Indonesian Journal of Islamic Jurisprudence,Economic and Legal Theory

TANGGUNG GUGAT BANK TERHADAP PENIPUAN SKEMA *SOCIAL ENGINERING* DALAM TRANSAKSI DIGITAL

Bambang Fitrianto[1], Cut Anggi Lestari[2], Deviyanti Gusnita[3] , Dhira Ahzara Permata [4], Erwin Juliandi Sipakar[5]

[1,2,3,4,5] Universitas Pembangunan Panca Budi, Indonesia

Email Korespondensi: bambangfitrianto@dosenpancabudi.ac.id

Received 10-08-2025| Revised form 22-09-2025 | Accepted 29-12-2025

Abstract

The development of information technology and the digitalization of banking services have significantly increased the use of digital transactions, offering efficiency and convenience while simultaneously giving rise to increasingly complex cybercrimes. One prevalent form of cybercrime in digital banking practices is fraud through social engineering schemes. This type of fraud exploits psychological manipulation to obtain customers' confidential information, authentication codes, or unauthorized transaction approvals, resulting in substantial financial losses. In the context of banking law, social engineering fraud raises legal issues concerning banks' liability for customer losses, particularly in determining the boundary between bank negligence and customer fault. The Indonesian banking regulatory framework has incorporated prudential principles, risk management, and consumer protection measures. However, regulations specifically addressing banks' liability in cases of social engineering fraud remain insufficient and lack comprehensive clarity, leading to potential legal uncertainty and inconsistent dispute resolution. This study aims to analyze banks' liability for social engineering fraud in digital transactions from the perspective of banking law and customer protection. The research employs a normative legal method with statutory and conceptual approaches by examining banking regulations, consumer protection laws, and legal doctrines related to liability and negligence. The findings indicate that banks may be held liable when customer losses arise from weaknesses in security systems, failure to properly implement prudential principles, or inadequate customer protection and education measures. Therefore, clearer legal regulation is necessary to define the allocation of liability between banks and customers in order to ensure legal certainty and strengthen customer protection in digital banking transactions.

Keyword: *Bank Liability; Social Engineering; Digital Transactions; Customer Protection.*

Abstrak

Perkembangan teknologi informasi dan digitalisasi layanan perbankan telah mendorong peningkatan signifikan penggunaan transaksi digital, yang di satu sisi memberikan kemudahan dan efisiensi, namun di sisi lain memunculkan berbagai bentuk kejahatan siber yang semakin kompleks. Salah satu bentuk kejahatan siber yang banyak terjadi dalam praktik perbankan digital adalah penipuan dengan skema social engineering. Modus ini memanfaatkan manipulasi psikologis terhadap nasabah untuk memperoleh data rahasia, kode otentikasi, atau persetujuan transaksi secara tidak sah, sehingga

menimbulkan kerugian finansial yang signifikan. Dalam konteks hukum perbankan, penipuan social engineering menimbulkan persoalan yuridis terkait tanggung gugat bank atas kerugian yang dialami nasabah, khususnya dalam menentukan batas antara kelalaian bank dan kesalahan nasabah. Kerangka regulasi perbankan di Indonesia telah mengatur prinsip kehati-hatian, manajemen risiko, serta perlindungan konsumen perbankan. Namun demikian, pengaturan mengenai tanggung gugat bank dalam kasus penipuan social engineering masih belum dirumuskan secara tegas dan komprehensif, sehingga berpotensi menimbulkan ketidakpastian hukum dan perbedaan penafsiran dalam penyelesaian sengketa. Penelitian ini bertujuan untuk menganalisis tanggung gugat bank terhadap penipuan dengan skema social engineering dalam transaksi digital dari perspektif hukum perbankan dan perlindungan nasabah. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan dan konseptual, melalui kajian terhadap regulasi perbankan, perlindungan konsumen, serta doktrin hukum mengenai tanggung jawab dan kelalaian. Hasil penelitian menunjukkan bahwa bank pada prinsipnya tetap dapat dimintai tanggung gugat hukum apabila kerugian nasabah disebabkan oleh kelemahan sistem keamanan, kelalaian dalam penerapan prinsip kehati-hatian, atau kurang optimalnya upaya perlindungan dan edukasi kepada nasabah. Oleh karena itu, diperlukan pengaturan hukum yang lebih jelas mengenai pembagian tanggung jawab antara bank dan nasabah guna menjamin kepastian hukum dan memperkuat perlindungan nasabah dalam transaksi perbankan digital.

Kata Kunci: Tanggung Gugat Bank; Social Engineering; Transaksi Digital; Perlindungan Nasabah

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa transformasi yang sangat signifikan dalam sektor perbankan, khususnya melalui digitalisasi layanan keuangan yang berlangsung secara masif dan berkelanjutan.[1] Bank tidak lagi hanya berfungsi sebagai lembaga intermediasi konvensional yang menghimpun dan menyalurkan dana masyarakat, melainkan juga bertransformasi menjadi penyedia layanan keuangan digital yang sangat bergantung pada pemanfaatan sistem elektronik, jaringan komputer, serta pengelolaan dan pemrosesan data dalam skala besar.[2] Transformasi ini mendorong perubahan mendasar dalam pola hubungan hukum antara bank dan nasabah, di mana transaksi keuangan tidak lagi dilakukan secara tatap muka, melainkan melalui sistem digital yang bersifat otomatis dan terintegrasi.

Perubahan tersebut ditandai dengan meningkatnya penggunaan layanan perbankan digital, seperti mobile banking, internet *banking*, dan berbagai kanal pembayaran elektronik yang memungkinkan transaksi dilakukan secara cepat, efisien, dan tanpa batasan ruang serta waktu.[3] Digitalisasi layanan ini memberikan kemudahan akses bagi masyarakat dalam memperoleh layanan keuangan, sekaligus meningkatkan efisiensi operasional bank. Melalui sistem digital, bank dapat memperluas jangkauan layanan, mempercepat proses transaksi, serta menekan biaya operasional yang sebelumnya timbul dalam praktik perbankan konvensional.[4]

Di sisi lain, ketergantungan bank terhadap teknologi digital juga membawa implikasi hukum yang semakin kompleks. Penggunaan sistem elektronik dan pengelolaan data dalam skala besar menempatkan bank dan nasabah pada posisi yang rentan terhadap berbagai risiko, baik yang bersifat teknis maupun yuridis. Hubungan hukum yang dibangun melalui sistem digital menuntut adanya kepastian hukum terkait keabsahan transaksi, keamanan sistem, perlindungan data nasabah, serta tanggung jawab hukum bank apabila terjadi gangguan sistem atau kejahatan siber.[5] Oleh karena itu, digitalisasi perbankan tidak hanya menjadi persoalan teknis, tetapi juga merupakan isu hukum yang memerlukan pengaturan dan pengawasan yang memadai.

Salah satu risiko hukum yang paling menonjol dalam praktik perbankan digital adalah meningkatnya penipuan dengan skema *social engineering*. Modus ini tidak

[1] Danrivanto Budhijanto, *Hukum Telekomunikasi, Penyiaran Dan Teknologi Informasi; Regulasi Dan Konvergansi* (Refika Aditama, 2013).

[2] Abdurrakhman Alhakim, 'Urgensi Perlindungan Hukum terhadap Jurnalis dari Risiko Kriminalisasi UU Informasi dan Transaksi Elektronik di Indonesia', *Jurnal Pembangunan Hukum Indonesia* 4, no. 1 (2022): 89–106, https://doi.org/10.14710/jphi.v4i1.89-106.

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

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

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

mengandalkan peretasan sistem secara teknis, melainkan memanfaatkan manipulasi psikologis terhadap nasabah agar secara sukarela memberikan data rahasia, kode otentikasi, atau persetujuan transaksi kepada pelaku kejahatan.[6] Penipuan *social engineering* kerap terjadi melalui sarana komunikasi digital seperti telepon, pesan singkat, atau aplikasi pesan instan yang menyerupai komunikasi resmi bank.[7] Akibatnya, nasabah mengalami kerugian finansial yang signifikan meskipun secara teknis sistem perbankan tidak mengalami gangguan.

Penipuan dengan skema *social engineering* menimbulkan persoalan hukum yang kompleks terkait tanggung gugat bank terhadap kerugian nasabah. Dalam banyak kasus, bank berpendapat bahwa kerugian timbul akibat kelalaian nasabah dalam menjaga kerahasiaan data, sementara nasabah memandang bahwa bank tetap bertanggung jawab karena transaksi terjadi melalui sistem perbankan yang disediakan oleh bank.[8] Perbedaan pandangan ini menimbulkan ketidakjelasan mengenai batas tanggung jawab bank dan nasabah, serta memicu sengketa hukum yang berpotensi melemahkan kepercayaan publik terhadap layanan perbankan digital.

Dalam sistem hukum Indonesia, regulasi perbankan telah mengatur prinsip kehati-hatian, manajemen risiko, dan perlindungan konsumen perbankan.[9] Namun demikian, pengaturan mengenai tanggung gugat bank dalam kasus penipuan *social engineering* belum dirumuskan secara tegas dan komprehensif. Ketiadaan pengaturan yang jelas tersebut berpotensi menimbulkan ketidakpastian hukum, baik bagi bank sebagai pelaku usaha jasa keuangan maupun bagi nasabah sebagai pengguna layanan transaksi digital.[10] Dalam praktik, penyelesaian kasus penipuan social engineering sering kali bergantung pada penafsiran subjektif mengenai kelalaian para pihak, tanpa adanya standar hukum yang jelas.

Kompleksitas penipuan *social engineering* tidak hanya berkaitan dengan aspek teknis keamanan sistem, tetapi juga mencakup dimensi hukum perdata, hukum perbankan, dan perlindungan konsumen. Bank sebagai lembaga kepercayaan memiliki tanggung jawab hukum untuk memastikan bahwa sistem dan prosedur transaksi digital yang diselenggarakannya memberikan perlindungan yang memadai bagi nasabah. Oleh karena itu, isu tanggung gugat bank dalam kasus penipuan *social engineering* harus

[6] Richard Tommy Pantow, *Tindak Pidana Penipuan Dalam Transaksi Online Sebagai Kejahatan Terorganisir Dan Kaitannya Dengan Pencucian Uang*, 2025.

[7] Sri Lidya Agustin et al., *KESADARAN KEAMANAN KONSUMEN DALAM PENGGUNAAN TRANSAKSI DIGITAL QRIS SEBAGAI PERLINDUNGAN KONSUMEN DIGITAL: STUDI KASUS PENIPUAN QRIS PADA PEDAGANG PAKAIAN DI KECAMATAN KIBIN, KABUPATEN SERANG*, 1 (2025).

[8] Octo Iskandar, 'ANALISIS KEJAHATAN ONLINE PHISHING PADA MASYARAKAT', *Leuser: Jurnal Hukum Nusantara* 1, no. 2 (2024).

[9] Deanne Destriani Firmansyah Putri and Muhammad Helmi Fahrozi, 'UPAYA PENCEGAHAN KEBOCORAN DATA KONSUMEN MELALUI PENGESAHAN RUU PERLINDUNGAN DATA PRIBADI (STUDI KASUS E-COMMERCE BHINNEKA.COM)', *Borneo Law Review* 5, no. 1 (2021): 46–68, https://doi.org/10.35334/bolrev.v5i1.2014.

[10] Muhammad Zaky, 'Eksploitasi Gaya Hidup dalam Penipuan Thrift Online Shop di Instagram', *Ranah Research : Journal of Multidisciplinary Research and Development* 7, no. 4 (2025).

ditempatkan dalam kerangka perlindungan nasabah dan prinsip kehati-hatian perbankan, bukan semata-mata sebagai kesalahan individual nasabah.

Berdasarkan latar belakang tersebut, diperlukan kajian yuridis yang mendalam mengenai tanggung gugat bank terhadap penipuan dengan skema social engineering dalam transaksi digital. Kajian ini menjadi penting untuk menilai sejauh mana bank dapat dimintai pertanggungjawaban hukum atas kerugian nasabah, sekaligus mengidentifikasi kelemahan pengaturan hukum yang ada. Tanpa adanya analisis dan pengaturan yang memadai, penipuan social engineering berpotensi terus menimbulkan ketidakpastian hukum dan melemahkan perlindungan nasabah dalam sistem perbankan digital.

Berdasarkan uraian di atas, penelitian ini berfokus pada analisis yuridis mengenai tanggung gugat bank terhadap penipuan dengan skema social engineering dalam transaksi digital. Penelitian ini diarahkan untuk mengkaji dasar tanggung jawab hukum bank, menelaah pengaturan hukum yang berlaku, serta merumuskan argumentasi normatif mengenai kebutuhan penguatan perlindungan hukum bagi nasabah guna menjamin kepastian hukum dan kepercayaan publik terhadap sistem perbankan digital.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan yuridis normatif dengan menitikberatkan pada analisis terhadap norma-norma hukum yang berlaku melalui penelaahan peraturan perundang-undangan, doktrin, dan teori hukum yang relevan.[11] Pendekatan ini dipilih untuk mengkaji secara mendalam persoalan tanggung gugat bank terhadap kerugian nasabah akibat penipuan dengan skema social engineering dalam transaksi digital, khususnya dalam kerangka hukum perbankan dan perlindungan konsumen di Indonesia. Analisis dilakukan dengan menggunakan pendekatan peraturan perundang-undangan, yaitu menelaah ketentuan hukum yang mengatur perbankan, transaksi elektronik, keamanan sistem dan data, serta perlindungan konsumen, guna menilai kecukupan dan konsistensi pengaturan yang ada sekaligus mengidentifikasi kelemahan atau kekosongan norma terkait pembagian tanggung jawab antara bank dan nasabah.[12] Selain itu, pendekatan konseptual digunakan untuk mengkaji konsep tanggung jawab hukum, kelalaian, prinsip kehati-hatian perbankan, serta perlindungan hukum bagi nasabah berdasarkan pandangan para ahli dan doktrin hukum. Bahan hukum dikumpulkan melalui studi kepustakaan yang mencakup bahan hukum primer berupa peraturan perundang-undangan terkait, bahan hukum sekunder berupa buku, artikel jurnal, dan hasil penelitian terdahulu mengenai kejahatan siber dan *social engineering*, serta bahan hukum tersier yang berfungsi memperjelas istilah dan konsep hukum.[13] Seluruh bahan hukum tersebut kemudian dianalisis secara kualitatif dan preskriptif untuk merumuskan argumentasi

[11] Mexsasai Indra et al., 'Pseudo-Judicial Review for the Dispute over the Result of the Regional Head Election in Indonesia', *Lentera Hukum* 10, no. 1 (2023): 111, https://doi.org/10.19184/ejlh.v10i1.36685.

[12] Elisabeth Nurhaini Butar-Butar, *Metode Penelitian Hukum, Langkah-Langkah Untuk Menemukan Kebenaran Dalam Ilmu Hukum* (PT. Refika Aditama, 2018).

[13] Zainuddin Ali, *Metode Penelitian Hukum* (Sinar Grafika, 2014).

hukum serta rekomendasi normatif yang bertujuan memperkuat kepastian hukum dan perlindungan nasabah dalam transaksi perbankan digital.

HASIL DAN PEMBAHASAN

Karakteristik Penipuan Skema *Social Engineering* dalam Transaksi Perbankan Digital

Penipuan dengan skema *social engineering* dalam transaksi perbankan digital merupakan bentuk kejahatan yang berangkat dari eksploitasi faktor manusia (*human factor*) sebagai titik paling rentan dalam ekosistem keamanan siber.[14] Berbeda dengan serangan siber yang menitikberatkan pada peretasan teknis terhadap sistem perbankan, *social engineering* bekerja dengan memanipulasi persepsi, emosi, dan perilaku korban agar secara sukarela menyerahkan informasi rahasia atau melakukan tindakan tertentu yang menguntungkan pelaku.[15] Dalam konteks perbankan digital, pelaku umumnya tidak perlu menembus sistem keamanan bank secara langsung; cukup dengan "mengakali" nasabah untuk membuka akses, memberikan kredensial, atau mengesahkan transaksi. Karakter ini menjadikan *social engineering* sebagai modus kejahatan yang sulit dideteksi melalui pendekatan keamanan teknologi semata, karena titik serangnya terletak pada keputusan manusia, bukan pada celah sistem.

Karakteristik utama *social engineering* terletak pada penggunaan strategi psikologis yang dirancang untuk menciptakan rasa urgensi, ketakutan, atau kepercayaan palsu. Pelaku biasanya melakukan impersonation (menyamar) sebagai pihak yang dianggap memiliki otoritas, seperti pegawai bank, petugas layanan pelanggan, kurir, aparat, atau perwakilan institusi tertentu.[16] Penyamarannya semakin meyakinkan karena memanfaatkan identitas visual dan bahasa komunikasi yang menyerupai institusi resmi, misalnya menggunakan logo, tautan palsu yang mirip situs resmi, atau gaya komunikasi formal seperti prosedur layanan bank. Dengan teknik tersebut, pelaku membangun legitimasi semu sehingga korban cenderung menurunkan kewaspadaan dan menganggap permintaan pelaku sebagai bagian dari prosedur normal layanan perbankan.

Dalam praktik transaksi perbankan digital, *social engineering* umumnya memiliki pola bertahap yang sistematis. Tahap awal biasanya berupa pengumpulan informasi dasar korban, yang dapat diperoleh dari berbagai sumber terbuka maupun kebocoran data. Informasi ini digunakan untuk menciptakan komunikasi yang personal dan meyakinkan, sehingga korban merasa "pelaku benar-benar tahu data saya" dan kemudian mempercayai percakapan tersebut. Tahap berikutnya adalah *grooming* atau proses membangun kepercayaan melalui percakapan yang tampak membantu, misalnya menawarkan solusi atas masalah akun, mengklaim ada transaksi mencurigakan, atau menyampaikan perintah

[14] Inaz Indra Nugroho et al., 'Optimalisasi Penanggulangan Kebocoran Data Melalui Regulatory Blockchain Guna Mewujudkan Keamanan Siber di Indonesia', *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal* 1, no. 2 (2021): 115–29, https://doi.org/10.15294/ipmhi.v1i2.53698.

[15] Alhakim and Sofia, 'Kajian Normatif Penanganan Cyber Crime Di Sektor Perbankan Di Indonesia'.

[16] Alhakim and Sofia, 'Kajian Normatif Penanganan Cyber Crime Di Sektor Perbankan Di Indonesia'.

"verifikasi" demi keamanan. Pada tahap akhir, pelaku mengarahkan korban untuk melakukan tindakan yang sebenarnya merupakan pintu masuk pengambilalihan akun, seperti mengklik tautan tertentu, memasukkan OTP, memberikan PIN, mengunduh aplikasi tertentu, atau menyetujui proses otorisasi transaksi.[17]

Ragam modus social engineering dalam perbankan digital berkembang seiring meningkatnya kompleksitas layanan dan kanal komunikasi. Modus yang sering ditemui meliputi phishing (tautan palsu yang meniru situs resmi bank), smishing (penipuan melalui SMS/pesan instan), vishing (penipuan lewat panggilan telepon), serta variasi yang memanfaatkan manipulasi sosial melalui platform digital dan aplikasi pesan.[18] Dalam setiap variasinya, esensi modus tetap sama, yaitu mengondisikan korban agar secara tidak sadar melakukan tindakan otorisasi. Persoalan krusial dalam transaksi digital adalah bahwa tindakan otorisasi tersebut secara teknis dapat "terlihat sah" oleh sistem bank, karena dilakukan melalui kanal resmi dan menggunakan kredensial autentik korban. Dengan kata lain, dari perspektif sistem, transaksi dapat memenuhi unsur otentikasi, tetapi dari perspektif substansi, persetujuan itu lahir dari penipuan dan manipulasi.

Karakter lain yang menonjol dari social engineering adalah kemampuannya memanfaatkan desain sistem keamanan yang justru dimaksudkan untuk melindungi nasabah. Misalnya, penggunaan OTP atau two-factor authentication bertujuan memperkuat keamanan, tetapi dalam skema social engineering mekanisme ini dibalik menjadi "alat" yang dipakai pelaku dengan cara membujuk korban menyerahkan OTP. Di sini terlihat bahwa keamanan teknologi tidak cukup jika tidak disertai literasi digital dan tata kelola komunikasi bank-nasabah yang ketat. Dengan demikian, *social engineering* menunjukkan hubungan kausal yang kuat antara kerentanan manusia, desain prosedur layanan, dan risiko kerugian finansial dalam transaksi digital.[19]

Lebih lanjut, *social engineering* memiliki karakter penyebaran yang cepat dan adaptif karena sangat bergantung pada kreativitas pelaku dalam menyesuaikan narasi dengan situasi sosial. Pelaku dapat memanfaatkan isu aktual, momen tertentu, atau kondisi emosional korban untuk meningkatkan efektivitas tipu daya. Hal ini membuat *social engineering* terus berevolusi dan sulit diberantas hanya melalui pemblokiran situs atau penguatan *firewall*. Bahkan, semakin banyak kanal digital yang digunakan bank untuk memperluas layanan, semakin banyak pula ruang interaksi yang berpotensi dieksploitasi pelaku, terutama bila terdapat inkonsistensi pola komunikasi resmi bank atau celah dalam prosedur verifikasi layanan.

Dari sudut pandang hukum, karakteristik social engineering menempatkan isu penipuan ini pada wilayah yang problematik terkait pembuktian dan pembagian tanggung

[17] M. Bagaric and R. Morgan, *Cybercrime: Current Perspectives from InfoSec and Law* (CRC Press, 2021).

[18] J. Black, *Cybercrime and the Law: Challenges, Issues, and Outcomes* (2022).

[19] Dyajeng Ayu Musdalifah et al., 'Dehumanisasi Penerapan Hukum Pidana Secara Berlebihan (Overspanning Van Het Strafrecht) Berdasarkan Teori Social Engineering', in *Book Chapter Hukum dan Politik dalam Berbagai Perspektif* (n.d.).

jawab. Kerugian nasabah sering kali muncul dari tindakan "sukarela" menyerahkan data atau melakukan otorisasi, sehingga bank dapat berargumen bahwa transaksi terjadi atas persetujuan nasabah. Namun, sifat persetujuan tersebut pada hakikatnya tercemar oleh penipuan dan manipulasi, sehingga memunculkan persoalan apakah dapat dipandang sebagai persetujuan yang sah secara hukum. Pada titik ini, analisis terhadap karakteristik *social engineering* menjadi kunci untuk menilai sejauh mana tindakan korban merupakan kelalaian pribadi atau merupakan akibat dari kegagalan sistem perlindungan yang seharusnya disediakan oleh bank melalui standar kehati-hatian dan perlindungan nasabah. *Social engineering* dalam transaksi perbankan digital adalah fenomena yang menempatkan manusia sebagai titik serangan utama, memanfaatkan legitimasi semu dan manipulasi psikologis untuk memperoleh akses dan otorisasi transaksi, serta menghasilkan kerugian yang secara teknis tampak sah namun secara substansial mengandung unsur penipuan. Kompleksitasnya tidak hanya terletak pada variasi modus, tetapi juga pada tantangan pembuktian dan penentuan tanggung jawab hukum antara bank dan nasabah. Pemahaman yang komprehensif terhadap karakteristik *social engineering* menjadi landasan penting untuk merumuskan standar perlindungan yang proporsional dan kerangka pertanggungjawaban yang adil dalam sistem perbankan digital.[20]

Dasar dan Batas Tanggung Gugat Bank atas Kerugian Nasabah akibat *Social Engineering*

Penentuan dasar dan batas tanggung gugat bank atas kerugian nasabah akibat penipuan dengan skema *social engineering* merupakan isu yuridis yang kompleks karena melibatkan irisan antara hukum perdata, hukum perbankan, dan rezim perlindungan konsumen. Dalam transaksi perbankan digital, hubungan hukum antara bank dan nasabah pada dasarnya bersumber dari perjanjian serta prinsip kepercayaan (*fiduciary relationship*), di mana bank berkewajiban menyediakan sistem dan layanan transaksi yang aman, andal, dan melindungi kepentingan nasabah.[21] Oleh karena itu, setiap kerugian yang timbul dalam proses transaksi digital tidak dapat serta-merta dibebankan kepada nasabah tanpa terlebih dahulu menilai apakah bank telah memenuhi kewajiban hukum dan standar kehati-hatian yang melekat pada kegiatan usahanya.

Dasar yuridis tanggung gugat bank dapat ditelusuri dari prinsip kehati-hatian (*prudential principle*) dan kewajiban perlindungan nasabah yang melekat dalam hukum perbankan.[22] Prinsip ini mengharuskan bank untuk mengelola risiko secara optimal, termasuk risiko operasional dan risiko teknologi informasi, serta memastikan bahwa sistem transaksi digital dirancang dengan standar keamanan yang memadai. Dalam konteks *social engineering*, meskipun modus penipuan tidak selalu melibatkan peretasan

[20] Muhammad Shendy Fatur Rahman, 'Kajian Kriminologis Terhadap Motif dan Modus Operandi Tindak Pidana Perubahan Data di Indonesia', *HARISA: Jurnal Hukum, Syariah, dan Sosial* 2, no. 1 (2025).

[21] Alhakim and Sofia, 'Kajian Normatif Penanganan Cyber Crime Di Sektor Perbankan Di Indonesia'.

[22] Bambang Fitrianto, 'Tinjauan Yuridis Tanggung Jawab Hukum Bank Terhadap Kerugian Nasabah Akibat Kecerdasan Buatan (AI) Dalam Pengambilan Keputusan Kredit', *Milthree Law Journal* 1, no. 3 (2025).

sistem secara teknis, bank tetap memiliki kewajiban untuk membangun mekanisme pencegahan, deteksi dini, dan respons yang proporsional terhadap transaksi mencurigakan. Apabila kerugian nasabah timbul akibat kegagalan bank dalam menerapkan standar keamanan, pengawasan transaksi, atau edukasi yang memadai, maka secara yuridis bank dapat dimintai tanggung gugat atas dasar kelalaian (*negligence*).[23]

Selain itu, dasar tanggung gugat bank juga dapat dikaitkan dengan konsep tanggung jawab atas perbuatan melawan hukum dan wanprestasi dalam hubungan kontraktual. Dalam transaksi digital, bank menyediakan sarana, prosedur, dan sistem yang memungkinkan terjadinya transaksi keuangan.[24] Apabila sistem tersebut tidak dilengkapi dengan pengamanan yang memadai atau memiliki kelemahan prosedural yang dapat dieksploitasi pelaku social engineering, maka bank dapat dipandang tidak memenuhi kewajiban kontraktualnya untuk memberikan layanan yang aman. Dalam perspektif ini, kerugian nasabah bukan semata-mata akibat kesalahan pribadi, melainkan juga merupakan konsekuensi dari kegagalan bank dalam memenuhi standar layanan yang seharusnya.

Namun demikian, tanggung gugat bank tidak bersifat mutlak dan tanpa batas. Penentuan batas tanggung gugat bank harus mempertimbangkan peran dan kontribusi nasabah dalam terjadinya kerugian. Dalam banyak kasus *social engineering*, nasabah secara aktif menyerahkan data rahasia, kode otentikasi, atau melakukan persetujuan transaksi atas permintaan pihak yang tidak berwenang.[25] Tindakan tersebut secara formal dapat dikualifikasikan sebagai pelanggaran terhadap kewajiban nasabah untuk menjaga kerahasiaan data dan sarana otentikasi. Oleh karena itu, apabila dapat dibuktikan bahwa bank telah menyediakan sistem yang aman, prosedur yang jelas, serta peringatan yang memadai kepada nasabah, maka kerugian yang timbul dapat dibebankan kepada nasabah sebagai akibat kelalaiannya sendiri.

Batas tanggung gugat bank juga harus ditentukan melalui analisis kausalitas antara perbuatan bank dan kerugian nasabah. Apabila kerugian terjadi semata-mata karena manipulasi psikologis pelaku terhadap nasabah, tanpa adanya kegagalan sistem atau prosedur bank, maka hubungan kausal antara tindakan bank dan kerugian tersebut menjadi lemah.[26] Sebaliknya, apabila social engineering berhasil karena adanya celah dalam desain layanan, lemahnya verifikasi transaksi berisiko tinggi, atau kurangnya mekanisme pengamanan tambahan, maka hubungan kausal tersebut menjadi kuat dan

[23] David Debenham, 'Big Data Analytics, Big Financial Institutions, and Big Money Fraud Litigation', *Westlaw, 32 Banking and Finance Law Review* 103 (2016).

[24] Namira Diffany Nuzan et al., 'Menelaah Lebih Dalam Perbedaan Perbuatan Melawan Hukum dan Wanprestasi', *Jurnal Kewarganegaraan* 8, no. 1 (2024): 2723–2328.

[25] Bambang Fitrianto, 'Tinjauan Yuridis Tanggung Jawab Hukum Bank Terhadap Kerugian Nasabah Akibat Kecerdasan Buatan (AI) Dalam Pengambilan Keputusan Kredit'.

[26] Nicholas Eubank and Adriane Fresh, 'Enfranchisement and Incarceration after the 1965 Voting Rights Act', *American Political Science Review* 116, no. 3 (2022): 791–806, https://doi.org/10.1017/S0003055421001337.

membuka ruang pertanggungjawaban bank. Penilaian tanggung gugat harus dilakukan secara kasuistik dan berbasis pada fakta serta bukti yang konkret.

Dalam konteks perlindungan konsumen perbankan, pembagian tanggung gugat juga harus memperhatikan prinsip keadilan dan keseimbangan. Nasabah pada umumnya berada pada posisi yang lebih lemah secara informasi dan teknis dibandingkan bank. Oleh karena itu, pembebanan seluruh risiko *social engineering* kepada nasabah berpotensi bertentangan dengan tujuan perlindungan konsumen. Di sisi lain, membebankan seluruh kerugian kepada bank tanpa mempertimbangkan kelalaian nasabah juga dapat menimbulkan moral hazard. Oleh sebab itu, batas tanggung gugat bank perlu dirumuskan melalui pendekatan proporsional, dengan mempertimbangkan standar kehati-hatian bank, tingkat kelalaian nasabah, serta kontribusi masing-masing pihak terhadap terjadinya kerugian.

Dasar dan batas tanggung gugat bank atas kerugian nasabah akibat social engineering tidak dapat ditentukan secara simplistik. Bank pada prinsipnya dapat dimintai pertanggungjawaban hukum apabila kerugian nasabah berkaitan dengan kegagalan sistem, kelemahan prosedur, atau pelanggaran prinsip kehati-hatian.[27] Namun, tanggung gugat tersebut dibatasi oleh kewajiban nasabah untuk menjaga keamanan data dan sarana transaksi. Kerangka pembagian tanggung jawab yang jelas dan proporsional menjadi prasyarat penting untuk menjamin kepastian hukum, keadilan bagi para pihak, serta keberlanjutan kepercayaan publik terhadap sistem perbankan digital.

Kebutuhan dan Arah Penguatan Pengaturan Hukum Tanggung Gugat Bank dalam Kasus *Social Engineering*

Meningkatnya frekuensi dan kompleksitas penipuan dengan skema *social engineering* dalam transaksi perbankan digital menunjukkan adanya kebutuhan yang bersifat mendesak untuk memperkuat pengaturan hukum terkait tanggung gugat bank. Fenomena ini tidak hanya mencerminkan perubahan modus kejahatan siber, tetapi juga menandai pergeseran sumber risiko dalam sistem perbankan digital, dari yang semula berfokus pada peretasan teknis menuju eksploitasi faktor manusia sebagai titik paling rentan. Dalam konteks ini, pengaturan hukum yang ada dituntut untuk mampu menjawab realitas baru tersebut agar perlindungan hukum terhadap nasabah tidak tertinggal oleh dinamika kejahatan digital.[28]

Kerangka regulasi perbankan yang berlaku saat ini pada umumnya masih berorientasi pada pengamanan sistem teknologi informasi dan penerapan prinsip kehati-hatian secara umum. Pendekatan ini memadai untuk menghadapi ancaman yang bersifat teknis, seperti peretasan sistem atau gangguan infrastruktur, namun menjadi kurang

[27] Elyana Novira and Uning Pratimaratri, 'Perubahan Sosial dan Hukum Perbankan di Indonesia', *UNES Law Review* 6, no. 3 (2024).

[28] Miguel Arana-Catania et al., 'Citizen Participation and Machine Learning for a Better Democracy', *Digital Government: Research and Practice* 2, no. 3 (2021): 1–22, https://doi.org/10.1145/3452118.

responsif terhadap karakter *social engineering* yang bertumpu pada manipulasi psikologis dan interaksi sosial antara pelaku dan nasabah. Dalam praktik, transaksi yang dihasilkan melalui *social engineering* sering kali memenuhi seluruh persyaratan otentikasi teknis, sehingga secara sistemik dipandang sah oleh bank, meskipun secara substansial transaksi tersebut lahir dari tipu daya dan penyesatan.[29]

Kondisi tersebut menimbulkan ketidakjelasan norma dalam menentukan pembagian tanggung jawab antara bank dan nasabah. Dari sudut pandang bank, kerugian sering kali dianggap sebagai akibat kelalaian nasabah dalam menjaga kerahasiaan data atau sarana otentikasi. Sebaliknya, dari perspektif nasabah, kerugian tersebut dipandang sebagai kegagalan sistem perlindungan yang seharusnya disediakan oleh bank sebagai lembaga kepercayaan. Ketegangan antara dua sudut pandang ini menunjukkan bahwa kerangka hukum yang ada belum memberikan panduan yang tegas dan konsisten mengenai kriteria pertanggungjawaban dalam kasus social engineering.

Lebih lanjut, ketidakjelasan pengaturan hukum tersebut berimplikasi langsung pada praktik penyelesaian sengketa. Tanpa standar normatif yang jelas, penilaian tanggung gugat bank dalam kasus *social engineering* cenderung dilakukan secara kasuistik dan bergantung pada interpretasi subjektif terhadap fakta-fakta tertentu. Hal ini berpotensi menimbulkan inkonsistensi putusan, ketidakpastian hukum, serta melemahkan posisi nasabah sebagai pihak yang secara struktural lebih lemah dalam hubungan perbankan digital.[30] Pada saat yang sama, ketidakpastian tersebut juga menyulitkan bank dalam merancang kebijakan manajemen risiko yang jelas dan terukur.

Oleh karena itu, penguatan pengaturan hukum terkait tanggung gugat bank dalam kasus *social engineering* perlu diarahkan pada perumusan norma yang secara eksplisit mengakomodasi karakter kejahatan ini.[31] Pengaturan tersebut harus mampu membedakan antara transaksi yang benar-benar lahir dari persetujuan bebas nasabah dan transaksi yang terjadi akibat manipulasi psikologis. Dengan demikian, keabsahan teknis transaksi tidak dapat dijadikan satu-satunya dasar untuk meniadakan tanggung jawab bank. Sebaliknya, perlu dilakukan penilaian yang lebih substantif terhadap proses terjadinya persetujuan dan peran sistem serta prosedur bank dalam mencegah atau memitigasi risiko social engineering.

Penguatan pengaturan hukum yang adaptif dan preskriptif menjadi prasyarat penting untuk menjamin keseimbangan antara perlindungan nasabah dan kepastian hukum bagi bank. Tanpa adanya pengaturan yang jelas dan responsif terhadap karakter social engineering, risiko pembebanan kerugian secara tidak proporsional akan terus terjadi dan berpotensi menggerus kepercayaan publik terhadap sistem perbankan digital. Oleh karena itu, pembaruan kerangka hukum menjadi langkah strategis untuk memastikan

[29] W. C. Banks and S. Dycus, *Counterterrorism Law* (Wolters Kluwer, 2020).

[30] Alifa Achmad Wahyu et al., 'Aspek Kepastian Hukum Dalam Perjanjian Jaminan Fidusia', *Binamulia Hukum* 13, no. 2 (2024).

[31] Iskandar, 'ANALISIS KEJAHATAN ONLINE PHISHING PADA MASYARAKAT'.

bahwa perkembangan teknologi perbankan tetap berjalan seiring dengan perlindungan hukum yang memadai dan berkeadilan.

Kebutuhan penguatan pengaturan hukum tersebut terutama didorong oleh perubahan paradigma risiko dalam perbankan digital. Risiko transaksi tidak lagi semata-mata bersumber dari kegagalan sistem atau peretasan teknis, melainkan juga dari kelemahan interaksi manusia dalam ekosistem layanan digital. Dalam konteks ini, pendekatan hukum yang hanya menilai keabsahan transaksi berdasarkan terpenuhinya aspek otentikasi teknis menjadi tidak memadai. Diperlukan pengaturan yang mengakui bahwa persetujuan nasabah yang diperoleh melalui manipulasi *social engineering* tidak dapat dipersamakan dengan persetujuan yang lahir dari kehendak bebas dan sadar. Tanpa pengakuan normatif tersebut, perlindungan hukum terhadap nasabah berpotensi tereduksi secara signifikan.

Arah penguatan pengaturan hukum tanggung gugat bank perlu dimulai dengan perumusan standar tanggung jawab yang lebih jelas dan berbasis risiko (*risk-based liability*). Pengaturan tersebut harus menegaskan bahwa bank tidak hanya bertanggung jawab atas keamanan teknis sistem, tetapi juga atas desain prosedur transaksi dan pola komunikasi yang berpotensi disalahgunakan oleh pelaku social engineering. Tanggung gugat bank tidak semata-mata ditentukan oleh ada atau tidaknya pelanggaran sistem, melainkan juga oleh sejauh mana bank telah menerapkan mekanisme pencegahan, deteksi transaksi mencurigakan, serta respons yang cepat dan efektif terhadap indikasi penipuan.

Selain itu, penguatan pengaturan hukum juga perlu mengatur secara eksplisit mekanisme pembuktian dan pembagian beban pembuktian dalam sengketa social engineering. Dalam praktik, nasabah sering berada pada posisi yang sulit karena keterbatasan akses terhadap data dan sistem transaksi. Oleh karena itu, arah pengaturan ke depan perlu mempertimbangkan prinsip pembalikan beban pembuktian secara terbatas, di mana bank diwajibkan menunjukkan bahwa sistem, prosedur, dan edukasi nasabah telah dijalankan sesuai standar kehati-hatian. Pendekatan ini sejalan dengan tujuan perlindungan konsumen dan dapat mencegah pembebanan risiko yang tidak proporsional kepada nasabah.

Penguatan pengaturan hukum tanggung gugat bank juga harus diintegrasikan dengan rezim pengawasan perbankan. Otoritas pengawas perlu memiliki dasar hukum yang jelas untuk menetapkan standar minimum pencegahan social engineering, termasuk kewajiban edukasi nasabah, kejelasan kanal komunikasi resmi, dan pembatasan prosedur otorisasi transaksi berisiko tinggi. Integrasi ini penting agar tanggung gugat bank tidak hanya bersifat reaktif melalui penyelesaian sengketa, tetapi juga preventif melalui pengawasan dan kepatuhan regulatif.

Lebih lanjut, arah pengaturan hukum yang ideal harus menyeimbangkan antara perlindungan nasabah dan pencegahan moral hazard.[32] Pengaturan yang terlalu

[32] Pristiwanto Bani, 'Asimetri Informasi dan Moral Hazard: Tinjauan Literatur tentang Dampaknya terhadap Klaim Asuransi Kesehatan', *Journal of Economics and Business UBS* 14, no. 3 (2025).

membebankan tanggung gugat kepada bank berpotensi melemahkan kesadaran dan kehati-hatian nasabah, sementara pengaturan yang terlalu menekankan kesalahan nasabah berpotensi mereduksi kepercayaan publik terhadap sistem perbankan digital. Oleh karena itu, diperlukan formulasi norma yang proporsional, dengan membedakan secara tegas antara kerugian yang timbul akibat kelalaian bank, kelalaian nasabah, maupun kombinasi keduanya.

Kebutuhan dan arah penguatan pengaturan hukum tanggung gugat bank dalam kasus social engineering merupakan bagian integral dari upaya membangun sistem perbankan digital yang aman dan berkeadilan. Pengaturan hukum yang adaptif, preskriptif, dan berbasis risiko akan memberikan kepastian hukum bagi bank dan nasabah, memperkuat perlindungan konsumen, serta menjaga kepercayaan publik terhadap layanan perbankan digital. Tanpa penguatan pengaturan yang memadai, penipuan social engineering berpotensi terus menjadi sumber sengketa dan ketidakpastian hukum yang menghambat perkembangan perbankan digital secara berkelanjutan

KESIMPULAN

Penipuan dengan skema *social engineering* dalam transaksi perbankan digital merupakan bentuk kejahatan siber yang memiliki karakteristik khusus karena memanfaatkan manipulasi psikologis nasabah dan menghasilkan transaksi yang secara teknis tampak sah, namun secara substansial mengandung unsur penipuan. Kondisi tersebut menimbulkan persoalan yuridis yang kompleks terkait penentuan tanggung gugat bank atas kerugian nasabah, karena melibatkan irisan antara kewajiban bank dalam menerapkan prinsip kehati-hatian dan perlindungan nasabah, serta kewajiban nasabah untuk menjaga kerahasiaan data dan sarana transaksi. Hasil penelitian menunjukkan bahwa bank pada prinsipnya dapat dimintai tanggung gugat hukum apabila kerugian nasabah berkaitan dengan kelemahan sistem, desain prosedur transaksi, kurang optimalnya deteksi transaksi mencurigakan, atau kelalaian dalam menjalankan standar kehati-hatian dan edukasi nasabah. Namun demikian, tanggung gugat tersebut tidak bersifat mutlak dan harus dibatasi secara proporsional dengan mempertimbangkan kontribusi kelalaian nasabah dalam terjadinya kerugian. Oleh karena itu, penelitian ini menegaskan perlunya penguatan pengaturan hukum yang secara eksplisit mengatur pembagian tanggung jawab antara bank dan nasabah dalam kasus social engineering, termasuk penetapan standar pencegahan, mekanisme pembuktian, dan integrasi pengawasan perbankan, guna menjamin kepastian hukum, keadilan bagi para pihak, serta keberlanjutan kepercayaan publik terhadap sistem perbankan digital.

DAFTAR PUSTAKA

Agustin, Sri Lidya, Anita Fitri, Franoto Siswantoro, and Faizal Alpiansyah. *KESADARAN KEAMANAN KONSUMEN DALAM PENGGUNAAN TRANSAKSI DIGITAL QRIS SEBAGAI PERLINDUNGAN KONSUMEN DIGITAL: STUDI KASUS PENIPUAN QRIS PADA PEDAGANG*

PAKAIAN DI KECAMATAN KIBIN, KABUPATEN SERANG. 1 (2025).

Alhakim, Abdurrakhman. 'Urgensi Perlindungan Hukum terhadap Jurnalis dari Risiko Kriminalisasi UU Informasi dan Transaksi Elektronik di Indonesia'. *Jurnal Pembangunan Hukum Indonesia* 4, no. 1 (2022): 89–106. https://doi.org/10.14710/jphi.v4i1.89-106.

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

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

Alifa Achmad Wahyu, Fokky Fuad, and Aris Machmud. 'Aspek Kepastian Hukum Dalam Perjanjian Jaminan Fidusia'. *Binamulia Hukum* 13, no. 2 (2024).

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

Arana-Catania, Miguel, Felix-Anselm Van Lier, Rob Procter, et al. 'Citizen Participation and Machine Learning for a Better Democracy'. *Digital Government: Research and Practice* 2, no. 3 (2021): 1–22. https://doi.org/10.1145/3452118.

Bagaric, M., and R. Morgan. *Cybercrime: Current Perspectives from InfoSec and Law*. CRC Press, 2021.

Bambang Fitrianto. 'Tinjauan Yuridis Tanggung Jawab Hukum Bank Terhadap Kerugian Nasabah Akibat Kecerdasan Buatan (AI) Dalam Pengambilan Keputusan Kredit'. *Milthree Law Journal* 1, no. 3 (2025).

Bani, Pristiwanto. 'Asimetri Informasi dan Moral Hazard: Tinjauan Literatur tentang Dampaknya terhadap Klaim Asuransi Kesehatan'. *Journal of Economics and Business UBS* 14, no. 3 (2025).

Banks, W. C., and S. Dycus. *Counterterrorism Law*. Wolters Kluwer, 2020.

Black, J. *Cybercrime and the Law: Challenges, Issues, and Outcomes*. 2022.

Budhijanto, Danrivanto. *Hukum Telekomunikasi, Penyiaran Dan Teknologi Informasi; Regulasi Dan Konvergansi*. Refika Aditama, 2013.

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

David Debenham. 'Big Data Analytics, Big Financial Institutions, and Big Money Fraud Litigation'. *Westlaw, 32 Banking and Finance Law Review* 103 (2016).

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

Elyana Novira and Uning Pratimaratri. 'Perubahan Sosial dan Hukum Perbankan di Indonesia'. *UNES Law Review* 6, no. 3 (2024).

Eubank, Nicholas, and Adriane Fresh. 'Enfranchisement and Incarceration after the 1965

Voting Rights Act'. *American Political Science Review* 116, no. 3 (2022): 791–806. https://doi.org/10.1017/S0003055421001337.

Firmansyah Putri, Deanne Destriani, and Muhammad Helmi Fahrozi. 'UPAYA PENCEGAHAN KEBOCORAN DATA KONSUMEN MELALUI PENGESAHAN RUU PERLINDUNGAN DATA PRIBADI (STUDI KASUS E-COMMERCE BHINNEKA.COM)'. *Borneo Law Review* 5, no. 1 (2021): 46–68. https://doi.org/10.35334/bolrev.v5i1.2014.

Indra, Mexsasai, Geofani Milthree Saragih, and Tito Handoko. 'Pseudo-Judicial Review for the Dispute over the Result of the Regional Head Election in Indonesia'. *Lentera Hukum* 10, no. 1 (2023): 111. https://doi.org/10.19184/ejlh.v10i1.36685.

Iskandar, Octo. 'ANALISIS KEJAHATAN ONLINE PHISHING PADA MASYARAKAT'. *Leuser: Jurnal Hukum Nusantara* 1, no. 2 (2024).

Muhammad Zaky. 'Eksploitasi Gaya Hidup dalam Penipuan Thrift Online Shop di Instagram'. *Ranah Research : Journal of Multidisciplinary Research and Development* 7, no. 4 (2025).

Musdalifah, Dyajeng Ayu, Amelia Eka Rahmawati, Zahra Az Shaidah, and Dewi Sulistyaningsih. 'Dehumanisasi Penerapan Hukum Pidana Secara Berlebihan (Overspanning Van Het Strafrecht) Berdasarkan Teori Social Engineering'. In *Book Chapter Hukum dan Politik dalam Berbagai Perspektif*. n.d.

Nugroho, Inaz Indra, Reza Pratiwi, and Salsabila Rahma Az Zahro. 'Optimalisasi Penanggulangan Kebocoran Data Melalui Regulatory Blockchain Guna Mewujudkan Keamanan Siber di Indonesia'. *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal* 1, no. 2 (2021): 115–29. https://doi.org/10.15294/ipmhi.v1i2.53698.

Nuzan, Namira Diffany, Fernanda Naulisa Situmorang, and Kaniko Dyon Geraldi. 'Menelaah Lebih Dalam Perbedaan Perbuatan Melawan Hukum dan Wanprestasi'. *Jurnal Kewarganegaraan* 8, no. 1 (2024): 2723–2328.

Pantow, Richard Tommy. *Tindak Pidana Penipuan Dalam Transaksi Online Sebagai Kejahatan Terorganisir Dan Kaitannya Dengan Pencucian Uang*. 2025.

Rahman, Muhammad Shendy Fatur. 'Kajian Kriminologis Terhadap Motif dan Modus Operandi Tindak Pidana Perubahan Data di Indonesia'. *HARISA: Jurnal Hukum, Syariah, dan Sosial* 2, no. 1 (2025).