JURISDICTIE JURNAL PROGRAM SARJANA ILMU HUKUM UNIVERSITAS ISLAM AS-SYAFI'IYAH Hal.16-25	E-ISSN 2809-8641	Naskah Dikirim 29/05/2025	Naskah Direview 22/08/2025	Naskah Diterbitkan 25/09/2025

PERLINDUNGAN HUKUM KONSUMEN DARI PENIPUAN M-BANKING: KAJIAN HUKUM PERBANKAN DAN STRATEGI PENCEGAHAN DI INDONESIA

Hidayat Muhammad Sugiharto[1], Baidhowi, S.Ag.[2]

[1] *Fakultas Hukum, Universitas Negeri Semarang, Indonesia,*
hidayatmuhs@students.unnes.ac.id
[2]Fakultas Hukum, Universitas Negeri Semarang, Indonesia,
baidhowi@mail.unnes.ac.id
DOI: https://doi.org/10.34005/jhj.v7i2.180

ABSTRACT

The development of digital banking in Indonesia, especially mobile banking (M-Banking) services, has increased the efficiency of people's financial transactions. However, this convenience is accompanied by increasingly complex fraud risks, such as phishing, account hacking, and misuse of personal data. This research aims to analyze M-Banking fraud prevention strategies and the legal handling process for victims in Indonesia. The research method uses a normative approach by reviewing legal regulations, case studies, and recommendations from banking and cybersecurity authorities.

Keywords: M-Banking Fraud; OJK (Financial Services Authority); Cybersecurity

ABSTRAK

Perkembangan perbankan digital di Indonesia, khususnya layanan mobile banking (M-Banking), telah meningkatkan efisiensi transaksi keuangan masyarakat. Namun, kemudahan ini diiringi risiko penipuan yang semakin kompleks, seperti phishing, peretasan akun, dan penyalahgunaan data pribadi. Penelitian ini bertujuan untuk menganalisis strategi pencegahan penipuan M-Banking dan proses penanganan hukum bagi korban di Indonesia. Metode penelitian menggunakan pendekatan normatif dengan mengkaji regulasi hukum, studi kasus, serta rekomendasi dari otoritas perbankan dan keamanan siber.

Kata Kunci: Penipuan M-Banking; OJK (Otoritas Jasa Keuangan); Keamanan Siber

I. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan signifikan dalam berbagai aspek kehidupan, termasuk sektor perbankan. Salah satu inovasi yang berkembang pesat adalah layanan perbankan digital, khususnya mobile banking (m-banking). Dengan adanya m-banking, nasabah dapat melakukan berbagai transaksi keuangan secara cepat dan praktis tanpa harus datang langsung ke kantor cabang bank. M-banking memungkinkan pengguna untuk melakukan transfer dana, pembayaran tagihan, pembelian produk digital, dan berbagai layanan lainnya hanya melalui perangkat seluler. Perkembangan ini sejalan dengan meningkatnya penetrasi internet dan penggunaan smartphone di Indonesia. Namun, di balik kemudahan yang ditawarkan, penggunaan m-banking juga menghadirkan berbagai tantangan, terutama dalam hal keamanan dan perlindungan konsumen.

Kasus penipuan m-banking semakin marak terjadi, dengan berbagai modus operandi seperti phishing, social engineering, SIM swap fraud, dan malware yang menargetkan data pribadi serta informasi finansial pengguna. Dalam banyak kasus, korban kehilangan dana dalam jumlah besar akibat kebocoran data atau aksi kriminal siber. Regulasi perbankan di Indonesia, seperti yang diterapkan oleh Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI), telah mengatur aspek keamanan sistem pembayaran digital dan perlindungan konsumen. Namun, masih terdapat berbagai tantangan dalam penerapannya, terutama dalam memberikan jaminan keamanan yang optimal bagi nasabah. Oleh karena itu, diperlukan kajian mendalam mengenai perlindungan hukum yang tersedia bagi konsumen m-banking serta strategi yang dapat diterapkan untuk mencegah terjadinya penipuan.

Penelitian ini menggunakan pendekatan kualitatif dengan metode yuridis normatif, yaitu dengan menganalisis peraturan perundang-undangan yang berlaku terkait perlindungan konsumen di bidang perbankan digital. Data yang digunakan meliputi Data Primer yang bersumber dari Undang-undang,

peraturan OJK, peraturan Bank Indonesia, serta kebijakan terkait perlindungan konsumen dalam transaksi digital. Data sekunder yang bersumber dari Studi literatur dari jurnal, artikel ilmiah, laporan keuangan perbankan, dan berita terkait kasus penipuan m-banking di Indonesia.

II. PEMBAHSAN

A. Modus Penipuan M-Banking Dan Implikasi Hukumnya

Penggunaan mobile banking (m-banking) semakin meningkat di era digital, namun hal ini juga memicu maraknya kejahatan siber yang mengincar nasabah perbankan. Pemahaman terhadap modus penipuan sangat penting untuk meningkatkan kewaspadaan dan mencegah kerugian. Artikel ini akan membahas berbagai jenis penipuan dalam layanan m-banking, modus operandi yang digunakan pelaku kejahatan siber, serta implikasi hukum yang dapat dikenakan kepada mereka.

Terdapat berbagai jenis penipuan dalam m-banking, salah satunya adalah phishing, yaitu teknik penipuan dengan mengelabui korban melalui email, pesan singkat, atau situs palsu untuk mencuri informasi sensitif. Selain itu, smishing atau SMS phishing juga marak terjadi, di mana pelaku mengirimkan pesan singkat berisi tautan berbahaya yang menjerumuskan korban. Vishing atau voice phishing dilakukan dengan cara menelepon korban dan mengaku sebagai pihak resmi untuk mendapatkan data pribadi. Kejahatan lainnya termasuk malware dan keylogger yang menyusup ke perangkat korban untuk mencuri informasi login, serta SIM swap fraud yang memungkinkan pelaku mengambil alih akun m-banking korban dengan mengganti kartu SIM.

Pelaku kejahatan siber memanfaatkan teknologi dan rekayasa sosial dalam menjalankan modus operandi mereka. Data pribadi korban dapat diperoleh dari dark web atau melalui penyalahgunaan informasi yang tersebar di media sosial. Studi kasus menunjukkan bahwa kejahatan siber yang berkaitan dengan m-banking terus meningkat, sehingga menuntut adanya tindakan hukum yang lebih ketat. Di Indonesia, kejahatan ini diatur dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta peraturan yang diterbitkan oleh Bank Indonesia dan Otoritas Jasa

Keuangan (OJK). Pelaku dapat dijatuhi hukuman pidana, termasuk denda dan penjara, tergantung pada jenis kejahatan yang dilakukan. Korban dapat melaporkan kasus ini kepada pihak berwenang dan memiliki hak untuk mendapatkan perlindungan hukum serta upaya pemulihan dana jika mengalami kerugian.

Untuk mencegah dan mengurangi risiko kejahatan m-banking, berbagai langkah perlu diambil, seperti peningkatan teknologi keamanan, edukasi kepada pengguna tentang keamanan transaksi digital, serta kebijakan perbankan yang lebih ketat dalam melindungi nasabah. Selain itu, kesadaran individu juga berperan penting dalam menghindari modus penipuan, seperti tidak membagikan data pribadi secara sembarangan dan selalu waspada terhadap pesan mencurigakan.

B. Analisis Perlindungan Hukum Konsumen dan Tanggung Jawab Perbankan

Perkembangan teknologi dalam sektor perbankan telah menghadirkan berbagai inovasi layanan, termasuk mobile banking (m-banking), yang memudahkan nasabah dalam melakukan transaksi finansial. Namun, di balik kemudahan ini, terdapat berbagai risiko yang dihadapi oleh konsumen, termasuk penipuan dan kejahatan siber yang dapat merugikan mereka. Oleh karena itu, perlindungan hukum terhadap konsumen dalam penggunaan layanan perbankan digital menjadi aspek krusial yang perlu dievaluasi. Perlindungan hukum konsumen dalam layanan m-banking diatur dalam berbagai regulasi, baik di tingkat nasional maupun internasional. Di Indonesia, perlindungan konsumen dalam sektor perbankan mengacu pada beberapa undang-undang, seperti Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen yang menjamin hak-hak konsumen atas keamanan, kenyamanan, dan kepastian hukum, serta Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan yang mengatur tanggung jawab perbankan terhadap nasabahnya. Selain itu, Peraturan Otoritas Jasa Keuangan (OJK) Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen di Sektor Jasa Keuangan memberikan

pedoman bagi perbankan dalam menangani sengketa dengan nasabah, sementara Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) mengatur aspek hukum dalam transaksi digital, termasuk m-banking.

Sebagai pengguna layanan perbankan digital, konsumen memiliki hak yang harus dijamin oleh penyedia layanan perbankan, antara lain hak atas keamanan data dan informasi pribadi, hak atas transparansi informasi terkait layanan m-banking, hak atas pengaduan dan penyelesaian sengketa yang adil, serta hak atas kompensasi jika mengalami kerugian akibat kelalaian bank. Di sisi lain, konsumen juga memiliki kewajiban, seperti menjaga kerahasiaan informasi akun dan mematuhi syarat serta ketentuan yang berlaku dalam layanan m-banking.

Perbankan memiliki tanggung jawab untuk memastikan keamanan sistem m-banking guna melindungi nasabah dari ancaman kejahatan siber. Beberapa langkah yang harus dilakukan bank meliputi menerapkan sistem keamanan berlapis, seperti autentikasi dua faktor dan enkripsi data, mengedukasi nasabah tentang risiko keamanan siber dan cara menghindari penipuan, melakukan pemantauan transaksi secara real-time guna mendeteksi aktivitas mencurigakan, serta memberikan kompensasi bagi nasabah yang mengalami kerugian akibat kelalaian sistem keamanan bank. Dalam kasus penipuan m-banking, tanggung jawab perbankan tergantung pada faktor penyebabnya. Jika kejahatan terjadi akibat kelalaian sistem bank, maka bank wajib mengganti kerugian nasabah. Namun, jika penipuan terjadi akibat kelalaian nasabah sendiri, misalnya membocorkan OTP atau PIN kepada pihak lain, bank dapat membebaskan diri dari tanggung jawab, kecuali jika terbukti terdapat unsur kesalahan dalam sistem keamanan bank.

Nasabah yang mengalami permasalahan dalam layanan m-banking dapat mengajukan pengaduan kepada bank melalui berbagai saluran, seperti call center atau layanan pelanggan bank, kantor cabang terdekat untuk pengaduan langsung, platform digital yang disediakan oleh bank, serta Otoritas Jasa Keuangan (OJK) jika penyelesaian dengan bank tidak

memuaskan. Bank wajib menanggapi pengaduan nasabah dalam jangka waktu tertentu sesuai ketentuan OJK, serta memberikan solusi yang adil dan transparan. Jika nasabah tidak puas dengan penyelesaian yang diberikan bank, mereka dapat mengajukan sengketa ke lembaga penyelesaian sengketa di luar pengadilan, seperti Lembaga Alternatif Penyelesaian Sengketa Sektor Jasa Keuangan (LAPS SJK), Badan Penyelesaian Sengketa Konsumen (BPSK), atau melalui mediasi dan arbitrase perbankan. Alternatif penyelesaian sengketa ini bertujuan untuk memberikan solusi yang lebih cepat dan biaya yang lebih rendah dibandingkan dengan proses litigasi di pengadilan.

Perlindungan hukum konsumen dalam layanan m-banking merupakan aspek penting dalam menjaga kepercayaan publik terhadap sektor perbankan digital. Regulasi yang ada telah mengatur hak-hak konsumen dan tanggung jawab perbankan dalam menjamin keamanan transaksi. Namun, implementasi perlindungan hukum masih menghadapi tantangan dalam hal efektivitas pengawasan dan penegakan hukum. Oleh karena itu, perlu adanya peningkatan kesadaran konsumen, penguatan regulasi, serta optimalisasi mekanisme penyelesaian sengketa guna menciptakan ekosistem perbankan digital yang lebih aman dan terpercaya.

C. Analisis Perlindungan Hukum Konsumen dan Tanggung Jawab Perbankan

Layanan mobile banking (m-banking) semakin menjadi bagian integral dari kehidupan modern, menawarkan kemudahan dalam melakukan transaksi keuangan. Namun, pertumbuhan pesat teknologi ini juga membawa tantangan keamanan, seperti penipuan siber dan pencurian data. Oleh karena itu, diperlukan strategi pencegahan yang komprehensif untuk meningkatkan keamanan layanan m-banking, termasuk peran aktif dari perbankan dan regulator dalam mencegah penipuan serta implementasi kebijakan yang memperkuat perlindungan konsumen.

Untuk meningkatkan keamanan m-banking, bank harus mengadopsi berbagai langkah pencegahan yang meliputi teknologi

canggih dan edukasi pengguna. Salah satu strategi utama adalah penerapan autentikasi multi-faktor (MFA) untuk memastikan bahwa hanya pengguna yang sah yang dapat mengakses akun mereka. Selain itu, teknologi enkripsi end-to-end harus digunakan untuk melindungi data selama transmisi antara perangkat pengguna dan server bank. Bank juga harus secara rutin melakukan pemantauan dan analisis terhadap aktivitas transaksi guna mendeteksi pola yang mencurigakan atau anomali yang dapat mengindikasikan adanya upaya penipuan. Penggunaan kecerdasan buatan (AI)) dan machine learning dapat membantu dalam mengidentifikasi pola serangan dan mencegah potensi ancaman sebelum merugikan pengguna.

Selain perlindungan teknologi, bank juga harus memberikan edukasi kepada nasabah mengenai pentingnya menjaga keamanan akun mereka. Kampanye kesadaran keamanan siber dapat meningkatkan pemahaman pengguna tentang risiko phishing, malware, dan teknik rekayasa sosial yang sering digunakan oleh pelaku kejahatan untuk mendapatkan informasi sensitif. Perbankan memiliki tanggung jawab besar dalam memastikan sistem mereka aman dan dapat diandalkan. Selain menerapkan teknologi keamanan tingkat tinggi, bank harus memiliki tim respons insiden siber yang siap menangani serangan dan pemulihan data secara cepat. Bank juga perlu bekerja sama dengan perusahaan keamanan siber untuk meningkatkan pertahanan mereka terhadap ancaman yang terus berkembang.

Di sisi lain, regulator memiliki peran penting dalam menetapkan standar keamanan yang harus dipatuhi oleh semua institusi keuangan. Otoritas seperti Bank Indonesia (BI) dan Otoritas Jasa Keuangan (OJK) harus merancang regulasi yang mewajibkan penerapan standar keamanan minimum, termasuk penggunaan enkripsi kuat, autentikasi ketat, dan sistem deteksi penipuan berbasis AI. Regulator juga perlu memastikan bahwa ada mekanisme pelaporan dan investigasi yang jelas terkait kasus penipuan. Bank harus diwajibkan untuk melaporkan semua insiden keamanan kepada regulator guna memungkinkan analisis lebih lanjut dan tindakan pencegahan yang lebih baik di masa depan. Kerjasama

internasional dalam berbagi informasi mengenai tren penipuan juga menjadi faktor penting dalam menangani ancaman yang bersifat global.

Untuk memperkuat perlindungan konsumen, kebijakan yang diterapkan harus mencakup berbagai aspek mulai dari teknologi hingga regulasi hukum. Beberapa rekomendasi kebijakan yang dapat diterapkan antara lain peningkatan standar keamanan digital dengan mewajibkan semua layanan m-banking untuk menggunakan sistem keamanan berlapis, termasuk MFA dan enkripsi tingkat lanjut, serta melakukan audit keamanan siber secara berkala. Selain itu, edukasi dan literasi keuangan digital harus ditingkatkan dengan menyelenggarakan program edukasi yang menargetkan pengguna dari berbagai latar belakang untuk meningkatkan kesadaran akan ancaman siber dan cara melindungi diri, serta memberikan notifikasi real-time mengenai aktivitas mencurigakan.

Regulasi perlindungan konsumen juga harus diperkuat dengan menetapkan kebijakan penggantian dana bagi nasabah yang menjadi korban kejahatan siber akibat kelemahan sistem perbankan serta memberikan sanksi kepada bank yang gagal menerapkan standar keamanan yang ditetapkan regulator. Peningkatan kolaborasi antar pihak menjadi aspek penting dalam menangani kasus penipuan, di mana bank, regulator, dan penegak hukum harus bekerja sama dalam menangani insiden serta mengembangkan sistem pemantauan nasional yang memungkinkan deteksi dini terhadap pola penipuan lintas lembaga.

Dengan menerapkan strategi pencegahan yang efektif, memperkuat peran perbankan dan regulator, serta menerapkan kebijakan perlindungan konsumen yang ketat, keamanan layanan m-banking dapat ditingkatkan secara signifikan. Upaya kolektif ini akan memberikan perlindungan yang lebih baik bagi nasabah dan memastikan ekosistem perbankan digital yang lebih aman dan terpercaya.

III. KESIMPULAN

Penipuan dalam layanan m-banking semakin marak dengan berbagai modus seperti phishing, smishing, vishing, malware, dan SIM swap fraud.

Pelaku kejahatan siber memanfaatkan teknologi dan rekayasa sosial untuk mencuri data pribadi korban. Kejahatan ini diatur oleh UU ITE serta peraturan Bank Indonesia dan OJK. Perlindungan hukum konsumen diatur oleh Undang-Undang Perlindungan Konsumen dan UU ITE, memberikan hak atas keamanan data, transparansi informasi, pengaduan, dan kompensasi. Bank bertanggung jawab atas keamanan sistem dan edukasi nasabah. Strategi pencegahan meliputi penerapan teknologi keamanan berlapis, edukasi pengguna, dan kerja sama dengan regulator. Regulator harus menetapkan standar keamanan minimum dan mekanisme pelaporan insiden. Tanggung jawab perbankan mencakup kompensasi jika terjadi kelalaian sistem, namun bank dapat membebaskan diri jika penipuan akibat kelalaian nasabah, kecuali ada kesalahan dalam sistem keamanan bank.

REFERENSI

References

[1] McKenzie J. A. (1993). *Power learning in the classroom*. California: Corwin Press, Inc. ← Book

[2] Yu, A. Y., Tian, S. W., Vogel, D., & Chi-Wai Kwok, R. (2010). Can learning be virtually boosted? An investigation of online social networking impacts. *Computers & Education* 55(4):1494-1503. ← Journal

[3] Bhavsar, D.S., Saraf, K.B. (2002). Morphology of PbI_2 Crystals Grown by Gel Method.

Crystal Research and Technology, 37: 51–55 ←Journal

[4] Hasling, D.W., Clancey, W.J., Rennels, G.R. (1983). Strategic Explanations in Consultation.

[5] *The International Journal of Man-Machine Studies*, 20(1): 3-19. ←Journal

[6] Clancey, W.J. (1983). Communication, Simulation, and In-telligent Agents: Implications of Personal Intelligent Machines for Medical

Education. In *Proceedings of the Eighth International Joint Conference on Artificial Intelligence*, 556-560. Menlo Park, Calif.: International Joint Conferences on Artificial Intelligence, Inc. ←Conferences

[7] Rice, J. (1986). Poligon: A System for Parallel Problem Solving, *Technical Report*,

KSL-86-19, Dept. of Computer Science, Stanford Univ. ←Report

[8] Clancey, W.J. (1979). Transfer of Rule-Based Expertise through a Tutorial Dialogue. *PhD Dissertation*, Department of Computer Science, Stanford University. ←Thesis

[9] Ivey, K.C. (2 September 1996). *Citing Internet sources* URL http://www.eei- alex.com/eye/utw/96aug.html. ←Website