Jurnal Retentum
Volume: 07, Number: 01, 2025, Page : 386-398
https://jurnal.darmaagung.ac.id/index.php/retentum

p-ISSN 2686-5432
e-ISSN 2686-5440

Rekonstruksi Perlindungan Hukum Bagi Konsumen Perbankan di Tengah Ancaman Kejahatan Teknologi

Miftakul Azis[1], Ahmad Redi[2]
[1,2]Universitas Borobudur
Email : azizmoeda@gmail.com[1*], redi.ahmad2010@gmail.com[2]

History:
Received : 15 Januari 2025
Revised : 18 Januari 2025
Accepted : 23 Januari 2025
Published: 25 Januari 2025

Publisher: Pascasarjana UDA

Abstrak

Kejahatan teknologi di sektor perbankan, seperti phishing, malware, dan hacking, menjadi ancaman signifikan terhadap keamanan data nasabah dan integritas institusi perbankan. Penelitian ini bertujuan untuk menganalisis dampak kejahatan teknologi terhadap nasabah dan industri perbankan, serta menggali tantangan yang dihadapi oleh lembaga perbankan dalam menghadapi ancaman ini. Temuan penelitian menunjukkan bahwa kejahatan teknologi tidak hanya mengakibatkan kerugian finansial langsung bagi nasabah, tetapi juga ancaman terhadap privasi dan kepercayaan publik terhadap institusi perbankan. Di sisi lain, bank menghadapi kerugian reputasi, kewajiban hukum, serta biaya mitigasi risiko yang tinggi, termasuk investasi dalam sistem keamanan dan pemulihan dari insiden kejahatan. Penelitian ini menyarankan perlunya peningkatan sistem keamanan perbankan, kolaborasi antara sektor perbankan, pemerintah, dan masyarakat, serta edukasi digital yang lebih luas untuk mengurangi dampak negatif dari kejahatan teknologi di sektor perbankan.

Kata Kunci : kejahatan teknologi, perbankan, phishing, malware, hacking

Abstract

Technological crimes in the banking sector, such as phishing, malware, and hacking, pose significant threats to customer data security and the integrity of banking institutions. This study aims to analyze the impact of technological crimes on customers and the banking industry, and explore the challenges faced by banking institutions in dealing with these threats. The study findings show that technological crimes not only result in direct financial losses for customers, but also threats to privacy and public trust in banking institutions. On the other hand, banks face reputational losses, legal liabilities, and high risk mitigation costs, including investment in security systems and recovery from crime incidents. This study suggests the need for improved banking security systems, collaboration between the banking sector, government, and the community, and broader digital education to reduce the negative impact of technological crimes in the banking sector.

Keywords: *technological crimes, banking, phishing, malware, hacking*

PENDAHULUAN

Digitalisasi sektor perbankan merupakan salah satu dampak signifikan dari Revolusi Industri 4.0, yang ditandai dengan penerapan teknologi canggih dalam berbagai layanan keuangan (Alidha et al., 2024). Internet banking, mobile banking, dan e-

wallet menjadi contoh nyata transformasi ini, menawarkan kemudahan dan efisiensi yang belum pernah ada sebelumnya. Layanan tersebut memungkinkan nasabah untuk melakukan transaksi keuangan kapan saja dan di mana saja tanpa harus mengunjungi kantor cabang bank. Selain itu, digitalisasi juga mendorong terciptanya inovasi seperti pembayaran tanpa kontak (contactless payment), pinjaman berbasis aplikasi, dan platform investasi digital, yang semakin meningkatkan kenyamanan serta aksesibilitas layanan perbankan bagi masyarakat (Andriani et al., 2022).

Pertumbuhan penggunaan layanan perbankan digital di Indonesia dan dunia terus meningkat secara signifikan dalam beberapa tahun terakhir. Menurut data Bank Indonesia, jumlah transaksi digital banking di Indonesia mencapai lebih dari 52,4 miliar pada tahun 2023, meningkat sekitar 20% dibandingkan tahun sebelumnya. Globalnya, laporan McKinsey & Company mencatat bahwa lebih dari 85% nasabah bank di seluruh dunia telah menggunakan setidaknya satu layanan perbankan digital, terutama di negara-negara dengan penetrasi internet yang tinggi. Angka-angka ini mencerminkan perubahan besar dalam pola transaksi keuangan masyarakat, yang kini semakin bergantung pada teknologi digital untuk memenuhi kebutuhan finansial sehari-hari (Purwanto & Perkasa, 2024).

Teknologi digital telah mengubah secara mendasar cara nasabah berinteraksi dengan bank. Jika sebelumnya nasabah harus mengantre di kantor cabang atau menggunakan ATM untuk berbagai layanan, kini mayoritas transaksi dilakukan melalui aplikasi mobile atau platform online (Anggraini & Sartika, 2024). Misalnya, transfer dana, pembayaran tagihan, pembukaan rekening, hingga pengajuan kredit dapat dilakukan secara mandiri tanpa tatap muka. Pola ini menunjukkan pergeseran dari layanan konvensional ke digital-first, di mana nasabah lebih memilih efisiensi waktu dan fleksibilitas yang ditawarkan teknologi. Selain itu, bank juga semakin fokus pada pengalaman pengguna (user experience) dengan menyediakan antarmuka yang ramah pengguna serta fitur-fitur yang mempermudah transaksi secara real-time.

Kejahatan siber telah menjadi ancaman yang serius dalam sektor perbankan digital, seiring meningkatnya adopsi teknologi oleh masyarakat. Salah satu bentuk kejahatan yang paling umum adalah phishing, yaitu upaya untuk mencuri data sensitif nasabah seperti nomor rekening, PIN, atau kata sandi melalui situs web palsu, email, atau pesan yang tampak berasal dari institusi resmi. Selain phishing, bentuk lain kejahatan teknologi di sektor perbankan mencakup hacking, penyebaran malware, dan serangan ransomware, yang semuanya bertujuan mengeksploitasi celah keamanan untuk keuntungan finansial. Dengan semakin canggihnya teknik para pelaku, ancaman kejahatan siber ini terus berkembang, menciptakan risiko baru yang harus dihadapi oleh perbankan dan konsumennya (Hasanudin & Babussalam, 2024).

Indonesia telah mencatat beberapa kasus kejahatan phishing yang merugikan konsumen dan bank. Salah satu kasus terjadi pada tahun 2023, ketika ribuan nasabah menjadi korban

pencurian data melalui situs palsu yang menyerupai halaman login internet banking dari bank besar di Indonesia. Modus lainnya adalah penyebaran malware melalui lampiran email yang tampak resmi, yang secara otomatis mencuri data login nasabah begitu file dibuka. Selain itu, laporan dari Otoritas Jasa Keuangan (OJK) menunjukkan peningkatan jumlah pengaduan terkait kehilangan dana akibat tautan palsu yang dikirim melalui pesan singkat atau media sosial. Kasus-kasus ini menunjukkan bahwa risiko kejahatan siber dalam perbankan digital bersifat nyata dan terus meningkat (Julianti & Sugiantari, 2021).

Kejahatan teknologi seperti phishing menimbulkan dampak yang signifikan baik bagi konsumen maupun perbankan. Bagi konsumen, kerugian finansial menjadi dampak paling nyata, di mana dana mereka dapat hilang dalam hitungan menit akibat akses ilegal. Selain itu, kerusakan reputasi pribadi akibat penyalahgunaan data juga menjadi risiko besar (Farihah et al., 2023). Di sisi lain, perbankan menghadapi tantangan hilangnya kepercayaan nasabah, yang dapat mengurangi loyalitas mereka terhadap layanan digital. Bank juga harus menanggung biaya tambahan untuk meningkatkan sistem keamanan dan menyelesaikan pengaduan nasabah. Secara keseluruhan, ancaman ini tidak hanya berdampak secara ekonomi tetapi juga mengancam stabilitas ekosistem perbankan digital di Indonesia.

Indonesia telah memiliki berbagai regulasi untuk melindungi konsumen perbankan dari ancaman kejahatan teknologi, seperti Undang-undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, serta peraturan Otoritas Jasa Keuangan (OJK) seperti POJK No. 12/POJK.03/2018 tentang Penyelenggaraan Layanan Perbankan Digital. Meskipun regulasi tersebut menjadi dasar hukum dalam menangani kasus phishing dan kejahatan siber lainnya, masih terdapat kelemahan yang dapat dimanfaatkan oleh pelaku. Celah hukum tersebut, misalnya, kurangnya pengaturan yang rinci terkait mekanisme kompensasi bagi korban phishing, serta keterbatasan dalam regulasi yang mengatur kewajiban bank untuk memastikan edukasi literasi digital nasabah secara efektif (Chairunnisa et al., 2024). Akibatnya, perlindungan terhadap nasabah belum sepenuhnya optimal, terutama dalam menghadapi modus kejahatan yang terus berkembang.

Penegakan hukum terhadap kejahatan teknologi seperti phishing menghadapi banyak tantangan, terutama dalam melacak dan menangkap pelaku. Salah satu kendala utama adalah sifat anonim dari kejahatan siber, di mana pelaku sering menggunakan identitas palsu atau jaringan yang sulit dilacak seperti dark web (Rahmana & Kartika, 2022). Selain itu, pelaku phishing sering kali beroperasi lintas negara, yang membutuhkan koordinasi antarnegara dalam rangka penyelidikan dan penegakan hukum. Kendala teknis ini diperparah oleh kurangnya sumber daya dan keahlian khusus pada aparat penegak hukum untuk menangani kasus kejahatan siber yang kompleks (Najwa,

2024). Akibatnya, meskipun regulasi telah ada, penerapan hukum yang efektif masih menjadi tantangan besar dalam melindungi konsumen perbankan dari ancaman kejahatan teknologi.

Perlindungan hukum yang ada saat ini perlu direkonstruksi agar mampu menghadapi perkembangan pesat teknologi, terutama ancaman phishing dan kejahatan siber lainnya di sektor perbankan. Regulasi seperti UU ITE dan aturan OJK sudah memberikan landasan hukum, tetapi belum sepenuhnya adaptif terhadap modus kejahatan baru yang semakin canggih. Sistem hukum yang responsif dan fleksibel sangat diperlukan untuk menutup celah yang dimanfaatkan oleh pelaku kejahatan siber. Hal ini mencakup penguatan sanksi hukum, peningkatan mekanisme kompensasi bagi korban, serta pengaturan kewajiban yang lebih ketat bagi bank untuk memastikan keamanan layanan digital mereka.

Sektor perbankan memiliki tanggung jawab besar untuk melindungi nasabah dari ancaman kejahatan teknologi. Selain menerapkan sistem keamanan teknologi yang canggih, bank juga perlu berperan aktif dalam memberikan edukasi literasi digital kepada konsumen untuk meningkatkan kewaspadaan terhadap ancaman seperti phishing (Sahrir et al., 2024). Bank harus memastikan bahwa nasabah memahami risiko transaksi digital dan mampu mengenali modus penipuan siber. Langkah ini tidak hanya untuk melindungi konsumen, tetapi juga untuk menjaga reputasi dan kepercayaan terhadap sektor perbankan digital. Penelitian ini berangkat dari kepentingan utama untuk melindungi hak-hak konsumen di tengah ancaman kejahatan teknologi yang terus meningkat. Dalam ekosistem perbankan digital, konsumen sering kali menjadi pihak yang paling rentan terhadap kejahatan siber. Oleh karena itu, penting untuk menciptakan lingkungan transaksi yang lebih aman dan terpercaya melalui regulasi yang komprehensif, penegakan hukum yang efektif, dan peningkatan literasi digital (Isnugraheny et al., 2024). Penelitian ini diharapkan dapat memberikan rekomendasi konkret untuk memperkuat perlindungan hukum dan mendukung terciptanya layanan perbankan digital yang aman bagi seluruh masyarakat.

Penelitian ini memberikan masukan penting bagi pembuat kebijakan dalam memperkuat regulasi terkait perlindungan konsumen di sektor perbankan digital. Dengan mengidentifikasi celah hukum yang ada dan menawarkan solusi berupa rekonstruksi peraturan, penelitian ini dapat membantu menciptakan kerangka hukum yang lebih adaptif terhadap perkembangan teknologi. Hasil penelitian ini juga dapat menjadi dasar untuk merevisi atau menambahkan ketentuan dalam UU ITE, UU Perbankan, dan peraturan OJK agar lebih efektif dalam menghadapi ancaman kejahatan siber seperti phishing. Dengan demikian, penelitian ini berkontribusi pada terciptanya sistem hukum yang mampu melindungi nasabah dan menjaga kepercayaan masyarakat terhadap layanan perbankan digital.

Hasil penelitian ini tidak hanya berfokus pada aspek regulasi tetapi juga memberikan rekomendasi praktis bagi sektor perbankan dalam meningkatkan sistem keamanan teknologi mereka.

Penelitian ini menawarkan panduan konkret bagi bank untuk mengidentifikasi risiko phishing dan ancaman siber lainnya, serta langkah-langkah preventif yang dapat diterapkan, seperti pengembangan sistem deteksi dini dan penyediaan program edukasi literasi digital bagi nasabah. Dengan mengintegrasikan hasil penelitian ini ke dalam kebijakan operasional, bank dapat memperkuat keamanan layanan mereka, meningkatkan kepercayaan nasabah, dan meminimalkan risiko kerugian yang diakibatkan oleh kejahatan siber.

METODE PENELITIAN

Penelitian ini menggunakan metode yuridis normatif, yang berfokus pada kajian terhadap aturan hukum yang berlaku serta konsep-konsep hukum yang relevan (Soekanto & Mamudji, 2015). Pendekatan yang digunakan meliputi pendekatan perundang-undangan (statute approach) untuk menganalisis regulasi terkini, seperti Undang-Undang (UU) Nomor 10 Tahun 1998 tentang Perubahan Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan dan Undang-Undang (UU) Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Selain itu, pendekatan konseptual (conceptual approach) digunakan untuk mengkaji tanggung jawab hukum perbankan serta perlindungan konsumen dalam menghadapi ancaman kejahatan teknologi, khususnya phishing. Sumber data primer yang digunakan meliputi regulasi yang relevan, sementara data sekunder mencakup studi kasus, literatur, dan laporan terkait kejahatan teknologi di sektor perbankan. Teknik analisis yang digunakan adalah deskriptif kualitatif, yang bertujuan mengevaluasi efektivitas perlindungan hukum terhadap nasabah serta tanggung jawab perbankan dalam mencegah dan menangani ancaman kejahatan siber. Penelitian ini diharapkan dapat memberikan kontribusi signifikan dalam menciptakan sistem hukum yang lebih responsif dan adaptif terhadap perkembangan teknologi.

HASIL DAN PEMBAHASAN

Perlindungan Hukum Terhadap Nasabah dan Tanggung Jawab Perbankan dalam Mencegah Kejatahatan Teknologi

Perlindungan konsumen merupakan upaya untuk menjamin hak-hak konsumen terhadap keamanan, kenyamanan, dan keadilan dalam transaksi ekonomi. Perlindungan konsumen menjadi semakin penting karena digitalisasi layanan perbankan membuka peluang baru bagi terjadinya kejahatan teknologi (Tondatuom, 2015). Definisi perlindungan konsumen dalam layanan digital mencakup aspek keamanan data pribadi, transparansi informasi, dan perlakuan adil terhadap nasabah. Prinsip dasar perlindungan konsumen dalam perbankan digital meliputi tanggung jawab bank untuk menjaga kerahasiaan data nasabah, memberikan informasi yang jelas terkait produk dan layanan, serta menyediakan mekanisme pengaduan yang efektif. Dalam hal ini, bank harus memastikan bahwa teknologi yang digunakan memenuhi standar keamanan, sehingga dapat meminimalkan risiko kejahatan teknologi seperti pencurian data atau

akses tidak sah.

Kejahatan teknologi di sektor perbankan mencakup berbagai modus operandi yang dirancang untuk mengeksploitasi kelemahan sistem keamanan atau memanfaatkan kelengahan nasabah. Salah satu bentuk paling umum adalah phishing, yaitu teknik manipulasi psikologis yang digunakan untuk mencuri informasi pribadi seperti nomor rekening, kata sandi, atau data kartu kredit (Caniago & Sutabri, 2023). Pelaku phishing biasanya mengirimkan email atau pesan yang menyerupai institusi resmi, sehingga korban tanpa sadar memberikan informasi sensitif mereka melalui tautan palsu. Dampak kejahatan teknologi terhadap nasabah dan institusi perbankan sangat signifikan. Bagi konsumen, kerugian yang paling nyata adalah kerugian finansial akibat pengurasan rekening atau transaksi yang tidak sah. Selain itu, kejahatan ini juga menimbulkan ancaman terhadap privasi, mengingat data pribadi yang dicuri dapat digunakan untuk tindakan kriminal lainnya, seperti pencurian identitas. Hilangnya rasa aman dan kepercayaan terhadap institusi perbankan menjadi efek psikologis yang tidak kalah penting.

Di sisi industri perbankan, kejahatan teknologi dapat merusak reputasi institusi tersebut. Kebocoran data atau kegagalan melindungi nasabah dapat membuat bank kehilangan kepercayaan publik, yang pada akhirnya memengaruhi loyalitas nasabah. Selain itu, institusi perbankan juga menghadapi tanggung jawab hukum yang berat akibat kegagalan menjaga keamanan data nasabah, termasuk potensi sanksi dari regulator (Nasution et al., 2024). Tantangan lainnya adalah biaya mitigasi risiko yang tinggi. Bank perlu mengeluarkan investasi besar untuk memperbarui sistem keamanan, melakukan audit rutin, dan memulihkan sistem yang terdampak kejahatan teknologi. Semua ini menjadi beban yang signifikan bagi institusi perbankan, terutama jika insiden kejahatan teknologi terjadi secara berulang. Kombinasi kerugian finansial, beban reputasi, dan tuntutan hukum ini menjadikan kejahatan teknologi sebagai ancaman besar yang harus ditangani secara serius oleh seluruh pihak yang terlibat.

Selain phishing, ancaman lain adalah malware atau perangkat lunak berbahaya yang sengaja dirancang untuk mencuri data atau mengendalikan perangkat korban tanpa izin. Malware sering kali disisipkan melalui unduhan aplikasi yang tidak terpercaya atau tautan berbahaya (Nur & Hafid, 2024). Ketika malware berhasil diinstal pada perangkat, pelaku dapat memantau aktivitas korban, mencuri informasi sensitif, atau bahkan menguras rekening bank korban secara diam-diam.Hacking juga menjadi ancaman serius dalam sektor perbankan. Dengan memanfaatkan celah keamanan dalam sistem teknologi informasi, hacker dapat menyusup ke sistem perbankan untuk mencuri data nasabah, mengalihkan dana, atau mengganggu layanan perbankan. Aksi hacking tidak hanya berdampak pada individu, tetapi juga dapat mengganggu operasional perbankan secara keseluruhan (Wicaksono et al., 2021).

Dalam menghadapi ancaman kejahatan siber terutama phishing, bank digital memegang peran yang sangat

penting dalam memastikan keamanan sistem mereka. Berdasarkan Peraturan Otoritas Jasa Keuangan (POJK) Nomor 11 Tahun 2022 tentang Penyelenggaraan Teknologi Informasi, bank digital diwajibkan untuk menerapkan tata kelola teknologi informasi yang baik serta menjaga ketahanan siber untuk mencegah risiko kejahatan siber, termasuk phishing dan peretasan. Pasal 2 dan Pasal 21 dalam peraturan ini secara jelas mengatur kewajiban bank digital untuk menyediakan layanan yang aman, andal, dan bertanggung jawab sebagai langkah preventif dalam menghadapi ancaman tersebut. Jika bank gagal dalam memenuhi ketentuan tersebut, sanksi administratif dapat diberikan, mulai dari teguran tertulis hingga pembekuan kegiatan usaha tertentu, atau bahkan penurunan nilai tata kelola yang dapat mempengaruhi tingkat kesehatan bank. Selain itu, bank juga bertanggung jawab untuk melindungi hak dan kepentingan nasabah melalui prinsip perlindungan konsumen sebagaimana diatur dalam POJK terkait Perlindungan Konsumen dan Masyarakat Sektor Jasa Keuangan.

Dalam hal ini bank digital juga diwajibkan untuk melakukan tindakan yang proaktif dalam memberikan perlindungan kepada konsumen, terutama dalam menangani kerugian yang mungkin timbul akibat kejahatan siber. Sesuai dengan Pasal 21 ayat (1) POJK tentang Penyelenggaraan Layanan Perbankan Digital, bank digital harus menerapkan prinsip perlindungan konsumen dengan menyediakan layanan yang responsif, termasuk menyediakan saluran pengaduan nasabah selama 24 jam. Ketika nasabah mengalami kerugian akibat layanan bank, tanggung jawab bank tidak hanya terbatas pada pemberian kompensasi materiil, tetapi juga mencakup aspek edukasi keuangan. Sebagai bagian dari upaya meningkatkan literasi keuangan, bank digital diwajibkan untuk melaksanakan program edukasi keuangan sesuai dengan POJK Nomor 3 Tahun 2023. Program ini bertujuan untuk meningkatkan pemahaman nasabah terhadap risiko-risiko yang ada dalam layanan perbankan digital, termasuk risiko terkait kejahatan siber. Bank digital diharapkan untuk bekerja sama dengan berbagai pihak, seperti instansi pemerintah, akademisi, dan organisasi non-pemerintah, guna memperluas cakupan edukasi ini.

Dari sisi hukum kejahatan phishing dalam sistem perbankan digital dapat dianalisis melalui ketentuan dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), mengingat karakteristik kejahatan ini yang melibatkan penyalahgunaan sistem elektronik. Pasal 28 ayat (1) UU ITE mengatur tentang larangan distribusi atau transmisi informasi elektronik yang berisi pemberitahuan palsu atau menyesatkan yang dapat menyebabkan kerugian materiil bagi konsumen dalam transaksi elektronik. Pelaku phishing yang terlibat dalam distribusi informasi bohong atau manipulasi data nasabah dapat dikenakan sanksi pidana sesuai dengan Pasal 45A ayat (1), dengan ancaman pidana penjara hingga enam tahun dan/atau denda maksimal satu miliar rupiah. Selain itu, jika pelaku menggunakan manipulasi terhadap informasi elektronik agar tampak otentik, tindakan tersebut dapat dijerat dengan Pasal 35 jo. Pasal 51 UU ITE, yang memberikan ancaman hukuman lebih berat, yaitu penjara hingga 12

tahun dan/atau denda maksimal Rp12 miliar. Tindakan lainnya, seperti menerobos sistem elektronik untuk mengambil data nasabah secara ilegal, dapat dijerat dengan Pasal 30 ayat (3) jo. Pasal 46 ayat (3) UU ITE yang mengatur ancaman pidana maksimal delapan tahun penjara dan/atau denda hingga Rp800 juta.

Dalam hal penerapan hukum pidana kejahatan phishing juga dapat dianalisis menggunakan ketentuan dalam Kitab Undang-Undang Hukum Pidana (KUHP). Misalnya, tindakan phishing yang terkait dengan pencurian data kartu kredit dapat dikualifikasikan sebagai tindak pidana pencurian berdasarkan Pasal 362 KUHP. Selain itu, phishing yang dilakukan dengan menggunakan situs palsu atau menipu nasabah juga dapat diproses sebagai tindak pidana penipuan menurut Pasal 378 KUHP. Ketentuan mengenai kejahatan berkelompok, seperti yang diatur dalam Pasal 363 ayat (4) KUHP, juga relevan untuk menangani kasus phishing yang melibatkan lebih dari satu pelaku. Pasal 55 KUHP tentang penyertaan dapat diterapkan untuk menjerat pihak-pihak yang membantu atau memiliki peran dalam melakukan kejahatan tersebut. Tak hanya itu, pasal lain seperti Pasal 263 KUHP tentang pemalsuan surat dapat diterapkan ketika pelaku membuat dokumen elektronik palsu, seperti email yang menyerupai komunikasi resmi bank, untuk menipu korban. Dengan menggabungkan berbagai ketentuan dalam UU ITE dan KUHP, penegak hukum dapat memberikan sanksi yang lebih komprehensif terhadap pelaku phishing dan memastikan perlindungan maksimal bagi nasabah dari kejahatan teknologi di sektor perbankan digital.

Pasal 40 Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan menetapkan bahwa bank wajib menjaga kerahasiaan data nasabah, baik data personal maupun informasi rekening. Hal ini menjadi salah satu pilar utama dalam melindungi nasabah dari kejahatan teknologi. Kejahatan seperti phishing, hacking, dan social engineering dapat memanfaatkan data nasabah yang tidak terlindungi dengan baik. Oleh karena itu, bank harus memiliki sistem yang memastikan data nasabah hanya dapat diakses oleh pihak yang berwenang sesuai ketentuan hukum. Selain itu, bank juga diwajibkan untuk melindungi data dari pihak ketiga yang tidak berkepentingan, termasuk penyedia layanan teknologi informasi eksternal. Dengan berkembangnya teknologi finansial, tantangan dalam menjaga kerahasiaan data semakin besar, terutama dengan meningkatnya risiko kebocoran data. Bank dituntut untuk memiliki langkah preventif yang jelas, termasuk audit reguler terhadap sistem keamanan data.

POJK Nomor 11 Tahun 2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank mengatur penerapan sistem keamanan berbasis teknologi untuk mencegah ancaman kejahatan digital. Bank wajib menerapkan langkah-langkah teknologi yang adaptif, seperti enkripsi data, multi-factor authentication (MFA), serta sistem deteksi dini terhadap potensi ancaman siber (Savitri, 2024). Sistem keamanan ini harus mencakup seluruh lapisan operasional bank, mulai dari pengelolaan data hingga transaksi elektronik. Selain itu, regulasi ini menekankan pentingnya penggunaan

teknologi artificial intelligence (AI) dan machine learning untuk memantau dan menganalisis aktivitas mencurigakan. Penggunaan teknologi ini memungkinkan bank untuk merespons ancaman secara real-time, mengurangi risiko terjadinya kejahatan seperti fraud atau penipuan digital. Penerapan sistem keamanan yang efektif juga mencerminkan tanggung jawab bank dalam menjaga stabilitas dan kepercayaan masyarakat terhadap industri perbankan.

POJK Nomor 3 Tahun 2023 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan menggarisbawahi pentingnya literasi digital dan edukasi bagi nasabah sebagai langkah preventif dalam menghadapi kejahatan teknologi. Bank memiliki kewajiban untuk memberikan informasi yang transparan mengenai risiko penggunaan layanan perbankan digital, termasuk cara mengenali dan menghindari modus penipuan. Program literasi digital ini dapat dilakukan melalui berbagai saluran, seperti media sosial, pelatihan langsung, atau penyebaran materi edukasi digital. Edukasi ini mencakup cara aman melakukan transaksi online, pentingnya menjaga kerahasiaan PIN dan OTP, serta mengenali ciri-ciri phishing atau serangan cyber lainnya. Dengan tingkat literasi yang tinggi, nasabah diharapkan dapat lebih waspada dan memiliki keterampilan untuk melindungi diri mereka sendiri dari kejahatan teknologi.

Rekontruksi Perlindungan Hukum Bagi Konsumen Perbankan terhadap Ancaman Kejahatan Teknologi

Dalam perlindungan hukum, salah satu tantangan utama adalah kelemahan regulasi yang menyebabkan ketidakpastian hukum atau kurangnya efektivitas dalam pelaksanaannya. Identifikasi kelemahan regulasi ini menjadi langkah awal untuk melakukan rekonstruksi yang bertujuan memperkuat perlindungan hukum di berbagai sektor, baik pidana, perdata, maupun administras. Kelemahan substansi regulasi sering kali muncul karena pengaturan yang tidak komprehensif atau adanya kekosongan hukum (legal vacuum). Misalnya, banyak regulasi tidak secara spesifik mengatur perkembangan teknologi, seperti perlindungan data pribadi atau kejahatan dunia maya. Hal ini menyebabkan regulasi yang ada menjadi ketinggalan zaman dan tidak relevan dengan kebutuhan masyarakat. Selain itu tumpang tindih aturan antar-undang-undang juga menjadi masalah. Ketidaksinkronan antar-regulasi sering kali menyebabkan kebingungan dalam implementasi, terutama ketika terdapat kewenangan yang tumpang tindih antar-lembaga. Contohnya, dalam kasus perlindungan konsumen, terdapat benturan antara Undang-Undang Perlindungan Konsumen dengan regulasi sektoral lain, yang akhirnya melemahkan perlindungan yang diberikan kepada konsumen.

Regulasi yang lemah dalam implementasi juga menjadi faktor yang menghambat perlindungan hukum. Dalam banyak kasus, kurangnya penegakan hukum yang tegas menyebabkan regulasi hanya menjadi "aturan di atas kertas." Contohnya, meskipun regulasi tentang perlindungan lingkungan telah ada, implementasinya sering kali terganggu oleh korupsi, minimnya pengawasan, atau lemahnya

sanksi terhadap pelanggar. Faktor lain yang turut berkontribusi adalah keterbatasan kapasitas lembaga pelaksana hukum, baik dari sisi sumber daya manusia maupun infrastruktur. Regulasi yang baik membutuhkan dukungan implementasi yang memadai, termasuk pengawasan yang transparan, teknologi pendukung, dan keberanian untuk menegakkan hukum tanpa diskriminasi.

Perubahan sosial, teknologi, dan ekonomi yang cepat sering kali tidak diikuti dengan penyesuaian regulasi yang memadai. Akibatnya, regulasi yang ada menjadi tidak relevan dengan situasi aktual (Ariyani & Nurcahyono, 2014). Misalnya, di era digital, muncul berbagai bentuk kejahatan baru seperti fraud berbasis cryptocurrency, yang tidak diatur secara eksplisit dalam hukum positif. Tidak adanya mekanisme regulasi yang adaptif terhadap perubahan ini mengakibatkan perlindungan hukum menjadi lemah. Hal ini mencerminkan perlunya rekonstruksi regulasi yang lebih dinamis, berbasis kebutuhan masyarakat, dan didukung oleh kajian ilmiah serta partisipasi publik yang luas.

Regulasi yang tidak melibatkan partisipasi publik secara memadai sering kali tidak mencerminkan kebutuhan masyarakat. Akibatnya, banyak aturan yang dianggap kurang efektif atau bahkan merugikan pihak tertentu. Partisipasi publik yang rendah juga menciptakan celah dalam mengidentifikasi permasalahan di lapangan sehingga regulasi menjadi kurang responsif terhadap isu-isu aktual. Identifikasi kelemahan-kelemahan ini menegaskan pentingnya rekonstruksi regulasi yang lebih terencana dan berbasis evidence. Upaya rekonstruksi ini harus melibatkan semua pihak yang berkepentingan, termasuk masyarakat, lembaga hukum, dan akademisi, agar perlindungan hukum yang dihasilkan dapat memberikan kepastian, keadilan, dan manfaat yang nyata bagi masyarakat.

Penguatan perlindungan hukum adalah upaya strategis untuk menghadapi tantangan yang muncul, terutama dalam konteks kejahatan teknologi yang semakin kompleks. Untuk mencapainya, diperlukan pendekatan holistik yang melibatkan pembaruan regulasi, kolaborasi antara berbagai pihak, dan peningkatan literasi digital masyarakat. Kejahatan berbasis teknologi terus berkembang, namun banyak regulasi yang belum mampu mengakomodasi perubahan ini. Oleh karena itu, pembaruan regulasi menjadi langkah prioritas. Undang-Undang yang ada, seperti UU ITE dan regulasi perbankan, perlu direvisi agar lebih responsif terhadap ancaman baru seperti serangan ransomware, pencurian identitas digital, hingga kejahatan berbasis cryptocurrency. Selain itu, diperlukan aturan khusus yang lebih rinci mengenai kewajiban lembaga keuangan dalam melindungi data nasabah dan mekanisme penanganan pelanggaran data. Misalnya, regulasi dapat mewajibkan institusi perbankan untuk mengadopsi standar keamanan siber terkini, melakukan audit berkala, dan menyediakan sistem pelaporan insiden yang efisien. Pembaruan regulasi ini juga harus mencakup sanksi yang lebih tegas bagi pelaku kejahatan teknologi maupun lembaga yang lalai dalam melaksanakan perlindungan.

Menghadapi kejahatan teknologi

membutuhkan sinergi antara pemerintah, sektor perbankan, dan masyarakat. Pemerintah dapat berperan sebagai regulator dan pengawas, sementara sektor perbankan bertindak sebagai pelaksana utama perlindungan data dan sistem keuangan. Kolaborasi ini dapat diwujudkan melalui pembentukan forum nasional keamanan siber yang melibatkan lembaga pemerintah, asosiasi perbankan, dan komunitas teknologi. Selain itu perlu ada mekanisme pertukaran informasi tentang ancaman keamanan antara pihak-pihak terkait untuk mempercepat respons terhadap kejahatan teknologi. Misalnya, perbankan dapat bekerja sama dengan Badan Siber dan Sandi Negara (BSSN) untuk mendeteksi dan mencegah ancaman siber. Di sisi lain, masyarakat juga perlu dilibatkan melalui kampanye edukasi dan program mitigasi risiko yang mudah diakses.

Sebagian besar kejahatan teknologi, seperti phishing dan social engineering, memanfaatkan rendahnya literasi digital masyarakat. Untuk itu, edukasi digital yang komprehensif bagi konsumen menjadi sangat penting. Perbankan dapat berperan dengan menyelenggarakan program literasi digital, seperti pelatihan keamanan bertransaksi online, panduan mengenali penipuan digital, serta cara melindungi data pribadi. Regulator seperti Otoritas Jasa Keuangan (OJK), juga dapat bekerja sama dengan lembaga pendidikan untuk memasukkan literasi digital ke dalam kurikulum formal maupun informal. Pendekatan ini akan membantu menciptakan konsumen yang lebih sadar dan tangguh dalam menghadapi ancaman siber. Selain itu, penyediaan panduan dalam berbagai platform digital, seperti media sosial atau aplikasi mobile banking, dapat membantu nasabah memahami risiko teknologi dan cara mengelolanya.

SIMPULAN

Perlindungan konsumen dalam perbankan digital merupakan tanggung jawab yang tidak hanya terbatas pada pemenuhan prinsip-prinsip dasar perlindungan konsumen, tetapi juga mencakup penerapan sistem keamanan yang komprehensif untuk melindungi nasabah dari kejahatan teknologi seperti phishing, hacking, dan malware. Bank wajib mengimplementasikan berbagai regulasi yang relevan, seperti UU ITE, UU Perbankan, dan POJK terkait, yang menegaskan kewajiban bank dalam menjaga kerahasiaan data nasabah, memberikan layanan pengaduan yang responsif, serta meningkatkan literasi dan edukasi nasabah melalui program-program yang terstruktur. Selain itu, hukum pidana dalam UU ITE dan KUHP memberikan landasan sanksi terhadap pelaku kejahatan teknologi, yang bertujuan memberikan perlindungan hukum yang kuat bagi konsumen. Di sisi lain, tantangan dalam penerapan teknologi keamanan seperti enkripsi, multi-factor authentication (MFA), dan AI, serta pentingnya audit reguler terhadap sistem keamanan, menuntut bank untuk terus beradaptasi dengan perkembangan teknologi guna memastikan keamanan transaksi digital. Dengan penggabungan langkah preventif, edukasi, dan penegakan hukum, diharapkan kepercayaan masyarakat terhadap layanan perbankan digital dapat terus terjaga, serta risiko kejahatan siber dapat diminimalisasi secara efektif.

Kelemahan regulasi yang meliputi kekosongan hukum, ketidaksinkronan antar-undang-undang, lemahnya penegakan hukum, serta minimnya adaptasi terhadap perubahan sosial dan teknologi menjadi tantangan utama dalam perlindungan hukum. Rekonstruksi regulasi yang responsif, berbasis evidence, dan melibatkan partisipasi publik menjadi solusi penting untuk memperkuat perlindungan hukum. Dalam menghadapi kompleksitas kejahatan berbasis teknologi, diperlukan pembaruan regulasi yang komprehensif, penguatan kolaborasi antar-lembaga, dan peningkatan literasi digital masyarakat untuk menciptakan sistem hukum yang adaptif dan berkeadilan. Pendekatan holistik ini diharapkan mampu memberikan kepastian hukum, melindungi kepentingan masyarakat, dan menjawab kebutuhan era digital yang terus berkembang.

DAFTAR PUSTAKA

Alidha, M., Sari, A. P., Sopiatunnisa, R., Azzahra, A., & Nurhalizah, L. (2024). Analisis Dampak Digitalisasi Layanan Perbankan terhadap Loyalitas Nasabah di Era Revolusi Industri 4.0. Contemporary Journal of Applied Sciences, 2(3).

Andriani, A. D., Yuniawati, R. I., Hamidin, D., Priambodo, A., Sulaeman, M., Susanti, L., Darmawan, A., & Martono, S. (2022). Transformasi Indonesia Menuju Cashless Society. TOHAR MEDIA. https://books.google.co.id/books?id=_ml7EAAAQBAJ

Anggraini, D., & Sartika, D. (2024). ANALISIS PERSEPSI NASABAH TERHADAP STRATEGI PEMASARAN PADA LAYANAN BSI MOBILE (STUDI KASUS PADA NASABAH BANK SYARIAH INDONESIA KANTOR CABANG JAMBI). MARGIN: Journal of Islamic Banking, 4(2), 171–191.

Ariyani, N. I., & Nurcahyono, O. (2014). Digitalisasi Pasar Tradisional: Perspektif Teori Perubahan Sosial. Jurnal Analisa Sosiologi, 3(1), 1–12. https://doi.org/10.20961/jas.v3i1.17442

Caniago, K., & Sutabri, T. (2023). Tindak Kejahatan Phising Di Sektor Pelayan Di Universitas Bina Insan Lubuklinggau. JURASIK (Jurnal Riset Sistem Informasi Dan Teknik Informatika), 8(1), 117–125.

Chairunnisa, S., Murwadji, T., & Harrieti, N. (2024). Perlindungan Hukum Terhadap Nasabah atas Kejahatan Phising dan Hacking pada Layanan Bank Digital Ditinjau Berdasarkan Hukum Positif Indonesia. Hakim: Jurnal Ilmu Hukum Dan Sosial, 2(1), 1–16.

Farihah, M., Sari, K., & Sumriyah, S. (2023). Pengaruh Penerapan Teknologi Digital Terhadap Penggunaan Bilyet Giro dalam Bisnis Perdagangan. Jurnal Riset Rumpun Ilmu Sosial, Politik Dan Humaniora, 2(2), 45–57.

Hasanudin, A. F., & Babussalam, A. B. (2024). Perlindungan Hukum Bagi Korban Kejahatan Phising Yang Menguras Saldo M-Banking. Jurnal Gagasan Hukum, 6(01), 16–29. https://doi.org/10.31849/jgh.v6i01.18827

Isnugraheny, R. F., Megawati, Z. E., & Susilawati, S. (2024). Optimalisasi Prinsip Kerahasiaan Data Nasabah dan Peranan Otoritas Jasa Keuangan

Dalam Mencegah Kebocoran Informasi. Media Hukum Indonesia (Mhi), 2(4), 258–264.

Julianti, L., & Sugiantari, A. A. P. W. (2021). TANGGUNG JAWAB HUKUM PIHAK PERBANKAN DALAM PENCURIAN DATA PRIBADI NASABAH DENGAN TEKHNIK "PHISING" PADA TRANSAKSI PERBANKAN. Prosiding Seminar Nasional Fakultas Hukum Universitas Mahasaraswati Denpasar 2020, 1(1), 96–105.

Najwa, F. R. (2024). Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia. AL-BAHTS: Jurnal Ilmu Sosial, Politik, Dah Hukum, 2(1), 8–16.

Nasution, R. A., Ginting, B., Siregar, M., & Azwar, T. K. D. (2024). Perlindungan Hukum Terhadap Data Pribadi Nasabah Layanan Perbankan Setelah Berlakunya Peraturan Otoritas Jasa Keuangan (POJK) Nomor 6/Pojk.O7/2022. Journal of Education, Humaniora and Social Sciences (JEHSS), 7(1), 71–78.

Nur, A., & Hafid, D. A. (2024). PERANAN IT SECURITY DALAM MENGAMANKAN INFRASTRUKTUR DAN TRANSAKSI DI PERUSAHAAN E-COMMERCE. Kohesi: Jurnal Sains Dan Teknologi, 4(10), 41–50.

Purwanto, S., & Perkasa, D. H. (2024). ANALISIS TRANSFORMASI BANK DIGITAL YANG TERDAFTAR DI BURSA EFEK INDONESIA. Jurnal Revenue: Jurnal Ilmiah Akuntansi, 4(2), 622–633.

Rahmana, R. D., & Kartika, A. W. (2022). Penegakan Hukum Bagi Pelaku Pembuatan Dan Penyebaran Scam Page (Studi Di Kepolisian Daerah Jawa Timur). Risalah Hukum, 18(2), 83–98.

Sahrir, I. F., Paridah, N., Yunitasari, K., & Putri, R. A. A. (2024). Perlindungan Hukum Terhadap Nasabah Bank Dalam Penggunaan Aplikasi Dana Di Indonesia. Jurnal Dunia Ilmu Hukum (JURDIKUM), 2(2), 43–48. https://doi.org/10.59435/jurdikum.v2i2.379

Savitri, P. (2024). Transformasi Digital dalam Industri Perbankan: Implikasi terhadap Akuntansi dan Teknologi Informasi. Penerbit NEM.

Soekanto, S., & Mamudji, S. (2015). Penelitian Hukum Normatif Suatu Tinjauan Singkat. Rajawali Press.

Tondatuom, S. K. (2015). PERTANGGUNGJAWABAN BANK SEBAGAI PELAKU USAHA ATAS PELANGGARAN HAK-HAK NASABAH SEBAGAI KONSUMEN. Lex Et Societatis, 3(6), 106–118.

Wicaksono, R., Nugroho, A. A., & Agustanti, R. D. (2021). Perlindungan Hukum Terhadap Konsumen Indihome Ditinjau Dari Undang-Undang Perlindungan Konsumen. Jurnal Ilmiah Penegakan Hukum, 8(2), 149–159. https://doi.org/10.31289/jiph.v8i2.4793