

TINJAUAN HUKUM EKONOMI SYARIAH TERHADAP PENGGUNAAN KEAMANAN SIBER (CYBER SECURITY) SEBAGAI OBJEK BARU ASURANSI SYARIAH DI ERA TRANSFORMASI DIGITAL

Ashqiya Azzahra, Budi Abdullah, Achmad Maulana Ramadhan, Naila Sakbani Fasya, Dwi Febri Linar, Nandita Saskya, Reysya YUSDIANINGSIH, Muhammad Muarif, Farhan Ananda Hanafi, Juliana Handayani

ashqiyazzahra.mhs@insan.ac.id, budiabdullah@insan.ac.id, achmadramadhan.mhs@insan.ac.id, nailafasya.mhs@insan.ac.id, nanditasaskya.mhs@insan.ac.id, reysyayusdianingsih.mhs@insan.ac.id, dwilinar.mhs@insan.ac.id, muhammadmuarif.mhs@insan.ac.id, farhanhanafi.mhs@insan.ac.id, ulisimatupang283@ygmail.com

Institut Syekh Abdul Halim Hasan Binjai

ARTICLE INFO

Keywords: Asuransi Syariah, Keamanan Siber, Pelindungan Data Pribadi, *Maqashid al-Syari'ah*, *Hifz al-Mal*, Hukum Ekonomi Syariah, DSN-MUI

Received : ...

Revised : ...

Accepted : ...

©2023 The Author(s): This is an open-access article distributed under the terms of the [Creative Commons Atribusi 4.0 Internasional](https://creativecommons.org/licenses/by-sa/4.0/)



ABSTRACT

Transformasi digital yang kian masif di berbagai sektor ekonomi dan keuangan telah memunculkan paradoks baru dalam lanskap bisnis modern. Di satu sisi, digitalisasi menciptakan efisiensi, inklusi, dan percepatan transaksi global, tetapi di sisi lain juga melahirkan kerentanan sistemik berupa eskalasi risiko kejahatan siber (*cyber crime*). Ancaman siber seperti peretasan sistem, kebocoran data pribadi, *ransomware*, pencurian identitas, hingga gangguan operasional infrastruktur teknologi menjadi risiko nyata yang berpotensi menimbulkan kerugian materiil berskala besar sekaligus memengaruhi reputasi dan kepercayaan publik terhadap suatu entitas bisnis. Sebagai respons mitigasi yang terstruktur, industri perasuransian telah mengembangkan *cyber insurance* sebagai instrumen transfer risiko. Namun, penerapan asuransi siber dalam ekosistem keuangan Islam menimbulkan persoalan hukum dan fikih, terutama mengenai kedudukan ontologis data digital sebagai harta (*mal muta'awwam*), potensi *gharar* dalam penentuan kontribusi dan kuantifikasi klaim, serta mekanisme pengelolaan dana perlindungan agar tetap sesuai dengan prinsip syariah. Penelitian ini bertujuan menganalisis penggunaan keamanan siber sebagai objek baru asuransi syariah melalui pendekatan hukum positif Indonesia, khususnya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dan regulasi Otoritas Jasa Keuangan, serta melalui kerangka *Maqashid al-Syari'ah*. Penelitian menggunakan metode hukum normatif dengan pendekatan perundang-undangan dan pendekatan konseptual. Hasil penelitian menunjukkan bahwa perlindungan aset digital dan data pribadi memiliki keterkaitan erat dengan prinsip *hifz al-mal* dan *hifz al-'ird*. Asuransi siber berbasis syariah dapat dikembangkan melalui prinsip *ta'awun* dan *takaful* dengan penggunaan akad *tabarru'* dan *wakalah bil ujah*. Potensi *gharar*, *maysir*, dan *riba* dapat diminimalkan melalui transparansi kontrak, pengukuran risiko yang objektif, tata kelola dana yang sesuai syariah, serta penerapan standar keamanan siber.

INTRODUCTION

Memasuki dekade ketiga abad ke-21, revolusi industri 4.0 dan perkembangan masyarakat digital telah mendisrupsi hampir seluruh aktivitas manusia dan mendorong migrasi dari sistem konvensional menuju sistem berbasis elektronik. Digitalisasi telah mengubah pola kegiatan ekonomi, perbankan, perdagangan elektronik, pelayanan publik, serta tata kelola pemerintahan. Perubahan tersebut memberikan manfaat berupa efisiensi, kecepatan transaksi, kemudahan akses, dan peningkatan konektivitas. Akan tetapi, semakin tingginya ketergantungan terhadap teknologi juga memperluas ruang munculnya risiko baru, khususnya risiko keamanan siber (Awais et al., 2025; Aisyah et al., 2026).

Perkembangan teknologi informasi telah menyebabkan data menjadi salah satu komponen penting dalam kegiatan ekonomi modern. Data pribadi, data transaksi, basis data pelanggan, informasi keuangan, sistem informasi, perangkat lunak, dan infrastruktur jaringan memiliki nilai strategis bagi organisasi. Dalam konteks tersebut, keamanan siber tidak lagi hanya dipahami sebagai persoalan teknis yang berkaitan dengan sistem komputer, tetapi telah menjadi bagian dari pengelolaan risiko organisasi dan perlindungan aset. Gangguan terhadap sistem informasi dapat menimbulkan kerugian finansial, gangguan operasional, kehilangan kepercayaan konsumen, serta konsekuensi hukum bagi pihak yang bertanggung jawab (Hutagalung et al., 2025; Junita et al., 2026).

Ancaman tersebut semakin kompleks karena serangan siber dapat berbentuk peretasan, *phishing*, pencurian identitas, *malware*, *ransomware*, kebocoran data, serangan terhadap infrastruktur digital, hingga manipulasi sistem. Dalam sektor keuangan, ancaman siber bahkan dapat memengaruhi stabilitas transaksi dan kepercayaan masyarakat. Aisyah et al. (2026) menunjukkan bahwa peningkatan digitalisasi pada sektor perbankan syariah harus diikuti

dengan penguatan manajemen risiko siber, infrastruktur teknologi, literasi keamanan siber, dan integrasi prinsip syariah ke dalam pengelolaan risiko.

Salah satu instrumen yang berkembang sebagai mekanisme mitigasi risiko tersebut adalah *cyber insurance*. Asuransi siber pada dasarnya dirancang untuk memberikan perlindungan terhadap risiko yang berkaitan dengan serangan atau insiden siber, termasuk biaya pemulihan sistem, investigasi forensik, gangguan operasional, pemberitahuan kepada pihak yang terdampak, serta jenis kerugian lain yang ditentukan dalam polis. Fitrianto et al. (2025) menunjukkan adanya kebutuhan untuk memberikan perhatian lebih besar terhadap pengaturan *cyber insurance*, khususnya dalam sektor perbankan yang memiliki tingkat ketergantungan tinggi terhadap sistem digital.

Namun, ketika konsep tersebut ditempatkan dalam sistem ekonomi syariah, persoalan yang muncul tidak hanya berkaitan dengan aspek teknis dan ekonomi, tetapi juga dengan aspek hukum Islam. Sistem asuransi syariah dibangun berdasarkan prinsip *ta'awun*, yaitu saling membantu dan saling menanggung risiko di antara peserta. Pengelolaan dana peserta harus dilakukan sesuai prinsip syariah dan tidak boleh mengandung unsur *riba*, *gharar*, *maysir*, *zhulm*, maupun praktik yang bertentangan dengan ketentuan syariah (Dewan Syariah Nasional-Majelis Ulama Indonesia [DSN-MUI], 2001; Priyatno et al., 2020).

Persoalan berikutnya berkaitan dengan kedudukan data digital dalam perspektif hukum Islam. Data tidak selalu berbentuk benda fisik, tetapi dapat mempunyai nilai ekonomi, manfaat, dan fungsi yang signifikan. Perkembangan ekonomi digital menuntut adanya kajian mengenai apakah data dan sistem digital dapat ditempatkan dalam kategori harta yang memiliki nilai menurut hukum Islam. Dalam perspektif fikih muamalah kontemporer, pengakuan terhadap manfaat dan nilai ekonomi suatu objek memberikan ruang bagi pengembangan hukum terhadap bentuk-bentuk kekayaan baru.

Karena itu, pembahasan mengenai *mal muta'awwam* menjadi relevan dalam menentukan kedudukan data digital sebagai salah satu objek yang perlu memperoleh perlindungan (Junita et al., 2026).

Selain persoalan harta, keamanan data juga berkaitan dengan amanah dan perlindungan terhadap kehormatan seseorang. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi mengatur asas, jenis data pribadi, hak subjek data, pemrosesan data, kewajiban pengendali dan prosesor data, transfer data, sanksi administratif, serta ketentuan pidana. Dengan demikian, pelindungan data pribadi tidak hanya berkaitan dengan kepentingan ekonomi, tetapi juga berkaitan dengan perlindungan hak pribadi masyarakat (Pemerintah Republik Indonesia, 2022).

Dalam perspektif *Maqashid al-Syari'ah*, perlindungan terhadap data dan sistem digital dapat dihubungkan dengan tujuan menjaga harta (*hifz al-mal*) dan menjaga kehormatan (*hifz al-'ird*). Kajian Farhana (2024) menunjukkan bahwa mekanisme asuransi syariah memiliki keterkaitan dengan prinsip-prinsip *Maqashid al-Syari'ah*, sedangkan penelitian Hutagalung et al. (2025) menunjukkan hubungan antara perilaku keamanan siber dengan konsep *hifz al-mal*. Kajian Junita et al. (2026) juga menempatkan kerangka *Maqashid al-Syari'ah* sebagai pendekatan yang relevan dalam pengelolaan risiko keamanan siber dan perlindungan data.

Permasalahan lainnya adalah potensi *gharar* dalam asuransi siber. Risiko siber memiliki karakteristik yang berbeda dengan risiko konvensional karena sifat serangannya dapat berubah dengan cepat dan kerugian yang timbul tidak selalu mudah diukur. Nilai suatu data yang bocor, biaya pemulihan sistem, kerugian reputasi, kehilangan kepercayaan pelanggan, serta potensi gangguan operasional dapat menghasilkan perhitungan kerugian yang kompleks. Karena itu, diperlukan mekanisme penilaian risiko yang jelas agar ketidakpastian dalam akad tidak berkembang menjadi *gharar fahish*.

Di sisi lain, penerapan asuransi siber juga dapat menghadapi persoalan *moral hazard*. Peserta yang telah memperoleh perlindungan asuransi dapat memiliki kecenderungan mengurangi perhatian terhadap keamanan sistem apabila tidak terdapat persyaratan keamanan yang ketat. Oleh karena itu, penerapan *cyber hygiene*, autentikasi berlapis, enkripsi, *Zero-Trust Architecture*, dan evaluasi keamanan sistem perlu ditempatkan sebagai bagian dari proses *underwriting* dan pengelolaan risiko (Awais et al., 2025; Aisyah et al., 2026).

Dalam kerangka hukum positif Indonesia, pengembangan produk asuransi juga harus memperhatikan regulasi Otoritas Jasa Keuangan. POJK Nomor 69/POJK.05/2016 mengatur penyelenggaraan usaha perusahaan asuransi, perusahaan asuransi syariah, perusahaan reasuransi, dan perusahaan reasuransi syariah, dan ketentuan tersebut telah mengalami perubahan. Sementara itu, POJK Nomor 8 Tahun 2024 memberikan pengaturan yang lebih mutakhir mengenai produk asuransi dan saluran pemasaran produk asuransi, termasuk perkembangan penyelenggaraan secara digital (Otoritas Jasa Keuangan [OJK], 2016, 2024).

Berdasarkan uraian tersebut, terdapat kesenjangan konseptual antara kebutuhan perlindungan terhadap aset digital yang semakin besar dengan kerangka hukum ekonomi syariah yang secara khusus membahas keamanan siber sebagai objek perlindungan asuransi. Oleh sebab itu, penelitian ini ditujukan untuk menganalisis kedudukan ontologis data digital dan keamanan siber dalam perspektif fikih muamalah, menganalisis kesesuaian asuransi siber dengan prinsip asuransi syariah, mengkaji perlindungan data pribadi dalam perspektif *Maqashid al-Syari'ah*, serta merumuskan bentuk mitigasi terhadap unsur *gharar*, *maysir*, *riba*, dan *moral hazard*.

LITERATURE REVIEW

Keamanan Siber dalam Transformasi Digital

Keamanan siber merupakan bagian penting dari tata kelola teknologi informasi

karena meningkatnya ketergantungan organisasi terhadap sistem digital menciptakan risiko baru yang dapat mengganggu keberlangsungan aktivitas ekonomi. Risiko tersebut dapat berupa akses tanpa hak, pencurian data, manipulasi informasi, gangguan sistem, dan serangan terhadap infrastruktur digital. Dalam sektor keuangan Islam, keamanan siber tidak hanya berkaitan dengan perlindungan sistem, tetapi juga berkaitan dengan perlindungan aset, kepercayaan nasabah, serta keberlangsungan aktivitas ekonomi (Awais et al., 2025).

Aisyah et al. (2026) menekankan bahwa pengelolaan risiko siber dalam perbankan syariah memerlukan kombinasi antara infrastruktur teknologi, kebijakan manajemen risiko, literasi keamanan siber, dan kepatuhan terhadap prinsip syariah. Dengan demikian, keamanan siber perlu dipandang sebagai bagian integral dari manajemen risiko, bukan sekadar fungsi teknis.

Hutagalung et al. (2025) menghubungkan perilaku keamanan siber dengan konsep *hifz al-mal*. Perspektif tersebut menunjukkan bahwa tindakan preventif terhadap ancaman digital memiliki relevansi dengan tujuan syariah dalam menjaga harta. Dengan demikian, keamanan siber mempunyai dimensi teknis sekaligus normatif.

Asuransi Syariah dan Prinsip Takaful

Asuransi syariah dibangun berdasarkan prinsip saling membantu dan saling menanggung risiko. DSN-MUI melalui Fatwa Nomor 21/DSN-MUI/X/2001 memberikan pedoman umum mengenai penyelenggaraan asuransi syariah dengan menekankan prinsip tolong-menolong (*ta'awun*) serta penggunaan akad yang sesuai syariah (DSN-MUI, 2001).

Berbeda dengan mekanisme asuransi konvensional yang pada dasarnya menggunakan mekanisme pengalihan risiko (*risk transfer*), asuransi syariah menempatkan peserta sebagai bagian dari mekanisme saling menanggung risiko. Dana *tabarru'* menjadi instrumen penting dalam mekanisme tersebut. Perusahaan asuransi berfungsi sebagai pengelola dana berdasarkan akad yang

disepakati, antara lain *wakalah bil ujah*.

Priyatno et al. (2020) menjelaskan bahwa mekanisme asuransi syariah dapat dikaji berdasarkan tujuan syariah dan prinsip tolong-menolong. Farhana (2024) juga menunjukkan bahwa penerapan *Maqashid al-Syari'ah* dalam asuransi syariah dapat memperkuat orientasi perlindungan dan kemaslahatan peserta.

Maqashid al-Syari'ah dan Hifz al-Mal

Maqashid al-Syari'ah merupakan kerangka yang digunakan untuk memahami tujuan hukum Islam dalam memberikan kemaslahatan dan mencegah kemudharatan. Dalam konteks perlindungan digital, *hifz al-mal* menjadi salah satu tujuan yang memiliki hubungan langsung dengan perlindungan data, sistem informasi, aset digital, dan sumber daya ekonomi.

Perlindungan terhadap harta dalam konteks digital tidak dapat dibatasi pada benda berwujud. Kerugian yang muncul akibat kehilangan akses sistem, pencurian data, atau serangan ransomware dapat menghasilkan konsekuensi ekonomi yang nyata. Karena itu, konsep *hifz al-mal* dapat digunakan sebagai salah satu landasan normatif dalam menganalisis pengembangan asuransi siber syariah (Hutagalung et al., 2025; Junita et al., 2026).

Selain *hifz al-mal*, perlindungan data juga berkaitan dengan *hifz al-'ird* atau perlindungan terhadap kehormatan dan martabat. Kebocoran data pribadi dapat menyebabkan penyalahgunaan identitas, pencemaran reputasi, dan kerugian sosial. Dengan demikian, perlindungan data memiliki dimensi yang lebih luas daripada sekadar nilai ekonomi.

Pelindungan Data Pribadi

Undang-Undang Nomor 27 Tahun 2022 menempatkan perlindungan data pribadi sebagai bagian dari perlindungan terhadap hak pribadi. Undang-undang tersebut mengatur jenis data pribadi, hak subjek data, kewajiban pengendali dan prosesor data, pemrosesan data, transfer data, serta sanksi atas pelanggaran (Pemerintah Republik Indonesia, 2022).

Kehadiran UU PDP memberikan dasar hukum bagi organisasi untuk meningkatkan tata kelola data. Dalam konteks asuransi siber syariah, kepatuhan terhadap regulasi data pribadi menjadi bagian penting karena perusahaan asuransi akan mengelola data peserta dan dapat memproses informasi sensitif dalam proses *underwriting* maupun penyelesaian klaim.

Manajemen Risiko Siber dalam Keuangan Syariah

Pengelolaan risiko siber dalam keuangan syariah harus menggabungkan manajemen risiko modern dengan prinsip syariah. Awais et al. (2025) menekankan pentingnya perspektif syariah dalam pengelolaan risiko siber pada sektor *Islamic fintech*. Sementara itu, Junita et al. (2026) mengembangkan kerangka *Maqashid al-Syari'ah* sebagai pendekatan terhadap pengelolaan risiko keamanan siber dan perlindungan data.

Berdasarkan kajian tersebut, pengembangan asuransi siber syariah dapat ditempatkan sebagai bagian dari ekosistem manajemen risiko yang bertujuan mengurangi dampak finansial dari serangan siber sekaligus mendorong peserta meningkatkan standar keamanan sistem mereka.

METHODOLOGY

Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan kualitatif yuridis. Penelitian hukum normatif digunakan untuk mengkaji asas, kaidah, norma, doktrin, dan regulasi yang berkaitan dengan penggunaan keamanan siber sebagai objek baru asuransi syariah. Penelitian dilakukan melalui *library research* dengan mengkaji bahan hukum primer dan bahan hukum sekunder.

Pendekatan yang digunakan terdiri atas pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Pendekatan perundang-undangan digunakan untuk menganalisis ketentuan hukum positif yang relevan, khususnya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, regulasi OJK mengenai

penyelenggaraan usaha asuransi dan asuransi syariah, serta regulasi mengenai produk asuransi dan pemasaran produk asuransi (OJK, 2016, 2024; Pemerintah Republik Indonesia, 2022).

Pendekatan konseptual digunakan untuk menganalisis konsep *Maqashid al-Syari'ah*, *hifz al-mal*, *hifz al-'ird*, *ta'awun*, *takaful*, *tabarru'*, *wakalah bil ujah*, *gharar*, *maysir*, *riba*, *amanah*, dan *taqsir*. Pendekatan ini digunakan untuk melihat apakah penggunaan keamanan siber sebagai objek perlindungan asuransi dapat ditempatkan dalam kerangka hukum ekonomi syariah.

Bahan hukum primer meliputi peraturan perundang-undangan, Fatwa DSN-MUI, serta sumber hukum Islam yang berkaitan dengan asuransi dan perlindungan harta. Bahan hukum sekunder meliputi artikel jurnal ilmiah, buku hukum ekonomi syariah, kajian mengenai keamanan siber, penelitian mengenai *Maqashid al-Syari'ah*, serta penelitian mengenai manajemen risiko siber dalam keuangan Islam.

Analisis dilakukan secara kualitatif dengan cara mengidentifikasi, mengklasifikasikan, menginterpretasikan, dan mensintesis bahan hukum yang relevan. Penalaran deduktif digunakan untuk menarik kesimpulan dari prinsip umum hukum ekonomi syariah dan regulasi yang berlaku menuju persoalan khusus berupa penggunaan keamanan siber sebagai objek asuransi syariah.

RESULT AND DISCUSSION

Kedudukan Ontologis Data Digital dan Keamanan Siber dalam Fiqh Muamalah

Persoalan pertama dalam pengembangan asuransi siber syariah adalah menentukan kedudukan data digital dan keamanan sistem dalam perspektif hukum ekonomi syariah. Data digital tidak selalu memiliki bentuk fisik, tetapi dapat mempunyai manfaat dan nilai ekonomi. Dalam ekonomi digital, data pelanggan, informasi transaksi, sistem informasi, perangkat lunak, dan infrastruktur digital dapat menjadi bagian penting dari kegiatan usaha.

Konsep *mal mutaqawwam* menjadi relevan dalam pembahasan tersebut. Harta dalam hukum Islam tidak hanya dapat dipahami dari bentuk fisiknya, tetapi juga dari nilai dan manfaat yang diakui secara hukum. Oleh karena itu, data digital yang mempunyai nilai ekonomi dan manfaat yang sah dapat dipertimbangkan sebagai objek yang mempunyai kepentingan hukum. Namun, pengakuan terhadap data sebagai harta tidak berarti seluruh bentuk data dapat dimiliki atau diperjualbelikan secara bebas. Data pribadi tetap dibatasi oleh hak subjek data dan ketentuan peraturan perundang-undangan. Dalam perspektif hukum positif Indonesia, data pribadi memperoleh perlindungan melalui UU Nomor 27 Tahun 2022. Undang-undang tersebut mengatur hak subjek data dan kewajiban pihak yang melakukan pemrosesan data. Dengan demikian, data pribadi memiliki dimensi ekonomi sekaligus dimensi hak pribadi (Pemerintah Republik Indonesia, 2022).

Kedudukan data sebagai amanah juga menjadi penting. Pihak yang menguasai atau memproses data tidak dapat memperlakukannya secara bebas tanpa memperhatikan hak pemilik data. Dalam konteks ini, keamanan siber menjadi instrumen untuk menjaga amanah tersebut. Kegagalan dalam melindungi data akibat kelalaian dapat dipandang sebagai bentuk *taqsir*, terutama ketika pihak yang bertanggung jawab tidak menerapkan standar keamanan yang wajar.

Kajian Junita et al. (2026) memperlihatkan bahwa perlindungan data dalam kerangka *Maqashid al-Syari'ah* dapat ditempatkan sebagai bagian dari perlindungan kepentingan manusia dan harta. Hal tersebut memperkuat argumentasi bahwa keamanan siber mempunyai relevansi dengan tujuan syariah.

Keamanan Siber sebagai Objek Baru Asuransi Syariah

Keamanan siber sebagai objek asuransi harus dipahami melalui risiko yang muncul akibat penggunaan teknologi digital. Risiko tersebut dapat mencakup kehilangan data, kebocoran data pribadi, kerusakan sistem, gangguan operasional, biaya pemulihan, biaya investigasi, serta kerugian lain yang secara

jelas ditentukan dalam polis.

Dalam konteks asuransi syariah, objek perlindungan bukan semata-mata teknologi atau perangkat keras, tetapi risiko yang dapat muncul akibat gangguan terhadap sistem digital. Dengan demikian, perlindungan dapat diarahkan pada dampak ekonomi dari risiko siber yang telah didefinisikan secara jelas.

Secara konseptual, terdapat dua kelompok kerugian yang dapat muncul. Pertama, *first-party loss*, yaitu kerugian langsung yang dialami peserta, seperti biaya pemulihan sistem, pengembalian data, investigasi forensik, dan gangguan operasional. Kedua, *third-party loss*, yaitu kewajiban peserta terhadap pihak lain sebagai akibat dari insiden keamanan siber, misalnya biaya pemberitahuan kepada konsumen atau tanggung jawab tertentu yang timbul berdasarkan hukum.

Pengembangan produk tersebut sejalan dengan kebutuhan manajemen risiko pada sektor digital. Fitrianto et al. (2025) menunjukkan adanya urgensi pembahasan *cyber insurance*, sedangkan Awais et al. (2025) menunjukkan bahwa risiko siber membutuhkan pendekatan yang tidak hanya teknis, tetapi juga mempertimbangkan prinsip syariah.

Dalam kerangka *Maqashid al-Syari'ah*, asuransi siber dapat berfungsi sebagai instrumen perlindungan terhadap harta (*hifz al-mal*) dan kehormatan (*hifz al-'ird*). Ketika terjadi kebocoran data, mekanisme perlindungan dapat menyediakan pembiayaan untuk pemulihan sistem, penanganan insiden, dan pemenuhan tanggung jawab kepada pihak yang terdampak.

Analisis Gharar, Maysir, dan Riba

Salah satu persoalan utama dalam pengembangan asuransi adalah kemungkinan adanya *gharar*. *Gharar* berkaitan dengan ketidakjelasan atau ketidakpastian yang dapat memengaruhi keabsahan akad. Dalam asuransi siber, tingkat ketidakpastian dapat lebih tinggi karena bentuk serangan siber berubah secara cepat dan kerugian yang muncul tidak selalu mudah diukur.

Untuk mengurangi *gharar*, produk asuransi siber syariah harus menjelaskan secara terperinci jenis risiko yang ditanggung, pengecualian, batas pertanggungan, metode penghitungan kerugian, mekanisme klaim, kewajiban peserta, serta standar keamanan minimum. Semakin jelas parameter tersebut, semakin kecil kemungkinan terjadinya ketidakpastian yang berlebihan.

Unsur *maysir* juga harus dihindari. Asuransi syariah tidak boleh dirancang sebagai mekanisme perjudian yang membuat peserta berharap memperoleh keuntungan tanpa dasar risiko yang nyata. Prinsip *ta'awun* dan *tabarru'* harus menjadi dasar pengelolaan risiko agar pembayaran klaim tidak diposisikan sebagai keuntungan spekulatif.

Demikian pula unsur *riba* harus dihindari dalam pengelolaan dana. Dana peserta harus ditempatkan dan diinvestasikan melalui instrumen yang sesuai prinsip syariah. Apabila terjadi defisit dana *tabarru'*, penyelesaiannya dapat menggunakan mekanisme *qardh* sesuai prinsip yang berlaku dalam pengelolaan asuransi syariah, bukan melalui pinjaman berbunga.

Dengan demikian, persoalan utama bukan apakah risiko siber mengandung ketidakpastian, tetapi bagaimana ketidakpastian tersebut dikelola melalui desain produk, proses *underwriting*, mekanisme klaim, dan tata kelola dana yang transparan.

Tabarru', Wakalah bil Ujrah, dan Tata Kelola Dana

Penerapan asuransi siber berbasis syariah dapat menggunakan akad *tabarru'* sebagai dasar kontribusi peserta dan *wakalah bil ujrah* sebagai mekanisme pengelolaan oleh perusahaan asuransi. Dalam akad *tabarru'*, peserta memberikan kontribusi untuk tujuan saling membantu ketika peserta lain mengalami risiko yang telah disepakati. Perusahaan berperan sebagai pengelola sesuai akad yang telah ditentukan (DSN-MUI, 2001).

Mekanisme tersebut dapat digunakan untuk menghindari konstruksi pertukaran risiko secara langsung antara peserta dan perusahaan. Risiko dikumpulkan dalam dana peserta dan digunakan untuk memberikan manfaat

kepada peserta yang mengalami musibah sesuai ketentuan polis.

Dalam konteks cyber insurance, pengelolaan dana harus memperhatikan karakteristik risiko yang berbeda-beda. Risiko perusahaan perbankan, rumah sakit, perusahaan perdagangan elektronik, dan penyedia layanan digital tidak memiliki karakteristik yang sama. Karena itu, proses *underwriting* perlu mempertimbangkan tingkat keamanan sistem, jumlah data yang diproses, jenis data, struktur jaringan, sistem pencadangan, prosedur respons insiden, dan tingkat kepatuhan peserta terhadap standar keamanan.

Persyaratan *cyber hygiene* dapat menjadi bagian dari mekanisme mitigasi. Peserta dapat diwajibkan menggunakan autentikasi multifaktor, melakukan pencadangan data, memperbarui sistem, menerapkan enkripsi, melakukan pengujian keamanan, serta memiliki prosedur respons terhadap insiden. Dengan demikian, asuransi tidak hanya berfungsi secara reaktif setelah terjadi serangan, tetapi juga mendorong tindakan preventif.

Pendekatan tersebut memiliki hubungan dengan prinsip *sadd al-dhara'i*, yaitu menutup jalan yang dapat mengantarkan pada kerusakan. Dalam konteks digital, kewajiban menjaga keamanan sistem sebelum memperoleh perlindungan dapat dipandang sebagai bentuk pencegahan terhadap kerugian yang lebih besar.

Maqashid al-Syari'ah dalam Perlindungan Keamanan Siber

Penggunaan keamanan siber sebagai objek asuransi syariah dapat dianalisis melalui beberapa dimensi *Maqashid al-Syari'ah*. Pertama, *hifz al-mal*. Serangan siber dapat menyebabkan kerugian ekonomi langsung maupun tidak langsung. Perlindungan asuransi memberikan mekanisme pemulihan terhadap kerugian yang dapat dibuktikan.

Kedua, *hifz al-'ird*. Kebocoran data pribadi dapat merusak privasi, kehormatan, dan reputasi seseorang. Asuransi siber dapat membantu menyediakan dana untuk menangani konsekuensi insiden dan memenuhi kewajiban kepada pihak terdampak.

Ketiga, *hifz al-nafs*. Pada infrastruktur kritis, serangan digital dapat berdampak pada keselamatan manusia. Contohnya adalah serangan terhadap sistem rumah sakit, perangkat kesehatan yang terhubung ke jaringan, atau sistem transportasi. Oleh karena itu, pemulihan cepat terhadap sistem kritis dapat mempunyai dimensi perlindungan jiwa.

Keempat, *hifz al-'aql*. Serangan berbasis *phishing*, penipuan digital, *scamming*, dan manipulasi informasi dapat memengaruhi keputusan pengguna. Peningkatan literasi keamanan digital merupakan salah satu bentuk preventif yang dapat dikembangkan dalam tata kelola asuransi siber (Awais et al., 2025).

Kelima, *hifz al-din*. Pada lembaga keuangan syariah, keamanan sistem juga berhubungan dengan integritas transaksi yang harus tetap sesuai prinsip syariah. Manipulasi sistem atau *smart contract* yang menyebabkan transaksi tidak sesuai prinsip syariah dapat mengganggu integritas tata kelola lembaga.

Dengan demikian, perlindungan keamanan siber dapat ditempatkan tidak hanya sebagai kebutuhan teknis, tetapi sebagai bagian dari upaya mewujudkan kemaslahatan. Farhana (2024) dan Junita et al. (2026) memperlihatkan bahwa pendekatan *Maqashid al-Syari'ah* relevan digunakan untuk menghubungkan perlindungan risiko modern dengan tujuan syariah.

Blockchain, Smart Contract, dan Teknologi Pelindungan Data

Untuk meningkatkan transparansi dan mengurangi perselisihan, pengelolaan asuransi siber syariah dapat dikembangkan dengan memanfaatkan teknologi *blockchain* dan *smart contract*. *Smart contract* memungkinkan ketentuan tertentu dalam kontrak dieksekusi berdasarkan parameter yang telah ditetapkan.

Sebagai contoh, apabila suatu polis secara jelas menetapkan bahwa biaya investigasi forensik akibat insiden siber tertentu dapat ditanggung, mekanisme digital dapat digunakan untuk memverifikasi terpenuhinya parameter klaim. Dengan demikian, proses dapat dilakukan secara lebih transparan dan terdokumentasi.

Namun, penggunaan teknologi tersebut tidak otomatis menjadikan kontrak

sesuai syariah. *Smart contract* tetap harus tunduk pada akad yang mendasarinya, ketentuan hukum positif, prinsip perlindungan konsumen, dan prinsip syariah. Teknologi hanya menjadi alat untuk meningkatkan efisiensi dan transparansi.

Dalam perlindungan data, penggunaan enkripsi yang kuat juga penting. Teknologi seperti AES-256, *quantum-resistant encryption*, dan *Zero-Knowledge Proofs* dapat dipertimbangkan sesuai kebutuhan risiko. *Zero-Knowledge Proofs*, misalnya, memungkinkan verifikasi informasi tertentu tanpa harus membuka keseluruhan informasi sensitif. Penerapan teknologi tersebut dapat mendukung prinsip perlindungan data dan mengurangi risiko penyebaran informasi yang tidak diperlukan.

Lanskap Regulasi Indonesia

Pengembangan asuransi siber syariah harus ditempatkan dalam kerangka hukum positif Indonesia. UU Nomor 27 Tahun 2022 memberikan landasan hukum terhadap perlindungan data pribadi dan mengatur hak subjek data, kewajiban pengendali serta prosesor data, pemrosesan data, transfer data, dan sanksi. Karena perusahaan asuransi mengelola berbagai jenis data peserta, kepatuhan terhadap ketentuan tersebut menjadi bagian penting dari tata kelola produk asuransi siber (Pemerintah Republik Indonesia, 2022).

Dalam bidang perasuransian, POJK Nomor 69/POJK.05/2016 mengatur penyelenggaraan usaha perusahaan asuransi, perusahaan asuransi syariah, perusahaan reasuransi, dan perusahaan reasuransi syariah. Regulasi tersebut kemudian mengalami perubahan, termasuk melalui POJK Nomor 36 Tahun 2024 yang antara lain memperbarui ketentuan terkait penyelenggaraan usaha secara digital dan penerapan prinsip syariah (OJK, 2016, 2024).

Selanjutnya, POJK Nomor 8 Tahun 2024 mengatur produk asuransi dan saluran pemasaran produk asuransi. Peraturan tersebut menunjukkan adanya perkembangan kerangka regulasi yang mengakomodasi produk dan saluran pemasaran dalam lingkungan digital (OJK, 2024).

Dengan demikian, pengembangan produk asuransi siber syariah perlu dilakukan dengan memperhatikan setidaknya tiga lapisan kepatuhan, yaitu kepatuhan terhadap hukum perasuransian, kepatuhan terhadap regulasi perlindungan data dan teknologi, serta kepatuhan terhadap prinsip syariah.

Tantangan Implementasi

Tantangan pertama adalah valuasi data dan kuantifikasi kerugian. Nilai data yang bocor tidak selalu dapat ditentukan secara objektif. Oleh karena itu, klaim sebaiknya diarahkan pada kerugian nyata yang dapat dibuktikan, seperti biaya pemulihan sistem, investigasi forensik, pemulihan data, dan biaya respons insiden yang secara jelas termasuk dalam pertanggungan.

Kerugian berupa penurunan reputasi atau hilangnya peluang keuntungan perlu diatur secara hati-hati karena memiliki tingkat ketidakpastian yang lebih tinggi. Perumusan polis harus membedakan kerugian aktual dengan kerugian yang bersifat spekulatif.

Tantangan kedua adalah *moral hazard*. Peserta dapat mengurangi perhatian terhadap keamanan sistem setelah memperoleh perlindungan. Oleh sebab itu, perusahaan asuransi perlu melakukan *underwriting* berbasis risiko dan menetapkan standar keamanan minimum. Awais et al. (2025) menekankan pentingnya penguatan praktik keamanan dalam menghadapi risiko siber.

Tantangan ketiga adalah keterbatasan literasi teknis pada pengawas syariah. Perkembangan teknologi yang sangat cepat menuntut Dewan Pengawas Syariah memahami karakteristik teknologi yang menjadi objek atau bagian dari risiko yang diasuransikan. Hal tersebut diperlukan agar penilaian kepatuhan syariah tidak berhenti pada aspek akad, tetapi juga memahami mekanisme teknologi yang menjadi dasar produk.

Tantangan keempat adalah kepatuhan terhadap UU PDP. Perusahaan yang mengelola data peserta harus memastikan bahwa pemrosesan data dilakukan sesuai ketentuan hukum. Pelindungan data tidak dapat dipisahkan dari keamanan sistem karena kegagalan keamanan dapat menimbulkan

konsekuensi hukum maupun reputasi (Pemerintah Republik Indonesia, 2022).

Tantangan kelima adalah koordinasi antarotoritas dan industri. Pengembangan produk cyber insurance syariah membutuhkan keterlibatan OJK, DSN-MUI, perusahaan asuransi, aktuaris, ahli keamanan siber, dan pihak yang memahami perlindungan data. Kolaborasi tersebut diperlukan untuk membangun standar produk yang dapat mengakomodasi perkembangan teknologi sekaligus mempertahankan kepatuhan syariah.

Dengan memperhatikan tantangan tersebut, pembentukan asuransi siber syariah di Indonesia bukan sekadar meniru perkembangan industri asuransi global. Produk tersebut dapat dipandang sebagai inovasi dalam fikih muamalah yang berupaya memberikan perlindungan terhadap bentuk risiko baru. Asuransi siber syariah diarahkan untuk membangun *collective safety net* berdasarkan prinsip *ukhuwah, siddiq, amanah, keadilan, dan transparansi*.

CONCLUSION AND RECOMMENDATION

Lanskap ekonomi digital menunjukkan bahwa keamanan siber telah mengalami perubahan fungsi dari sekadar bagian teknis teknologi informasi menjadi salah satu instrumen penting dalam menjaga keberlangsungan ekonomi dan perlindungan aset. Dalam konteks tersebut, penggunaan keamanan siber sebagai objek baru dalam asuransi syariah memiliki dasar konseptual yang dapat dikembangkan dalam perspektif Hukum Ekonomi Syariah.

Data digital, sistem informasi, dan infrastruktur teknologi memiliki nilai ekonomi dan manfaat yang dapat menjadi kepentingan hukum. Dalam perspektif fikih muamalah, data yang memiliki manfaat dan nilai yang sah dapat dianalisis melalui konsep *mal mutaqawwam*, meskipun penggunaannya tetap dibatasi oleh hak subjek data dan ketentuan hukum positif. UU Nomor 27 Tahun 2022 memperkuat kedudukan perlindungan data pribadi sebagai bagian dari perlindungan hak masyarakat.

Dari perspektif *Maqashid al-Syari'ah*, perlindungan keamanan siber memiliki

keterkaitan kuat dengan *hifz al-mal* dan *hifz al-'ird*. Perlindungan terhadap sistem digital dapat mencegah kerugian ekonomi, sedangkan perlindungan terhadap data pribadi dapat mencegah penyalahgunaan informasi yang berpotensi merusak privasi dan kehormatan seseorang. Dalam kondisi tertentu, keamanan sistem juga berkaitan dengan perlindungan jiwa dan akal. Asuransi siber syariah secara konseptual dapat dikembangkan melalui prinsip *ta'awun* dan *takaful* dengan menggunakan akad *tabarru'* dan *wakalah bil ujah*. Potensi *gharar*, *maysir*, dan *riba* harus dikendalikan melalui kejelasan objek pertanggungjawaban, definisi risiko, metode penghitungan kerugian, pengelolaan dana sesuai syariah, serta transparansi kontrak.

Pengembangan asuransi siber syariah juga memerlukan penerapan keamanan teknis yang memadai, seperti enkripsi, autentikasi berlapis, pencadangan sistem, *Zero-Trust Architecture*, evaluasi keamanan, dan prosedur respons insiden. Dengan demikian, asuransi tidak hanya menjadi mekanisme kompensasi setelah terjadi kerugian, tetapi juga menjadi instrumen yang mendorong peserta meningkatkan ketahanan sistem.

REFERENCES

- Aisyah, S. N., Wulandari, F., Tursina, & Hendra K., J. (2026). Optimalisasi manajemen risiko siber pada perbankan syariah di Indonesia dalam menghadapi era fintech. *Jurnal Ekonomi Bisnis, Manajemen dan Akuntansi*, 5(2), 331–344. <https://doi.org/10.61930/jebmak.v5i2.1550>
- Awais, A., Mehmood, M. U., & Goraya, M. M. (2025). Managing cyber security risks in Islamic fintech: A Shariah perspective. *Contemporary Journal of Social Science Review*, 3(4), 1674–1688. <https://doi.org/10.63878/cjssr.v3i4.1784>
- Dewan Syariah Nasional–Majelis Ulama Indonesia. (2001). *Fatwa DSN-MUI Nomor 21/DSN-MUI/X/2001 tentang Pedoman Umum Asuransi Syariah*.
- Farhana, N. (2024). Implementasi maqashid syariah pada asuransi syariah di

<https://doi.org/10.29040/jiei.v10i1.12305>

Fitrianto, B., Armayanti, R., & Siagian, S. (2025). Urgensi pengaturan cyber insurance (asuransi siber) wajib bagi bank. *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory*, 3(4).

<https://doi.org/10.62976/ijjel.v3i4.1564>

Hutagalung, M. W. R., Siregar, S., Furqan, M., & Pulungan, I. (2025). Cybersecurity behavior as a reflection of ḥifz al-māl in Islamic banking: A behavioral model based on Protection Motivation Theory. *el-Qist Journal of Islamic Economics and Business*, 15(2), 127–153.

<https://doi.org/10.15642/elqist.2025.15.2.127-153>

Junita, B., Brennaf, M. S., Octaviano, D., & Fatiha, Z. D. (2026). Maqasid Al Shariah framework for cybersecurity risk management and data protection in global Islamic banking. *Journal of Business Management and Islamic Banking*, 5(1), 77–94. <https://doi.org/10.14421/jbmib.2026.0501-05>

Ningrum, S. T. W. (2025). Tinjauan maqasid syariah dalam asuransi syariah: Implementasi dan tantangan. *El-Arbah: Jurnal Ekonomi, Bisnis dan Perbankan Syariah*, 9(1). <https://doi.org/10.34005/elarbah.v9i1.4253>

Otoritas Jasa Keuangan. (2016). *Peraturan Otoritas Jasa Keuangan Nomor 69/POJK.05/2016 tentang Penyelenggaraan Usaha Perusahaan Asuransi, Perusahaan Asuransi Syariah, Perusahaan Reasuransi, dan Perusahaan Reasuransi Syariah*.

Otoritas Jasa Keuangan. (2024a). *Peraturan Otoritas Jasa Keuangan Nomor 8 Tahun 2024 tentang Produk Asuransi dan Saluran Pemasaran Produk Asuransi*.

- International Journal Research and Community Services (Penelitian dan Pengabdian Masyarakat) Vol. 2, No. 2, 2026
- Otoritas Jasa Keuangan. (2024b). *Peraturan Otoritas Jasa Keuangan Nomor 36 Tahun 2024 tentang Perubahan atas Peraturan Otoritas Jasa Keuangan Nomor 69/POJK.05/2016 tentang Penyelenggaraan Usaha Perusahaan Asuransi, Perusahaan Asuransi Syariah, Perusahaan Reasuransi, dan Perusahaan Reasuransi Syariah.*
- Pemerintah Republik Indonesia. (2022). *Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.*
- Priyatno, P. D., Sari, L. P., & Atiah, I. N. (2020). Penerapan maqashid syariah pada mekanisme asuransi syariah. *Journal of Islamic Economics and Finance Studies*, 1(1). <https://doi.org/10.47700/jiefes.v1i1.1927>