Jejakdigital
JURNAL ILMIAH MULTIDISIPLIN
Available online at https://indojurnal.com/index.php/jejakdigital

eISSN 3089-7734; pISSN 3089-7742
Vol. 2, No.5, Tahun 2026
doi.org/10.63822/q1te5a08
Hal. 10189-10195

Analisis Hukum Perbankan Indonesia terhadap Tanggung Jawab Bank atas Kejahatan Siber dengan Modus *Social Engineering*

Andini Putri[1], Hambali H[2]
Program Studi Ilmu Hukum, Universitas Halu Oleo, Kota Kendari, Sulawesi Tenggara, Indonesia[1,2]

*Email: andiniputricantiq@gmail.com ; hambalihusaini@uho.ac.id

Sejarah Artikel:

Diterima *25-08-2026*
Disetujui *30-08-2026*
Diterbitkan *01-09-2026*

ABSTRACT

Social engineering-based digital crime has increased alongside the growth of digital banking services in Indonesia, causing financial losses to customers. This study aims to analyze the legal liability of banks for customer losses resulting from social engineering under Indonesian banking law. This research employs a normative legal research method using statutory, conceptual, and case approaches. The findings indicate that a bank's liability depends on whether there is negligence in implementing the prudential principle, system security, and customer data protection. Conversely, when losses arise from the customer's own negligence in disclosing confidential information, the bank's liability is limited. Therefore, strengthening digital security systems, improving digital literacy, and harmonizing regulations are essential to enhance legal protection for banking customers.

Keywords*: bank liability, social engineering, customer protection, banking law.*

ABSTRAK

Kejahatan digital berbasis social engineering semakin meningkat seiring berkembangnya layanan perbankan digital di Indonesia dan menimbulkan kerugian bagi nasabah. Penelitian ini bertujuan menganalisis pertanggungjawaban hukum bank terhadap kerugian nasabah akibat kejahatan social engineering berdasarkan hukum perbankan Indonesia. Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan peraturan perundang-undangan, konseptual, dan kasus. Hasil penelitian menunjukkan bahwa tanggung jawab bank bergantung pada adanya kelalaian dalam penerapan prinsip kehati-hatian, keamanan sistem, dan perlindungan data nasabah. Sebaliknya, apabila kerugian terjadi karena kelalaian nasabah dalam memberikan informasi kepada pelaku, tanggung jawab bank menjadi terbatas. Oleh karena itu, diperlukan penguatan keamanan sistem, peningkatan literasi digital, dan harmonisasi regulasi untuk memberikan perlindungan hukum yang lebih optimal kepada nasabah.

Kata Kunci: pertanggungjawaban bank, social engineering, perlindungan nasabah, hukum perbankan.

Bagaimana Cara Sitasi Artikel ini:

Putri, A., & H, H. . (2026). Analisis Hukum Perbankan Indonesia terhadap Tanggung Jawab Bank atas Kejahatan Siber dengan Modus Social Engineering. Jejak Digital: Jurnal Ilmiah Multidisiplin, 2(5), 10189-10195. https://doi.org/10.63822/q1te5a08

PENDAHULUAN

Perkembangan teknologi digital telah membawa perubahan signifikan dalam industri perbankan, terutama melalui hadirnya layanan elektronik seperti mobile banking, internet banking, transaksi nirsentuh, dan berbagai inovasi pembayaran digital yang mempermudah aktivitas keuangan masyarakat. Transformasi ini memungkinkan proses transaksi menjadi lebih cepat, efisien, dan dapat dilakukan kapan saja, sehingga meningkatkan kualitas layanan bank dan memperluas akses keuangan masyarakat (Rahman, 2021). Namun, kemajuan teknologi tersebut juga memunculkan ancaman baru berupa kejahatan digital yang semakin kompleks, seperti phishing, skimming, malware injection, carding, pembobolan akun mobile banking, dan berbagai bentuk rekayasa sosial atau social engineering yang memanipulasi nasabah agar menyerahkan data pribadinya (Nurhayati, 2020). Berbagai metode serangan ini terus berkembang, sehingga menjadikan sektor perbankan sebagai target yang rentan karena tingginya nilai ekonomi dan sensitifnya data yang dikelola oleh lembaga keuangan (Setiawan & Putri, 2022).

Tingginya angka kejahatan digital dalam perbankan menciptakan ancaman serius terhadap keamanan dana masyarakat serta kepercayaan publik terhadap sistem keuangan nasional. Kasus-kasus pembobolan rekening, pencurian data kartu ATM, dan penipuan melalui aplikasi mobile banking menunjukkan bahwa sistem perlindungan digital masih memiliki celah yang dapat dimanfaatkan oleh pelaku kejahatan siber (Lestari, 2023). Kondisi tersebut menegaskan pentingnya penerapan hukum yang kuat dan efektif untuk melindungi nasabah serta memastikan bank menjalankan standar keamanan yang memadai. Tanpa perlindungan hukum yang jelas dan tegas, kejahatan digital berpotensi meningkat dan menimbulkan instabilitas dalam sektor perbankan, yang pada akhirnya melemahkan kepercayaan masyarakat terhadap lembaga keuangan formal (Halim, 2021).

Perkembangan teknologi digital telah membawa perubahan signifikan dalam industri perbankan, terutama melalui hadirnya layanan elektronik seperti mobile banking, internet banking, transaksi nirsentuh, dan berbagai inovasi pembayaran digital yang mempermudah aktivitas keuangan masyarakat. Transformasi ini memungkinkan proses transaksi menjadi lebih cepat, efisien, dan dapat dilakukan kapan saja, sehingga meningkatkan kualitas layanan bank dan memperluas akses keuangan masyarakat (Rahman, 2021). Namun, kemajuan teknologi tersebut juga memunculkan ancaman baru berupa kejahatan digital yang semakin kompleks, seperti phishing, skimming, malware injection, carding, pembobolan akun mobile banking, serta berbagai bentuk rekayasa sosial (social engineering) yang memanipulasi nasabah agar menyerahkan data pribadinya (Nurhayati, 2020). Berbagai metode serangan ini terus berkembang dan menjadikan sektor perbankan sebagai target utama karena tingginya nilai ekonomi dan sensitifnya data yang dikelola oleh lembaga keuangan (Setiawan & Putri, 2022).

Hingga saat ini, belum terdapat kajian yang secara komprehensif menilai efektivitas penerapan hukum perbankan dalam menangani kejahatan digital berbasis social engineering dari perspektif perlindungan nasabah. Ketiadaan kajian yang mengintegrasikan analisis antara hukum perbankan, perlindungan konsumen, regulasi Otoritas Jasa Keuangan, serta tanggung jawab bank sebagai penyedia sistem digital menunjukkan adanya celah penelitian (research gap) yang penting untuk diisi. Padahal, dalam praktik, sebagian besar kasus pembobolan rekening justru tidak disebabkan oleh kegagalan sistem teknologi bank semata, melainkan oleh manipulasi psikologis terhadap nasabah yang belum sepenuhnya terakomodasi secara adil dalam kerangka pertanggungjawaban hukum.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif, yaitu penelitian yang dilakukan dengan mengkaji dan menganalisis norma-norma hukum yang berlaku terkait tanggung jawab bank dalam memberikan perlindungan dan keamanan kepada nasabah dari kejahatan siber dengan modus *social engineering*. Penelitian hukum normatif digunakan karena objek utama penelitian berupa peraturan perundang-undangan, prinsip-prinsip hukum, doktrin hukum, serta kasus yang berkaitan dengan kejahatan siber dalam sektor perbankan. Penelitian ini bersifat deskriptif-analitis, yaitu menggambarkan ketentuan hukum yang mengatur tanggung jawab bank dan perlindungan nasabah, kemudian menganalisis penerapannya terhadap kejahatan siber dengan modus *social engineering*.

Pendekatan yang digunakan dalam penelitian ini meliputi pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan kasus (*case approach*). Pendekatan perundang-undangan dilakukan dengan menelaah berbagai ketentuan hukum yang berkaitan dengan kegiatan perbankan, perlindungan nasabah, transaksi elektronik, pelindungan data pribadi, keamanan sistem elektronik, serta kewajiban dan tanggung jawab bank dalam penyelenggaraan layanan perbankan digital. Pendekatan konseptual digunakan untuk menganalisis konsep tanggung jawab hukum bank, perlindungan hukum nasabah, keamanan siber, dan *social engineering*. Sementara itu, pendekatan kasus digunakan untuk mengkaji kasus kejahatan siber yang terjadi pada sektor perbankan di Indonesia sebagai bahan untuk melihat penerapan ketentuan hukum terhadap permasalahan yang dialami nasabah.

Sumber bahan hukum dalam penelitian ini terdiri atas bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Bahan hukum primer meliputi peraturan perundang-undangan yang berkaitan dengan perbankan, transaksi elektronik, pelindungan data pribadi, perlindungan konsumen, serta peraturan Otoritas Jasa Keuangan dan Bank Indonesia yang berkaitan dengan penyelenggaraan layanan perbankan digital dan manajemen risiko teknologi informasi. Bahan hukum sekunder meliputi buku-buku hukum, jurnal ilmiah, artikel akademik, hasil penelitian terdahulu, pendapat para ahli, serta dokumen resmi yang relevan dengan permasalahan penelitian. Adapun bahan hukum tersier berupa kamus hukum, ensiklopedia, dan sumber lain yang digunakan untuk memberikan penjelasan terhadap istilah dan konsep hukum yang digunakan dalam penelitian.

Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan (*library research*), yaitu dengan mengidentifikasi, menginventarisasi, membaca, dan mengkaji berbagai bahan hukum yang relevan dengan objek penelitian. Bahan hukum yang telah dikumpulkan kemudian diklasifikasikan berdasarkan permasalahan penelitian, khususnya mengenai bentuk kejahatan siber dengan modus *social engineering*, kewajiban bank dalam menjaga keamanan transaksi dan data nasabah, serta bentuk tanggung jawab hukum bank apabila nasabah mengalami kerugian akibat kejahatan tersebut.

Analisis bahan hukum dilakukan secara kualitatif dengan menggunakan metode analisis yuridis-normatif. Bahan hukum yang diperoleh dianalisis dengan menghubungkan ketentuan peraturan perundang-undangan dengan konsep dan doktrin hukum serta fakta hukum dalam kasus *social engineering* pada sektor perbankan. Analisis tersebut dilakukan untuk mengetahui sejauh mana hukum perbankan Indonesia memberikan dasar pertanggungjawaban kepada bank, bagaimana batas tanggung jawab antara bank dan nasabah dalam transaksi digital, serta apakah mekanisme perlindungan hukum yang tersedia telah memberikan kepastian dan keadilan bagi nasabah yang mengalami kerugian. Hasil analisis selanjutnya disusun secara sistematis untuk memperoleh kesimpulan mengenai tanggung jawab hukum bank dan upaya penguatan perlindungan nasabah terhadap kejahatan siber dengan modus *social engineering*.

HASIL DAN PEMBAHASAN

Bentuk-Bentuk Kejahatan Digital Di Dunia Perbankan

Kejahatan digital di sektor perbankan terus berkembang seiring pesatnya inovasi layanan keuangan berbasis teknologi. Bentuk kejahatan ini tidak hanya mengandalkan kemampuan teknis tinggi, tetapi juga memanfaatkan kelemahan manusia melalui *social engineering* yang semakin canggih. Salah satu bentuk kejahatan digital yang paling umum adalah *phishing*, yaitu upaya memperoleh informasi rahasia seperti PIN, OTP, atau username dan password dengan cara menyamar sebagai pihak bank melalui email, SMS, atau tautan palsu. Teknik ini semakin meningkat setiap tahun karena banyak nasabah belum memahami ciri-ciri penipuan digital, sehingga membuat phishing menjadi salah satu modus paling efektif bagi pelaku (Mahendra, 2022). Selain itu, terdapat pula kejahatan smishing atau vishing, yaitu penipuan melalui SMS atau panggilan telepon yang menggunakan teknik manipulatif untuk membuat korban menyerahkan data pribadinya (Hartono & Lestari, 2023).

Modus lainnya yang sering digunakan adalah skimming, yaitu pencurian data kartu nasabah melalui alat kecil yang dipasang pada mesin ATM atau mesin EDC. Pelaku kemudian merekam informasi kartu untuk menggandakan kartu tersebut dan menguras saldo rekening korban. Meski penggunaan kartu chip telah mengurangi risiko skimming, pelaku tetap menemukan cara baru untuk memodifikasi alat skimming sehingga lebih sulit dideteksi oleh bank maupun nasabah (Wijayanti, 2021). Selain skimming, kejahatan malware injection juga menjadi ancaman serius. *Malware* disisipkan ke perangkat nasabah melalui aplikasi palsu atau tautan berbahaya, kemudian mencuri data perbankan atau mengalihkan transaksi tanpa sepengetahuan pengguna. Serangan malware ini meningkat signifikan sejak maraknya aplikasi keuangan dan transaksi mobile banking (Sutanto, 2020).

Di era digital, *carding* atau pencurian data kartu kredit juga menjadi salah satu bentuk kejahatan yang sering terjadi. Data kartu kredit diperoleh melalui pembobolan sistem *ecommerce, phishing*, atau peretasan jaringan publik, lalu digunakan untuk transaksi ilegal.

Pelaku carding memanfaatkan celah keamanan pada merchant atau kurangnya proteksi data pribadi konsumen, sehingga menyebabkan kerugian finansial yang cukup besar bagi nasabah maupun bank (Yuliani, 2022). Selain itu, pembobolan akun *mobile banking* melalui teknik *credential stuffing, brute force*, atau pencurian data login melalui *malware* menjadi semakin umum. Serangan ini biasanya terjadi ketika nasabah menggunakan kata sandi yang lemah, menyimpan data pada aplikasi tidak aman, atau terhubung ke jaringan Wi-Fi publik yang rentan diretas (Hakim, 2021).

Salah satu bentuk yang paling berbahaya adalah social engineering, yaitu penipuan yang memanfaatkan psikologi korban, bukan kelemahan teknis sistem. Pelaku sering mengaku sebagai petugas bank, kurir paket, pegawai e-commerce, atau petugas pemutakhiran data, kemudian membujuk korban untuk memberikan OTP atau akses aplikasi perbankan. Pola serangan ini sangat efektif karena pelaku mengeksploitasi rasa panik atau kepercayaan korban terhadap pihak tertentu. Social engineering telah menjadi penyebab utama meningkatnya kasus pembobolan rekening nasabah, bahkan lebih dominan daripada peretasan sistem bank itu sendiri (Prasetyo, 2023). Hal ini menunjukkan bahwa unsur manusia menjadi titik terlemah dalam keamanan digital perbankan.

Penerapan Hukum Positif Dalam Menangani Kejahatan Digital Di Perbankan

Penerapan hukum positif dalam menangani kejahatan digital di sektor perbankan di Indonesia pada dasarnya telah memiliki landasan normatif yang cukup kuat melalui sejumlah regulasi seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Perbankan, Undang-Undang Perlindungan Data Pribadi (UU PDP), serta berbagai peraturan Otoritas Jasa Keuangan (OJK) yang mengatur keamanan sistem elektronik dan perlindungan konsumen. UU ITE menjadisalah satu instrumen utama dalam penanganan kejahatan digital karena mengatur ketentuan mengenai akses ilegal, intersepsi, manipulasi data, dan perbuatan melawan hukum yang dilakukan melalui sistem elektronik. Ketentuan dalam pasal 30 hingga 33 UU ITE memberikan dasar hukum bagi penindakan peretasan, pencurian data, dan manipulasi transaksi elektronik yang sering terjadi dalam kejahatan perbankan digital (Sihombing, 2022). Implementasi UU ITE dalam kasus-kasus perbankan menunjukkan bahwa regulasi ini cukup efektif sebagai dasar untuk menjerat pelaku, meskipun tantangan pembuktian digital masih menjadi kendala penting karena sifat bukti

elektronik yang mudah dimanipulasi dan memerlukan keahlian forensik khusus (Ramadhani, 2021).

Selain UU ITE, UU Perbankan memiliki peran signifikan dalam mengatur tanggung jawab bank dalam menjaga kerahasiaan data nasabah serta memastikan keamanan transaksi. Melalui ketentuan mengenai kerahasiaan bank dan tata kelola pengelolaan data nasabah, UU Perbankan menuntut bank untuk menerapkan standar keamanan berlapis dan memastikan sistem perbankan bebas dari celah yang dapat dimanfaatkan pelaku kejahatan digital (Hidayat, 2020). Jika bank lalai dalam memberikan perlindungan terhadap nasabah, maka bank dapat dikenai sanksi administratif oleh OJK atau bahkan dituntut secara perdata oleh nasabah yang mengalami kerugian. Namun demikian, evaluasi implementasi UU Perbankan menunjukkan bahwa penegakan tanggung jawab bank masih belum optimal, terutama dalam kasus pembobolan rekening yang melibatkan social engineering. Banyak bank beralasan bahwa kesalahan berasal dari kelalaian nasabah, sehingga tanggung jawab digeser kepada korban, dan hal ini sering menimbulkan ketidakpuasan publik (Wulandari & Prasetyo, 2022).

Perkembangan terbaru yang memberikan penguatan bagi perlindungan hukum adalah diterbitkannya Undang-Undang Perlindungan Data Pribadi (UU PDP), yang secara komprehensif mengatur aspek pengumpulan, penyimpanan, pemrosesan, dan keamanan data pribadi, termasuk data keuangan nasabah. UU PDP mewajibkan bank selaku pengendali data untuk memastikan data pribadi terlindungi dari aksesilegal dan kebocoran, serta memberikan hak kepada nasabah untuk memperoleh informasi mengenai penggunaan data mereka. Jika terjadi kebocoran data, bank wajib melaporkan insiden kepada pemerintah dan pihak terkait, serta dapat dikenakan sanksi administratif maupun pidana jika terbukti lalai (Santoso, 2023). Implementasi UU PDP di sektor perbankan merupakan langkah besar dalam memperkuat perlindungan nasabah, meskipun tantangannya adalah kesiapan infrastruktur keamanan bank dan penyesuaian sistem internal agar selaras dengan ketentuan UU PDP.

KESIMPULAN

Perkembangan teknologi digital di industri perbankan telah membawa kemudahan dan efisiensi, namun sekaligus meningkatkan kompleksitas risiko kejahatan siber yang menargetkan bank dan nasabah. Kejahatan digital seperti phishing, malware, carding, social engineering, hingga peretasan akun mobile banking menunjukkan peningkatan signifikan dari tahun ke tahun, sejalan dengan meningkatnya penggunaan layanan keuangan digital.

Situasi ini mengancam stabilitas perbankan dan kepercayaan publik, sehingga perlindungan hukum menjadi sangat penting. Penerapan hukum positif melalui UU ITE, UU Perbankan, UU Perlindungan Data Pribadi, serta regulasi OJK dan Bank Indonesia pada dasarnya telah menyediakan dasar normatif untuk pencegahan dan penindakan kejahatan digital. Namun, efektivitasnya masih terhambat oleh disharmonisasi aturan, tumpang tindih kewenangan, dan perbedaan standar keamanan digital antar lembaga.

Aparat penegak hukum seperti POLRI, OJK, PPATK, dan BI telah menjalankan perannya, tetapi koordinasi antar lembaga masih perlu ditingkatkan agar proses penindakan lebih terpadu. Dari perspektif perlindungan konsumen, bank memiliki tanggung jawab besar untuk memastikan keamanan sistem teknologi informasi, melakukan pengawasan internal, serta menyediakan edukasi kepada masyarakat. Akan tetapi, masih banyak insiden terjadi akibat kelemahan sistem keamanan atau rendahnya literasi digital nasabah. Hal ini menunjukkan bahwa tanggung jawab hukum bank belum sepenuhnya terlaksana secara optimal, terutama dalam aspek early warning system, fraud detection, dan preventive measures (Rahmawati, 2021).

DAFTAR PUSTAKA

Ardian, R. (2021). Penegakan hukum terhadap kejahatan siber di Indonesia. *Jurnal Kriminologi Nusantara, 5*(2), 77–91.

Fadilah, N. (2021). Penyelesaian sengketa konsumen dalam layanan perbankan digital. *Jurnal Perlindungan Konsumen Indonesia, 4*(2), 55–70.

Fauzan, A. (2020). Pengelolaan risiko teknologi informasi pada perbankan digital. *Journal of Financial Technology, 3*(1), 88–102.

Fauzi, D. (2021). Perlindungan konsumen dalam layanan digital banking. *Journal of Financial Regulation, 4*(1), 101–118.

Gunawan, S. (2020). Peran PPATK dalam mendeteksi transaksi keuangan ilegal. *Jurnal Anti Pencucian Uang, 3*(2), 55–70.

Hakim, R. (2021). Mobile banking security and cyber threats. *Journal of Digital Finance, 3*(2), 77–89.

Halim, R. (2021). *Cybersecurity challenges in digital banking*. Prenada Media.

Halimah, R. (2023). Analisis tanggung jawab bank dalam kasus *social engineering*. *Jurnal Hukum & Keamanan Siber, 2*(1), 34–49.

Harsono, B. (2018). *Hukum agraria Indonesia: Sejarah pembentukan Undang-Undang Pokok Agraria, isi dan pelaksanaannya*. Universitas Trisakti Press.

Hartono, B., & Lestari, M. (2023). Social engineering and fraud in digital banking. *Journal of Cybersecurity Studies, 4*(1), 45–61.

Haryanto, B. (2022). Analisis yuridis kasus *cybercrime* di Indonesia. *Jurnal Hukum Teknologi, 4*(1), 55–70.

Hidayat, A. (2020). Tanggung jawab bank dalam pengamanan data nasabah. *Jurnal Hukum Perbankan, 8*(1), 44–58.

Lestari, M. (2023). Kejahatan siber pada layanan *mobile banking* di Indonesia. *Jurnal Hukum & Teknologi, 5*(2), 112–128.

Mahendra, A. (2022). Modus *phishing* dalam kejahatan siber perbankan. *Jurnal Hukum Siber Indonesia, 2*(3), 102–118.

Marzuki, P. M. (2021). *Penelitian hukum*. Kencana.

Nurhayati, S. (2020). Ancaman kejahatan digital dalam industri keuangan. *Indonesian Journal of Cyber Law, 4*(1), 33–47.

Prabowo, A. (2023). Cybercrime investigation challenges in Indonesia's digital banking sector. *Journal of Digital Law, 5*(2), 112–130.

Prasetyo, D. (2023). Tren penipuan digital dan perlindungan nasabah. *Jurnal Keamanan Siber Nasional, 1*(1), 55–70.

Putra, R., & Lestari, M. (2022). Kelalaian bank dalam pengamanan data nasabah. *Jurnal Hukum Perbankan, 7*(2), 101–115.

Rahardjo, S. (2023). Penerapan keamanan digital pada layanan *mobile banking*. *Digital Banking Security Review, 1*(1), 15–29.

Rahman, F. (2021). Transformasi digital dalam perbankan modern. *Jurnal Ekonomi dan Bisnis, 10*(3), 201–215.

Rahmawati, N. (2021). Legal protection for consumers in digital banking services in Indonesia. *Indonesian Banking Law Review, 9*(1), 45–59.

Ramadhani, N. (2021). Tantangan pembuktian digital dalam kejahatan siber. *Cyber Law Journal*, *6*(1), 23–39.

Ramli, F. (2021). Implementasi prinsip *due diligence* dalam sistem perbankan digital. *Journal of Banking Law*, *6*(3), 112–128.

Salim, H. (2021). *Pengantar metode penelitian hukum*. Rajawali Pers.

Santoso, B. (2023). Implikasi Undang-Undang Perlindungan Data Pribadi pada sektor keuangan. *Jurnal Regulasi Digital*, *1*(2), 66–82.

Sari, R., & Wibowo, T. (2021). Analisis kerentanan pengguna terhadap kejahatan digital. *Jurnal Teknologi Informasi*, *7*(2), 98–110.

Sari, W. (2022). Sinergi lembaga dalam penegakan hukum siber. *Journal of Law and Cybersecurity*, *3*(1), 88–104.

Sembiring, D. (2022). Perlindungan nasabah sebagai fondasi kepercayaan publik dalam *digital banking*. *Jurnal Ekonomi & Keuangan Modern*, *5*(1), 77–93.