E-ISSN: 3031-0458

Indonesian Journal of Islamic Jurisprudence,Economic and Legal Theory

Urgensi Pengaturan *Cyber Insurance* (Asuransi Siber) Wajib Bagi Bank

Bambang Fitrianto[1], Rika Armayanti [2], Sahat Siagian[3]

[1, 2,3] Universitas Pembangunan Panca Budi

Email Korespondensi: bambangfitrianto@dosenpancabudi.ac.id

Received 02-08-2025| Revised form 17-08-2025 | Accepted 28-12-2025

Abstract

The rapid development of information technology and the digitalization of banking services have brought convenience as well as new risks in the form of increasingly complex cyber threats, such as data breaches, system hacking, and operational disruptions. These cyber risks not only affect the internal stability of banks but also potentially cause losses to customers and undermine public trust in the national financial system. Although the Indonesian banking regulatory framework has addressed risk management and data protection, specific regulations concerning mandatory cyber insurance for banks have not yet been comprehensively established. This study aims to analyze the urgency of regulating cyber insurance as a legal obligation for banks in order to strengthen legal protection, risk mitigation, and banking system stability. The research employs a normative legal method with statutory and conceptual approaches by examining banking regulations, data protection laws, and legal doctrines related to risk management and insurance. The findings indicate that cyber insurance plays a strategic role as a non-financial risk mitigation instrument by providing financial protection against losses caused by cyber attacks. Therefore, the mandatory regulation of cyber insurance for banks is an urgent necessity to ensure customer protection, enhance banking resilience, and support trust and stability within the national financial system.

Keyword: Cyber Insurance; Banking; Cyber Crime; Risk Management

Abstrak

Perkembangan teknologi informasi dan digitalisasi layanan perbankan telah membawa kemudahan sekaligus risiko baru berupa ancaman kejahatan siber (*cyber crime*) yang semakin kompleks, seperti kebocoran data, peretasan sistem, dan gangguan operasional bank. Risiko siber tersebut tidak hanya berdampak pada stabilitas internal perbankan, tetapi juga berpotensi merugikan nasabah dan mengganggu kepercayaan publik terhadap sistem keuangan nasional. Meskipun kerangka regulasi perbankan di Indonesia telah mengatur manajemen risiko dan perlindungan data, pengaturan khusus mengenai kewajiban *cyber insurance* (asuransi siber) bagi bank masih belum diatur secara komprehensif. Penelitian ini bertujuan untuk menganalisis urgensi pengaturan *cyber insurance* sebagai kewajiban hukum bagi bank dalam rangka memperkuat perlindungan hukum, mitigasi risiko, dan stabilitas sistem perbankan. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan dan konseptual, melalui kajian terhadap regulasi perbankan, perlindungan data, serta doktrin hukum terkait manajemen risiko dan asuransi. Hasil penelitian menunjukkan bahwa *cyber insurance* memiliki peran strategis sebagai instrumen mitigasi risiko non-keuangan yang mampu memberikan perlindungan finansial terhadap kerugian akibat serangan siber. Oleh karena itu, pengaturan cyber insurance secara wajib bagi bank menjadi kebutuhan mendesak guna menjamin perlindungan nasabah, meningkatkan ketahanan perbankan, serta mendukung kepercayaan dan stabilitas sistem keuangan nasional.

Kata Kunci: *Cyber Insurance*; Perbankan; Kejahatan Siber; Manajemen Risiko.

A. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa transformasi signifikan dalam sektor perbankan, khususnya melalui digitalisasi layanan keuangan yang semakin masif.[1] Bank tidak lagi hanya berfungsi sebagai lembaga intermediasi konvensional, melainkan juga sebagai penyedia layanan digital yang bergantung pada sistem elektronik, jaringan komputer, dan pengelolaan data dalam skala besar. Digitalisasi tersebut di satu sisi meningkatkan efisiensi, aksesibilitas, dan kecepatan layanan perbankan, namun di sisi lain juga menimbulkan risiko baru berupa ancaman kejahatan siber (*cyber crime*) yang semakin kompleks dan sulit diprediksi.[2] Serangan siber seperti peretasan sistem, kebocoran data nasabah, malware, ransomware, hingga gangguan operasional berpotensi menimbulkan kerugian finansial dan non-finansial yang signifikan bagi bank maupun masyarakat pengguna jasa perbankan.[3]

Perkembangan teknologi informasi dan komunikasi telah membawa transformasi yang sangat signifikan dalam sektor perbankan, terutama melalui digitalisasi layanan keuangan yang berlangsung secara masif dan berkelanjutan.[4] Bank tidak lagi hanya menjalankan fungsi tradisionalnya sebagai lembaga intermediasi yang menghimpun dan menyalurkan dana masyarakat, melainkan juga bertransformasi menjadi penyedia layanan keuangan digital yang sangat bergantung pada pemanfaatan sistem elektronik, jaringan komputer, serta pengelolaan dan pemrosesan data dalam skala besar. Perubahan ini ditandai dengan meningkatnya penggunaan layanan perbankan digital seperti mobile banking, internet banking, dan berbagai platform pembayaran elektronik yang memungkinkan transaksi keuangan dilakukan secara cepat, efisien, dan tanpa batasan ruang serta waktu.

Digitalisasi layanan perbankan pada satu sisi memberikan manfaat yang sangat besar, baik bagi bank maupun nasabah, antara lain peningkatan efisiensi operasional, perluasan akses layanan keuangan, serta peningkatan kualitas dan kecepatan pelayanan.[5] Namun, di sisi lain, ketergantungan yang tinggi terhadap sistem teknologi informasi juga membawa konsekuensi berupa munculnya berbagai risiko baru yang sebelumnya tidak dikenal dalam sistem perbankan

[1] Anung Adityatjahja, "Tanggung Jawab Nahkoda Dalam Pengangkutan Barang Melalui Laut," *Jurnal Sains Teknologi Transportasi Maritim* 4, no. 1 (2022): 22–27, https://doi.org/10.51578/j.sitektransmar.v4i1.45.

[2] Abdurrakhman Alhakim and Sofia Sofia, "Kajian Normatif Penanganan Cyber Crime Di Sektor Perbankan Di Indonesia," *Jurnal Komunitas Yustisia* 4, no. 2 (2021): 377–85, https://doi.org/10.23887/jatayu.v4i2.38089.

[3] Raden Budiarto Hadiprakoso et al., "Analisis Statis Deteksi Malware Android Menggunakan Algoritma Supervised Machine Learning," *Cyber Security dan Forensik Digital* 5, no. 1 (2022): 1–5, https://doi.org/10.14421/csecurity.2022.5.1.3116.

[4] Ahmad Mukri Aji et al., "Implementasi Harmonisasi Akad Perbankan Syariah dengan Hukum Positif di Indonesia," *Mizan: Journal of Islamic Law* 6, no. 2 (2022): 267, https://doi.org/10.32507/mizan.v6i2.1639.

[5] Bob Ben Salomoan Silalahi Alna Aulin Miftakhul Muflikh, "Peran Otoritas Jasa Keuangan (OJK) Dalam Pengawasan dan Penegakan Hukum di Sektor Perbankan," *Media Hukum Indonesia (MHI)* 2, no. 4 (2024): 387–91, https://doi.org/10.5281/ZENODO.14201714.

konvensional. Salah satu risiko yang paling menonjol adalah meningkatnya ancaman kejahatan siber (*cyber crime*) yang bersifat dinamis, kompleks, dan sulit diprediksi. Risiko siber tidak hanya berasal dari serangan eksternal seperti peretasan sistem dan malware, tetapi juga dapat bersumber dari kelemahan sistem internal, kesalahan manusia (*human error*), maupun kegagalan infrastruktur teknologi.[6]

Serangan siber dalam sektor perbankan dapat mengambil berbagai bentuk, mulai dari peretasan sistem (*hacking*), pencurian dan kebocoran data nasabah, penyebaran malware dan ransomware, hingga gangguan operasional yang menyebabkan terhentinya layanan perbankan dalam jangka waktu tertentu.[7] Dampak dari serangan tersebut tidak hanya terbatas pada kerugian finansial yang dialami oleh bank, tetapi juga mencakup kerugian non-finansial yang bersifat jangka panjang, seperti menurunnya kepercayaan masyarakat, rusaknya reputasi bank, serta terganggunya stabilitas sistem perbankan secara keseluruhan. Dalam kondisi tertentu, serangan siber bahkan dapat memicu risiko sistemik yang berpotensi mengganggu stabilitas sistem keuangan nasional.

Selain berdampak pada bank sebagai pelaku usaha jasa keuangan, risiko siber juga secara langsung menyentuh kepentingan nasabah sebagai pengguna layanan perbankan digital. Kebocoran data pribadi dan informasi keuangan nasabah dapat menimbulkan kerugian materiil maupun immateriil, seperti penyalahgunaan data, pencurian identitas, dan kerugian finansial akibat transaksi ilegal. Dalam konteks ini, bank memiliki tanggung jawab hukum dan moral untuk menjamin keamanan sistem serta melindungi data dan kepentingan nasabah. Namun, realitas menunjukkan bahwa tidak semua risiko siber dapat sepenuhnya dicegah melalui penerapan sistem keamanan teknologi informasi yang canggih, mengingat perkembangan metode dan pola serangan siber yang terus mengalami evolusi.

Kompleksitas risiko siber dalam sektor perbankan menuntut adanya pendekatan manajemen risiko yang tidak hanya berorientasi pada upaya pencegahan dan pengendalian, tetapi juga mencakup mekanisme mitigasi dan pemulihan apabila serangan siber benar-benar terjadi. Dalam hal ini, perlindungan terhadap risiko siber tidak cukup hanya mengandalkan pengamanan sistem teknologi informasi dan kepatuhan terhadap standar keamanan, melainkan juga memerlukan instrumen hukum dan finansial yang mampu memberikan jaminan perlindungan terhadap potensi kerugian.[8] Oleh karena itu, risiko siber perlu dipandang sebagai risiko strategis yang harus dikelola secara komprehensif dalam kerangka tata kelola perbankan yang baik (*good corporate governance*).

Dalam konteks sistem keuangan nasional, bank memiliki kedudukan strategis sebagai lembaga yang mengelola dana masyarakat dan menjaga stabilitas ekonomi. Oleh karena itu, keamanan sistem perbankan tidak hanya menjadi kepentingan internal bank, tetapi juga berkaitan langsung dengan kepentingan publik dan kepercayaan masyarakat. Namun demikian,

[6] Barda Nawawi Arief, *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime Di Indonesia* (PT Raja Grafindo Persada, 2006).

[7] Qorry Aina Fitroh and Bambang Sugiantoro, "Peran Ethical Hacking Dalam Memerangi Cyberthreats," *JURNAL ILMIAH INFORMATIKA* 11, no. 01 (2023): 27–31, https://doi.org/10.33884/jif.v11i01.6593.

[8] Klarisa Desi Ananta et al., "Pengaruh Media Sosial terhadap Peningkatan Kejahatan Siber di Indonesia," *Islamic Law: Jurnal Siyasah* 9, no. 2 (2024).

meningkatnya ketergantungan bank terhadap teknologi digital berbanding lurus dengan meningkatnya eksposur terhadap risiko siber. Berbagai insiden kebocoran data dan gangguan sistem perbankan menunjukkan bahwa risiko siber telah menjadi salah satu risiko utama (emerging risk) yang dapat mengancam keberlangsungan usaha bank serta stabilitas sistem keuangan secara keseluruhan.

Secara normatif, pengaturan perbankan di Indonesia telah mengatur kewajiban penerapan manajemen risiko dan prinsip kehati-hatian (*prudential banking principle*), termasuk pengelolaan risiko teknologi informasi. Selain itu, regulasi terkait perlindungan data pribadi dan keamanan sistem elektronik juga telah memberikan kerangka dasar bagi perlindungan data nasabah. [9] Namun, pengaturan tersebut pada umumnya masih berfokus pada aspek pencegahan (*preventive measures*) dan pengendalian risiko internal, sementara aspek mitigasi kerugian finansial akibat terjadinya serangan siber belum diatur secara komprehensif. Dalam kondisi ini, bank pada umumnya menanggung sendiri risiko kerugian yang timbul akibat insiden siber, yang pada akhirnya dapat berdampak pada nasabah dan stabilitas perbankan.

Cyber insurance atau asuransi siber muncul sebagai instrumen mitigasi risiko yang dirancang untuk memberikan perlindungan finansial terhadap kerugian yang timbul akibat serangan siber, termasuk biaya pemulihan sistem, kompensasi kepada nasabah, tuntutan hukum, serta kerugian reputasi.[10] Meskipun demikian, di Indonesia pengaturan mengenai *cyber insurance* bagi bank masih bersifat sukarela dan belum menjadi kewajiban hukum.[11] Kondisi ini menimbulkan kesenjangan perlindungan hukum, mengingat besarnya potensi kerugian akibat risiko siber serta kedudukan bank sebagai lembaga yang menghimpun dan mengelola dana masyarakat. Tanpa pengaturan yang jelas dan mengikat, penerapan *cyber insurance* sangat bergantung pada kebijakan masing-masing bank, yang berpotensi menimbulkan ketidakseragaman tingkat perlindungan.

Kompleksitas risiko siber dalam sektor perbankan tidak hanya berkaitan dengan aspek teknis, tetapi juga mencakup dimensi hukum, ekonomi, dan perlindungan konsumen. Serangan siber dapat menimbulkan sengketa antara bank dan nasabah akibat kerugian finansial maupun kebocoran data pribadi, yang pada akhirnya membebani sistem penyelesaian sengketa dan merusak kepercayaan publik. Oleh karena itu, diperlukan suatu instrumen hukum yang tidak hanya bersifat preventif, tetapi juga mampu memberikan mekanisme pemulihan (recovery mechanism) yang efektif apabila risiko siber benar-benar terjadi. Dalam hal ini, cyber insurance dapat diposisikan sebagai bagian integral dari rezim manajemen risiko perbankan yang berorientasi pada perlindungan nasabah dan stabilitas sistem keuangan.

Berdasarkan latar belakang tersebut, pengaturan cyber insurance sebagai kewajiban bagi bank menjadi isu yang memiliki urgensi tinggi dalam kerangka hukum perbankan modern. Pengaturan tersebut diharapkan tidak hanya memperkuat mitigasi risiko non-keuangan, tetapi

[9] Yingsi Chen, "Research on Regulation of Personal Financial Data Sharing in Open Banking," *Asian Journal of Education and Social Studies* 45, no. 3 (2023): 31–41, https://doi.org/10.9734/ajess/2023/v45i3985.
[10] Mutaz Alkhedhairy, "Fundamental Principles In Saudi Arabia's Marine Insurance Law With Reference To The Law And Practice In Egypt And The UK: A Comparative Study," *University of Leicester*, 2022.
[11] Suaibatul Aslamiyah and Rahmat Agus Santoso, *Implementasi Strategi Pemasaran Pada PT. Bank Perkreditan Rakyat (BPR) MCM*, n.d.

juga memberikan kepastian hukum terkait tanggung jawab bank terhadap kerugian akibat serangan siber. Selain itu, kewajiban cyber insurance dapat menjadi instrumen pendukung bagi perlindungan konsumen perbankan serta menjaga kepercayaan masyarakat terhadap sistem perbankan digital.

Berdasarkan uraian di atas, penelitian ini berfokus pada pengkajian secara mendalam mengenai urgensi pengaturan *cyber insurance* (asuransi siber) sebagai kewajiban hukum bagi bank di Indonesia. Kajian ini diarahkan untuk menganalisis posisi *cyber insurance* dalam kerangka manajemen risiko perbankan, menelaah kekosongan dan kelemahan pengaturan yang ada, serta merumuskan argumentasi normatif mengenai pentingnya pengaturan cyber insurance wajib guna memperkuat perlindungan hukum bagi bank, nasabah, dan stabilitas sistem keuangan nasional.

B. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian yuridis normatif, yaitu penelitian hukum yang dilakukan dengan cara menelaah dan menganalisis norma-norma hukum yang berlaku, baik yang tertuang dalam peraturan perundang-undangan maupun dalam doktrin dan teori hukum.[12] Metode ini digunakan untuk mengkaji secara mendalam pengaturan hukum terkait risiko siber dalam sektor perbankan serta urgensi pengaturan cyber insurance (asuransi siber) sebagai kewajiban hukum bagi bank di Indonesia. Pendekatan penelitian yang digunakan meliputi pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*).[13] Pendekatan perundang-undangan dilakukan dengan menelaah berbagai regulasi yang berkaitan dengan perbankan, teknologi informasi, perlindungan data pribadi, serta asuransi, guna mengidentifikasi norma hukum yang telah ada serta menemukan kekosongan atau kelemahan pengaturan mengenai *cyber insurance* bagi bank. Sementara itu, pendekatan konseptual digunakan untuk mengkaji konsep *cyber insurance*, manajemen risiko perbankan, prinsip kehati-hatian, dan perlindungan hukum terhadap nasabah, berdasarkan pandangan para ahli dan doktrin hukum yang relevan. Teknik pengumpulan bahan hukum dalam penelitian ini dilakukan melalui studi kepustakaan (*library research*).[14] Bahan hukum yang digunakan terdiri atas bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Bahan hukum primer meliputi peraturan perundang-undangan yang berkaitan dengan sektor perbankan, sistem elektronik, perlindungan data pribadi, dan perasuransian. Bahan hukum sekunder berupa buku, artikel jurnal ilmiah, hasil penelitian terdahulu, serta publikasi ilmiah lainnya yang relevan dengan topik *cyber risk* dan *cyber insurance*. Adapun bahan hukum tersier meliputi kamus hukum dan sumber pendukung lainnya yang berfungsi untuk memperjelas istilah dan konsep hukum yang digunakan

Teknik analisis bahan hukum dilakukan secara kualitatif, yaitu dengan cara mengidentifikasi, mengklasifikasikan, dan menafsirkan bahan hukum yang telah dikumpulkan secara sistematis untuk menemukan prinsip, asas, dan norma hukum yang relevan. Selanjutnya,

[12] Zainuddin Ali, *Metode Penelitian Hukum* (Sinar Grafika, 2014), hlm. 15.
[13] Geofani Milthree Saragih, "Pancasila Sebagai Landasan Filosofis Pembentukan Peraturan Perundang-Undangan Di Indonesia," *Jurnal Pancasila dan Kewarganegaraan* 2, no. 1 (2022).
[14] Elisabeth Nurhaini Butar-Butar, *Metode Penelitian Hukum, Langkah-Langkah Untuk Menemukan Kebenaran Dalam Ilmu Hukum* (PT. Refika Aditama, 2018), hlm. 76.

bahan hukum tersebut dianalisis secara preskriptif untuk merumuskan argumentasi hukum mengenai urgensi pengaturan *cyber insurance* sebagai kewajiban bagi bank, sehingga dapat memberikan rekomendasi normatif dalam rangka memperkuat perlindungan hukum, manajemen risiko perbankan, serta stabilitas sistem keuangan nasional.

C. RESULTS AND DISCUSSION

1. Risiko Siber dalam Sistem Perbankan Digital dan Implikasinya terhadap Stabilitas Keuangan

Transformasi digital dalam sektor perbankan telah mengubah secara fundamental cara bank menjalankan fungsi intermediasi keuangan, pengelolaan dana, serta pelayanan kepada nasabah. Ketergantungan yang tinggi terhadap teknologi informasi, sistem elektronik, dan infrastruktur digital menjadikan bank sebagai salah satu sektor paling rentan terhadap risiko siber. Risiko siber dalam konteks perbankan tidak lagi dapat dipahami semata-mata sebagai persoalan teknis, melainkan sebagai risiko hukum, operasional, reputasi, dan sistemik yang saling berkaitan.[15] Karakteristik risiko siber yang bersifat lintas batas (*borderless*), adaptif, dan sulit diprediksi menempatkannya sebagai salah satu risiko paling kompleks dalam tata kelola perbankan modern.

Risiko siber dalam sistem perbankan digital mencakup berbagai bentuk ancaman, seperti peretasan sistem (*hacking*), serangan malware dan ransomware, pencurian serta kebocoran data nasabah, manipulasi transaksi elektronik, hingga gangguan operasional yang menyebabkan terhentinya layanan perbankan.[16] Ancaman tersebut tidak hanya berasal dari pihak eksternal, tetapi juga dapat bersumber dari kelemahan sistem internal, kesalahan manusia (*human error*), maupun kegagalan tata kelola teknologi informasi. Dalam praktiknya, serangan siber sering kali tidak hanya berdampak pada satu institusi perbankan, tetapi dapat menyebar secara cepat dan menimbulkan efek berantai yang mengganggu sistem pembayaran, jaringan antarbank, serta kepercayaan publik terhadap sistem keuangan secara keseluruhan.

Implikasi hukum dari risiko siber dalam sektor perbankan menjadi semakin signifikan seiring dengan meningkatnya peran bank sebagai pengelola data dan penyelenggara sistem elektronik. Kebocoran data nasabah, misalnya, tidak hanya menimbulkan kerugian finansial, tetapi juga memunculkan tanggung jawab hukum bank terkait perlindungan data pribadi dan kewajiban menjaga kerahasiaan informasi nasabah.[17] Dalam konteks ini, risiko siber berpotensi melahirkan sengketa hukum antara bank dan nasabah, tuntutan ganti rugi, serta sanksi administratif maupun pidana, yang pada akhirnya memperbesar eksposur risiko hukum bagi bank. Risiko hukum tersebut

[15] Aggeliki Tsohou et al., "Cyber Insurance: State of the Art, Trends and Future Directions," *International Journal of Information Security* 22, no. 3 (2023): 737–48, https://doi.org/10.1007/s10207-023-00660-8.
[16] Adelina Damayanti and Rina Arum Prastyanti, "Kajian Hukum Dan Regulasi Terkait Serangan Hacking Pada Platform Digital Di Indonesia," *Multidisciplinary Indonesian Center Journal (MICJO)* 1, no. 2 (2024): 1043–54, https://doi.org/10.62567/micjo.v1i2.117.
[17] Renaldi Aditya, *Perlindungan Hukum Bagi Pengguna Jasa Rekber (Penjual) Oleh Pihak Bank Sesuai Dengan Peraturan Bank Indonesia Nomor: 3/10/PBI/2001 Tentang Prinsip Mengenal Nasabah*, n.d.

sering kali berjalan beriringan dengan risiko reputasi, karena menurunnya kepercayaan publik dapat berdampak langsung terhadap keberlangsungan usaha bank.

Lebih jauh, risiko siber memiliki potensi untuk berkembang menjadi risiko sistemik yang mengancam stabilitas keuangan. Gangguan pada sistem perbankan digital, khususnya pada bank-bank yang memiliki peran sistemik, dapat menghambat fungsi sistem pembayaran, menurunkan likuiditas pasar, dan memicu kepanikan di kalangan nasabah. Dalam situasi tertentu, serangan siber yang berskala besar dapat mengganggu kepercayaan terhadap sistem keuangan nasional dan memicu instabilitas ekonomi yang lebih luas. Oleh karena itu, risiko siber tidak dapat diperlakukan sebagai risiko individual semata, melainkan harus dipahami sebagai risiko kolektif yang memerlukan pengelolaan dan pengaturan secara sistemik dalam kerangka stabilitas keuangan.

Meskipun bank telah menerapkan berbagai standar keamanan teknologi informasi dan manajemen risiko untuk mencegah terjadinya serangan siber, realitas menunjukkan bahwa upaya pencegahan tersebut tidak selalu mampu mengeliminasi risiko secara total.[18] Dinamika dan evolusi metode serangan siber yang semakin canggih menyebabkan sistem keamanan yang ada sering kali tertinggal dari ancaman yang berkembang. Kondisi ini menegaskan adanya keterbatasan pendekatan preventif semata dalam menghadapi risiko siber. Dalam konteks hukum perbankan, keterbatasan tersebut menuntut adanya pendekatan yang lebih komprehensif, yang tidak hanya berfokus pada pencegahan, tetapi juga pada mitigasi dan pemulihan kerugian akibat risiko siber.

Implikasi terhadap stabilitas keuangan juga berkaitan dengan beban finansial yang harus ditanggung bank akibat insiden siber. Biaya pemulihan sistem, kompensasi kepada nasabah, penyelesaian sengketa hukum, serta kerugian reputasi dapat menggerus modal dan likuiditas bank.[19] Apabila kerugian tersebut tidak dikelola secara memadai, bank dapat mengalami tekanan keuangan yang signifikan, yang pada akhirnya berpotensi menular ke sektor keuangan lainnya. Dalam konteks ini, risiko siber beririsan langsung dengan prinsip kehati-hatian (*prudential principle*) dan kewajiban bank untuk menjaga kesehatan serta keberlanjutan usahanya.

Risiko siber dalam sistem perbankan digital merupakan fenomena multidimensional yang memiliki implikasi luas terhadap aspek hukum, ekonomi, dan stabilitas keuangan. Pengelolaan risiko siber tidak dapat hanya dibebankan pada kebijakan internal masing-masing bank, tetapi memerlukan kerangka pengaturan yang mampu menjamin perlindungan sistemik dan kepentingan publik. Pemahaman yang komprehensif terhadap karakteristik dan implikasi risiko siber menjadi landasan penting dalam merumuskan instrumen hukum dan kebijakan yang adaptif, termasuk kebutuhan akan mekanisme mitigasi risiko yang bersifat finansial dan terintegrasi dalam sistem perbankan nasional.

[18] Budi Raharjo, *Fintech: Teknologi Finansial Perbankan Digital* (Yayasan Prima Agus Teknik Bekerja sama dengan Universitas Sains & Teknologi Komputer (Universitas STEKOM), 2021).
[19] Ivan Krisna Aji and Gusganda Suria Manda, "Pengaruh Risiko Kredit Dan Risiko Likuiditas Terhadap Profitabilitas Pada Bank BUMN," *JAD : Jurnal Riset Akuntansi & Keuangan Dewantara* 4, no. 1 (1970): 36–45, https://doi.org/10.26533/jad.v4i1.748.

2. Keterbatasan Kerangka Regulasi Perbankan dalam Mitigasi Kerugian Akibat Serangan Siber

Kerangka regulasi perbankan pada umumnya dirancang untuk menjamin stabilitas sistem keuangan melalui penerapan prinsip kehati-hatian, manajemen risiko, dan tata kelola yang baik.[20] Dalam konteks perkembangan perbankan digital, berbagai regulasi telah mengakui keberadaan risiko teknologi informasi dan mewajibkan bank untuk menerapkan sistem pengamanan, pengendalian internal, serta manajemen risiko teknologi. Namun demikian, kerangka regulasi tersebut pada dasarnya masih berorientasi pada upaya pencegahan (*preventive approach*) dan pengendalian internal, sehingga belum sepenuhnya menjawab kebutuhan mitigasi kerugian finansial ketika risiko siber benar-benar terjadi.[21] Akibatnya, terdapat kesenjangan normatif antara kewajiban bank dalam mengelola risiko siber dan mekanisme perlindungan hukum terhadap dampak kerugian yang ditimbulkan.

Salah satu keterbatasan utama regulasi perbankan terletak pada penekanan yang dominan terhadap kepatuhan teknis dan prosedural dalam pengamanan sistem elektronik. Bank diwajibkan untuk menjaga keamanan sistem, melindungi data nasabah, serta memastikan keberlangsungan operasional layanan digital.[22] Namun, regulasi tersebut relatif minim dalam mengatur mekanisme pemulihan kerugian (*loss recovery*) secara sistematis, baik bagi bank maupun nasabah. Ketika terjadi serangan siber yang mengakibatkan kebocoran data atau kerugian finansial, penyelesaiannya sering kali bergantung pada kebijakan internal bank atau mekanisme penyelesaian sengketa secara individual, yang tidak selalu memberikan kepastian dan keadilan bagi pihak yang dirugikan.

Keterbatasan regulasi juga tercermin dalam pembagian tanggung jawab hukum antara bank dan nasabah akibat insiden siber. Dalam praktik, bank sering kali menempatkan klausul pembatasan tanggung jawab dalam perjanjian layanan digital, yang berpotensi mengalihkan sebagian risiko kepada nasabah. Kondisi ini menimbulkan persoalan perlindungan konsumen, karena posisi tawar nasabah dalam hubungan hukum perbankan relatif lemah. Regulasi perbankan yang ada belum secara tegas mengatur standar kompensasi dan mekanisme ganti rugi yang wajib diterapkan oleh bank apabila kerugian nasabah timbul akibat kegagalan sistem atau serangan siber.[23] Akibatnya, mitigasi kerugian masih bersifat parsial dan tidak seragam antar bank.

Selain itu, regulasi perbankan cenderung memandang risiko siber sebagai bagian dari risiko operasional internal bank, tanpa secara eksplisit mengaitkannya dengan risiko sistemik dan dampaknya terhadap stabilitas keuangan nasional. Pendekatan ini menyebabkan pengelolaan risiko siber lebih bersifat individual dan terfragmentasi, padahal serangan siber berpotensi menimbulkan efek domino yang melampaui satu institusi perbankan. Ketiadaan instrumen mitigasi

[20] Indra Gunawan Purba et al., "Pengaturan pemberian kredit pada dunia perbankan di indonesia," *Jurnal Normatif* 2, no. 2 (2022): 203–11, https://doi.org/10.54123/jn.v2i2.230.
[21] Ulviatur Rohmah et al., "Regulasi Dan Pengawasan Perbankan Oleh Otoritas Jasa Keuangan," *Jurnal Penelitian Nusantara* 1, no. 5 (2025): 314–19.
[22] Izzy Al Kautsar and Danang Wahyu Muhammad, "Sistem Hukum Modern Lawrance M. Friedman: Budaya Hukum dan Perubahan Sosial Masyarakat dari Industrial ke Digital," *Sapientia Et Virtus* 7, no. 2 (2022): 84–99, https://doi.org/10.37477/sev.v7i2.358.
[23] Johanes Desmon et al., "Systematic Literature Review: Serangan Deface Website Sebagai Bentuk Kejahatan Siber," *Jurnal Sistem Informasi* 14, no. 2 (2024).

kerugian yang bersifat kolektif dan terstandar memperbesar kemungkinan terjadinya tekanan sistemik apabila insiden siber terjadi secara masif atau menargetkan bank-bank dengan peran sistemik.

Lebih jauh, regulasi perbankan juga belum mengintegrasikan secara optimal sektor perasuransian sebagai bagian dari rezim mitigasi risiko siber. Meskipun secara konseptual asuransi merupakan instrumen yang lazim digunakan untuk mengalihkan dan mendistribusikan risiko, kerangka hukum perbankan belum secara tegas mengakui atau mewajibkan penggunaan cyber insurance sebagai bagian dari manajemen risiko bank.[24] Akibatnya, penerapan asuransi siber sepenuhnya diserahkan pada kebijakan masing-masing bank, yang pada praktiknya sangat bervariasi dan tidak jarang diabaikan karena pertimbangan biaya atau kurangnya kewajiban normatif. Kondisi ini menciptakan ketidakpastian perlindungan, baik bagi bank maupun nasabah, ketika risiko siber benar-benar terjadi.

Keterbatasan lainnya berkaitan dengan pendekatan regulasi yang masih bersifat reaktif dan sektoral. Pengaturan terkait perbankan, teknologi informasi, perlindungan data, dan asuransi sering kali berjalan secara terpisah tanpa integrasi yang memadai.[25] Fragmentasi regulasi tersebut menyebabkan tidak adanya mekanisme mitigasi kerugian yang holistik dan berkelanjutan. Dalam konteks serangan siber yang bersifat lintas sektor dan lintas yurisdiksi, pendekatan regulasi yang terfragmentasi justru memperlemah kapasitas sistem hukum dalam memberikan perlindungan yang efektif dan adaptif.

Keterbatasan kerangka regulasi perbankan dalam mitigasi kerugian akibat serangan siber menunjukkan adanya kebutuhan mendesak untuk melakukan penguatan dan pembaruan pengaturan hukum. Regulasi perbankan tidak lagi cukup hanya mengandalkan kewajiban pengamanan sistem dan manajemen risiko internal, tetapi perlu dilengkapi dengan instrumen mitigasi kerugian yang memberikan kepastian hukum, perlindungan finansial, dan distribusi risiko yang adil. Ketiadaan mekanisme tersebut berpotensi memperbesar dampak negatif serangan siber terhadap bank, nasabah, dan stabilitas sistem keuangan nasional, sekaligus menegaskan urgensi pencarian solusi normatif yang lebih komprehensif.

3. Urgensi dan Model Pengaturan Cyber Insurance Wajib bagi Bank sebagai Instrumen Perlindungan Hukum dan Manajemen Risiko

Meningkatnya eskalasi risiko siber dalam sektor perbankan digital, serta keterbatasan kerangka regulasi yang ada dalam memitigasi kerugian akibat serangan siber, menegaskan urgensi pengaturan cyber insurance sebagai kewajiban hukum bagi bank. *Cyber insurance* tidak hanya berfungsi sebagai instrumen perlindungan finansial, tetapi juga sebagai bagian integral dari rezim manajemen risiko perbankan yang berorientasi pada perlindungan hukum dan stabilitas sistem

[24] Andrew Shandy Utama, "Digitalisasi Produk Bank Konvensional Dan Bank Syariah Di Indonesia," *Jurnal Justisia : Jurnal Ilmu Hukum, Perundang-undangan dan Pranata Sosial* 6, no. 2 (2021): 113, https://doi.org/10.22373/justisia.v6i2.11532.

[25] Milenisha Andani et al., "Analisis Penerapan Asas-asas Good Corporate Governance Pada Badan Usaha Milik Negara (BUMN) Di Indonesia," *Prosiding Seminar Nasional Ilmu Sosial & Teknologi (SNISTEK)* 6 (2024).

keuangan.[26] Dalam konteks ini, pengaturan cyber insurance wajib perlu dipandang sebagai respons normatif terhadap karakter risiko siber yang bersifat tidak pasti, berpotensi sistemik, dan memiliki dampak luas terhadap kepentingan publik.

Urgensi pengaturan *cyber insurance* wajib bagi bank dapat ditinjau dari perspektif perlindungan hukum nasabah. Bank sebagai lembaga kepercayaan memiliki kewajiban hukum untuk melindungi dana dan data nasabah dari berbagai bentuk risiko, termasuk risiko siber.[27] Ketika serangan siber menyebabkan kebocoran data atau kerugian finansial, nasabah berada pada posisi yang rentan karena keterbatasan akses terhadap mekanisme pemulihan yang efektif. *Cyber insurance* berperan sebagai instrumen yang menjamin ketersediaan dana kompensasi, sehingga hak-hak nasabah dapat dipulihkan tanpa harus melalui proses sengketa yang panjang dan berbiaya tinggi. Dengan demikian, kewajiban *cyber insurance* dapat memperkuat posisi hukum nasabah serta meningkatkan kepercayaan publik terhadap sistem perbankan digital.

Selain aspek perlindungan konsumen, *cyber insurance* wajib juga memiliki urgensi yang kuat dalam konteks manajemen risiko perbankan. Risiko siber merupakan risiko non-keuangan yang sulit diprediksi dan berpotensi menimbulkan kerugian dalam jumlah besar.[28] Dengan adanya *cyber insurance*, bank dapat mengalihkan sebagian risiko tersebut kepada pihak penanggung, sehingga beban kerugian tidak sepenuhnya ditanggung oleh bank. Pengalihan risiko ini berkontribusi pada penguatan ketahanan keuangan bank, khususnya dalam menghadapi insiden siber yang berskala besar. Dalam kerangka prudential banking, cyber insurance dapat diposisikan sebagai instrumen pelengkap yang mendukung prinsip kehati-hatian dan keberlanjutan usaha perbankan.

Lebih lanjut, kewajiban *cyber insurance* juga memiliki implikasi positif terhadap stabilitas sistem keuangan. Dalam situasi serangan siber yang berdampak luas, ketersediaan perlindungan asuransi dapat mencegah terjadinya tekanan likuiditas dan penurunan kepercayaan yang berpotensi menimbulkan risiko sistemik.[29] Dengan adanya mekanisme pembiayaan pemulihan melalui *cyber insurance*, gangguan operasional dan kerugian finansial dapat ditangani secara lebih cepat dan terukur. Hal ini menunjukkan bahwa cyber insurance tidak hanya berfungsi pada tingkat mikro (individual bank), tetapi juga memiliki peran strategis pada tingkat makro dalam menjaga stabilitas sistem keuangan nasional.

Dalam merumuskan model pengaturan *cyber insurance* wajib bagi bank, diperlukan pendekatan yang komprehensif dan proporsional. Pengaturan tersebut perlu mengintegrasikan sektor perbankan dan perasuransian secara sistematis, dengan menetapkan standar minimum perlindungan yang harus dimiliki oleh bank.[30] Standar tersebut dapat mencakup cakupan risiko

[26] Richard McGregor et al., "Cyberspace and Personal Cyber Insurance: A Systematic Review," *Journal of Computer Information Systems* 64, no. 1 (2024): 157–71, https://doi.org/10.1080/08874417.2023.2185551.
[27] Kerstin Awiszus et al., "Modeling and Pricing Cyber Insurance: Idiosyncratic, Systematic, and Systemic Risks," *European Actuarial Journal* 13, no. 1 (2023): 1–53, https://doi.org/10.1007/s13385-023-00341-9.
[28] Aristeidis Farao et al., "INCHAIN: A Cyber Insurance Architecture with Smart Contracts and Self-Sovereign Identity on Top of Blockchain," *International Journal of Information Security* 23, no. 1 (2024): 347–71, https://doi.org/10.1007/s10207-023-00741-8.
[29] Tom Baker and Anja Shortland, "Insurance and Enterprise: Cyber Insurance for Ransomware," *The Geneva Papers on Risk and Insurance - Issues and Practice* 48, no. 2 (2023): 275–99, https://doi.org/10.1057/s41288-022-00281-7.
[30] Alexander Braun et al., "Cyber Insurance-Linked Securities," *ASTIN Bulletin* 53, no. 3 (2023): 684–705, https://doi.org/10.1017/asb.2023.22.

yang diasuransikan, batas pertanggungan, serta mekanisme klaim yang transparan dan akuntabel. Selain itu, model pengaturan perlu mempertimbangkan perbedaan karakteristik dan skala usaha bank, sehingga kewajiban cyber insurance diterapkan secara proporsional tanpa menghambat efisiensi operasional perbankan.

Model pengaturan *cyber insurance* wajib juga harus ditempatkan dalam kerangka pengawasan yang efektif. Otoritas pengawas perbankan dan perasuransian memiliki peran penting dalam memastikan kepatuhan bank terhadap kewajiban asuransi siber, sekaligus menjaga kesehatan industri asuransi. Dalam hal ini, *cyber insurance* dapat dijadikan sebagai salah satu komponen penilaian manajemen risiko dan tata kelola bank. Pengawasan yang terintegrasi akan mendorong bank untuk tidak hanya memenuhi kewajiban formal, tetapi juga menginternalisasi *cyber insurance* sebagai bagian dari strategi pengelolaan risiko yang berkelanjutan.

Pengaturan *cyber insurance* wajib bagi bank merupakan kebutuhan normatif yang mendesak dalam menghadapi tantangan perbankan digital. *Cyber insurance* dapat berfungsi sebagai instrumen perlindungan hukum yang memberikan kepastian dan keadilan bagi nasabah, sekaligus sebagai instrumen manajemen risiko yang memperkuat ketahanan perbankan dan stabilitas sistem keuangan. Model pengaturan yang komprehensif, proporsional, dan terintegrasi akan menjadi fondasi penting dalam membangun sistem perbankan digital yang aman, terpercaya, dan berkelanjutan di era transformasi teknologi.

KESIMPULAN

Perkembangan digitalisasi perbankan telah meningkatkan eksposur bank terhadap risiko siber yang kompleks dan berpotensi menimbulkan dampak hukum, finansial, serta sistemik yang signifikan, baik bagi bank maupun nasabah. Penelitian ini menunjukkan bahwa kerangka regulasi perbankan yang berlaku saat ini masih berfokus pada aspek pencegahan dan pengendalian internal, sehingga belum mampu memberikan mekanisme mitigasi dan pemulihan kerugian akibat serangan siber secara komprehensif. Oleh karena itu, pengaturan cyber insurance sebagai kewajiban hukum bagi bank menjadi kebutuhan mendesak untuk memperkuat perlindungan hukum nasabah, mendukung manajemen risiko perbankan, serta menjaga stabilitas sistem keuangan nasional. Integrasi cyber insurance dalam kerangka hukum perbankan diharapkan mampu memberikan kepastian hukum, meningkatkan ketahanan perbankan, dan membangun kepercayaan publik terhadap sistem perbankan digital yang berkelanjutan.

BIBLIOGRAPHY

Aditya, Renaldi. Perlindungan Hukum Bagi Pengguna Jasa Rekber (Penjual) Oleh Pihak Bank Sesuai Dengan Peraturan Bank Indonesia Nomor: 3/10/PBI/2001 Tentang Prinsip Mengenal Nasabah. n.d.

Adityatjahja, Anung. "Tanggung Jawab Nahkoda Dalam Pengangkutan Barang Melalui Laut." Jurnal Sains Teknologi Transportasi Maritim 4, no. 1 (2022): 22–27. https://doi.org/10.51578/j.sitektransmar.v4i1.45.

Aji, Ahmad Mukri, Syarifah Gustiawati Mukri, and Gilang Rizki Aji Putra. "Implementasi Harmonisasi Akad Perbankan Syariah dengan Hukum Positif di Indonesia." Mizan: Journal of Islamic Law 6, no. 2 (2022): 267. https://doi.org/10.32507/mizan.v6i2.1639.

Aji, Ivan Krisna, and Gusganda Suria Manda. "Pengaruh Risiko Kredit Dan Risiko Likuiditas Terhadap Profitabilitas Pada Bank BUMN." JAD : Jurnal Riset Akuntansi & Keuangan Dewantara 4, no. 1 (1970): 36–45. https://doi.org/10.26533/jad.v4i1.748.

Al Kautsar, Izzy, and Danang Wahyu Muhammad. "Sistem Hukum Modern Lawrance M. Friedman: Budaya Hukum dan Perubahan Sosial Masyarakat dari Industrial ke Digital." Sapientia Et Virtus 7, no. 2 (2022): 84–99. https://doi.org/10.37477/sev.v7i2.358.

Alhakim, Abdurrakhman, and Sofia Sofia. "Kajian Normatif Penanganan Cyber Crime Di Sektor Perbankan Di Indonesia." Jurnal Komunitas Yustisia 4, no. 2 (2021): 377–85. https://doi.org/10.23887/jatayu.v4i2.38089.

Ali, Zainuddin. Metode Penelitian Hukum. Sinar Grafika, 2014.

Alkhedhairy, Mutaz. "Fundamental Principles In Saudi Arabia's Marine Insurance Law With Reference To The Law And Practice In Egypt And The UK: A Comparative Study." University of Leicester, 2022.

Alna Aulin Miftakhul Muflikh, Bob Ben Salomoan Silalahi. "Peran Otoritas Jasa Keuangan (OJK) Dalam Pengawasan dan Penegakan Hukum di Sektor Perbankan." Media Hukum Indonesia (MHI) 2, no. 4 (2024): 387–91. https://doi.org/10.5281/ZENODO.14201714.

Ananta, Klarisa Desi, Triyo Ambodo, and Agus Tohawi. "Pengaruh Media Sosial terhadap Peningkatan Kejahatan Siber di Indonesia." Islamic Law: Jurnal Siyasah 9, no. 2 (2024).

Andani, Milenisha, Karol Teovani Lodan, and Etika Khairina. "Analisis Penerapan Asas-asas Good Corporate Governance Pada Badan Usaha Milik Negara (BUMN) Di Indonesia." Prosiding Seminar Nasional Ilmu Sosial & Teknologi (SNISTEK) 6 (2024).

Arief, Barda Nawawi. Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime Di Indonesia. PT Raja Grafindo Persada, 2006.

Aslamiyah, Suaibatul, and Rahmat Agus Santoso. Implementasi Strategi Pemasaran Pada PT. Bank Perkreditan Rakyat (BPR) MCM. n.d.

Awiszus, Kerstin, Thomas Knispel, Irina Penner, Gregor Svindland, Alexander Voß, and Stefan Weber. "Modeling and Pricing Cyber Insurance: Idiosyncratic, Systematic, and Systemic Risks." European Actuarial Journal 13, no. 1 (2023): 1–53. https://doi.org/10.1007/s13385-023-00341-9.

Baker, Tom, and Anja Shortland. "Insurance and Enterprise: Cyber Insurance for Ransomware."

The Geneva Papers on Risk and Insurance - Issues and Practice 48, no. 2 (2023): 275–99. https://doi.org/10.1057/s41288-022-00281-7.

Braun, Alexander, Martin Eling, and Christoph Jaenicke. "Cyber Insurance-Linked Securities." ASTIN Bulletin 53, no. 3 (2023): 684–705. https://doi.org/10.1017/asb.2023.22.

Budi Raharjo. Fintech: Teknologi Finansial Perbankan Digital. Yayasan Prima Agus Teknik Bekerja sama dengan Universitas Sains & Teknologi Komputer (Universitas STEKOM), 2021.

Chen, Yingsi. "Research on Regulation of Personal Financial Data Sharing in Open Banking." Asian Journal of Education and Social Studies 45, no. 3 (2023): 31–41. https://doi.org/10.9734/ajess/2023/v45i3985.

Damayanti, Adelina, and Rina Arum Prastyanti. "Kajian Hukum Dan Regulasi Terkait Serangan Hacking Pada Platform Digital Di Indonesia." Multidisciplinary Indonesian Center Journal (MICJO) 1, no. 2 (2024): 1043–54. https://doi.org/10.62567/micjo.v1i2.117.

Desmon, Johanes, Syarief Hidayatulloh, and Yuwan Jumaryadi. "Systematic Literature Review: Serangan Deface Website Sebagai Bentuk Kejahatan Siber." Jurnal Sistem Informasi 14, no. 2 (2024).

Elisabeth Nurhaini Butar-Butar. Metode Penelitian Hukum, Langkah-Langkah Untuk Menemukan Kebenaran Dalam Ilmu Hukum. PT. Refika Aditama, 2018.

Farao, Aristeidis, Georgios Paparis, Sakshyam Panda, Emmanouil Panaousis, Apostolis Zarras, and Christos Xenakis. "INCHAIN: A Cyber Insurance Architecture with Smart Contracts and Self-Sovereign Identity on Top of Blockchain." International Journal of Information Security 23, no. 1 (2024): 347–71. https://doi.org/10.1007/s10207-023-00741-8.

Fitroh, Qorry Aina, and Bambang Sugiantoro. "Peran Ethical Hacking Dalam Memerangi Cyberthreats." JURNAL ILMIAH INFORMATIKA 11, no. 01 (2023): 27–31. https://doi.org/10.33884/jif.v11i01.6593.

Hadiprakoso, Raden Budiarto, Wahyu Rendra Aditya, and Febriora Nevia Pramitha. "Analisis Statis Deteksi Malware Android Menggunakan Algoritma Supervised Machine Learning." Cyber Security dan Forensik Digital 5, no. 1 (2022): 1–5. https://doi.org/10.14421/csecurity.2022.5.1.3116.

McGregor, Richard, Carmen Reaiche, Stephen Boyle, and Graciela Corral De Zubielqui. "Cyberspace and Personal Cyber Insurance: A Systematic Review." Journal of Computer Information Systems 64, no. 1 (2024): 157–71. https://doi.org/10.1080/08874417.2023.2185551.

Purba, Indra Gunawan, Anjani Sipahutar, and Irwansyah Irwansyah. "Pengaturan pemberian kredit pada dunia perbankan di indonesia." Jurnal Normatif 2, no. 2 (2022): 203–11.

https://doi.org/10.54123/jn.v2i2.230.

Rohmah, Ulviatur, Nur Alvinatul Hasanah, and Rini Puji Astuti. "Regulasi Dan Pengawasan Perbankan Oleh Otoritas Jasa Keuangan." Jurnal Penelitian Nusantara 1, no. 5 (2025): 314–19.

Saragih, Geofani Milthree. "Pancasila Sebagai Landasan Filosofis Pembentukan Peraturan Perundang-Undangan Di Indonesia." Jurnal Pancasila dan Kewarganegaraan 2, no. 1 (2022).

Tsohou, Aggeliki, Vasiliki Diamantopoulou, Stefanos Gritzalis, and Costas Lambrinoudakis. "Cyber Insurance: State of the Art, Trends and Future Directions." International Journal of Information Security 22, no. 3 (2023): 737–48. https://doi.org/10.1007/s10207-023-00660-8.

Utama, Andrew Shandy. "Digitalisasi Produk Bank Konvensional Dan Bank Syariah Di Indonesia." Jurnal Justisia : Jurnal Ilmu Hukum, Perundang-undangan dan Pranata Sosial 6, no. 2 (2021): 113. https://doi.org/10.22373/justisia.v6i2.11532.