابلیت بیمه‌پذیری ریسک‌های سایبری از منظر فقهی، راهکارهایی چون تعریف دقیق پوشش‌ها و استثنائات، استفاده از مدل‌های پیشرفته ارزیابی ریسک، مشارکت بیمه‌گذار در مدیریت ریسک، و تقسیم ریسک و بیمه‌گذاری مجدد قابل طرح است.

اکنون با عنایت به این چهارچوب، پوشش‌های بیمه سایبری عموماً حول دو محور اصلی

24. Lloyd's and University of Cambridge Centre for Risk Studies
25. Swiss Re

«خسارات شخص اول» و «مسئولیت‌های شخص ثالث» طراحی می‌شوند و ساختار آن‌ها در میان بیمه‌گران پیشرو از انسجام نسبی برخوردار است *(پژوهشکده بیمه، ۱۴۰۲؛ Miller, 2021; Romanosky et al., 2019)*.

**خسارات شخص اول**

این دسته از پوشش‌ها، خسارات مستقیمی را که به خود بیمه‌گذار وارد می‌شود جبران می‌کند و شامل موارد زیر است:

بازیابی داده و سیستم: هزینه‌های بازیابی، بازسازی یا جایگزینی داده‌ها و سیستم‌های الکترونیکی آسیب‌دیده پس از حمله سایبری یا خرابکاری دیجیتال، از اصلی‌ترین پوشش‌های شخص اول محسوب می‌شوند *(Miller, 2021)*. این پوشش به‌ویژه در مواجهه با حملات باج‌افزاری که داده‌ها را رمزگذاری یا نابود می‌کنند، اهمیت حیاتی دارد.

وقفه در کسب‌وکار: جبران درآمد از دست رفته و هزینه‌های اضافی عملیاتی در دوران توقف یا اختلال در فعالیت ناشی از حوادث سایبری. مؤسسه پونمون و امنیت آی‌بی‌ام (۲۰۲۳) گزارش می‌دهد که میانگین دوره شناسایی و مهار یک حمله سایبری ۲۷۷ روز است و خسارات وقفه در کسب‌وکار می‌تواند بخش عمده‌ای از کل خسارت را تشکیل دهد.

اخاذی سایبری: پوشش هزینه‌های مرتبط با باج‌افزار، شامل مبلغ باج پرداختی (مشروط به رعایت مقررات قانونی حاکم و اخذ موافقت قبلی بیمه‌گر) و هزینه‌های متخصصان مذاکره با باج‌خواهان. لازم به ذکر است که این پوشش در برخی حوزه‌های قضائی به دلیل مقررات مرتبط با تأمین مالی تروریسم با محدودیت‌های قانونی مواجه است *(کسان و هایز، ۲۰۱۹؛ بازار لویدز لندن، ۲۰۲۱)*.

هزینه‌های مدیریت بحران: این پوشش گسترده‌ترین بخش خسارات شخص اول است و شامل هزینه‌های استخدام متخصصان پاسخ به حادثه، وکلای تخصصی، حسابداران قضایی و مشاوران روابط عمومی برای کنترل بحران ناشی از حادثه می‌شود *(Miller, 2021؛ پژوهشکده بیمه، ۱۴۰۲)*.

**خسارات شخص ثالث (مسئولیت‌های بیمه‌گذار)**

این دسته، مسئولیت‌های قانونی بیمه‌گذار در قبال اشخاص ثالث آسیب‌دیده را پوشش می‌دهد:

مسئولیت حریم خصوصی و امنیت داده: پوشش هزینه‌های دفاع حقوقی، جریمه‌های نظارتی صادره توسط مراجع حمایت از داده (از جمله جریمه‌های مقرر در مقررات عمومی حفاظت از داده اتحادیه اروپا) و غرامت پرداختی به اشخاص ثالث به دلیل افشا، سرقت یا سوءاستفاده از داده‌های شخصی آنان. آژانس اتحادیه اروپا برای امنیت سایبری (۲۰۲۳) تأکید می‌کند که جریمه‌های ناشی از نقض مقررات حفاظت از داده می‌تواند تا ٤ درصد گردش مالی سالانه جهانی شرکت باشد.

مسئولیت رسانه‌های الکترونیکی: پوشش دعاوی مطروحه علیه بیمه‌گذار به دلیل انتشار محتوای برخط، ازجمله دعاوی افترا، توهین، نقض حق نشر، یا سوءاستفاده از نام دامنه *(السان، ۱۳۹۱؛ Miller, 2021)*.

مسئولیت امنیت شبکه: پوشش خسارات وارده به اشخاص ثالث به دلیل قصور بیمه‌گذار در تأمین امنیت کافی زیرساخت‌های خود، نظیر حالتی که سیستم‌های بیمه‌گذار به منبع حملات توزیع‌شده منع سرویس (DDoS) علیه سایرین تبدیل شوند *(Romanosky et al., 2019)*.

**پوشش‌های تکمیلی**

هزینه‌های اطلاع‌رسانی: بسیاری از نظام‌های حقوقی، از جمله مقررات عمومی حفاظت از داده اتحادیه اروپا و قوانین ایالتی ایالات متحده، سازمان‌ها را ملزم به اطلاع‌رسانی فوری به قربانیان نقض داده می‌کنند. این پوشش، هزینه‌های اجرای این تکلیف قانونی را جبران می‌کند *(پژوهشکده بیمه، ۱٤۰۲)*.

مالکیت فکری: برخی بیمه‌نامه‌های پیشرفته‌تر هم خسارات وارده به دارایی‌های فکری بیمه‌گذار در اثر جاسوسی سایبری یا سرقت اطلاعات را (پوشش شخص اول) و هم مسئولیت ناشی از ادعای نقض مالکیت فکری دیگران توسط بیمه‌گذار را (پوشش شخص ثالث) تحت پوشش قرار می‌دهند *(السان، ۱۳۹۱)*.

**استثنائات مهم بیمه سایبری**

هیچ بیمه‌نامه‌ای پوشش نامحدود ارائه نمی‌دهد و شناخت دقیق استثنائات برای ارزیابی میزان انتقال واقعی ریسک ضروری است. موارد زیر به طور معمول از شمول پوشش بیمه سایبری مستثنی هستند *(پژوهشکده بیمه، ۱٤۰۲؛ Swiss Re, 2020)*.

خسارات ناشی از جنگ و تروریسم سایبری، به‌ویژه عملیات سایبری دولت‌ها یا

گروه‌های تروریستی، از پوشش مستثنی است. این استثناء پس از حمله نات‌پتیا[۲۶] در سال ۲۰۱۷ به موضوع محل مناقشه جدی تبدیل شد. خساراتی که عمداً توسط خود بیمه‌گذار یا با همدستی او ایجاد شده‌اند نیز تحت پوشش نیستند. همچنین حملاتی که قبل از تاریخ شروع یا در دوره انتظار قرارداد رخ داده‌اند، آسیب به اموال فیزیکی یا صدمات جسمانی که معمولاً تحت بیمه‌نامه‌های مسئولیت عمومی یا مالکیت پوشش داده می‌شوند، هزینه‌های بهبود یا ارتقاء سیستم‌ها به سطحی بالاتر از وضعیت قبل از حادثه، خسارات ناشی از عدم تهیه نسخه پشتیبان مناسب از داده‌ها که نشانه‌ای از قصور بیمه‌گذار تلقی می‌شود، برخی جریمه‌های تنبیهی دولتی بسته به قانون حاکم، و خسارات ناشی از قطعی گسترده اینترنت، برق یا سایر خدمات زیرساختی که خارج از کنترل بیمه‌گذار است، از دیگر استثنائات رایج به‌شمار می‌روند.

شایان ذکر است که استثناء «جنگ سایبری» پس از رأی دیوان عالی آمریکا در پرونده مرک علیه ایس آمریکن اینشورنس (۲۰۲۳)[۲۷] که بیمه‌گر را ملزم به پرداخت خسارات حمله نات‌پتیا کرد، بازتعریف قابل‌توجهی در بازارهای بیمه‌ای جهان داشته است *(بازار لویدز لندن، ۲۰۲۱)*.

بیمه سایبری پاسخی بازارمحور به نیاز فزاینده مدیریت ریسک‌های نوظهور دیجیتال است. اگرچه تطبیق کامل ریسک سایبری با معیارهای کلاسیک بیمه‌پذیری با چالش‌هایی مواجه است، با توسعه مدل‌های نوین ارزیابی ریسک، تعریف دقیق پوشش‌ها و استثنائات، و الزام بیمه‌گذاران به ارتقاء مستمر سطح امنیتی خود، این بیمه در حال تبدیل شدن به رکنی مکمل در راهبرد جامع امنیت سایبری سازمان‌ها است *(Munich Re, 2021)*. این جایگاه، بستر لازم را برای طرح پرسش‌های فقهی درباره مشروعیت، شرایط و حدود مسئولیت در این عقد نوین فراهم می‌آورد.

## ۱-۴. تحلیل فنی-حقوقی انواع ریسک‌ها و پوشش‌های بیمه سایبری

پس از تشریح ساختار پوشش‌های بیمه سایبری در بخش پیشین، اکنون لازم است این پوشش‌ها از منظر فنی-حقوقی تحلیل شوند. با توجه به آنکه بحث فقه حکومتی بایستی از

26. NotPetya Attack
27. Merck v. ACE American Insurance

سطح کلیات فراتر رفته و ناظر به واقعیات عینی بازار بیمه باشد، ضروری است ریسک‌های سایبری را بر اساس قابلیت بیمه‌پذیری دسته‌بندی کرده و مبنای حقوقی و فقهی هر دسته را بررسی نمود. بر اساس مطالعات معتبر بین‌المللی (*Adriko & Nurse, 2024; Woods & Simpson, 2017*)، ریسک‌های سایبری به چهار دسته با قابلیت بیمه‌پذیری متفاوت تقسیم می‌شوند:

دسته اول: ریسک‌های شخص اول. این دسته شامل هزینه‌های بازیابی داده‌ها، وقفه در کسب‌وکار، باج‌افزاری و هزینه‌های پاسخ به حادثه می‌شود. این ریسک‌ها بالاترین قابلیت بیمه‌پذیری را دارند؛ زیرا تصادفی، قابل اندازه‌گیری و قابل توزیع هستند. از منظر فقهی، مشمول قاعده «لاضرر» و «تسبیب» بوده و بیمه آن با رویکرد «التزام به جبران خسارت» (*خمینی، ۱٤۳٤ق، ص. ٦٤٦*) منطبق است.

دسته دوم: ریسک‌های شخص ثالث. این دسته شامل مواردی مانند افشای داده‌های مشتریان، نقض حریم خصوصی و مسئولیت مدنی ناشی از انتشار محتوای مجرمانه می‌شود. این ریسک‌ها قابلیت بیمه‌پذیری متوسطی دارند؛ زیرا پیش‌بینی میزان خسارت وارده به اشخاص ثالث دشوارتر است. از دیدگاه فقهی، این دسته نیازمند تحلیل دقیق قاعده «اتلاف» و «تسبیب» در فضای مجازی است (*انصاری، ۱٤۱۰ق، ج۱۰، ص. ۵۸*).

دسته سوم: ریسک‌های سایبری-فیزیکی. این دسته شامل مواردی مانند هک تأسیسات صنعتی، نیروگاه‌ها یا تجهیزات پزشکی متصل به شبکه می‌شود. به دلیل تداخل با بیمه‌نامه‌های سنتی (مانند آتش‌سوزی یا ماشین‌آلات)، قابلیت بیمه‌پذیری پایینی دارند و نیازمند طراحی پوشش‌های ترکیبی هستند.

دسته چهارم: ریسک‌های سیستمی. این دسته شامل حملات هماهنگ به زیرساخت ابری، قطع گسترده اینترنت یا خرابی نرم‌افزارهای حیاتی در سطح ملی می‌شود. این ریسک‌ها کمترین قابلیت بیمه‌پذیری را دارند؛ زیرا اصل پراکندگی ریسک (قانون اعداد بزرگ) در آن‌ها نقض می‌شود. در این موارد، مداخله مستقیم حکومت از طریق صندوق‌های تضمین دولتی ضروری می‌گردد (*Woods & Simpson, 2017*).

این دسته‌بندی چهارگانه نشان می‌دهد که بازار بیمه به‌تنهایی قادر به پوشش تمامی

ریسک‌های سایبری نیست و در دو دسته اخیر (ریسک‌های سایبری-فیزیکی و سیستمی)، حضور تنظیم‌گر حکومتی و طراحی ابزارهای مکمل مالی ضرورت می‌یابد. این ضرورت، مبانی فقهی مسئولیت حکومت اسلامی در ساماندهی بیمه سایبری را که در مباحث آتی بررسی خواهد شد، از منظر اقتصادی-حقوقی نیز تأیید می‌کند.

## ۲. مبانی فقهی مشروعیت بیمه سایبری

پذیرش و نهادینه‌سازی این ابزار نوین در نظام حقوقی جمهوری اسلامی ایران که ریشه در شریعت اسلام و فقه امامیه دارد مستلزم بررسی و تدقیق مبانی فقهی آن در دو سطح اساسی است: نخست اثبات مالیت موضوع یعنی دارایی‌های سایبری و دوم احراز مشروعیت خود عقد بیمه سایبری.

### ۲-۱. مالیت دارایی‌های دیجیتال (با تأکید بر آرای امام خمینی و شهید صدر)

در منظومه فقه امامیه مال به چیزی اطلاق می‌شود که دارای ارزش اقتصادی بوده و نزد عقلا دارای ارزش مبادله‌ای باشد و شارع مقدس نیز استفاده از آن را حلال بداند. شیخ انصاری در کتاب المکاسب دو معیار کلیدی منفعت مقصود عقلایی و حلال بودن در شرع را به‌عنوان شرط تحقق مالیت برمی‌شمارد *(انصاری، ۱٤۱۰ق، ص. ۵۸)*. تطبیق این معیارهای دیرپا و استوار بر دارایی‌های سایبری نشان می‌دهد که به ویژه داده‌های تولیدی و فعالیت‌محور مانند نرم‌افزارهای تخصصی پایگاه‌های داده پیچیده و محتوای دیجیتال دارای ارزش اقتصادی واجد منفعت مقصود عقلایی و نزد عرف امروز به‌شدت مورد رغبت و دادوستد هستند و بنابراین واجد مالیت عرفی می‌باشند.

شهید صدر در تحلیل اقتصادی خود با تأکید بر ذاتاً اعتباری بودن مفهوم مالیت و نقش محوری مورد رغبت عقلا بودن و کمیابی *(صدر، ۱۳۸۹، ص. ۲۳)* و امام خمینی با تفکیک دقیق و راهگشای بین مالیت عرفی که ملاک آن صرفاً رغبت و پذیرش عقلاست و آثار شرعی مالیت که شارع می‌تواند آن را سلب یا تأیید کند *(خمینی، ۱۳۹۲، ص. ۱۰)*. راه را برای پذیرش مالیت دارایی‌های نوین بدون تن دادن به جمود بر اشکال ظاهری هموار ساخته‌اند. پژوهش‌های فقهی معاصر نیز بر این تطبیق و انطباق صحه گذاشته و مال بودن داده‌های

رایانه‌ای را با ملاک‌های فقهی سازگار دانسته‌اند *(بهمن‌پوری و همکاران، ۱۳۹۳)*؛ بنابراین با احراز مالیت عرفی دارایی سایبری و عدم وجود دلیل شرعی قطعی بر سلب کامل آثار مالیت از آن مانند حرمت ذاتی این دارایی‌ها می‌توان آنها را به‌عنوان موضوع مشروع قواعد ضمان اتلاف تسبیب و سایر تصرفات مالی از جمله عقد بیمه قرار داد.

## ۲-۲. مشروعیت عقد بیمه و مصادیق آن در فقه امامیه

نخستین فقیهی که به مسئله بیمه پرداخت، سیدمحمدکاظم یزدی (متوفای ۱۳۳۷ق) صاحب کتاب «عروه الوثقی» بود. ایشان در پاسخ به استفتائی درباره بیمه کالا و بیمه عمر، قرارداد بیمه را فاقد جهت شرعی دانسته و آن را باطل اعلام کرد (یزدی، ۱۳۸۱، ص. ۱۸۸). پس از ایشان، باب گفت‌وگو درباره بیمه گشوده شد و فقهای بعدی اگرچه هیچ‌یک از نظر مرحوم یزدی تبعیت نکرده و قرارداد بیمه را باطل ندانستند؛ اما درباره ماهیت آن دچار اختلاف‌نظر شدند.

در فقه معاصر امامیه، دیدگاه‌های مستحکمی نسبت به ماهیت و مشروعیت کلی عقد بیمه ارائه شده است. مواجهه فقهی با این پدیده جدید، منجر به شکل‌گیری چند دیدگاه کلی شده است. برخی فقها تلاش کردند بیمه را در قالب یکی از عقود رایج شرعی مانند ضمان *(حلی، ۱۳۸٤، ص. ۳٤)*، صلح *(صافی گلپایگانی، ۱٤۳۲ق، ص. ۲۸۸۵)*، هبه معوضه *(خویی، ۱٤۱۲ق، ص. ۵۵۳)*، جعاله *(حکیم، ۱۳۵۳، ص. ۱۵۳)* یا ترکیبی از چند عقد *(سند، ۱۳۹۷)* قرار دهند. برخی دیگر مانند آیت‌الله جوادی آملی آن را یک شرط یا تعهد ابتدایی می‌دانند *(جوادی آملی، ۱۳۹۱)*. بااین‌حال، دیدگاهی که امروزه از سوی بسیاری از فقهای معاصر پذیرفته شده، قائل به استقلال عقد بیمه است. این دیدگاه نخستین‌بار از سوی امام خمینی در دهه چهل شمسی مطرح شد و بر آن است که بیمه همانند بیع و اجاره، عقدی مستقل با احکام خاص خود است. امام خمینی به‌صراحت در تحریرالوسیله می‌فرمایند: «به نظر می‌رسد که بیمه عقدی مستقل است. آشکارتر آن است که این استقلال، از نوع ضمان عهده نیست بلکه از باب التزام به جبران خسارت است[۲۸]» *(خمینی، ۱٤۳٤ق، ص. ٦٤٦)*. این نظر توسط فقهایی چون آیت‌الله فاضل

۲۸. الظَّاهِرُ أَنَّ التَّأْمِينَ عَقْدٌ مُسْتَقِلٌ. وَمَا هُوَ الرَّائِجُ لَيْسَ صُلْحًا وَلَا هِبَةً مُعَوَّضَةً بِلَا شُبْهَةٍ، وَيُحْتَمَلُ أَنْ يَكُونَ ضَمَانًا بِعِوَضٍ، وَالْأَظْهَرُ أَنَّهُ مُسْتَقِلٌ لَيْسَ مِنْ بَابِ ضَمَانِ الْعُهْدَةِ، بَلْ مِنْ بَابِ الِالْتِزَامِ بِجَبْرِ الْخَسَارَةِ

لنکرانی که بیان می‌دارند «بیمه عقد مستقلی است و احکام خاص خود را دارد» *(فاضل لنکرانی، ۱۳۸۳، ص. ۲۹۳)* و آیت‌الله مکارم شیرازی نیز تأیید شده است *(مکارم شیرازی، ۱٤۲۷ق، ص. ٤۸۰)*.

مشروعیت این عقد مستقل، بر ادله عام شرعی نیز استوار است. مشروعیت این عقد مستقل، بر ادله عام شرعی نیز استوار است که در دو دسته ادله قرآنی و ادله روایی قابل دسته‌بندی بوده و در ادامه به اختصار تبیین می‌گردد.

عمومات و اطلاقات آیاتی از قرآن بر اعتبار عقود مستحدثه دلالت می‌نماید. آیه شریفه «أَوْفُوا بِالْعُقُودِ» *(سوره مائده: آیه ۱)* با عموم خود، وفا به تمامی پیمان‌های عقلایی را لازم می‌شمارد *(آخوند خراسانی، بی‌تا، ج۱، ص. ۹۲)*. همچنین، مفاد آیه «لَا تَأْكُلُوا أَمْوَالَكُمْ بَيْنَكُمْ بِالْبَاطِلِ» *(سوره نساء: آیه ۲۹)* نیز نه‌تنها منعی ایجاد نمی‌کند بلکه مؤید مشروعیت بیمه است؛ چرا که پول در بیمه با هدف عقلایی محضِ "تأمین و امنیت" مبادله می‌شود، نه به باطل *(مطهری، ۱۳۷٤، ص. ۲۸۵)*.

قاعده فقهی مشهور «الْمُؤْمِنُونَ عِنْدَ شُرُوطِهِمْ» که از احادیث معتبر شیعه استنباط شده، پشتوانه محکمی برای اعتباربخشی به شروط و قراردادهای نوینی مانند بیمه است *(موسوی بجنوردی، ۱٤۱۹ق، ص. ۱۲۲)*. شهید مطهری با تمسک به همین اصل و عمومات قرآنی استدلال می‌کنند که اصل اولی، صحّت هر معامله و عقدی است که میان دو نفر صورت می‌گیرد، مگر آنکه دلیلی خاص بر فساد آن اقامه شود *(مطهری، ۱۳۷٤)*.

با وجود این ادله، مخالفان شبهاتی مبتنی بر قواعد فقهی مطرح کرده‌اند. نخستین شبهه مبتنی بر غرر و جهالت است. مخالفان می‌گویند در بیمه نسبت به تحقق حادثه و مقدار خسارت جهل وجود دارد. در پاسخ باید گفت این اشکال ناشی از شناسایی نادرست موضوع معامله است. آنچه در این معامله مبادله می‌شود، پولِ آینده مجهول در برابر پولِ فعلی نیست. بلکه بیمه‌گذار در قبال پرداخت حق بیمه معلوم، تعهد معلوم بیمه‌گر به ارائه تأمین و امنیت روانی را می‌خرد. این تعهد خود دارای ارزش اقتصادی مسلم است. شهید مطهری تصریح می‌کنند: «در معامله بیمه آنچه که از طرف بیمه‌گر به بیمه‌گزار می‌رسد پول نیست بلکه آنچه که بیمه را یک عمل معقول و مشروع می‌کند، نفس تعهد بیمه‌گر است» *(مطهری، ۱۳۷٤، ص. ۲۸۱)*؛ بنابراین معامله بر دو امر معلوم استوار است و غرر منتفی است.

شبهه دوم مربوط به تعلیق است. ادعا شده بیمه عقدی معلق است و اجماع بر بطلان عقود

معلق وجود دارد. در پاسخ می‌توان گفت: یکم، این اجماع ثابت نیست و استناد آن تنها در ابواب خاصی مانند وقف است. دوم، در تحلیل دقیق، اصل انشاء و ایجاد تعهد در عقد بیمه، منجّز و غیرمعلّق است. آنچه معلق است، فعلِ اجرای تعهد (یعنی پرداخت خسارت) بر وقوع شرط خارجی (حادثه) می‌باشد. از این رو، تعبیر «عقد معلق» درباره بیمه تسامحی است.

شبهه سوم، ربوی بودن احتمالی بیمه است. امام خمینی به‌طور صریح این اشکال را رد می‌کنند. ایشان در تحریرالوسیله می‌فرمایند: «ظاهر آن است که اشکالی ندارد... این زیاده، از ربای قرضی نیست؛ برای آن که پرداخت قسط‌ها از جهت قرض نیست. بلکه بیمه، معاملهٔ مستقلی است... و این شرط جایز و نافذ است» *(خمینی، ١٤٣٤ق، ص. ٦٤٧)*.

بر پایه این ادله کلی، تحلیل ماهوی صحیح و ردّ استدلالی شبهات، مشروعیت اولیه عقد بیمه به‌عنوان نهادی مستقل احراز می‌گردد. امام خمینی به‌صراحت حکم صحت را به همه اقسام بیمه تسری می‌دهند و می‌فرمایند: «ظاهر آن است که بیمه با شرایط گذشته صحیح است و بین انواع آن فرقی نیست از بیمه بر حیات یا بر اتومبیل و هواپیما و کشتی‌ها و مانند آنها» *(خمینی، ١٤٣٤ق، ص. ٦٤٨)*. بر اساس قاعده سرایت حکم از کلی به جزئی، این حکم صحت به تمامی مصادیق نوین و تخصصی این عقد، ازجمله «بیمه سایبری»، نیز تعمیم می‌یابد؛ بنابراین، بیمه سایبری به‌عنوان یکی از اقسام پیچیده و تخصصی عقد بیمه، در صورت رعایت شرایط عمومی صحت معامله، از مبانی فقهی لازم برای مشروعیت برخوردار است. این مشروعیت اولیه، سنگ‌بنای استواری برای ورود به پرسش کلان‌تر این پژوهش، یعنی تبیین مسئولیت و حدود مداخله حکومت اسلامی در توسعه و تنظیم این نهاد نوپدید در چهارچوب فقه حکومتی، فراهم می‌آورد.

## ۳. مسائل مستحدثه در بیمه سایبری (چالش‌های فقهی خاص)

اگرچه مشروعیت ذاتی عقد بیمه سایبری با ادله عام اثبات گردید؛ اما کارآمدی فقه حکومتی در عرصه سیاست‌گذاری، مستلزم ورود به لایه‌های ظریف‌تر است. مسائل مستحدثه‌ای نظیر جواز پرداخت باج‌افزاری، قلمرو جبران سود منتفی و مسئولیت ناشی از خطای هوش مصنوعی، پرسش‌هایی هستند که پاسخ شرعی به آنها، مبنای تصمیم‌گیری حکومت در

تنظیم بازار بیمه سایبری قرار خواهد گرفت. در ادامه، پنج چالش اصلی و راهکارهای آنها در پرتو فقه امامیه ارائه می‌شود.

**حکم پرداخت باج‌افزار (تزاحم قاعده نفی سبیل و قاعده اضطرار)**

در حملات باج‌افزاری، هکرها داده‌های قربانی را رمزنگاری کرده و در ازای دریافت بیت‌کوین یا ارز دیجیتال، کلید رمزگشایی را ارائه می‌دهند. پرسش فقهی آن است که آیا بیمه‌گر می‌تواند به نمایندگی از بیمه‌گذار، باج را پرداخت کند؟

از یک‌سو، قاعده نفی سبیل *(سوره نساء: آیه ۱۴۱)* «وَ لَنْ یَجْعَلَ اللَّهُ لِلْکافِرینَ عَلَی الْمُؤْمِنینَ سَبیلاً» پرداخت هرگونه وجه به دشمن برای سلطه یافتن بر مسلمانان را حرام می‌داند. امام خمینی در این‌باره می‌فرمایند: «هرگونه عملی که موجب سلطه کفار بر مسلمانان شود، حرام است» *(خمینی، ۱۳۸۹، ج۲۰، ص. ۴۵۲)*.

از سوی‌دیگر، قاعده اضطرار *(سوره بقره: آیه ۱۷۳)* «فَمَنِ اضْطُرَّ غَیْرَ باغٍ وَ لا عادٍ فَلا إِثْمَ عَلَیْهِ» در موارد حفظ جان، مال محترم یا حیثیت، جواز موقت و به مقدار ضرورت می‌دهد.

باتوجه به قاعده تزاحم (اهم و مهم)، حکومت اسلامی موظف است برای رفع این ابهام، ضوابط روشنی وضع کند:

۱. تفکیک مصادیق: پرداخت باج فقط در داده‌های حیاتی (سلامت، انرژی، دفاعی، اطلاعات محرمانه ملی) مجاز است.

۲. شرط عدم وجود بک‌آپ: بیمه‌گر موظف است پیش از پذیرش پوشش باج‌افزاری، از وجود بک‌آپ منظم و امن اطمینان حاصل کند.

۳. الزام به استعلام شرعی: هر مورد پرداخت باج باید به تأیید کمیته فقهی بیمه‌گر و در موارد بالای آستانه مشخص (مثلاً ۵۰۰ میلیون ریال) به استعلام از مرکز افتای کشور برسد.

۴. گزارش به نهادهای امنیتی: بیمه‌گر موظف است مشخصات هکر (در صورت امکان) و میزان باج پرداختی را جهت پیگیری قضائی به پلیس فتا گزارش دهد.

این رویکرد، جمع بین قاعده نفی سبیل (منع سلطه‌پذیری) و قاعده اضطرار (حفظ ضروریات) در قالب یک سیاست حکومتی منسجم است.

**جبران سود منتفی (تمایز سود قطعی و احتمالی)**

در پوشش «وقفه کسب‌وکار» بیمه سایبری، بخشی از خسارت ناشی از سودی است که کسب‌وکار در مدت توقف فعالیت، از دست می‌دهد. بنابراین با این چالش روبه‌رو هستیم که سود منتفی، شرعاً قابل جبران و بیمه استیا خیر؟

برخی فقها قاعده «ما لم یوجد لم یتلف» را مستند عدم جواز جبران سود ازدست‌رفته می‌دانند؛ زیرا سود موجودیتی مادی نداشته تا «تلف» یافته باشد *(موسوی بجنوردی، ۱٤۱۹ق، ج۲، ص. ۱٥٦)*.

درمقابل، شهید مطهری با تفکیک دقیق راهگشایی می‌فرمایند: «اگر سودی که از دست می‌رود از نوع سود قطعی است که بر اساس قراردادهای موجود و منعقده قابل اثبات باشد، عرفاً از دست رفتن چنین سودی اتلاف مال محسوب می‌شود؛ اما اگر سود احتمالی باشد که فقط بر اساس میانگین صنعت و بدون سابقه قراردادی پیش‌بینی می‌شود، قابل بیمه نیست» *(مطهری، ۱۳۷٤، ص. ۲۸٥)*.

**مسئولیت ناشی از خطای هوش مصنوعی (قاعده تسبیب و اثبات تقصیر)**

بسیاری از سیستم‌های دفاع سایبری مبتنی بر هوش مصنوعی به صورت خودکار تصمیم می‌گیرند (مانند مسدودسازی خودکار ترافیک مشکوک، حذف فایل‌های آلوده). اگر این سیستم به اشتباه، داده‌های سالم را پاک کند یا سرویس حیاتی را قطع نماید، مسئولیت جبران خسارت با کیست؟

قاعده «تسبیب» می‌گوید: «مَن سَبَّبَ فِی إتلافِ مالِ الغَیرِ بِفِعلٍ یَصدُرُ مِنهُ عادَةً یا یَکونُ مُؤَثِّراً فِیهِ فَهُوَ ضامِنٌ» *(انصاری، ۱٤۱۰ق، ج۱۰، ص. ٥۸)*؛ یعنی اگر کسی به وسیله فعل خود (هرچند غیرمستقیم) زمینه تلف مال دیگری را فراهم کند، ضامن است.

اما در هوش مصنوعی که تصمیم‌گیری مستقل از برنامه‌نویس دارد، اثبات تقصیر برنامه‌نویس بسیار دشوار است. آیا می‌توان گفت «نرم‌افزار» خود عاملیت دارد؟ در صورت اثبات خطای برنامه‌نویس (مثلاً کدنویسی نادرست الگوریتم تشخیص)، قاعده تسبیب جاری و سازنده ضامن است لیکن در صورت عدم اثبات تقصیر، جبران خسارت از محل بیمه، نه از باب ضمان، بلکه از باب «تعاون علی البر» *(سوره مائده: آیه ۲)* جایز است.

حکومت اسلامی نیز با استناد به قاعده «حفظ نظام» و «لاضرر» موظف است

ارائه‌دهندگان سامانه‌های هوشمند حساس (مانند سیستم‌های تشخیص نفوذ در زیرساخت‌های حیاتی) را ملزم به خرید بیمه مسئولیت مدنی کند و برای سامانه‌های هوشمند پرخطر، استانداردهای حداقلی «قابلیت توضیح‌پذیری» را تعیین نماید تا در صورت بروز خطا، قابل ردیابی و تحلیل باشد.

**تداخل بیمه‌نامه‌ها در حملات سایبری-فیزیکی (اصل غرامت و قاعده لاضرر)**

در حملات سایبری-فیزیکی (مانند هک یک نیروگاه که باعث آتش‌سوزی شود یا هک یک خودروی متصل که باعث تصادف گردد)، هم بیمه سایبری و هم بیمه آتش‌سوزی یا ماشین‌آلات می‌توانند ادعای پوشش داشته باشند. پرسش اصلی آن است که چگونه از دریافت مضاعف خسارت (بیش از میزان واقعی) جلوگیری می‌شود؟

در پاسخ باید گفت اصل بنیادین حاکم بر حقوق بیمه، «اصل غرامت» (یا اصل جبرانی) است که بر اساس آن، بیمه‌گذار نباید بیش از میزان خسارت واقعی وارده دریافت کند. در حقوق ایران، این اصل به صورت متمرکز در یک ماده مجزا تعریف نشده؛ اما از ماده ۱ قانون بیمه که بیمه را عقدی می‌داند که به موجب آن بیمه‌گر «خسارت وارده را جبران نموده» و نیز از ماده ۳۰ قانون بیمه که قائم‌مقامی بیمه‌گر را در «حدودی که خسارات وارده را قبول یا پرداخت می‌کند» مقرر داشته، قابل استنباط است. در خسارت مختلط، تقسیم خسارت به نسبت علت و معلول بین بیمه سایبری و بیمه آتش‌سوزی یا ماشین‌آلات انجام می‌شود تا از پرداخت مضاعف جلوگیری گردد. این اصل با قاعده فقهی «لاضرر» که ناظر بر جبران ضرر وارده و منع اضرار به غیر است، هماهنگی کامل دارد.

**قائم‌مقامی بیمه‌گر در فرض ناشناس بودن هکر**

ماده ۳۰ قانون بیمه مقرر می‌دارد: «بیمه‌گر در حدودی که خسارات وارده را قبول یا پرداخت می‌کند درمقابل اشخاصی که مسئول وقوع حادثه یا خسارت هستند قائم‌مقام بیمه‌گذار خواهد بود...» این ماده به‌روشنی حق رجوع بیمه‌گر به عامل زیان را پیش‌بینی کرده است؛ اما در حملات سایبری، چالش اساسی آن است که اغلب هکر ناشناس است و امکان رجوع عملی به وی وجود ندارد. در این فرض، اگر پس از گذشت مدت معقول (مثلاً یک سال) عاملی که موجب خسارت شده شناسایی نشود، قاعده فقهی «لاضرر» اقتضا می‌کند که بیمه‌گر بدون امکان رجوع، خسارت را بپردازد. از سوی‌دیگر، قاعده فقهی

«اسباب» نیز مقرر می‌دارد که اگر عاملی که موجب خسارت شده قابل شناسایی نباشد، خسارت به خود زیان‌دیده وارد نمی‌شود *(موسوی بجنوردی، ۱٤۱۹ق، ج۱، ص۲۱۲)*؛ بنابراین، در شرایط ناشناس بودن هکر، بیمه‌گر نمی‌تواند پرداخت خسارت را منوط به شناسایی عامل زیان و احراز امکان رجوع نماید.

## ۴. مفهوم و سیر تطور فقه حکومتی

فقه حکومتی به‌عنوان شاخه‌ای نوپدید و رویکردی کلان‌نگر در دانش فقه، در پاسخ به ضرورت اداره جامعه اسلامی بر اساس شریعت شکل گرفته است این رویکرد، فقه را از حیطه تنظیم روابط فردی فراتر برده و آن را به نظامی معرفتی برای تدبیر شرعی، مطلوب و کارآمد جامعه تبدیل می‌کند *(ایزدهی و صدیق‌پور، ۱۳۹۹)*. در این چهارچوب، فقیه دیگر تنها پاسخ‌گوی پرسش‌های شخصی مکلفین نیست بلکه به مثابه مدیر جامعه، احکام را با نگاه به مصالح کلان نظام اسلامی، کارآمدی و تأثیر اجتماعی آنها استنباط می‌نماید.

### ۴-۱. تعریف فقه حکومتی

برای تعریف دقیق، تمایز بین سه مفهوم مرتبط ضروری است. «فقه سیاسی» دانشی تخصصی است که صرفاً به مسائل عرصه سیاست می‌پردازد *(مهریزی، ۱۳۷٦)*. «فقه الحکومه» یا فقه حکومت، زیرشاخه‌ای از فقه سیاسی است و تنها مباحث مربوط به نهاد حکومت، مانند مشروعیت و ساختار آن را بررسی می‌کند *(ایزدهی و صدیق‌پور، ۱۳۹۹)*. اما «فقه حکومتی» مفهومی فراتر و عام‌تر دارد. این اصطلاح به رویکردی اطلاق می‌شود که بر تمامی ابواب فقه سایه افکنده و استنباط احکام در آن، با هدف اداره جامعه و تحقق «حیات طیبه اسلامی» صورت می‌گیرد. به تعبیر رهبر معظم انقلاب، فقه حکومتی یعنی «استخراج احکام الهی در همه شؤون یک حکومت و نظر به همه احکام فقهی» و ملاحظه تأثیر هر حکم در تشکیل جامعه اسلامی *(خامنه‌ای، ۱۳۷۱)*.

### ۴-۲. سیر تطورفقه حکومتی و چهار برداشت تکاملی آن

تکوین این رویکرد را می‌توان در قالب چهار برداشت تکاملی دنبال کرد که نشان‌دهنده گسترش

تدریجی دایره شمول و عمق مسئولیت فقه در مواجهه با حکومت است *(میرباقری، ۱۳۹۲)*.

۱. برداشت محدود (فقه احکام حکومتی): در این نگاه، فقه حکومتی صرفاً مجموعه احکامی است که اجرای آنها مانند حدود و قضاء، به عهده حکومت نهاده شده است *(رشاد، ۱۳۸۱، ص. ۱۲)*.

۲. برداشت روشی (رویکرد حکومتی در استنباط): در این مرحله، فقه حکومتی به یک «نگرش» در اجتهاد تبدیل می‌شود. فقیه در فرایند استنباط، خود را در جایگاه حاکم فرض کرده و مصلحت نظام، کارآمدی و اقتضائات اداره جامعه را لحاظ می‌کند *(مهریزی، ۱۳۷۶، ص۱٤۰)*.

۳. برداشت مدیریتی (فقه ناظر به مقام اجرا): این برداشت، مسئولیت فقیه را به مرحله پس از استنباط یعنی «اجرا» نیز تسری می‌دهد. فقیه در مقام حاکم، عهده‌دار تشخیص اولویت‌ها و حل «تزاحم» میان مصالح مختلف در مرحله اجرای احکام است *(علیدوست، ۱۳۹۰)*.

٤. برداشت نظام‌ساز (فقه منطقه‌الفراغ): متأثر از اندیشه شهید صدر، این برداشت عالی‌ترین سطح را ترسیم می‌کند. در این نگاه، فقه حکومتی ناظر به «منطقه‌الفراغ» است؛ یعنی قلمرویی از مباحات که شارع حکم ثابتی برای آنها مقرر نکرده و ولی امر می‌تواند با رعایت اهداف کلان شریعت، احکام الزامی متغیر و متناسب با مصالح زمان صادر کند *(صدر، ۱٤۱۰ق، ج۲)*.

اگرچه برداشت‌های چهارگانه مذکور، سیر تکاملی فقه حکومتی را ترسیم می‌کند؛ اما اندیشه امام خمینی را نمی‌توان صرفاً در چهارچوب یکی از این مراحل محدود دانست. دیدگاه ایشان فراتر از برداشت نظام‌ساز (مرحله چهارم) نیز می‌رود. امام خمینی با طرح «ولایت مطلقه فقیه» و تأکید بر این که «حکومت، فلسفه عملی تمامی فقه است»، فقه را نه صرفاً پرکننده منطقه‌الفراغ، بلکه «ابزار خلق نظامات اجتماعی و تمدنی» معرفی می‌کند. به تعبیر ایشان، «الإسلام هو الحکومۀ بشؤونها» *(خمینی، ۱۳۹۲)*؛ یعنی اسلام با همه شئونش همان حکومت است؛ بنابراین، می‌توان اندیشه امام را «برداشت تمدنی» یا «فقه حاکم بر نظام‌سازی» نامید که در عین بهره‌گیری از دستاوردهای چهار برداشت پیشین، افق‌های فراتری را برای فقه حکومتی ترسیم می‌کند. این برداشت تمدنی از فقه حکومتی، در ادامه با تأکید بر آرای امام خمینی تبیین خواهد شد.

فقه حکومتی، با توجه به ماهیت کلان‌نگر و حکمرانانه‌اش، دارای ویژگی‌های مشخص و متمایزی است *(ایزدهی و صدیق‌پور، ۱۳۹۹)*. این ویژگی‌ها عبارت‌اند از:

باور به جامعیت دین: پایه این فقه بر این اعتقاد است که شریعت اسلام توانایی پاسخگویی به همه نیازهای اداره جامعه، و نه فقط مسائل فردی، را داراست.
گستره همه‌شمول: مخاطب احکام در این نگرش، همه شهروندان جامعه اسلامی است، نه‌تنها مؤمنان. همچنین، همه ابواب فقه (از عبادات و اقتصاد تا سیاست و قضا) با نگاهی کلان و مرتبط با اداره جامعه بررسی می‌شوند.
نگرش نظام‌وار: احکام به صورت مجزا و منفک استنباط نمی‌شوند، بلکه به‌عنوان اجزای یک سیستم یکپارچه در نظر گرفته می‌شوند. تأثیر متقابل احکام بر یکدیگر و بر کل جامعه، در فرایند استنباط لحاظ می‌گردد.
توجه به کارآمدی و مصلحت نظام: در این فقه، معیار نهایی تنها استناد شرعی حکم نیست، بلکه کارآمدی و اثربخشی آن در مدیریت جامعه و تحقق اهداف کلان نظام اسلامی نیز به‌طور جدی مورد توجه قرار می‌گیرد.

## ۴-۳. فقه حکومتی در اندیشه امام خمینی(ره) و شهید صدر

در منظومه فکری امام خمینی، حکومت هویت و حقیقت اسلام است. ایشان می‌فرمایند: «الإسلام هو الحکومة بشؤونها والأحکام قوانین الإسلام و هی شأن من شؤونها بل الأحکام مطلوبات بالعرض وأمور آلیة لإجرائها وبسط العدالة» *(خمینی، ۱۳۹۲، ص. ۶۷۲)*. در این نگاه، حکومت در متن فقه قرار دارد و فقه وظیفه اداره جامعه را بر عهده دارد. عدالت در دیدگاه امام، فرایندی تربیتی و همه‌جانبه است که تحقق آن مستلزم اداره جامعه است. بنابراین حکومت، وسیله تربیت اجتماعی و بسط عدالت معنوی است *(خمینی، ۱۳۸۹، ص. ۱۱۲)*. ولایت در تفسیر امام، عین مفهوم حکومت و مدیریت اجتماعی شریعت است. واقعه غدیر، حکایت از جعل حکومت دارد و امام تصریح می‌کنند: «قضیه غدیر، قضیه جعل حکومت است، این است که قابل نصب است والّا مقامات معنوی قابل نصب نیست» *(خمینی، ۱۳۸۹، ص. ۱۱۳)*.

نظریه ولایت مطلقه فقیه در اندیشه امام، حکمی اولی و مقدم بر احکام فرعیه است. حاکم صلاحیت دارد در چهارچوب مصالح اسلام، تدابیری اتخاذ کند که گاه در اجرا بر برخی احکام فرعیه تقدم می‌یابد. این اختیارات، رکن اساسی نظم شرعی است. امام تصریح می‌کنند این ولایت به‌معنای استبداد نیست و تصمیمات حکومتی در چهارچوب مصلحت

اسلام اتخاذ می‌شود. ایشان می‌فرمایند: «حکومت که شعبه‌ای از ولایت مطلقه رسول‌الله است، یکی از احکام اولیه اسلام است و مقدم بر تمام احکام فرعیه حتی نماز و روزه و حج است» *(خمینی، ۱۳۸۹، ص. ٤٥٢)*. ایشان در جای دیگری دلیل این امر را چنین بیان می‌دارند: «لا یبقی شک فی أنّ الفقیه لا یکون حصناً للإسلام إلّا بأن یکون حافظاً لجمیع الشؤون من بسط العدالة وإجراء الحدود وإلّا فصرف الأحکام لیس بإسلام» *(خمینی، ۱۳۹۲، ص. ٦٥٦)*.

از منظر امام، مأموریت حکومت دینی، مقابله فکری، فرهنگی و ساختاری با تمدن مادی غرب و ایفای نقشی تاریخی و تمدنی است؛ بنابراین، فقه حکومتی در اندیشه امام در سه سطح تحلیل می‌شود: سطح هستی‌شناختی (حکومت به مثابه جوهر اسلام)، سطح فقهی و حقوقی (ولایت مطلقه به‌عنوان حکم اولی) و سطح تمدنی و راهبردی (مواجهه فعال با تمدن نوین).

شهید صدر نظریه «منطقه‌الفراغ» را مطرح می‌کند. در این نظریه، ولایت حکومتی در قلمرویی از امور که شارع حکم ثابت نیاورده محدود می‌شود و حاکم می‌تواند در آن احکام الزامی جعل کند. ایشان می‌نویسد: «فألوان النشاط المباحة بطبیعتها فی الحیاة الاقتصادیّة هی التی تشکّل منطقة الفراغ فإذا منع الإمام عن فعل مباح بطبیعته أصبح حراماً وإذا أمر به أصبح واجباً» *(صدر، ۱۳۸۹)*. این نگرش بر هماهنگی میان احکام ثابت و متغیر تأکید دارد و فقه حکومتی را در چهارچوب تکمیل و تنظیم نظام فقهی موجود در قلمروی مشخص (منطقه‌الفراغ) می‌بیند.

درمقابل، امام خمینی ولایت را مطلق و فراتر از پر کردن منطقه‌الفراغ می‌داند و حکمت آن را در سرپرستی کلی اراده‌ها و توسعه تاریخی اسلام می‌جوید. تفاوت کلیدی این است که شهید صدر فقه حکومتی را در چهارچوب تکمیل نظام فقهی موجود می‌بیند، درحالی‌که امام خمینی فقه را ابزار خلق و هدایت نظامات کلان اجتماعی و تمدنی می‌داند. این فهم جامع و فعال از فقه حکومتی، مسیر روشنی برای تحلیل و ساماندهی مسائل مستحدثه‌ای مانند بیمه سایبری ارائه می‌دهد.

## ۵. مسئولیت‌های حکومت اسلامی در عرصه امنیت

در اندیشه سیاسی اسلام، تأمین امنیت نه یک انتخاب، که تکلیفی بنیادین برای حاکم اسلامی

است. این مسئولیت ریشه در فلسفه تشکیل حکومت دارد و ابعاد گوناگونی را شامل می‌شود. برای تبیین دقیق این مسئولیت، لازم است نخست مستندات شرعی آن واکاوی شود و سپس ابعاد گوناگون آن مورد بررسی قرار گیرد.

## ۵-۱. مبانی فقهی مسئولیت حکومت در تأمین امنیت

در چهارچوب فقه حکومتی، مسئولیت حاکم اسلامی در تأمین امنیت شهروندان، تکلیفی شرعی بنیادین و رکنی اساسی از فلسفه وجودی حکومت دینی است. این مسئولیت ذاتی را می‌توان بر سه رکن مبانی نقلی (قرآن و سنت)، مبانی فقهی و مبانی عقلی استوار دانست.

الف. مبانی نقلی

نصوص دینی با صراحت، امنیت را نعمتی الهی و پیش‌شرط تحقق حیات فردی و اجتماعی توأم با عبادت و تعالی معرفی می‌کنند. قرآن کریم در شبکه‌ای معنادار از واژگان مرتبط (مانند «آمن»، «سلام»، «اطمینان») و تقابل‌های مفهومی، تصویر جامعی از جایگاه امنیت ترسیم می‌کند. در نگرش قرآنی، امنیت تنها نبود تهدید فیزیکی نیست، بلکه حکومت روابط سالم و عاری از دشمنی (سلام) در جامعه است *(طباطبایی، ۱٤۱۷ق، ج٥، ص. ۳۲)*.

آیات کلیدی، زنجیره علّی روشنی را نشان می‌دهند: امنیت پایدار («آمنۀ») سبب آرامش روانی و اطمینان («مطمئنۀ») می‌شود و این دو، زمینه رزق فراگیر و برکت («یأتیها رزقها رغداً») را فراهم می‌آورند *(سوره نحل: آیه ۱۱۲)*. این تقدم رتبی و علّی امنیت بر رزق، در دعای حضرت ابراهیم(ع) نیز آشکار است: «رَبِّ اجْعَلْ هَذَا بَلَدًا آمِنًا وَارْزُقْ أَهْلَهُ مِنَ الثَّمَرَاتِ» *(سوره بقره: آیه ۱۲٦)*.

فقدان امنیت، این زنجیره حیات‌بخش را از ریشه قطع می‌کند. تحلیل‌های معناشناختی نیز نشان می‌دهد که امنیت در قرآن، مفهومی چندبعدی و دارای لوازمی چون داشتن سرزمین و تحول در باورها و رفتارهاست *(نوری و اسماعیلی، ۱۳۹۹، ص. ۲٦۷)*.

سخن اهل بیت(ع)، واضح‌ترین دلیل بر وجوب امنیت‌آفرینی برای حاکم اسلامی است. در منظومه فکری معصومین(ع)، امنیت مفهومی چندبعدی است که هم به‌عنوان هدف حکومت و هم به‌عنوان پیش‌شرط حیات دینی و اجتماعی مورد تأکید قرار گرفته است.

امیرالمؤمنین علی(ع) در خطبه‌ای که فلسفه حکومت خویش را تبیین می‌کند، با بیانی

جامع و هدفمند، غایت نهایی حکمرانی را ترسیم می‌فرمایند: «فَلَسْتُ فِی سُلْطَانِی بِمُسْتَبِدٍّ بِرَأْیِی، وَ لَا آخذ فِیمَا آخُذُ بِهَوًی، وَ لَکِنِّی أَسْمَعُ مَا یُقَالُ لِی، وَ أَنْظُرُ بِمَا یُرَی لِی، وَ أَفْعَلُ مَا یُعْلَمُ لِی أَنَّهُ الرَّشَادُ لِنَرُدَّ الْمَعَالِمَ مِنْ دِینِکُمْ، وَ نُظْهِرَ الْإِصْلَاحَ فِی بِلَادِکُمْ، فَیَأْمَنَ الْمَظْلُومُونَ مِنْ عِبَادِکُمْ، وَ تَتَّفِقَ کَلِمَتُکُمْ، وَ تَلْتَئِمَ أُمُورُکُمْ» *(نهج‌البلاغه: خطبه ۱۳۱)*.

در این فراز تاریخی، امام علی(ع) «امنیت یافتن مظلومان از بندگان خدا» را در زمره اهداف اصلی حکومت خویش برمی‌شمارند. تحلیل این بیان نشان می‌دهد که امنیت اجتماعی و قضائی بخشی جدایی‌ناپذیر از پروژه کلی «احیای دین» و «اصلاح جامعه» است. عبارت «فَیَأْمَنَ الْمَظْلُومُونَ» (تا مظلومان در امان باشند) به‌صورت یک جمله نتیجه بیان شده است که نشان می‌دهد امنیت، ثمره و نتیجه طبیعی حکمرانی عادلانه و اصلاح‌گراست. این تقدم و تأخر منطقی، جایگاه امنیت را به‌عنوان بستر سازنده برای همبستگی اجتماعی و کارآمدی نظام تثبیت می‌کند.

در خطبه دیگری، امام علی(ع) «امن‌سازی راه‌ها» را به‌صراحت در شمار وظایف اصلی حکومت و والی برمی‌شمارند و می‌فرمایند: «... وَ أَمْنَ السَّبِیلِ...» (نهج‌البلاغه: خطبه ٤٠). این فرمان عملیاتی، امنیت را از حیطه نظریه‌پردازی خارج کرده و آن را به‌عنوان یک وظیفه اجرایی و عینی بر دوش حاکمیت می‌نهد. تأکید بر امنیت راه‌ها که شریان‌های ارتباطی و تجاری جامعه هستند نشان می‌دهد تأمین امنیت، مستلزم برنامه‌ریزی، نظارت و اقدام عملی در عرصه‌های مختلف اجتماعی است.

در بیانی دیگر، امام علی(ع) بر پیوند ناگسستنی میان امنیت و حیات دینی تأکید می‌ورزند و می‌فرمایند: «مَنِ اسْتَحْکَمَتْ فِیهِ خَصْلَةٌ مِنْ خِصَالِ الْخَیْرِ اغْتَفَرْتُ مَا سِوَاهَا وَ لَا أَغْتَفِرُ فَقْدَ عَقْلٍ وَ لَا دِینٍ لِأَنَّ مُفَارَقَةَ الدِّینِ مُفَارَقَةُ الْأَمْنِ وَ لَا حَیَاةَ مَعَ مَخَافَةٍ» *(ابن شعبه حرانی، ج۱، ص. ۲۱۹)*. این کلام ژرف دارای دو دلالت کلیدی است: نخست، هم‌عرضی دین و امنیت که در آن «مفارقة الدین» (جدایی از دین) مساوی با «مفارقة الأمن» (جدایی از امنیت) دانسته شده و نشان می‌دهد امنیت، جزء لاینفک حیات دینی است. دوم، نفی حیات توأم با ترس در عبارت «لا حیاة مع مخافة» که به‌روشنی ناامنی را نافی حیات واقعی و شرافتمندانه می‌داند؛ بنابراین، مسئولیت حکومت دینی در حراست از دین، مستلزم زدودن ترس و ایجاد امنیت است.

امام صادق(ع) نیز در بیانی بنیادین، جایگاه امنیت را در زندگی انسان تبیین می‌فرمایند: «خَمْسُ خِصَالٍ مَنْ فَقَدَ مِنْهُنَّ وَاحِدَةً لَمْ يَزَلْ نَاقِصَ الْعَيْشِ زَائِلَ الْعَقْلِ مَشْغُولَ الْقَلْبِ... وَ الثَّانِيَةُ الْأَمْنُ» *(مجلسی، ۱۴۰۳ق، ج۷۱، ص. ۱۸۶)*. در این روایت، امنیت در ردیف پنج خصلت ضروری برای یک زندگی کامل قرار گرفته است. تحلیل این روایت نشان می‌دهد که فقدان امنیت به «زوال عقل» منجر می‌شود؛ یعنی امنیت پیش‌شرط فعالیت عقلانی و تصمیم‌گیری صحیح در زندگی فردی و اجتماعی است. همچنین عبارت «مشغول القلب» (دل مشغول) اشاره به آشفتگی روانی ناشی از ناامنی دارد که امنیت را شرط لازم برای آرامش درونی و سلامت روان جامعه معرفی می‌کند. قرار گرفتن امنیت پس از سلامت جسمانی و پیش از گشایش در روزی، نشان‌دهنده اولویت و تقدم آن بر بسیاری از نیازهای مادی است.

در سطحی کلان‌تر، امام علی(ع) در غررالحکم، ناامنی و بی‌برکتی را دو ویژگی مکمل و همزاد یک جامعه ویران معرفی می‌کنند: «شَرُّ الْبِلَادِ بَلَدٌ لَا أَمْنَ فِيهِ وَلَا خِصْبَ» *(تمیمی آمدی، ۱۴۱۰ق، حکمت ۱۰۲۵۵)*. این کلام گویا، پیوند ناگسستنی میان امنیت و رفاه اقتصادی (خصب و حاصلخیزی) را آشکار می‌سازد. امام با ترکیب «لا أمن فیه و لا خصب» به رابطه علّی مستقیم بین این دو مفهوم اشاره می‌فرمایند: فقدان امنیت، نه‌تنها یک ناگواری اجتماعی، بلکه عامل محرومیت از برکات الهی و رونق اقتصادی است. جامعه‌ای که امنیت ندارد، زمین حاصلخیز و پربرکت (خصب) نیز نخواهد داشت. این تحلیل، امنیت را به‌عنوان پیش‌شرط ضروری برای شکوفایی اقتصادی و بهره‌مندی از نعمت‌های الهی معرفی می‌کند و وظیفه حکومت در ایجاد امنیت را با مسئولیت آن در تأمین رفاه عمومی گره می‌زند.

مجموعه این روایات نشان می‌دهد در منظومه فکری معصومین(ع)، امنیت دارای سه جایگاه کلان است: نخست به‌عنوان هدف غایی حکمرانی در کنار احیای دین و اصلاح جامعه؛ دوم به‌عنوان شرط ضروری تحقق حیات دینی و عاری از ترس؛ و سوم به‌عنوان رکن اساسی زندگی عاقلانه، آرام و کامل. از این مبانی نقلی می‌توان نتیجه گرفت که تأمین امنیت نه یک توصیه اخلاقی یا یک وظیفه اداری صرف، بلکه تکلیفی شرعی، حاکمیتی و عقلانی برای حکومت اسلامی است. این تکلیف، ریشه در فلسفه وجودی حکومت دینی دارد که همانا تحقق جامعه‌ای امن، عادل و دینی است. هرگونه قصور در این امر، به‌منزله قصور

در انجام یکی از اساسی‌ترین مأموریت‌های ولایی است. این مبانی، پشتوانه‌ای محکم برای استنباط مسئولیت حکومت در برابر تهدیدات نوینی چون ناامنی سایبری فراهم می‌آورد؛ زیرا فضای سایبر امروزه به عرصه‌ای حیاتی برای حیات دینی، عقلانی و اجتماعی جامعه تبدیل شده است.

ب. مبانی فقهی

فقهای امامیه با استناد به ادله استنباطی، تأمین امنیت را از واجبات قطعی حکومت می‌دانند. در تعریف فقهی، امنیت به معنای «ایمنی داشتن جانی، مالی، عرضی یا معنوی» است و مراد از امنیت معنوی، «ایمن بودن از وقوع در حرام یا ترک واجب» می‌باشد *(هاشمی شاهرودی، ۱۳۸۲، ج۱، ص. ٦٦٤)*. این تعریف جامع، حفاظت از تمامی ابعاد وجودی انسان را در دایره مسئولیت حکومت قرار می‌دهد.

براین‌اساس، «ایجاد امنیت در شئون مختلف زندگی مردم از وظایف اساسی و حتمی حکومت اسلامی» شناخته شده است. امنیت از مهم‌ترین و ضروری‌ترین نیازهای زندگی بشر به‌شمار می‌آید و فلسفه تشکیل حکومت اسلامی نیز در گرو تحقق همین نیاز اساسی است؛ چرا که انسان تنها در پرتو آن می‌تواند «امور دنیوی و اخروی خویش را با آسایش‌خاطر سامان دهد» *(هاشمی شاهرودی، ۱۳۸۲، ج۱، ص. ٦٦٤)*.

در این میان، قاعده کلیدی «حفظ نظام» مهم‌ترین دلیل فقهی این تکلیف محسوب می‌شود. ازآنجاکه بقا و تعالی هر جامعه‌ای منوط به برقراری نظم و امنیت است، این امر به‌عنوان تکلیفی الزامی بر عهده حاکمیت قرار می‌گیرد.

افزون‌براین، قاعده نفی سبیل به‌عنوان دلیلی فقهی-سیاسی، لزوم مقابله با تهدیدات امنیتی را اثبات می‌کند. ناامنی داخلی، راه نفوذ و سلطه بیگانگان را هموار می‌سازد و تأمین امنیت، ضامن استقلال و عزت جامعه اسلامی است. در تحلیل وظایف حکومت، قاعده نفی سبیل به‌عنوان دلیلی عقلی-فقهی بر لزوم مقابله با تهدیدات امنیتی در تمام عرصه‌ها مورد استناد قرار گرفته است *(حسنی و کریمیان، ۱٤۰۰، ص. ۱۱۱)*.

ج. مبانی عقلی

استدلال عقلی، مسئولیت حکومت در تأمین امنیت را امری بدیهی و ضروری برای تشکیل

و تداوم هر جامعه‌ای می‌داند. این استدلال را می‌توان در چند محور اساسی تبیین کرد:
الف) امنیت به‌عنوان نیاز اولیه: عقل به روشنی درک می‌کند که «امنیّت از نیازهای اوّلیهٔ همهٔ مردم است که بدون آن زندگی گوارا نخواهد بود» *(مکارم شیرازی، ۱٤۲۷ق، ج۲، ص. ۲۱٥)*. این نیاز اولیه، پایه‌ای عقلایی برای وظیفه‌مندی حکومت است.
ب) امنیت به‌عنوان پیش‌شرط توسعه: ازهمین‌رو امنیت از شاخص‌های رشد و توسعه شمرده شده است. جامعه ناامن به طور طبیعی، جامعه‌ای توسعه‌نیافته است که به‌سبب ناامنی، دیگر عوامل رشد و توسعه را نیز از دست می‌دهد. در چنین جامعه‌ای، سرمایه‌گذاری، تولید و تجارت، راه‌اندازی کارخانه‌های صنعتی و مانند آن بی‌رونق خواهد بود. همچنین، ناامنی فرار سرمایه‌ها و مغزها را در پی دارد که نتیجهٔ آن فقر و عقب‌ماندگی است *(مکارم شیرازی، ۱٤۲۷ق، ج۲، ص. ۲۱٦)*.
ج) استدلال قرآنی مبتنی بر عقل سلیم: آیات قرآن کریم نیز بر این رابطه علّی عقلانی تأکید دارند. در سوره قریش (آیه ٤)، نعمت «امنیت از ترس» در کنار نعمت «طعام از گرسنگی» قرار گرفته که گواه اهمیت این نعمت و شدت ارتباط این دو با هم است. در آیات دیگر، ترتیب علّی روشنی دیده می‌شود: حضرت ابراهیم(ع) نخست نعمت امنیت را و سپس روزی فراوان مردم مکه را از خداوند طلب می‌کند (رب اجعل هذا بلدا آمنا و ارزق اهله من الثمرات) *(سوره بقره: آیه ۱۲٦)*. همچنین در آیه ۱۱۲ سوره نحل، ترتیب سه‌گانه «امنیت، اطمینان، روزی فراوان» ذکر شده است. این ترتیب طبیعی، حلقه‌های زنجیری علت و معلول را نشان می‌دهد؛ چرا که تا امنیّت نباشد، کسی اطمینان به ادامهٔ زندگی در محلّی پیدا نمی‌کند و تا این دو نباشند، کسی علاقه‌مند به تولید و سروسامان دادن به وضع اقتصادی نمی‌شود *(مکارم شیرازی، ۱٤۲۷ق، ج۲، ص. ۲۱٦)*.
د) دفع ضرر محتمل: از منظر فقه حکومتی، حکومتی که نتواند بستر امن را فراهم آورد، درحقیقت زمینه‌ساز «ضرر نوعی» گسترده به جان، مال و آبروی شهروندان شده است. قاعده مسلّم فقهی «لاضرر و لاضرار» که ریشه در حکم قطعی عقل عملی دارد، این مسئولیت را بر عهده حاکمیت می‌گذارد. این قاعده با تعابیر مختلفی از معصومین(ع) نقل شده است، ازجمله: «لا ضرر و لا ضرار علی مؤمن» و «لا ضرر و لا ضرار فی الإسلام». این تعابیر،

حرمت وارد کردن ضرر و نیز لزوم دفع آن را به‌صورت قاعده‌ای کلی و عمومی در شریعت اثبات می‌کند *(موسوی بجنوردی، ۱٤۱۹ق، ج۱، ص. ۲۱۲)*؛ بنابراین، تکلیف حکومت به تأمین امنیت، تجلی عملی قاعده لاضرر در سطح کلان جامعه است. غفلت از این وظیفه، خود مصداق بارز «اضرار» به آحاد مردم محسوب می‌شود.

استدلال عقلی مبتنی بر مطالعات معاصر: بررسی‌های حقوقی معاصر نیز بر این ضرورت عقلی صحه می‌گذارند. همان‌گونه که تحلیل‌ها نشان می‌دهد، زندگی در «جامعه‌ای غیرمنظم و ناامن»، خود به‌عنوان عاملی برای سوق یافتن به‌سوی شر و اختلال در روابط اجتماعی شناخته می‌شود؛ زیرا تنها در سایه نظم و امنیت است که عدالت به‌مثابه نعمتی بنیادین محقق گشته و تعادل لازم میان حقوق و تکالیف افراد برقرار می‌گردد. فقدان این امنیت، به‌طور مستقیم به فقدان ثبات اجتماعی می‌انجامد *(ایوب و البغدادی، ۲۰۲۲، ص. ۷)*. براین‌اساس، تأمین امنیت و در عصر حاضر، امنیت سایبری به‌عنوان پیش‌شرط عقلی تحقق عدالت و بقای نظام اجتماعی، مسئولیتی بدیهی بر عهده حاکمیت است.

بر پایه این سه رکن استوار که ریشه در سنت قطعی معصومین(ع) دارد، با ادله استنباطی فقهی تقویت می‌شود و بر بداهت عقلی و ضرورت اجتماعی استوار است، تأمین امنیت جامع، تکلیفی شرعی، فقهی و عقلی برای حاکم اسلامی است. این مسئولیت ذاتی که گستره آن شامل حفاظت از جان، مال، عرض، معنویت و به تبع آن تمامی دارایی‌ها و تعاملات نوین (ازجمله فضای سایبر) می‌شود، مبنای محکمی برای تحلیل تکلیف حکومت در مواجهه با تهدیدات نوپدید فراهم می‌آورد. هرگونه تلاش حکومت برای ایفای این مسئولیت، ازجمله در عرصه‌های نوین، در راستای تحقق اهداف عالیه شریعت و ادای تکلیف شرعی است.

## ۵-۲. تحول مفهومی امنیت در عصر سایبر

در دوران معاصر، مفهوم امنیت دچار دگردیسی شده و از قالب سنتی (جانی و مالی) فراتر رفته است. ظهور «فضای سایبری» به‌عنوان عرصه‌ای حیاتی برای تعاملات اجتماعی، اقتصادی و امنیتی، «امنیت سایبری» را به بخشی جدایی‌ناپذیر از مسئولیت ذاتی حکومت تبدیل کرده است.

امروزه، حفاظت از داده‌ها، دارایی‌های دیجیتال، زیرساخت‌های حیاتی و حریم خصوصی شهروندان در فضای مجازی، در ذیل همان ضروریات پنجگانه (خصوصاً حفظ مال و آبرو) قرار می‌گیرد. حکومتی که نتواند از این «ثغور جدید» امت اسلامی صیانت کند، در انجام مسئولیت اصلی خود قاصر است.

در مواجهه با تهدیدات پیچیده و فراگیر سایبری، ابزارهای سنتی پاسخگو نیستند. بیمه سایبری، به‌عنوان یک سازوکار نوین مدیریت ریسک، می‌تواند در کنار سیاست‌های دفاعی و امنیتی، به‌مثابه ابزاری حکومتی و کارآمد برای ایفای همان مسئولیت کلاسیک تأمین امنیت مورد توجه قرار گیرد.

کارکردهای چندوجهی بیمه سایبری آن را به ابزاری مشروع و بلکه لازم در دست حکومت تبدیل می‌کند:

کارکرد اقتصادی–امنیتی: ایجاد تاب‌آوری مالی برای بنگاه‌ها و نهادها در برابر خسارات کلان سایبری، جلوگیری از سرریز بحران‌های منفرد به کل اقتصاد ملی، و کاهش بار مالی دولت در جبران خسارات.

کارکرد روانی–اجتماعی: ایجاد اعتماد و اطمینان در فضای دیجیتال، مدیریت بحران‌های امنیتی با پشتیبانی مالی و مشاوره‌ای، و کمک به ترمیم سرمایه اجتماعی پس از حوادث.

کارکرد پیشگیرانه و فرهنگ‌ساز: شرکت‌های بیمه با تعیین استانداردهای امنیتی حداقلی برای صدور بیمه‌نامه و ارائه مشوق‌های مالی (تخفیف حق بیمه) به مشتریان دارای سطوح بالای امنیت، به ناظران غیررسمی و تسهیل‌گران ارتقای فرهنگ امنیت سایبری تبدیل می‌شوند *(Woods & Simpson, 2017)*.

بر پایه آنچه گذشت، مسئولیت حکومت اسلامی در تأمین امنیت، ریشه‌ای عمیق در ادله نقلی، عقلی و فقهی دارد و در عصر حاضر، امنیت سایبری را به‌عنوان بستری حیاتی دربرمی‌گیرد.

بیمه سایبری، در صورت انطباق با موازین شرعی، نه تنها منافاتی با اصول اسلام ندارد، بلکه در راستای تحقق اصل قرآنی «تعاونوا علی البر والتقوی» (سوره مائده: آیه ۲)، کمک به استقرار عدالت اجتماعی (با جبران خسارت مظلومان در فضای سایبر) و افزایش

تاب‌آوری ملی ارزیابی می‌شود. بنابراین، این نهاد می‌تواند به‌عنوان سازوکاری مشروع و کارآمد در اختیار حکومت قرار گیرد تا مسئولیت ذاتی خویش در «حفظ نظام» و «صیانت از ضروریات» را در عصر دیجیتال به انجام رساند. بخش بعدی به تحلیل مبانی مشروعیت مداخله حکومت برای هدایت و تنظیم این ابزار نوین خواهد پرداخت.

## ۶. نقش بیمه سایبری در ایجاد امنیت روانی و اجتماعی

در تحلیل نهایی، کارکرد بیمه سایبری فراتر از جبران مالی، ایجاد زیرساخت روانی و اجتماعیِ امن برای زیست دیجیتال است. این نهاد با ایفای نقش در چهار محور زیر، تاب‌آوری و اعتماد جمعی را نهادینه می‌کند.

۱. مدیریت بحران و بازسازی اعتماد: یک حادثه سایبری، با ایجاد شوک روانی، می‌تواند به سرعت به بحران بی‌اعتمادی اجتماعی تبدیل شود. بیمه سایبری با ارائه پشتیبانی یکپارچه پس از حادثه (شامل خدمات حقوقی، رسانه‌ای و روانی)، از تشدید این بحران جلوگیری کرده و روند بازیابی اعتماد به نظام اقتصادی-اجتماعی را تسهیل می‌نماید.

۲. جامعه‌سازی و ایمنی جمعی: با تحت پوشش قرار دادن طیف گسترده‌ای از بازیگران، بیمه سایبری یک اکوسیستم دانش‌بنیان و تاب‌آور ایجاد می‌کند. تجمیع داده‌های تهدیدات و اشتراک آن با بیمه‌گذاران، استانداردهای امنیتی کل جامعه را ارتقا داده و از گسترش آسیب‌ها به‌ویژه در بخش‌های حیاتی (مانند سلامت) جلوگیری می‌کند.

۳. فرهنگ‌سازی و نهادینه‌سازی سواد امنیتی: بیمه با مشوق‌های مالی (تخفیف حق بیمه برای رعایت استانداردها) و آموزش مستمر (کارگاه‌ها، به‌روزرسانی تهدیدات)، امنیت را از یک امر فنی به یک فرهنگ سازمانی و عمومی تبدیل می‌کند و پایدارترین شکل مصونیت را ایجاد می‌نماید.

٤. ترمیم و تقویت سرمایه اجتماعی: پرداخت منصفانه خسارت و برخورد مسئولانه پس از حادثه، اعتماد اجتماعیِ خدشه‌دار شده را ترمیم می‌کند. همچنین، احساس امنیت ناشی از پوشش بیمه‌ای، زمینه همکاری و اشتراک اطلاعات بین سازمان‌ها در مواجهه با تهدیدات مشترک را فراهم می‌آورد.

در چهارچوب فقه حکومتی، ایجاد «اطمینان‌خاطر عمومی» و حفظ «سرمایه اجتماعی»

ذیل تکلیف کلان «حفظ نظام» قرار می‌گیرد. بیمه سایبری با کارکردهای چندلایه خود (مدیریت بحران، جامعه‌سازی، فرهنگ‌سازی و تقویت اعتماد)، ابزاری بی‌بدیل برای ایفای این مسئولیت در عصر دیجیتال است. ازاین‌رو، ساماندهی و توسعه این نهاد، تکلیفی راهبردی برای حکومت اسلامی به‌شمار می‌آید.

## ۷. مبانی مشروعیت مداخله حکومت در بیمه سایبری

بر پایه مسئولیت ذاتی حکومت اسلامی در تأمین امنیت و با توجه به دگردیسی مفهوم امنیت در عصر سایبر، مشروعیت مداخله حکومت برای توسعه و تنظیم نهاد نوپدید «بیمه سایبری» نیازمند تبیین مبانی مستحکم فقهی است. این مبانی در چهارچوب فقه حکومتی و با محوریت مفاهیم «مصلحت» و «ضرورت» که معیار پذیرفته‌شده در تصرفات ولی امر است در چهار بُعد اصلی قابل استخراج است. هر یک از این ابعاد نه‌تنها با اهداف کلان شریعت (حفظ دین، عقل، نفس، نسل و مال) همسو هستند، بلکه از طریق کارکردهای عینی و چندلایه بیمه سایبری محقق می‌شوند.

### ۷-۱. بُعد مصلحتی (حفظ نظام اقتصادی دیجیتال)

حفظ تمامیت و استمرار نظام اجتماعی و اقتصادی از واجبات اولیه حکومت اسلامی است. قاعده فقهی «حفظ نظام» که از واجبات اهم شمرده می‌شود *(موسوی بجنوردی، ۱٤۱۹ق، ص. ۲٤۹)*.

در عصر حاضر دامنه خود را به «فضای سایبری» به‌عنوان ستون فقرات اقتصاد و اداره جامعه گسترش می‌دهد. یک حمله هماهنگ سایبری به زیرساخت‌های بانکی، انرژی یا سلامت می‌تواند نه‌تنها یک بنگاه، بلکه نظم یک منطقه یا حتی کل کشور را مختل کند. بیمه سایبری در این بُعد، با کارکرد «جبران خسارت و ایجاد تاب‌آوری مالی» وارد عمل می‌شود. این نهاد با تبدیل ریسک‌های فاجعه‌بار به هزینه‌های قابل پیش‌بینی و مدیریت، نقش یک ضربه‌گیر کلان اقتصادی را ایفا می‌نماید؛ برای‌مثال، با جبران هزینه‌های سرسام‌آور بازیابی داده‌های یک بیمارستان بزرگ پس از یک حمله باج‌افزاری، از ورشکستگی آن مؤسسه حیاتی و ایجاد بحران در نظام سلامت جلوگیری می‌کند *(پورقصاب امیری و حسنی کاخ، ۱۳۹۷)*.

همچنین، با تأمین نقدینگی برای بازیابی سیستم‌های پرداخت یک بانک پس از حمله، از ایجاد هرج و مرج اقتصادی و از دست رفتن اعتماد عمومی جلوگیری می‌کند. این عملکرد، عینیت بخشیدن به حکم شرعی «حفظ نظام» در دنیای دیجیتال است. بدون چنین ابزاری، نظام اقتصادی در برابر شوک‌های سایبری شکننده خواهد بود و این با تکلیف حکومت در صیانت از کلیت نظام در تعارض است.

## ۷-۲. امنیتی-دفاعی (صیانت از مرزهای سایبری)

امنیت سایبری امروزه جزئی جدایی‌ناپذیر از امنیت ملی و دفاع از تمامیت ارضی است. تهدیدات سایبری می‌توانند بدون عبور از مرزهای فیزیکی، حاکمیت و امنیت داخلی یک کشور را هدف قرار دهند. مسئولیت حکومت در «دفاع» و «حراست از کیان جامعه» در این عرصه نوین نیز جاری است. بیمه سایبری در این بُعد، با کارکرد «پیشگیرانه (تنظیم‌گری و توسعه)» به‌عنوان یک بازوی کمکی و غیرمستقیم حکومت عمل می‌کند. شرکت‌های بیمه به طور طبیعی و برای محاسبه حق بیمه و مدیریت ریسک خود، به ارزیابی سطح امنیت مشتریان و تعیین استانداردهای حداقلی امنیتی (مانند استفاده از فایروال، رمزنگاری و آموزش کارکنان) می‌پردازند. این فرایند، آن‌ها را به ناظران مستمر و مشوق‌های اقتصادی برای ارتقای امنیت سایبری تبدیل می‌کند *(Woods & Simpson, 2017)*.

حکومت می‌تواند با هدایت و تنظیم این بازار، از این سازوکار ذاتی برای ارتقای سطح ایمنی کل کشور بهره ببرد؛ به‌عنوان‌مثال، می‌تواند با حمایت از تأسیس «مرکز ملی رصد تهدیدات سایبری» که داده‌های بومی را در اختیار بیمه‌گران قرار می‌دهد، هم دقت ارزیابی ریسک را افزایش دهد و هم خود به‌عنوان دیده‌بان امنیت ملی عمل نماید *(السان و همکاران، ۱۳۹۵)*. بنابراین، مداخله حکومت برای ساماندهی این نهاد، درواقع تقویت خط مقدم دفاع غیرنظامی و اقتصادی در برابر تهدیدات سایبری و تجلی تکلیف «صیانت از مرزهای نوین ملی» است.

## ۷-۳. بُعد اقتصادی (نفی ضرر نوعی و حفظ اموال)

یکی از اهداف مهم شریعت، «حفظ مال» و منع اتلاف ثروت است. قاعده فقهی «لاضرر و

لاضرار فی الاسلام» *(موسوی بجنوردی، ۱٤۱۹ق)* نه‌تنها در سطح فردی، که در سطح کلان و برای دفع «ضرر نوعی» نیز جاری است. خسارات سنگین و گسترده ناشی از حملات سایبری که می‌تواند منجر به نابودی دارایی‌های دیجیتال، ورشکستگی بنگاه‌های متوسط و کوچک و اتلاف سرمایه‌های ملی شود، مصداق بارز چنین ضرر عمومی است. بیمه سایبری با سازوکار «جبران خسارت»، وسیله‌ای برای تحقق عملی این قاعده و صیانت از اموال عمومی است. این نهاد با ایجاد یک صندوق مشترک (حق بیمه‌ها)، بار مالی حوادث را از دوش یک واحد اقتصادی خاص برداشته و آن را در جامعه بیمه‌گذاران توزیع می‌کند، و از این راه از ورشکستگی بنگاه‌ها و در نتیجه، حفظ اشتغال و تداوم چرخه تولید حمایت می‌کند. از منظر کلان‌تر، وجود چنین بازار بیمه‌ای کارآمد، بار مالی دولت را در مواقع وقوع حوادث گسترده کاهش می‌دهد، چرا که در غیر این صورت دولت مجبور است از بودجه عمومی برای نجات بنگاه‌های ورشکسته شده استفاده کند *(Woods & Simpson, 2017)*.

بنابراین، تنظیم این بازار توسط حکومت، اقدامی پیش‌دستانه برای «دفع ضرر» احتمالی بزرگ از کیان اقتصاد ملی و عمل به فریضه «حفظ اموال مردم» است.

## ۷-۴. بُعد اجتماعی (تحقق عدالت و تنظیم بازار)

حکومت اسلامی متکفل برقراری عدالت و نظارت بر بازار (حسبه) برای جلوگیری از ظلم و انحراف است. بیمه سایبری در این بُعد، با کارکردهای «پیشگیرانه (فرهنگ‌سازی و تقویت سرمایه اجتماعی)» و «ترمیم خسارت» می‌تواند ابزاری برای تحقق این اهداف باشد. این نقش در چند محور مستند می‌شود:

نخست، از منظر عدالت ترمیمی و تعاون اجتماعی، این نهاد با جبران خسارت قربانیان بی‌گناه حملات سایبری (مانند یک فروشگاه اینترنتی کوچک که قربانی سرقت داده می‌شود)، به تعدیل ثروت و حمایت از اقشار آسیب‌پذیر در فضای مجازی کمک می‌کند. این عملکرد، عینیت بخشیدن به روح آیه شریفه «تعاونوا علی البر والتقوی» (سوره مائده: آیه ۲) است که بر همکاری در کارهای نیک و پرهیزکاری تأکید دارد. جبران خسارت زیان‌دیده، مصداقی از «بر» و همکاری اجتماعی برای رفع آسیب است.

دوم، از نظر تنظیم بازار و پیشگیری از ضرر عمومی، بیمه با سازوکارهای هوشمند

خود، نقش تنظیم‌گر غیرمستقیم را ایفا می‌کند. شرکت‌های بیمه با اعطای مشوق‌های مالی (مانند تخفیف حق بیمه) به کسب‌وکارهایی که استانداردهای امنیتی بالاتری را رعایت می‌کنند، عملاً آنان را به سرمایه‌گذاری در امنیت و مسئولیت‌پذیری بیشتر سوق می‌دهند *(Woods & Simpson, 2017)*.

این فرایند، درواقع اجرای حکومتی قاعده فقهی «لاضرر و لاضرار فی الاسلام» در سطح کلان است؛ زیرا با تشویق به رعایت اصول احتیاطی، از وقوع ضررهای گسترده و نوعی در جامعه جلوگیری می‌کند. حکومت با هدایت این بازار، می‌تواند بدون دخالت مستقیم و سنگین، سطح سلامت و انصاف در بازار دیجیتال را ارتقا دهد.

سوم، در حوزه فرهنگ‌سازی و سرمایه اجتماعی، بیمه سایبری با کاهش اضطراب و ترس ناشی از ریسک‌های سایبری، به مشارکت فعال‌تر افراد و بنگاه‌ها در اقتصاد دیجیتال و تقویت «سرمایه اجتماعی» کمک می‌کند. احساس امنیت ناشی از پوشش بیمه‌ای، زمینه اعتماد و همکاری بیشتر بین فعالان بازار را فراهم می‌آورد. افزون‌براین، برنامه‌های آموزشی و ترویجی که بسیاری از بیمه‌گران به‌عنوان بخشی از خدمات خود ارائه می‌دهند (مانند کارگاه‌های شبیه‌سازی حملات فیشینگ و انتشار گزارش‌های تهدیدات)، به نهادینه‌سازی «سواد امنیتی» به‌عنوان یک فرهنگ عمومی پایدار کمک شایانی می‌نماید. این آموزش‌ها که گاه به‌صورت رایگان ارائه می‌شوند، بازوی فرهنگی حکومت در ارتقای آگاهی عمومی محسوب می‌گردند.

نتیجه این بخش آن است که بیمه سایبری از طریق سازوکارهای جبران خسارت، مشوق‌های اقتصادی و آموزش، می‌تواند در خدمت اهداف اجتماعی حکومت یعنی تحقق عدالت، تنظیم عادلانه بازار و تقویت سرمایه اجتماعی قرار گیرد. این کارکردها، مستند به مبانی قرآنی (تعاون)، قواعد فقهی (نفی ضرر) و سازوکارهای عقلایی پذیرفته‌شده در مدیریت جامعه است.

با تحلیل چهاربعد فوق روشن می‌گردد که بیمه سایبری صرفاً یک قرارداد خصوصی نیست، بلکه نهادی است با کارکردهای چندلایه جبرانی، پیشگیرانه (تنظیم‌گری) و فرهنگ‌ساز که دقیقاً در مسیر تحقق مصالح قطعی نظام اسلامی (حفظ نظام، صیانت از امنیت، نفی ضرر عمومی و تحقق عدالت) قرار دارد.

از سوی‌دیگر، اجتناب‌ناپذیر بودن فضای دیجیتال و حرج شدید ناشی از فعالیت در آن بدون پوشش مدیریت ریسک، «ضرورت» توجه حکومت به این عرصه را با استناد به آیه نفی حرج و قاعده عسر و حرج تأکید می‌نماید؛ بنابراین، با عنایت به اینکه «مصلحت» معیار مشروعیت تصرفات حکومتی است و این نهاد هم مصلحت‌های کلان را محقق می‌سازد و هم پاسخی به یک ضرورت عصر است، مداخله حکومت اسلامی در هدایت، تقنین، تنظیم و توسعه بیمه سایبری، نه‌تنها یک اختیار، که یک تکلیف شرعی راهبردی در چهارچوب فقه حکومتی محسوب می‌شود. غفلت از این مسئولیت، با توجه به قاعده لاضرر، قصور در انجام وظیفه ولایی خواهد بود.

## ۸. تحلیل تطبیقی مبانی فقهی بیمه سایبری با رویکردهای حقوقی غربی و اسلامی

پس از اثبات مشروعیت اولیه عقد بیمه سایبری بر اساس مبانی فقه امامیه درمباحث پیشین، اینک نوبت به تحلیل تطبیقی این مبانی با رویکردهای حقوقی حاکم بر بیمه سایبری در نظام‌های حقوقی غربی و تجربه کشورهای اسلامی می‌رسد. این تحلیل تطبیقی از آن رو ضروری است که نشان دهد مبانی فقهی نه‌تنها با اصول پذیرفته‌شده جهانی در تعارض نیست بلکه در بسیاری از موارد همپوشانی دارد و می‌تواند مبنایی مستحکم برای طراحی الگوی بومی فراهم آورد.

در حقوق غربی، بیمه سایبری همانند سایر انواع بیمه، بر پایه چهار اصل بنیادین استوار است که هر یک در فقه امامیه دارای معادل و مبنای قابل تطبیق است.

نخست، اصل «نهایت حسن نیت» که به موجب آن طرفین قرارداد ملزم به ارائه اطلاعات کامل و صادقانه هستند و هرگونه کتمان یا تحریف اطلاعات می‌تواند موجب بطلان قرارداد شود. این اصل با قاعده فقهی «المؤمنون عند شروطهم» و لزوم صداقت در معاملات قابل انطباق است. در بیمه سایبری، این اصل اهمیت مضاعفی می‌یابد؛ زیرا بیمه‌گذار باید اطلاعات دقیقی از زیرساخت‌های امنیتی، سوابق حملات و اقدامات حفاظتی خود ارائه دهد و بیمه‌گر نیز باید دامنه پوشش‌ها و استثنائات را به‌روشنی بیان کند *(انصاری و عسکری*

*دهنوی، ۱۳۹٤).*

دوم، اصل «منفعت بیمه‌پذیر» که بر اساس آن بیمه‌گذار باید نسبت به موضوع بیمه ذی‌نفع باشد. مطابق ماده ٤ قانون بیمه ایران، «بیمه‌گذار باید در بقای مال مورد بیمه ذی‌نفع باشد، والا عقد بیمه باطل است». به‌عبارت‌دیگر، شخصی که مال مورد بیمه برای او منفعتی دارد و در صورت بروز حادثه، ضرر و زیانی متوجه او می‌شود، می‌تواند آن مال را بیمه کند. این اصل با قاعده فقهی «مَنْ لَهُ الْغَنَمُ فَعَلَيْهِ الْغُرْمُ» تطابق کامل دارد؛ به این معنا که هر کس از چیزی منفعت می‌برد، باید زیان آن را نیز متحمل شود. در بیمه سایبری، این اصل ایجاب می‌کند که بیمه‌گذار حتماً مالک یا مسئول قانونی دارایی‌های دیجیتال موضوع بیمه باشد؛ زیرا در غیراین‌صورت قرارداد به دلیل فقدان نفع قابل بیمه، باطل خواهد بود. در عصر دیجیتال، اعمال این اصل با چالش‌هایی مواجه است؛ ازجمله نبود شناسایی قانونی صریح برای دارایی‌های دیجیتال، دشواری ارزش‌گذاری داده‌ها و نوسانات شدید ارزش ارزهای دیجیتال. بااین‌حال، با توجه به اثبات مالیت عرفی دارایی‌های دیجیتال و قابلیت تعیین ارزش اقتصادی آن‌ها، می‌توان رابطه ذی‌نفعی را بر اساس مالکیت یا مسئولیت قانونی احراز نمود.

سوم، اصل «جبران خسارت» که هدف از عقد بیمه را بازگرداندن وضعیت مالی بیمه‌گذار به وضعیت پیش از حادثه می‌داند، نه ایجاد منفعت یا سود برای وی. این اصل با قاعده «لاضرر» در فقه امامیه کاملاً قابل تطبیق است. بر اساس قاعده لاضرر، هرگونه ضرر و زیان وارده باید جبران شود و بیمه دقیقاً سازوکاری برای تحقق همین هدف در قالبی سازمان‌یافته است. در بیمه سایبری، این اصل ایجاب می‌کند که خسارت پرداختی از سوی بیمه‌گر نباید بیش از میزان واقعی زیان وارده باشد *(افراسیابی تحسین، ۱۳۹۳).*

چهارم، اصل «قائم‌مقامی» که به بیمه‌گر اجازه می‌دهد پس از پرداخت خسارت به بیمه‌گذار، برای بازیافت مبلغ پرداختی به عامل زیان رجوع کند. این اصل با قاعده «تسبیب» در فقه و ماده ۳۰ قانون بیمه ایران قابل انطباق است. در فضای سایبری، اعمال این اصل با چالش‌هایی مواجه است، به‌ویژه زمانی که عامل حمله ناشناس یا در حوزه قضائی دیگری باشد. بااین‌حال، این چالش‌ها به اصل قاعده خدشه‌ای وارد نمی‌کنند و صرفاً نیازمند طراحی سازوکارهای اجرایی مناسب هستند *(احمدی و بدرزاده، ۱۳۹۹).*

مقررات و استانداردهای بین‌المللی که چهارچوب بیمه سایبری را شکل می‌دهند نیز از منظر فقهی قابل تحلیل و تطبیق هستند. استاندارد ایزو ۲۷۱۰۲ که به‌طور خاص به راهنمایی برای بیمه سایبری می‌پردازد، و قوانین نمونه آنسیترال در حوزه تجارت الکترونیک، الزاماتی را برای افشای اطلاعات، رعایت شروط ایمنی و تعیین استثنائات پوشش مقرر کرده‌اند.

در زمینه افشای اطلاعات، استانداردهای بین‌المللی بیمه‌گر را ملزم به شفاف‌سازی کامل شرایط و استثنائات بیمه‌نامه و بیمه‌گذار را ملزم به ارائه اطلاعات دقیق درباره وضعیت امنیتی خود می‌کنند. از منظر فقهی، این الزام مشروط به دو قید است: نخست، عدم افشای داده‌های محرمانه تجاری و حریم خصوصی افراد، و دوم، محدود بودن دامنه افشا به رفع جهالت مؤثر در قرارداد. به‌عبارت‌دیگر، صرفاً اطلاعاتی باید افشا شود که در تصمیم‌گیری طرف مقابل برای انعقاد یا قیمت‌گذاری قرارداد مؤثر است و افشای بیش از این مقدار، خود می‌تواند مصداق تجاوز به حقوق مالکیت فکری یا حریم خصوصی باشد.

در مورد شروط ایمنی مانند الزام به رمزنگاری، نصب فایروال، انجام ممیزی‌های دوره‌ای و آموزش کارکنان، قاعده «المؤمنون عند شروطهم» مبنای فقهی محکمی برای پذیرش و الزام‌آوری این شروط فراهم می‌کند. بر اساس این قاعده، بیمه‌گذار با امضای قرارداد، به تمامی شروط مندرج در آن ملتزم می‌شود و تخلف از این شروط می‌تواند به کاهش یا سلب تعهد بیمه‌گر بینجامد.

در خصوص استثنائات پوشش، به‌ویژه استثنای «جنگ سایبری» که در بسیاری از بیمه‌نامه‌های بین‌المللی گنجانده شده، قاعده لاضرر و مسئولیت حکومت در حفظ نظام اقتضا می‌کند که دولت از محل منابع عمومی خسارات ناشی از این قبیل حملات را که خارج از ظرفیت بازار بیمه است، جبران کند. این همان منطقی است که ایجاد صندوق تضمین دولتی برای ریسک‌های سیستمی را توجیه می‌کند.

در ایالات متحده، قوانین متعددی در حوزه بیمه سایبری و حفاظت از داده‌ها تصویب شده که هر یک به‌نوعی با مبانی فقهی قابل تطبیق هستند: قانون تقلب و سوءاستفاده رایانه‌ای (CFAA)برای مقابله با جرایم رایانه‌ای که با قواعد فقهی منع افساد و حرمت مال مسلمان هم‌راستاست؛ قانون حفاظت از اطلاعات پزشکی (HIPAA) برای حفاظت از اطلاعات سلامت

افراد که با قاعده حرمت افشای اسرار و کرامت انسانی تطابق دارد؛ قانون حفاظت از اطلاعات مالی (GLBA) برای مؤسسات مالی که با قاعده حفظ اموال و مسئولیت امانی سازگار است؛ قانون به اشتراک‌گذاری اطلاعات سایبری (CISA) برای تبادل اطلاعات تهدیدات که با قاعده تعاون و همکاری در دفع ضرر همخوانی دارد؛ و قانون حفاظت از حریم خصوصی مصرف‌کنندگان کالیفرنیا (CCPA) برای کنترل اطلاعات شخصی که با قاعده تسلیط و حق کنترل بر اطلاعات شخصی قابل انطباق است. در کانادا نیز قانون حفاظت از اطلاعات شخصی و اسناد الکترونیکی (PIPEDA) و در اتحادیه اروپا، مقررات عمومی حفاظت از داده‌ها (GDPR)مهم‌ترین قوانین حفاظت از داده‌ها هستند که همگی بر ضرورت جبران خسارت ناشی از نقض داده‌ها تأکید دارند *(فتاحی زفرقندی و کلانتری، ۱۴۰۳)*.

در کشورهای اسلامی مانند مالزی، بحرین و امارات، مدل «بیمه متقابل سایبری» (تکافل سایبری) مبتنی بر عقد تبرع (هدیه) توسعه یافته که از منظر فقهی دارای مزایای قابل‌توجهی است. در این مدل، بیمه‌گذاران حق بیمه را نه به‌عنوان عوض در یک معامله معوّض، بلکه به‌عنوان هدیه و تبرع به صندوق مشترک پرداخت می‌کنند. این ساختار، شبهه غرر را که یکی از مهم‌ترین چالش‌های فقهی فراروی بیمه متعارف است، به‌طور اساسی مرتفع می‌سازد. همچنین شبهه ربا نیز در این مدل منتفی است؛ زیرا هیچ‌گونه سود تضمین‌شده یا بهره‌ای در کار نیست و مازاد صندوق پس از کسر هزینه‌ها میان بیمه‌گذاران توزیع می‌شود. این مدل با آیه «تعاونوا علی البر و التقوی» *(سوره مائده: آیه ۲)* همخوانی کامل دارد.

بر اساس ضوابط بانک مرکزی مالزی در چهارچوب مجوزدهی به اپراتورهای دیجیتال بیمه و بیمه متقابل مصوب ۲۰۲۴-۲۰۲۲، مدل‌های مشارکت در ریسک ازجمله طرح‌های حمایت متقابل به‌رسمیت شناخته شده و الزام به رعایت شریعت برای متقاضیان دریافت مجوز بیمه متقابل دیجیتال تصریح گردیده است. این چهارچوب مقرراتی نشان می‌دهد که کشورهای اسلامی پیشرو، به‌خوبی دریافته‌اند که مدل تکافل می‌تواند راهکاری برای توسعه بیمه سایبری در جوامع اسلامی بدون مخدوش ساختن موازین شرعی باشد *(Bank Negara Malaysia, 2022)*.

با وجود ظرفیت‌های موجود در مدل بیمه متقابل سایبری و مبانی مستحکم فقهی برای مشروعیت بیمه سایبری، اجرای این نوع بیمه در ایران با چالش‌های مهمی مواجه است که

شناخت آن‌ها برای طراحی الگوی مناسب ضروری است. مهم‌ترین این چالش‌ها عبارت‌اند از:

نخست، نبود داده‌های آماری معتبر برای محاسبه ریسک. صنعت بیمه بر اساس مدل‌های آماری و اکچوئری کار می‌کند و فقدان داده‌های تاریخی درباره حملات سایبری در ایران، محاسبه حق بیمه مناسب را دشوار می‌سازد *(پژوهشکده بیمه، ۱۴۰۲)*.

دوم، ابهام در مالیت برخی دارایی‌های دیجیتال. اگرچه در فصول پیشین مالیت دارایی‌های دیجیتال با استناد به آرای امام خمینی و شهید صدر اثبات شد؛ اما در عمل هنوز برخی از انواع داده‌ها و دارایی‌های دیجیتال از نظر عرفی و قانونی با ابهام در ارزش‌گذاری مواجه‌اند *(بهمن‌پوری و همکاران، ۱۳۹۳)*.

سوم، نبود قانون جامع حریم خصوصی. قوانین موجود در ایران فاقد چهارچوب منسجم برای حفاظت از داده‌های شخصی هستند و این خلأ، تعیین حدود مسئولیت بیمه‌گذار و بیمه‌گر را با دشواری مواجه می‌کند.

چهارم، ضعف زیرساخت‌های فنی ارزیابی خسارت. ارزیابی دقیق خسارات سایبری نیازمند تخصص فنی بالاست و کمبود کارشناسان زبده در این حوزه، فرآیند رسیدگی به خسارات را کند و پرهزینه می‌کند.

پنجم، فقدان استاندارد واحد برای قراردادها. نبود یک استاندارد ملی برای بیمه‌نامه‌های سایبری، موجب سردرگمی بیمه‌گران و بیمه‌گذاران و افزایش ریسک حقوقی قراردادها می‌شود.

و ششم، خطر شکست‌های آبشاری ناشی از ریسک‌های سیستمی. حملات سایبری می‌توانند به‌سرعت از یک بخش به بخش‌های دیگر سرایت کنند و این امر مدیریت ریسک انباشت را برای بیمه‌گران ایرانی که تجربه محدودی در این حوزه دارند، بسیار دشوار می‌سازد *(فتاحی زفرقندی و کلانتری، ۱۴۰۳)*.

نظام حقوقی ایران می‌تواند با بهره‌گیری از ظرفیت‌های فقه امامیه، به‌ویژه نظریه ولایت مطلقه فقیه، و استفاده از تجارب کشورهای اسلامی در مدل بیمه متقابل سایبری، زمینه رفع تدریجی این چالش‌ها را فراهم آورد. رویکرد تدریجی و گام‌به‌گام در طراحی مدل پیشنهادی برای ایران که در بخش‌های بعدی این فصل تشریح خواهد شد، دقیقاً با هدف مدیریت همین چالش‌ها تدوین شده است.

## ۹. وضعیت حقوق موضوعه ایران در مواجهه با بیمه سایبری و خلأهای قانونی

پیش از آنکه حکومت اسلامی بتواند مداخله فعال در بیمه سایبری داشته باشد، باید ظرفیت‌ها و خلأهای نظام حقوقی موجود را به‌دقت بشناسد. این شناخت، خود بخشی از تکلیف «حفظ نظام» در چهارچوب فقه حکومتی است؛ زیرا بدون احراز خلأهای قانونی، نمی‌توان مسئولیت حکومت در قانون‌گذاری و تنظیم‌گری را تعیین نمود. بررسی قوانین موجود نشان می‌دهد که نظام حقوقی ایران فاقد چهارچوب اختصاصی برای بیمه سایبری است و قوانین عام موجود نیز کارآمدی لازم را ندارند.

۱. قانون بیمه مصوب ۱۳۱٦. ماده ۱ این قانون، بیمه را چنین تعریف می‌کند: «بیمه عقدی است که به‌موجب آن یک‌طرف تعهد می‌کند در ازای پرداخت وجه یا وجوهی از طرف‌دیگر، در صورت وقوع یا بروز حادثه، خسارت وارده به او را جبران نموده یا وجه معینی به وی یا به شخص ثالث بپردازد». هرچند این تعریف کلیت مناسبی دارد و می‌تواند مبنای عقود بیمه‌ای قرار گیرد؛ اما برای ریسک‌های ناملموس سایبری (مانند سرقت داده، وقفه کسب‌وکار دیجیتال، یا آسیب به شهرت) کافی نیست. در این تعریف، مفهوم «خسارت» به‌صورت سنتی بر خسارت به اموال مادی حمل می‌شود، حال آنکه در فضای سایبری، بسیاری از دارایی‌ها ماهیت دیجیتال و غیرملموس دارند. ازاین‌رو، اصلاح ماده ۱ با افزودن عبارت «اعم از خسارت به اموال مادی یا دارایی‌های دیجیتال» ضروری به نظر می‌رسد *(فتاحی زفرقندی و کلانتری، ۱٤۰۳)*.

۲. قانون تجارت الکترونیک مصوب ۱۳۸۲. مواد ٤٦ تا ٥٤ این قانون به مسئولیت ارائه‌دهندگان خدمات در فضای الکترونیکی پرداخته است. این مواد شامل تکالیفی برای حفاظت از داده‌های مصرف‌کنندگان و جبران خسارات ناشی از نقض این تکالیف می‌شود. بااین‌حال، قانون مذکور هیچ اشاره‌ای به بیمه به‌عنوان ابزار جبران خسارت یا مدیریت ریسک نکرده است. فقدان پیوند میان مسئولیت‌های قانونی و سازوکار بیمه‌ای، خلأ مهمی در نظام حقوق تجارت الکترونیک ایران ایجاد کرده است.

۳. قانون جرایم رایانه‌ای مصوب ۱۳۸۸. این قانون عمدتاً جنبه کیفری دارد و به جرم‌انگاری رفتارهای مخرب در فضای سایبری پرداخته است؛ اما سازوکار اجرایی مشخصی برای

جبران خسارت مدنی ناشی از جرایم سایبری پیش‌بینی نکرده است. به‌عبارت‌دیگر، قانون‌گذار صرفاً به تعیین مجازات برای مرتکب بسنده کرده و از طراحی نظام جبران خسارت برای قربانیان غفلت نموده است. بیمه سایبری می‌تواند این خلأ را پر کند؛ اما تا زمانی که چهارچوب قانونی برای آن تعریف نشود، قربانیان حملات سایبری در عمل راهی برای جبران خسارت نخواهند داشت.

از منظر فقه حکومتی، این خلأهای سه‌گانه صرفاً نقص فنی حقوقی نیستند بلکه قصور در ایفای مسئولیت ذاتی حکومت در «حفظ نظام اقتصادی دیجیتال» و «صیانت از اموال عمومی» تلقی می‌شوند. حکومت اسلامی بر اساس نظریه ولایت مطلقه فقیه، مکلف به تأمین امنیت اقتصادی جامعه است و بخشی از این امنیت، در گرو وجود نظام جبران خسارت کارآمد برای ریسک‌های نوظهور سایبری است. ازاین‌رو، ورود فوری حکومت به عرصه قانون‌گذاری و تنظیم‌گری بیمه سایبری، نه یک اختیار که یک تکلیف شرعی و قانونی است.

## نتیجه‌گیری

این پژوهش با هدف تحلیل مسئولیت و مشروعیت مداخله حکومت اسلامی در بیمه سایبری، در چهارچوب فقه حکومتی و نظریه ولایت مطلقه فقیه انجام شد. یافته‌ها نشان داد تأمین امنیت سایبری ذیل قاعده «حفظ نظام»، مسئولیتی ذاتی و شرعی برای حکومت اسلامی است. مالیت دارایی‌های دیجیتال با استناد به آرای امام خمینی و شهید صدر اثبات شد و مشروعیت عقد بیمه سایبری با تکیه بر نظریه «عقد مستقل» امام خمینی و ادله قرآنی (أوفوا بالعقود، تعاونوا علی البر) احراز گردید. پنج چالش فقهی خاص (باج‌افزار، سود منتفی، خطای هوش مصنوعی، تداخل بیمه‌نامه‌ها و قائم‌مقامی در فرض ناشناس بودن هکر) بررسی و راهکارهای میانی ارائه شد.

مشروعیت مداخله حکومت در چهار بُعد مصلحتی، امنیتی–دفاعی، اقتصادی و اجتماعی مستند گردید. مطالعه تطبیقی نشان داد الگوی ترکیبی شامل الزام تدریجی بخش‌های حیاتی، مدل دوگانه بیمه متعارف و تکافل سایبری، استانداردهای فنی و صندوق تضمین دولتی برای ایران مناسب است. حکومت اسلامی با اتکا به نظریه ولایت مطلقه فقیه، مکلف به اتخاذ رویکردی چندسطحی (تقنین، تنظیم‌گری، نظارت و توانمندسازی) برای ساماندهی بیمه سایبری است. فقه

امامیه با ظرفیت اجتهاد پویا، توانایی پاسخگویی به مسائل مستحدثه را دارد.

## پیشنهادات تخصصی و عملیاتی (مبتنی بر تحلیل فقه حکومتی)

بر اساس مبانی فقه حکومتی و با توجه به خلأهای شناسایی شده در بخش‌های پیشین، پیشنهادات ذیل در چهار سطح تدوین می‌گردد:

الف) پیشنهادات به مجلس شورای اسلامی(تقنین)

۱. اصلاح ماده ۱ قانون بیمه با افزودن عبارت «اعم از خسارت به اموال مادی یا دارایی‌های دیجیتال و همچنین سود قابل پیش‌بینی ناشی از وقفه کسب‌وکار مستند به رویه عرفی».

۲. تصویب قانون جامع حفاظت از داده‌های شخصی با الهام از GDPR اروپا، مشتمل بر:

- جریمه‌های مؤثر حداقل ۲درصد درآمد سالانه برای نقض داده
- الزام به اطلاع‌رسانی نقض داده ظرف ۷۲ ساعت
- تعریف حریم خصوصی دیجیتال به‌عنوان «مال معنوی» با ارزش اقتصادی

۳. الحاق ماده ۲۹ مکرر به قانون بیمه برای الزام تدریجی بخش‌های حیاتی (بانک‌ها، بیمه‌ها، بیمارستان‌ها، نیروگاه‌ها، اپراتورهای مخابراتی) به خرید بیمه سایبری ظرف حداکثر ۳ سال با الهام از تجربه ترکیه .

ب) پیشنهادات به بیمه مرکزی جمهوری اسلامی ایران

٤. تدوین و ابلاغ «دستورالعمل ارزیابی ریسک سایبری برای بیمه‌گران» با الهام از دستورالعمل EIOPA (2023) مشتمل بر:

- حداقل استانداردهای امنیتی برای بیمه‌پذیری (رمزنگاری، فایروال، بک‌آپ منظم)
- مدل‌های کمی ارزیابی ریسک متناسب با داده‌های بومی
- الزام به گزارش حملات سایبری به سامانه ملی ثبت خسارت

۵ . تدوین نمونه قرارداد استاندارد بیمه سایبری در دو نسخه متعارف و تکافل با الهام از مدل مالزی *(Bank Negara Malaysia, 2022)* .

- شرایط عمومی (همکاری در تحقیق، اطلاع‌دهی فوری حداکثر ۷۲ ساعت، رازداری متقابل)

- استثنائات استاندارد (اقدام عمدی بیمه‌گذار، جنگ سایبری، جریمه‌های دولتی)
- شروط فقهی در نسخه تکافل (عقد تبرع، نقش متولی، صندوق قرض‌الحسنه)

٦. ایجاد سامانه ملی ثبت خسارت سایبری برای رفع مشکل نبود داده آماری

۷. صدور مجوز تخصصی بیمه سایبری جدا از مجوز عمومی، با الزام به داشتن گروه فنی ارزیابی ریسک سایبری.

ج) پیشنهادات به شورای عالی فضای مجازی (راهبری کلان)

۸. تأسیس «مرکز ملی داده‌های سایبری» برای جمع‌آوری، پردازش و اشتراک کنترل‌شده داده‌های حملات سایبری با بیمه مرکزی و بیمه‌گران (مستند: قاعده «حفظ نظام» و تکلیف حکومت به امنیت‌آفرینی).

۹. تدوین «سند ملی بیمه سایبری» با رویکرد فقه حکومتی و تصویب در شورای عالی، مشتمل بر:

- چشم‌انداز ۱۰ ساله توسعه بازار بیمه سایبری
- تعیین مصادیق جنگ سایبری برای رفع ابهام از استثنای قراردادها
- ترسیم حدود مداخله حکومت در نرخ‌گذاری و نظارت

د) پیشنهادات به دستگاه‌های اجرایی (دولت، قوه قضائیه، نهادهای نظارتی)

۱۰. اعطای تخفیف ۱۰ درصد مالیاتی به شرکت‌های دارای گواهی ISO 27001 و بیمه سایبری معتبر

۱۱. گنجاندن سرفصل «مدیریت ریسک سایبری و بیمه دیجیتال» در دوره‌های کارشناسی ارشد حقوق، فقه اسلامی، مدیریت بیمه و مهندسی فناوری اطلاعات (وزارت علوم) همچنین دوره‌های مهارت‌آموزی شهروندی (وزارت آموزش و پرورش و سازمان فنی و حرفه‌ای)

۱۲. تشکیل کمیته فقهی–حقوقی ویژه بیمه سایبری در قوه قضائیه برای تدوین رویه قضائی منسجم در خصوص مسئولیت مدنی ناشی از حملات سایبری.

## منابع


قرآن کریم.

نهج‌البلاغه

آخوند خراسانی، محمدکاظم (بی‌تا). *کفایة الاصول* (ج۱). قم: مؤسسه آل البیت (علیهم‌السلام).

ابن‌شعبه حرانی، حسن بن علی (١٤٠٤ق). *تحف العقول عن آل الرسول علیهم‌السلام* (علی‌اکبر غفاری، تحقیق و تعلیق). قم: جامعه مدرسین حوزه علمیه قم.

احمدی، مریم و بدرزاده، اکبر (۱۳۹۹). بررسی تطبیقی اصل قائم‌مقامی بیمه‌گر در حقوق بیمه ایران و فرانسه. *مطالعات فقه اقتصادی*، ۲(۳)، ۷۲-۵۵.

افراسیابی تحسین، حمید (۱۳۹۳). *اصل غرامت در حقوق بیمه* (پایان‌نامه کارشناسی ارشد). دانشگاه آزاد اسلامی واحد کرمانشاه، کرمانشاه.

السان، مصطفی (۱۳۹۱). *حقوق تجارت الکترونیکی*. تهران: انتشارات سمت.

السان، مصطفی؛ کلانتری، رضا و سجادی، سعید (۱۳۹۵). بیمهٔ مسئولیت و خسارت‌های وارده در فضای مجازی. *پژوهشنامه بیمه*، ٦(۱)، ٥٥-٤١.
https://doi.org/10.22056/ijir.2017.01.04

انصاری، علی و عسکری دهنوی، جواد (١٣٩٤). مطالعهٔ تطبیقی نقش حسن‌نیت بیمه‌گر در انعقاد عقد بیمه (حقوق ایران و نظام‌های حقوقی معاصر). *پژوهشنامه بیمه*، ۳۰(۲)، ٦٨-٤٥.
https://doi.org/10.22056/ijir.2015.03.07

انصاری، مرتضی (١٤١٠ق). *المکاسب* (جلد ۱۰و۷). قم: دار الکتاب.

ایزدهی، سیدسجاد و صدیق تقی‌زاده، صدیقه (۱۳۹۹). ماهیت و ویژگی‌های فقه حکومتی. *حکومت اسلامی* ۱. ٥-٢٦.

ایوب، عبدالناصر محمد و البغدادی، أحمد محمد (٢٠٢٢). الأخلاق والقانون والأمن السیبرانی. *مجلة بنها للعلوم الإنسانیة*، ۲(۱)، ۲۵-۱.

بابایی، ایرج (١٤٠١). *حقوق بیمه*. تهران: انتشارات سمت.

بهمن پوری، ع.؛ شادمانفر، م. ر. و پورغلامی فراشبندی، م. (۱۳۹۳). بررسی فقهی حقوقی مال بودن داده‌های رایانه‌ای. *فقه و مبانی حقوق اسلامی*، ٤٧(۲)، ۲۳۱-٢٤٤.

https://doi.org/10.22059/JJFIL.2014.53403
پلیس فتا (۱٤۰۲). گزارش عملکرد سالانه جرایم سایبری کشور. تهران: پلیس فضای تولید و تبادل اطلاعات (فتا)
پژوهشکده بیمه (۱۳۹۳). دانشنامه بیمه (ج. ۱). تهران: پژوهشکده بیمه.
پژوهشکده بیمه (۱٤۰۲). *مطالعه و بررسی مقدماتی تجربیات سایر کشورها در حوزه ریسک‌ها و بیمه‌های سایبری* (گروه پژوهشی فناوری‌های نوین، شماره ۱۷٤).
پورقصاب امیری، علی و حسنی کاخ، محمدعلی (۱۳۹۷). بیمه سایبری راهکاری برای ایجاد امنیت در فضای مجازی. ارائه شده در *ششمین کنفرانس ملی حقوق و مطالعات قضائی*، تهران.
https://civilica.com/doc/877249
تمیمی آمدی، عبدالواحد بن محمد (۱٤۱۰ق). *غرر الحکم و درر الکلم* (سیدمهدی رجائی، محقق و مصحح). قم: دار الکتاب الإسلامی.
جوادی آملی، عبدالله (۱۳۹۱). درس خارج فقه، ۱۳۹۱/۲/۳۰.
حسن‌پور، مجید، و اولوخانی، نفیسه (۱٤۰۰). شناسایی و اولویت‌بندی چالش‌های پیش‌روی بیمه سایبری در ایران. ارائه شده در *بیست و هشتمین همایش بیمه و توسعه*، تهران.
https://civilica.com/doc/1390777
حسنی، سعید و کریمیان، نورالله (۱٤۰۰). وظیفه حکومت اسلامی نسبت به تأمین امنیت در فضای سایبر با تأکید بر بیانیه گام دوم انقلاب اسلامی. *مطالعات انقلاب اسلامی*، ۱۷(٦۳)، ۱۱٦-۹۵. https://www.magiran.com/p2314144
حکیم، سیدمحسن (۱۳۵۳). *منهاج‌الصالحین*. تهران: لطفی.
حلی، حسین (۱۳۸٤). *بحوث فقهیه*. بیروت: دارالزهرا.
خالقی دخت، محمود (۱٤۰۱). *مباحث تخصصی پدافند سایبر*. تهران: سبک نو.
خمینی، سیدروح‌الله (۱۳۸۹). *صحیفه امام: مجموعه آثار امام خمینی(س): بیانات، پیام‌ها، مصاحبه‌ها، احکام، اجازات شرعی و نامه‌ها* (ج۲۰). تهران: مؤسسه تنظیم و نشر آثار امام خمینی(س).
خمینی، سیدروح‌الله (۱۳۹۲). *کتاب البیع (ج۲)*. تهران: مؤسسه تنظیم و نشر آثار امام خمینی.
خمینی، سیدروح‌الله (۱٤۳٤ق). *تحریر الوسیله (ج۲)*. تهران: مؤسسهٔ تنظیم و نشر آثار الإمام الخمینی.

خویی، سیدابوالقاسم (۱٤۱۲ق). *توضیح‌المسائل*. قم: انتشارات مهر.

دفتر حفظ و نشر آثار حضرت آیت‌الله العظمی خامنه‌ای (۱۳۷۱/۰۸/۲٤). پیام به جامعه مدرسین حوزه علمیه قم. بازیابی از https://khamenei.ir

دهخدا، علی‌اکبر (۱۳۷۲). *لغت‌نامه* (چاپ اول). تهران: انتشارات دانشگاه تهران.

رشاد، علی‌اکبر (۱۳۸۱). اجتهاد موجود و اجتهاد مطلوب. *پژوهش و حوزه*، ۳(۱۲)، ٤۳.

سند، محمد (۱۳۹۷). گفت‌وگو با شبکه اینترنتی اجتهاد، ۱۳۹۷/۸/۲٦.

شریف الرضی، محمد بن حسین (۱۳۷۹). *نهج‌البلاغه* (محمد دشتی، مترجم). قم: مؤسسه تحقیقاتی امیرالمؤمنین(ع).

صابری، م. (۱۳۹۹). بررسی ریسک‌های سایبری و فاکتورهای مؤثر بر تمایل شرکت‌های بیمه به ارائه این بیمه‌نامه به‌صورت مستقل. مقاله ارائه شده در *بیست و هفتمین همایش ملی بیمه و توسعه*. https://civilica.com/doc/1238001

صافی گلپایگانی، ل. (۱٤۳۲ق). *توضیح‌المسائل*. قم: دفتر تنظیم و نشر آثار حضرت آیت‌الله العظمی صافی گلپایگانی.

صدر، سیدمحمدباقر (۱۳۸۹). *بانک بدون ربا*. تهران: فرهنگ سبز.

صدر، سیدمحمدباقر (۱٤۱۰ق). *الإسلام یقود الحیاة*. قم: مجمع جهانی اهل بیت(ع).

طباطبائی، سیدمحمدحسین (۱٤۱۷ق). *المیزان فی تفسیر القرآن*. قم: دفتر انتشارات اسلامی جامعه مدرسین حوزه علمیه قم.

علیدوست، ابوالقاسم (۱۳۹۰، ۸ آذر). *چهار گام برای پویایی فقه حکومتی*. پایگاه اطلاع‌رسانی آیت‌الله علیدوست.

علیدوست، ابوالقاسم (۱٤۰۲). *فقه و مصلحت*. تهران: سازمان انتشارات پژوهشگاه فرهنگ و اندیشه اسلامی.

فاضل لنکرانی، محمد. (۱۳۸۳). جامع المسائل. قم: نشر امیر.

فتاحی زفرقندی، سجاد و کلانتری، رضا (۱٤۰۳). *چالش‌های حقوقی و غیرحقوقی بیمه سایبری*. تهران: پژوهشگاه وزارت ارتباطات و فناوری اطلاعات.
https://civilica.com/doc/1881832

قانون بیمه. مصوب (۱۳۱٦). قابل دسترسی در: پایگاه ملی قوانین و مقررات کشور.

کنفرانس ملی امنیت سایبری. (۱٤۰۰). تهران: دبیرخانه شورای عالی فضای مجازی.

مجلسی، سیدمحمدباقر (۱٤۰۳ق). *بحار الأنوار الجامعة لدرر أخبار الأئمة الأطهار علیهم‌السلام*. بیروت: دار إحیاء التراث العربی.

محمد، آمنه علی البشیر (۲۰۲۱). الأمن السیبرانی فی ضوء مقاصد الشریعة. *مجلة کلیة الدراسات الإسلامیة والعربیة للبنات بالإسکندریة*، ۳۷(٤)، ۲۵۰-۲۱۵.

https://doi.org/10.56793/pcra22136

مرکز ملی فضای مجازی. (۱٤۰۲). *گزارش آماری جرائم و حملات سایبری در سال ۱٤۰۲*. تهران: مرکز ملی فضای مجازی.

مطهری، مرتضی (۱۳۷٤). *مسأله ربا به ضمیمه بیمه*. تهران: انتشارات صدرا.

مکارم شیرازی، ناصر (۱٤۲۷ق). *دائرةالمعارف فقه مقارن* (جلد ۲). قم: مدرسه امام علی بن ابی طالب(ع).

موسوی بجنوردی، سیدمحمد (۱٤۱۹ق). *القواعد الفقهیة* (ج۱). قم: نشر الهادی.

مهریزی، م. (۱۳۷٦). فقه حکومتی. نقد و نظر، ۳(۱۲)، ۱٤۷-۱٤٦.

میرباقری، سیدمحمدمهدی (۱۳۹۲). *درس‌های خارج فقه حکومتی (اردیبهشت ماه)*. قم: برگرفته از پایگاه اطلاع‌رسانی فرهنگستان علوم اسلامی.

نوری، علیرضا و اسماعیلی، علی (۱۳۹۹). مفهوم‌شناسی امنیت در قرآن و زمینه‌های شکل‌گیری آن با تأکید بر روش معناشناسی ایزوتسو. *امنیت ملی*، ۱۰(۳٦)، ۲۷۰-۲۳۳.

20.1001.1.33292538.1399.10.36.8.9

هاشمی شاهرودی، محمود (۱۳۸۲). *فرهنگ فقه مطابق مذهب اهل بیت علیهم السلام* (ج٦). قم: مؤسسه دائرةالمعارف فقه اسلامی بر مذهب اهل بیت (علیهم‌السلام).

یزدی، سیدمحمدکاظم (۱۳۸۱). غایة القصوی فی ترجمة العروة الوثقی (ج ۲). (عباس قمی، مترجم). قم: صبح پیروزی.

Adriko, R., & Nurse, J. R. C. (2024). Cybersecurity, cyber insurance and small-to-medium-sized enterprises: A systematic review. Information & Computer Security, 32(5), 691–710. https://doi.org/10.1108/ICS-01-2024-0025

Allianz. (2023). Allianz risk barometer 2023: Top business risks for 2023. Allianz Global Corporate & Specialty. https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html

Bank Negara Malaysia. (2022). Digital Insurance and Takaful Operators (DITO) Framework. Kuala Lumpur: Bank Negara Allianz Global Corporate & Specialty. Allianz Risk Barometer 2022. 2022.

Biener, C., Eling, M., & Wirfs, J. H. Insurability of Cyber Risk: An Empirical Analysis. The Geneva Papers on Risk and Insurance—Issues and Practice. 2015.

Böhme, R. (2015). Cyber-Insurance Revisited. Workshop on the Economics of Information Security (WEIS).

Böhme, R., & Schwartz, G. (2010). Modeling cyber-insurance: Towards a unifying framework. Proceedings of the Workshop on the Economics of Information Security (WEIS 2010). Harvard University.

Camillo, M. (2017). Cyber risk and the changing role of insurance. Geneva Association Information Newsletter—Cyber Risk, 10, 1–6.

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. The Geneva Papers on Risk and Insurance - Issues and Practice, 47(3), 698-736. https://doi.org/10.1057/s41288-022-00266-6

CrowdStrike. (2024). 2024 global threat report. CrowdStrike Intelligence. https://www.crowdstrike.com/resources/reports/global-threat-report/

Cummins, J. D., & Mahul, O. (2009). Catastrophe risk financing in developing countries: Principles for public intervention. World Bank Publications. https://doi.org/10.1596/978-0-8213-7736-9

Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? The Journal of Risk Finance, 17(5), 474-491. doi: 10.1108/JRF-09-2016-0122

Fitch Ratings. (2022). Cyber Insurance Market Dynamics: Growth and Challenges. Special Report.

Insurance Information Institute. Data Breach Costs: Trends and Analysis. 2013.

Kaspersky. IT Security Economics in 2019: How Businesses Are Losing Money and Saving Costs Amid Cyberattacks. 2019.

Kesan, J. P., & Hayes, C. M. (2019). Strengthening cybersecurity with cyber insurance markets and better risk assessment. Minnesota Law Review, 102(1), 191–264.

Lloyd's of London. (2021). Cyber risk: How insurers can help to build resilience in the face of digital threats [Market bulletin]. Lloyd's Market Association.

Magma Insurance. (2024). Cyber Liability Insurance Policy Wording.

Majuca, R., Yurcik, W., & Kesan, J. P. (2016). The Evolution of Cyberinsurance. ACM Computing Surveys.

Merkin, R., & Steele, J. (2013). Insurance and the law of obligations. Oxford University Press.

Miller, L. (2019). Cyber insurance: An incentive alignment solution to corporate cyber-insecurity. Journal of Law & Cyber Warfare, 7, 147-182.

Microsoft. (2023). Microsoft digital defense report 2023. Microsoft Corporation. https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report

Munich Re. (2021). Cyber Risk: Trends and Insurance Solutions. Munich: Munich Re Group.

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version

1.1. National Institute of Standards and Technology, U.S. Department of Commerce.
Ponemon Institute & IBM Security. (2023). Cost of a Data Breach Report 2023. IBM.
Springer, J. (2015). A Brief History of Cyber Insurance. In Cybersecurity and Insurance (pp. 15-30). Palgrave Macmillan.
Swiss Re. (2020). Cyber: The accumulation risk. Swiss Re Institute.
Turkish Insurance Association. (2016). Cyber Insurance Market in Turkey: Development and Regulation. Istanbul: TIA Publications.
Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: How do carriers price cyber risk? Journal of Cybersecurity, 5(1), tyz002. https://doi.org/10.1093/cybsec/tyz002
University of Maryland, A. James Clark School of Engineering. Study: Hackers Attack Every 39 Seconds. 2007.Malaysia.
Verizon. (2024). Verizon Data Breach Investigations Report (DBIR) 2024. Verizon.
Woods, D., & Simpson, A. (2017). Policy measures and cyber insurance: A framework. Journal of Cyber Policy, 2(2), 209-226. https://doi.org/10.1080/23738871.2017.1360927
World Economic Forum. (2023). Global Cybersecurity Outlook 2023. WEF.