KAMPUS AKADEMIK PUBLISING
Jurnal Ilmiah Penelitian Mahasiswa
Vol.2, No.6 Desember 2024
e-ISSN: 3025-5465; p-ISSN: 3025-7964, Hal 397-406
DOI : https://doi.org/10.61722/jipm.v2i6.571

Peran Hukum serta Kendala dalam Menjalankan Strategi Bank Melindungi Nasabah di Era Digital untuk Keamanan Transaksi Online

Revalina Gita Ananda
revalinaga@students.unnes.ac.id
Universitas Negeri Semarang
Permata Intan Maharani
intanmahaharani@students.unnes.ac.id
Universitas Negeri Semarang
Fara Diva Arrum Clarisa Putri
faradivaarrum@students.unnes.ac.id
Universitas Negeri Semarang
Davina Nurfadilah
davinanurfadilah23@students.unnes.ac.id
Fakultas Hukum, Universitas Negeri Semarang
Coressponding email: faradivaarrum@students.unnes.ac.id

Abstrak Artikel ini membahas tentang strategi perbankan dalam melindungi nasabah di era digital, dengan fokus pada keamanan transaksi online. Transformasi digital di era industri 4.0 mendorong sektor perbankan untuk beradaptasi dengan teknologi guna memenuhi kebutuhan konsumen dan menghadapi persaingan. Namun, perkembangan ini juga menghadirkan risiko kejahatan siber, seperti phishing, malware, skimming, dan social engineering, yang mengancam keamanan transaksi online nasabah. Menggunakan metode penelitian pendekatan yuridis normatif untuk menganalisis peran hukum dalam menetapkan standar perlindungan nasabah, yang bertujuan untuk menganalisis strategi dan peran hukum dalam melindungi nasabah dari ancaman tersebut. Undang-Undang seperti UU Perlindungan Data Pribadi, UU ITE, dan regulasi OJK menjadi landasan hukum yang penting bagi bank untuk menerapkan langkah mitigasi. Selain itu, kendala seperti ketertinggalan regulasi, keterbatasan teknologi, dan kurangnya edukasi nasabah menjadi tantangan dalam penerapan strategi perlindungan. Pentingnya kerja sama antara bank, regulator, dan penegak hukum untuk memastikan keamanan data serta meningkatkan kepercayaan publik terhadap layanan perbankan digital.

Kata kunci : Transaksi Online, Perbankan Digital, Kejahatan Siber

Pendahuluan

Era industri 4.0 adalah fase transformasi yang signifikan dalam berbagai aspek kegiatan industri dan kehidupan manusia, yang ditandai dengan pemanfaatan teknologi digital dan internet secara masif. Konsep ini mencakup proses produksi yang terorganisir menggunakan teknologi nirkabel dan big data, yang memungkinkan pengelolaan data secara lebih akurat melalui sistem server. Semua proses diintegrasikan untuk beroperasi secara otomatis dalam satu sistem yang terpadu.[1] Industri perbankan global mengalami perubahan besar dengan munculnya perbankan digital sebagai faktor kunci untuk bersaing di tengah ketatnya persaingan di sektor keuangan. Digitalisasi dalam perbankan kini bukan lagi pilihan, melainkan suatu keharusan untuk memenuhi kebutuhan

[1] Tambunan, Ria Tifanny, and M. Irwan Padli Nasution. "Tantangan dan strategi perbankan dalam menghadapi perkembangan transformasi digitalisasi di era 4.0." *Sci-Tech Journal* 2, no. 2 (2023): 148-156.

Received Agustus 30, 2024; Revised Oktober 31, 2024; Desember 05, 2024
* **Revalina Gita Ananda**, revalinaga@students.unnes.ac.id

konsumen yang terus berkembang, meningkatkan efisiensi operasional, serta menghadapi tantangan dari perusahaan teknologi finansial (fintech) dan startup lainnya.[2]

Berbagai fasilitas yang ditawarkan oleh bank melalui layanan internet banking memberikan kemudahan bagi masyarakat dalam menjalani aktivitas keuangan. Kemampuan untuk melakukan berbagai transaksi tanpa harus mengunjungi bank secara langsung menjadi nilai tambah yang signifikan bagi nasabah. Perkembangan internet banking ini mendorong sektor perbankan untuk terus meningkatkan kinerja dan layanan mereka, termasuk memastikan keamanan transaksi online, memberikan pelayanan pelanggan yang optimal, serta menghadirkan inovasi produk yang sesuai dengan kebutuhan nasabah yang semakin kompleks. [3]

Perbankan yang memiliki peran penting dalam infrastruktur ekonomi dan sistem transaksi keuangan, sangat rentan terhadap berbagai bentuk tindak kejahatan. Masyarakat seringkali menjadi sasaran potensial akibat keterbatasan pengetahuan mereka tentang potensi risiko yang mengintai. Dalam konteks keamanan jasa keuangan, terdapat dua kategori utama praktik kejahatan, yaitu *skimming* dan *social engineering*, yang keduanya memiliki mekanisme dan dampak yang berbeda dalam mengancam keamanan transaksi keuangan.[4] Kejahatan di sektor jasa keuangan, seperti *skimming* dan *social engineering*, memiliki modus operandi berbeda. Skimming adalah pencurian data kartu menggunakan alat khusus di ATM atau perangkat pembayaran untuk menduplikasi kartu korban. Sementara itu, social engineering melibatkan manipulasi psikologis, di mana pelaku berpura-pura sebagai pihak resmi untuk memperoleh informasi rahasia korban, seperti PIN atau password.

Selain itu, kejahatan lain juga banyak berkembang seperti kejahatan siber, seperti phishing dan malware. Phishing dan malware adalah ancaman utama kejahatan siber bagi nasabah bank. Phishing melibatkan pelaku yang menyamar sebagai bank untuk mencuri informasi pribadi korban melalui email atau pesan palsu. Sementara malware adalah perangkat lunak berbahaya yang mencuri data atau merusak sistem korban setelah masuk melalui email atau situs web tidak aman.

Pemerintah menyadari pentingnya perlindungan bagi nasabah (konsumen) dan bank, sehingga telah menetapkan sejumlah regulasi hukum. Di antaranya adalah UU Nomor 8 Tahun 1999 tentang Perlindungan Konsumen dan UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Salah satu alasan diterbitkannya undang-undang tersebut adalah untuk mendukung pengembangan teknologi informasi dengan menyediakan infrastruktur hukum dan regulasi yang memungkinkan pemanfaatan teknologi informasi secara aman. Hal ini bertujuan mencegah penyalahgunaan teknologi dengan tetap mempertimbangkan nilai-nilai agama dan budaya masyarakat Indonesia.[5]

---

[2] Safitri, Novia Amanda, Riska Julia, Septi Swinta, Nining Novia Elisah, Dinda Nadya Anastasya Hutapea, and Nadiva Ariyana. "Strategi Inovasi Perbankan Digital dalam Menghadapi Persaingan Industri Keuangan." *Indonesian Journal of Economics, Management and Accounting* 1, no. 5 (2023): 414-419.

[3] Balaka, Kemal Idris, Aulia Rahman Hakim, and Frygyta Dwi Sulistyany. "Pencurian Informasi Nasabah Di Sektor Perbankan: Ancaman Serius Di Era Digital." *Yustitiabelen* 10, no. 2 (2024): 105-130.

[4] Ratulangi, Christian Henry. "Tindak pidana cyber crime dalam kegiatan perbankan." *Lex Privatum* 9, no. 5 (2021).

[5] Nani Widya Sari, "Kejahatan Cyber Dalam Perkembangan Teknologi Informasi Berbasis Komputer", Jurnal Surya Kencana Dua: Dinamika Masalah Hukum dan Keadilan 5, no. 2 (Desember 2020): 579.

Undang-undang seperti UU Perlindungan Data Pribadi dan UU Informasi dan Transaksi Elektronik memberikan landasan bagi bank untuk mengimplementasikan sistem keamanan yang memenuhi standar perlindungan data dan mencegah penyalahgunaan informasi. Selain itu, hukum juga mengatur kewajiban bank dalam mengedukasi nasabah mengenai risiko transaksi online dan langkah-langkah pencegahan yang perlu diambil.

Peran hukum dalam strategi bank melindungi nasabah di era digital sangat krusial untuk memastikan keamanan transaksi online. Hukum berfungsi sebagai dasar regulasi yang mengatur dan menetapkan standar keamanan yang harus dipatuhi oleh bank dalam melindungi data pribadi dan keuangan nasabah. Strategi bank dalam melindungi nasabah di era digital sangat penting, terutama untuk memastikan keamanan transaksi online. Seiring dengan meningkatnya ancaman kejahatan siber seperti phishing, malware, dan pencurian identitas, bank perlu mengimplementasikan langkah-langkah perlindungan yang efektif untuk mencegah kerugian finansial dan melindungi data pribadi nasabah. Perbankan memiliki peran penting dalam meningkatkan keamanan transaksi online karena mereka menjaga kepercayaan nasabah dengan melindungi informasi finansial. Selain itu, bank juga wajib mematuhi peraturan hukum terkait perlindungan data dan transaksi online, seperti UU Perlindungan Data Pribadi, guna menghindari sanksi hukum. Dengan strategi perlindungan yang tepat, bank dapat mencegah kerugian, menjaga reputasi, dan memastikan nasabah merasa aman dalam bertransaksi di dunia digital sesuai dengan perundang-undangan.

Metode Penelitian

Metode penelitian yang digunakan adalah yuridis normatif yaitu pendekatan yang digunakan dalam studi hukum dengan fokus pada norma-norma atau aturan-aturan hukum yang berlaku, baik yang tertulis dalam perundang-undangan maupun yang berkembang dalam praktik. Penelitian ini bertujuan untuk menganalisis, mengkaji, dan memahami peraturan hukum yang relevan dengan isu hukum tertentu. Dengan pendekatan ini, peneliti berusaha mengidentifikasi prinsip-prinsip hukum yang mendasari suatu permasalahan serta memberikan interpretasi terhadap norma yang ada untuk mencari solusi atas masalah hukum yang dihadapi.

Pembahasan

A. Peran Hukum dalam Mengatur Kewajiban Bank dalam Melindungi Nasabah dari Ancaman Kejahatan Siber pada Transaksi Online

Lembaga perbankan berperan sebagai penghubung dalam aktivitas keuangan, di mana mereka menghimpun dana dari masyarakat yang memiliki surplus keuangan dan menyalurkan dalam bentuk pinjaman kepada pihak yang membutuhkan. Hubungan antara bank serta nasabah didasarkan pada kepercayaan, yang dikenal sebagai "*fiduciary relation*".[6] Tanpa kepercayaan dari masyarakat, operasional perbankan tidak tidak dapat berjalan sebagaimana mestinya. Oleh karena itu, bank harus memastikan kondisi keuangannya tetap sehat untuk mempertahankan kepercayaan masyarakat.

[6] Kurniawan, Kukuh Dwi, and Dwi Ratna Indri Hapsari. "Kejahatan dunia maya pada sektor perbankan Di Indonesia: analisa perlindungan hukum terhadap nasabah." *Pleno Jure*10, no. 2 (2021): 122-133.

Kemajuan teknologi berkembang pesat dengan tujuan utama untuk mendukung kemudahan aktivitas manusia. Pada dunia perbankan, efektivitas serta efisiensi menjadi kunci yang mendorong lahirnya berbagai inovasi dalam produk dan layanan. Meskipun perkembangan tersebut harus tetap mematuhi ketentuan yang diatur dalam Undang-Undang Nomor 7 Tahun 1992 tentang perbankan, yang telah diperbarui melalui Undang-Undang Nomor 10 Tahun 1998 (UU Perbankan).

Dalam menghadapi kasus kejahatan siber yang melibatkan sektor perbankan, Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) menjadi acuan hukum yang relevan. Peraturan ini mencakup pengamanan data serta transaksi elektronik, termasuk perlindungan terhadap pencurian data dan ancaman serangan siber. Oleh karena itu, lembaga perbankan wajib mematuhi aturan tersebut dengan menerapkan strategi keamanan siber yang efektif untuk melindungi data dan informasi nasabah. Selain itu, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi memberikan dasar hukum untuk melindungi privasi individu dan memastikan keamanan data pribadi. Undang-undang ini bertujuan untuk menjamin hak-hak masyarakat atas privasi, meningkatkan kesadaran publik, dan menghormati pentingnya perlindungan data pribadi. Perlindungan data nasabah bertujuan untuk memastikan hak nasabah atas keamanan data pribadi mereka sekaligus menegaskan pentingnya penghormatan terhadap data tersebut oleh lembaga perbankan. Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan mengatur kewajiban perbankan untuk melindungi dana masyarakat melalui pembentukan Lembaga Penjamin Simpanan, yang berfungsi menjamin keamanan simpanan nasabah di bank.[7]

Penerapan ketiga peraturan tersebut sangat penting untuk menjaga stabilitas operasional perbankan serta mencegah tindak kejahatan di dunia maya. Dukungan pengawasan ketat dan penegakan hukum yang konsisten juga diperlukan agar masyarakat tetap percaya pada institusi perbankan.[8]

Pemanfaatan teknologi informasi dalam sektor perbankan, yang dikenal sebagai Electronic Banking (E-banking), memungkinkan layanan perbankan diakses dengan mudah melalui perangkat pribadi. Meski menawarkan berbagai kemudahan, hal ini juga membuka peluang terjadinya penyalahgunaan data nasabah melalui tindakan kejahatan siber. Oleh karena itu, lembaga perbankan perlu memastikan adanya sistem keamanan yang andal untuk menjaga kepercayaan masyarakat dan menjamin bahwa penggunaan teknologi dalam layanan perbankan tetap aman.

Berdasarkan Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (UUPK), Pasal 1 ayat 1 mengatur bahwa perlindungan konsumen mencakup segala upaya yang memastikan kepastian hukum untuk melindungi

[7] Situngkir, Tiar Lina, dkk. 2022. Bank dan Lembaga Keuangan Non Bank. Magelang: Pustaka Rumah C1nta.
[8] Rosadi, Sinta Dewi. 2023. Pembahasan UU Perlindungan Data Pribadi (UU RI No. 27 Tahun 2022). Sinar Grafika.

hak-hak konsumen. Negara, melalui berbagai sistem dan lembaga terkait, memberikan jaminan hukum untuk melindungi konsumen di Indonesia, sekaligus mencegah tindakan dari pelaku usaha yang tidak bertanggung jawab atau merugikan. Dalam hal perbankan, UUPK memberikan jaminan kepastian hukum untuk menjamin pencegahan ancaman siber. UUPK memiliki peran untuk memberikan rasa aman bagi konsumen.

Regulasi spesifik lainnya yang diterbitkan oleh Otoritas Jasa Keuangan (OJK), seperti POJK No. 13/POJK.02/2018 tentang Inovasi Keuangan Digital, mengatur kewajiban bank dalam menerapkan manajemen risiko teknologi informasi, termasuk memastikan adanya langkah mitigasi terhadap ancaman siber. Bank diwajibkan untuk menggunakan teknologi enkripsi mutakhir, sistem otentikasi multi-faktor, serta mekanisme pengawasan berbasis kecerdasan buatan (AI) untuk mendeteksi dan mencegah potensi penipuan atau peretasan. Selain itu, bank juga harus menyediakan infrastruktur yang tahan terhadap serangan siber, seperti Distributed Denial of Service (DDoS), serta memastikan sistem mereka diaudit secara berkala oleh lembaga independen.[9]

Tak hanya dari sisi teknologi, hukum juga mengatur kewajiban bank dalam hal edukasi nasabah. Bank diwajibkan memberikan informasi yang jelas mengenai potensi risiko siber dan langkah-langkah yang harus diambil oleh nasabah untuk menjaga keamanan akun mereka. Misalnya, larangan membagikan data sensitif seperti One-Time Password (OTP) atau penggunaan jaringan internet publik saat mengakses layanan perbankan. Apabila terjadi pelanggaran atau kegagalan sistem yang mengakibatkan kerugian bagi nasabah, bank juga wajib memberikan kompensasi sesuai dengan ketentuan hukum yang berlaku.

Jika nasabah mengalami kerugian finansial akibat transaksi perbankan melalui e-banking, sengketa yang timbul dapat diselesaikan melalui jalur litigasi maupun non-litigasi sebagai alternatif penyelesaian. Apabila kerugian disebabkan oleh tindakan kejahatan siber, nasabah berhak untuk melaporkan masalah tersebut kepada pihak bank. Pengaduan ini akan ditindaklanjuti oleh bank sebagai bagian dari upaya perlindungan terhadap hak-hak nasabah dalam konteks hubungan hukum dengan bank. Jika pengaduan nasabah tidak mendapatkan tanggapan yang memadai, hal ini dapat merusak citra dan reputasi bank, yang pada gilirannya dapat menurunkan kepercayaan publik terhadap sektor perbankan. Oleh karena itu, setiap bank diharuskan untuk membentuk unit khusus yang bertugas menangani aduan dari nasabah.[10]

Prosedur penyelesaian sengketa antara lembaga perbankan dan nasabahnya sebagai konsumen diatur dalam berbagai peraturan, termasuk Undang-Undang Perlindungan Konsumen (UUPK) sebagai undang-undang

[9] Kusumaningtyas, Rindia Fanny, Ristina Yudhanti, and Afifah Widyastuti. "The Urgency of Organizing Insurtech in Improving Insurance Services Based on POJK No. 13/POJK. 02/2018 Regarding Digital Financial Innovation in the Financial Services Sector." *Pandecta Research Law Journal* 18, no. 2 (2023): 403-423.
[10] *Ibid.*

pokok, serta sejumlah regulasi lainnya. Ini meliputi Keputusan Menteri Perindustrian dan Perdagangan Republik Indonesia Nomor 350/MPP/Kep/12/2001 tentang Pelaksanaan Tugas dan Wewenang Badan Penyelesaian Sengketa Konsumen, Peraturan Bank Indonesia Nomor 10/10/PBI/2008 yang mengubah Peraturan Bank Indonesia Nomor 7/7/PBI/2005 mengenai Penyelesaian Pengaduan Nasabah, dan Peraturan Otoritas Jasa Keuangan Nomor 1/POJK.07/2013 terkait Perlindungan Konsumen di Sektor Jasa Keuangan.

B. Kendala Bank dalam Penerapan Strategi Berbasis Hukum untuk Perlindungan Nasabah dari Kejahatan Siber

Dalam era digital yang semakin maju, kejahatan siber telah menjadi ancaman serius bagi industri perbankan. Dengan meningkatnya penggunaan teknologi dalam layanan keuangan, risiko serangan siber seperti pencurian data, phishing, dan ransomware semakin besar. Bank, sebagai institusi yang bertanggung jawab atas keamanan dana dan informasi nasabah, menghadapi tekanan untuk memastikan sistem mereka tahan terhadap berbagai ancaman ini. Salah satu upaya yang dilakukan adalah mengintegrasikan strategi berbasis hukum sebagai langkah perlindungan. Namun, penerapan strategi ini bukan tanpa tantangan, terutama karena kompleksitas dan dinamika yang terus berkembang dalam ranah hukum dan teknologi.

Salah satu kendala utama yang dihadapi bank dalam menerapkan strategi berbasis hukum untuk melindungi nasabah dari kejahatan siber adalah aspek regulasi dan hukum. Dalam banyak kasus, peraturan yang mengatur keamanan siber tidak selalu selaras dengan perkembangan teknologi yang sangat cepat. Ketidakpastian atau kekosongan hukum sering kali terjadi, terutama ketika menghadapi ancaman baru yang belum diakomodasi dalam regulasi yang ada. Selain itu, perbedaan interpretasi terhadap aturan di berbagai yurisdiksi dapat menyulitkan bank, terutama yang beroperasi lintas negara, untuk mematuhi semua persyaratan hukum secara konsisten. Keterlambatan adaptasi regulasi terhadap modus kejahatan siber yang terus berkembang juga menjadi tantangan serius, mengingat penjahat siber selalu mencari celah hukum untuk mengeksploitasi sistem perbankan.[11] Akibatnya, meskipun bank berupaya mematuhi regulasi yang ada, mereka masih rentan terhadap serangan yang tidak terduga.

Selain kendala regulasi, kesiapan teknologi dan infrastruktur juga menjadi tantangan signifikan bagi bank dalam melindungi nasabah dari kejahatan siber. Sistem keamanan yang digunakan oleh bank seringkali tertinggal dibandingkan dengan perkembangan ancaman siber yang semakin kompleks. Implementasi teknologi perlindungan yang canggih, seperti enkripsi data tingkat tinggi dan sistem deteksi ancaman berbasis kecerdasan buatan, membutuhkan investasi yang

[11] Irawati, Ana, Hasan Bachtiar Fadholi, Alfarozi Nur Alamsyah, Dimas Pramodya Dwipayana, and Moh Muslih. "Urgensi Cyber Law dalam Kehidupan Masyarakat Indonesia Di Era Digital." In *Proceeding of Conference on Law and Social Studies*. 2021.

sangat besar. Hal ini menjadi beban, terutama bagi bank kecil atau regional yang memiliki keterbatasan anggaran dan sumber daya teknologi. Selain itu, keterbatasan tenaga ahli di bidang keamanan siber memperburuk situasi, karena tidak semua bank mampu merekrut atau mempertahankan profesional yang kompeten. Tanpa infrastruktur dan teknologi yang memadai, upaya perlindungan terhadap nasabah menjadi kurang efektif, sehingga meningkatkan risiko terjadinya pelanggaran keamanan.

Di sisi lain, kurangnya edukasi kepada nasabah juga menjadi kendala penting dalam melindungi mereka dari kejahatan siber. Banyak nasabah yang belum sepenuhnya memahami risiko keamanan saat melakukan transaksi online, seperti bahaya phishing, penggunaan perangkat yang tidak aman, atau membagikan informasi pribadi secara sembarangan. Minimnya kesadaran ini sering dimanfaatkan oleh pelaku kejahatan siber untuk mengelabui nasabah melalui modus-modus yang tampak meyakinkan.[12] Bank seringkali menghadapi tantangan dalam menyosialisasikan langkah-langkah pencegahan kejahatan siber kepada nasabah, baik karena keterbatasan saluran komunikasi maupun rendahnya respons dari nasabah itu sendiri. Padahal, perlindungan keamanan siber bukan hanya tanggung jawab bank, tetapi juga membutuhkan peran aktif nasabah untuk menjaga kerahasiaan data dan menggunakan layanan digital secara bijak. Tanpa edukasi yang memadai, nasabah cenderung menjadi target yang rentan, meskipun bank telah menyediakan sistem keamanan yang kuat.

Kerja sama antara bank dengan penegak hukum dan regulator juga menghadapi berbagai hambatan dalam upaya melindungi nasabah dari kejahatan siber. Koordinasi yang kurang efektif sering kali menjadi penghalang utama, terutama dalam penanganan insiden yang melibatkan banyak pihak. Proses investigasi kejahatan siber, misalnya, sering kali memerlukan waktu yang panjang karena kompleksitas sistem digital dan kerahasiaan data yang harus dijaga. Selain itu, bank kerap menghadapi kesulitan dalam melaporkan kasus kejahatan siber secara cepat dan memperoleh tindak lanjut yang memadai dari pihak berwenang.[13] Regulasi yang mengatur mekanisme pelaporan juga terkadang tidak cukup jelas atau tidak selaras antara berbagai lembaga terkait, sehingga memperumit upaya kolaborasi. Kurangnya mekanisme yang terstandarisasi untuk menangani kejahatan siber ini dapat memperlambat respons, meningkatkan kerugian nasabah, dan melemahkan kepercayaan terhadap keamanan layanan perbankan digital.

Selain ancaman dari luar, bank juga harus menghadapi potensi ancaman internal yang dapat melemahkan upaya perlindungan terhadap nasabah. Salah satu bentuk ancaman ini adalah kebocoran data yang dilakukan oleh karyawan, baik secara sengaja maupun tidak sengaja. Beberapa kasus menunjukkan bahwa

[12] Prasetyo, Yunan Dwi. "Strategi Penerapan Manajemen Risiko Untuk Mencegah Kejahatan Siber Di Mobile banking Pada Bank Pembangunan Daerah Yogyakarta Kantor Cabang Syariah." PhD diss., Universitas Islam Indonesia, 2024.
[13] Ju, Ade Borami, Angel Tng, Nadia Carolina Weley, and Hari Sutra Disemadi. "Perlindungan Nasabah Dalam Penerapan Electronic Banking Sebagai Bagian Aktifitas Bisnis Perbankan Di Indonesia." *Jurnal Perspektif Administrasi Dan Bisnis* 2, no. 1 (2021): 27-40.

kejahatan siber dapat melibatkan pihak internal yang memiliki akses langsung ke sistem dan data sensitif. Kelemahan dalam pengawasan internal, seperti kurangnya audit berkala atau minimnya sistem kontrol akses yang ketat, dapat memberikan celah bagi pihak internal untuk menyalahgunakan wewenang. Selain itu, rendahnya tingkat kesadaran keamanan siber di kalangan karyawan juga dapat meningkatkan risiko, misalnya melalui penggunaan perangkat kerja yang tidak aman atau ketidaktahuan terhadap ancaman phishing.[14] Oleh karena itu, bank perlu memperkuat pengawasan internal dan memberikan pelatihan keamanan siber secara rutin untuk meminimalkan risiko dari dalam.

Dinamika ancaman siber yang terus berkembang juga menjadi kendala utama bagi bank dalam melindungi nasabah. Modus operandi kejahatan siber kini semakin beragam dan canggih, dengan serangan yang menggunakan teknologi seperti kecerdasan buatan (AI) dan machine learning untuk mengelabui sistem keamanan. Serangan seperti ransomware, malware, dan phishing kini dirancang agar sulit terdeteksi, bahkan oleh sistem keamanan yang canggih sekalipun. Selain itu, penjahat siber seringkali memanfaatkan celah yang muncul dari integrasi teknologi baru, seperti Internet of Things (IoT) dan aplikasi berbasis cloud, yang belum sepenuhnya aman.[15] Ketidakpastian dalam memprediksi pola serangan berikutnya membuat bank harus selalu bersikap reaktif, yang sering kali terlambat untuk mencegah kerugian. Kondisi ini memaksa bank untuk terus meningkatkan sistem deteksi dan respons mereka, yang tidak hanya memerlukan investasi besar tetapi juga membutuhkan pembaruan teknologi secara berkala.

Kendala lain yang tidak kalah penting adalah tingginya biaya yang harus dikeluarkan bank untuk memenuhi standar keamanan yang sesuai dengan peraturan. Pengembangan dan penerapan sistem keamanan siber yang mutakhir, seperti enkripsi data tingkat lanjut, firewall, dan analitik ancaman berbasis AI, membutuhkan investasi yang signifikan. Selain itu, biaya untuk pelatihan karyawan, peningkatan infrastruktur, dan audit keamanan secara berkala juga menambah beban operasional bank. Hal ini menjadi tantangan terutama bagi bank kecil atau menengah yang memiliki keterbatasan anggaran. Bank juga sering kali dihadapkan pada dilema antara efisiensi operasional dan kebutuhan untuk memenuhi regulasi keamanan siber yang ketat. Jika langkah perlindungan dianggap terlalu mahal, beberapa bank mungkin terpaksa mengambil pendekatan minimal, yang pada akhirnya meningkatkan risiko keamanan bagi nasabah.

Selain tantangan teknis dan operasional, menjaga kepercayaan nasabah menjadi kendala strategis yang harus dihadapi bank dalam melindungi mereka

[14] Malunsenge, Leticia, Cornelis Massie, and Ronald Rorie. "Penegakan Hukum Terhadap Pelaku Dan Korban Tindak Pidana Cyber Crime Berbentuk Phising Di Indonesia." *Lex Crimen* 11, no. 3 (2022).
[15] Wulan, Wulan, Hadita Hadita, Achmad Fauzi, Ajeng Maharani Putri, Fika Fitriyani, Rini Astriyani, Vina Arisana, and Yuyun Indah Cahyani. "Tinjauan Ancaman dan Risiko pada Sistem Keamanan Internet of Things, Berbasis Cloud Computing dalam Penggunaan E-Commerce dan Rencana Strategis." *Jurnal Kewirausahaan dan Multi Talenta* 2, no. 2 (2024): 126-137.

dari kejahatan siber. Ketika terjadi pelanggaran keamanan, meskipun bank telah berupaya melindungi data dan transaksi nasabah, insiden tersebut seringkali berdampak pada menurunnya kepercayaan publik terhadap kemampuan bank dalam menjaga keamanan. Reputasi yang rusak akibat kebocoran data atau serangan siber besar membutuhkan waktu dan upaya yang tidak sedikit untuk dipulihkan. Lebih jauh, nasabah yang merasa tidak aman dapat memutuskan untuk beralih ke lembaga keuangan lain yang dianggap lebih terpercaya. Dalam situasi ini, bank tidak hanya harus fokus pada penguatan sistem keamanan, tetapi juga pada komunikasi krisis yang efektif untuk meyakinkan nasabah bahwa langkah-langkah pencegahan telah diambil. Tanpa kepercayaan nasabah, upaya perlindungan yang dilakukan bank akan kehilangan esensinya, karena loyalitas nasabah adalah inti dari keberlangsungan bisnis perbankan di era digital. Dengan demikian, keberhasilan dalam mengatasi kendala-kendala ini tidak hanya bergantung pada teknologi atau regulasi, tetapi juga pada kemampuan bank untuk membangun dan mempertahankan hubungan yang kuat dengan nasabah mereka.

KESIMPULAN

Peran hukum dan regulasi sangat penting dalam melindungi nasabah dari ancaman kejahatan siber di era digital. Undang-undang seperti UU Informasi dan Transaksi Elektronik serta UU Pelindungan Data Pribadi menjadi landasan utama yang mengatur standar keamanan bagi bank dalam menjaga data pribadi dan transaksi nasabah. Dalam praktiknya, bank harus menerapkan strategi perlindungan yang melibatkan teknologi mutakhir, seperti enkripsi data, otentikasi multifaktor, dan kecerdasan buatan untuk mencegah tindak kejahatan. Edukasi kepada nasabah juga menjadi komponen penting, mengingat rendahnya kesadaran masyarakat terhadap risiko keamanan digital sering dimanfaatkan oleh pelaku kejahatan. Namun, implementasi strategi berbasis hukum menghadapi berbagai kendala, seperti ketertinggalan regulasi dibandingkan perkembangan teknologi, keterbatasan anggaran untuk investasi keamanan, serta kurangnya tenaga ahli di bidang siber. Selain itu, kurangnya pemahaman nasabah tentang langkah-langkah pencegahan risiko juga menjadi tantangan signifikan. Untuk mengatasi masalah ini, dibutuhkan kolaborasi antara bank, pemerintah, regulator, dan masyarakat dalam menciptakan ekosistem perbankan digital yang aman. Edukasi berkelanjutan kepada nasabah dan percepatan adaptasi regulasi yang sesuai dengan dinamika teknologi menjadi langkah strategis. Dengan pendekatan ini, bank tidak hanya dapat menjaga kepercayaan nasabah, tetapi juga mencegah kerugian yang lebih besar akibat kejahatan siber.

DAFTAR PUSTAKA

Balaka, Kemal Idris, Aulia Rahman Hakim, and Frygyta Dwi Sulistyany. 2024. "Pencurian Informasi Nasabah Di Sektor Perbankan: Ancaman Serius Di Era Digital." Yustitiabelen 10, no. 2 105-130.

Irawati, Ana, Hasan Bachtiar Fadholi, Alfarozi Nur Alamsyah, Dimas Pramodya Dwipayana, and Moh Muslih. 2021. "Urgensi Cyber Law dalam Kehidupan

Masyarakat Indonesia Di Era Digital." Proceeding of Conference on Law and Social Studies.

Ju, Ade Borami, Angel Tng, Nadia Carolina Weley, and Hari Sutra Disemadi. 2021. "Perlindungan Nasabah dalam Penerapan Electronic Banking sebagai Bagian Aktifitas Bisnis Perbankan di Indonesia." Jurnal Perspektif Administrasi dan Bisnis 2, no. 1 27-40.

Kurniawan, Kukuh Dwi, and Dwi Ratna Indri Hapsari. 2021. "Kejahatan Dunia Maya pada Sektor Perbankan di Indonesia: Analisa Perlindungan Hukum terhadap Nasabah." Pleno Jure 10, no. 2 122-133.

Kusumaningtyas, Rindia Fanny, Ristina Yudhanti, and Afifah Widyastuti. 2023. "The Urgency of Organizing Insurtech in Improving Insurance Services Based on POJK No. 13/POJK.02/2018 Regarding Digital Financial Innovation in the Financial Services Sector." Pandecta Research Law Journal 403-423.

Malunsenge, Leticia, Cornelis Massie, and Ronald Rorie. 2022. "Penegakan Hukum Terhadap Pelaku dan Korban Tindak Pidana Cyber Crime Berbentuk Phising di Indonesia." Lex Crimen 11, no. 3.

Prasetyo, Yunan Dwi. 2024. Strategi Penerapan Manajemen Risiko untuk Mencegah Kejahatan Siber di Mobile Banking Pada Bank Pembangunan Daerah Yogyakarta Kntor Cabang Syariah. PhD diss, Yogyakarta: Univestitas Islam Indonesia.

Ratulangi, Christian Henry. 2021. "Tindak Pidana Cyber Crime dalam Kegiatan Perbankan." Lex Privatum 9, no. 5.

Rosadi, Sinta Dewi. 2023. Pembahasan UU Perlindungan Data Pribadi (UU RI No. 27 Tahun 2022). Sinar Grafika.

Safitri, Novia Novia Amanda, Riska Julia, Septi Swinta, Nining Novia Elisah, Dinda Nadya Anastasya Hutapea, and Nadiva Ariyana. 2023. "Strategi Inovasi Perbankan Digital dalam Menghadapi Persaingan Industri Keuangan." Indonesian Journal of Economics, Management and Accounting 1, no. 5 414-419.

Sari, Nani Widya. 2020. "Kejahatan Cyber dalam Perkembangan Teknologi Informasi Berbasis Komputer." Jurnal Surya Kencana Dua: Dinamika Masalah Hukum dan Keadilan 5, no 2 579.

Situngkir, Tiar Lina, Ananda Dewi Nur Faidah, Bram Indra Maulana, Farhan Rahdian, Nuri Irma, Okky Wirandana, Qirsa Zahrota Zar'in, and Simbolon Paulina Karolin. 2022. Bank dan Lembaga Keuangan Non Bank. Magelang: Pustaka Rumah Cinta.

Tambunan, Ria Tiffany, and M. Irwan Padli Nasution. 2023. "Tantangan dan Strategi Perbankan Dalam Menghadapi Perkembangan Transformasi Digitalisasi di Era 4.0." Sci-Tech Journal 2, no. 2 148-156.

Wulan, Wulan, Hadita Hadita, Achmad Fauzi, Ajeng Maharani Putri, Fika Fitriyani, Rini Astriyani, Vina Arisana, and Yuyun Indah Cahyani. 2024. "Tinjauan Ancaman dan Risiko pada Sistem Keamanan Internet of Things, Berbasis Cloud Computing dalam Penggunaan E-Commerce dan Rencana Strategis." Jurnal Kewirausahaan dan Multi Talenta 2, no. 2 126-137.