

Penegakan Hukum atas Kejahatan Siber Bermodus Pesan Whatsapp dalam Sektor Perbankan

I Gede Krisna Dana Yasa^{1*} , Johannes Ibrahim Kosasih² , I Made Aditya Mantara Putra³ 

¹⁻³ Fakultas Hukum, Universitas Warmadewa, Denpasar, Bali 80239, Indonesia

Law Enforcement of WhatsApp-Based Cybercrime in the Banking Sector	
ARTICLE INFO	ABSTRACT
Received: 26 March 2026	The rapid advancement of digital information and communication technology has significantly transformed banking services by enabling customers to conduct financial transactions through electronic platforms with greater efficiency, accessibility, and convenience. Despite these benefits, technological developments have also created opportunities for cybercrime, particularly through the misuse of WhatsApp as a medium for fraudulent activities targeting banking customers. This phenomenon raises important legal issues concerning the regulatory framework governing digital communication via WhatsApp and the effectiveness of law enforcement mechanisms in addressing cybercrime that results in financial losses for banking customers. Accordingly, this study examines two principal issues: (1) the legal regulation governing the use of WhatsApp digital messaging in relation to cybercrime within the banking sector; and (2) the implementation of law enforcement against perpetrators of WhatsApp-based cybercrime that causes customer losses. This research employs a normative legal method using statutory and conceptual approaches to analyze relevant legal principles and regulations. The findings demonstrate that the legal framework governing cybercrime is primarily established under the Law on Electronic Information and Transactions, the Personal Data Protection Law, the Indonesian Criminal Code, and various regulations concerning the banking sector. Law enforcement is implemented through the imposition of criminal penalties and monetary fines aimed at providing legal certainty and deterrence. Nevertheless, the effectiveness of law enforcement remains constrained by several challenges, including limited public awareness of cyber threats, technological limitations in digital investigations, and difficulties in identifying and prosecuting cybercrime perpetrators operating through electronic communication platforms.
Accepted: 04 May 2026	
Published: 30 May 2026	
Keywords:	
Law Enforcement, Crime, WhatsApp- Based Cybercrime, Banking	

Copyright © 2026 The Author(s)

Published by CV Wahana Publikasi.

This article is an open access article under the [CC BY-NC 4.0 License](https://creativecommons.org/licenses/by-nc/4.0/)

1. Pendahuluan

Negara hukum merupakan suatu bentuk negara yang penyelenggaraan kekuasaan pemerintahannya didasarkan pada supremasi hukum sebagai landasan utama dalam mengatur kehidupan berbangsa dan bernegara.¹ Kedudukan Indonesia sebagai negara hukum ditegaskan secara eksplisit dalam Pasal 1 ayat (3) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 yang menyatakan bahwa "*Negara Indonesia adalah negara hukum.*" Pencantuman ketentuan tersebut menunjukkan semakin kokohnya landasan konstitusional penyelenggaraan negara sekaligus menjadi amanat bahwa seluruh aktivitas pemerintahan dan penyelenggaraan kekuasaan harus dilaksanakan berdasarkan hukum.² Sejalan dengan prinsip tersebut, Pasal 27 ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 menegaskan bahwa setiap warga negara memiliki kedudukan yang sama di hadapan hukum (*equality before the law*). Prinsip persamaan di hadapan hukum merupakan salah satu manifestasi keadilan yang harus diwujudkan melalui penyelenggaraan sistem hukum yang memberikan perlindungan yang setara kepada seluruh warga negara tanpa adanya perlakuan diskriminatif.³ Oleh karena itu, negara berkewajiban membentuk dan menegakkan hukum yang menjamin kepastian, keadilan, serta perlindungan hukum bagi seluruh masyarakat.⁴ Dalam implementasi negara hukum, setiap lembaga negara maupun institusi yang memiliki peran strategis wajib menjalankan fungsi dan kewenangannya berdasarkan prinsip-prinsip hukum yang berlaku. Salah satu sektor yang sangat membutuhkan kepastian hukum adalah sektor perbankan karena aktivitasnya berkaitan langsung dengan pengelolaan dana masyarakat serta pemeliharaan stabilitas sistem keuangan nasional.

Pembangunan ekonomi nasional memerlukan pengelolaan sumber daya ekonomi yang dilakukan secara terencana, terpadu, dan optimal guna meningkatkan kesejahteraan masyarakat. Dalam mewujudkan tujuan tersebut, lembaga keuangan, baik bank maupun lembaga keuangan non-bank, memiliki peran penting dalam mengelola dan mengoptimalkan potensi ekonomi secara efektif dan efisien. Di antara berbagai lembaga keuangan tersebut, perbankan memiliki fungsi yang semakin strategis sebagai lembaga intermediasi yang menghubungkan pihak yang memiliki kelebihan dana dengan pihak yang membutuhkan pembiayaan sehingga menjadi penggerak utama aktivitas perekonomian nasional. Oleh karena itu, sektor perbankan dipandang sebagai salah satu pilar utama dalam mendukung pembangunan ekonomi nasional.⁵ Dalam menjalankan kegiatan usahanya, bank wajib menerapkan prinsip kehati-hatian (*prudential banking principle*) sebagaimana diatur dalam Pasal 2 Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan.⁶ Penerapan prinsip tersebut bertujuan menjaga stabilitas dan kesehatan sistem perbankan sekaligus memberikan perlindungan terhadap kepentingan masyarakat, khususnya nasabah penyimpan dana. Pelaksanaan fungsi perbankan tidak hanya bergantung pada modal yang dimiliki bank, tetapi juga sangat ditentukan oleh tingkat kepercayaan masyarakat dan kerja sama dengan berbagai lembaga keuangan lainnya.⁷ Mengingat dana masyarakat merupakan sumber utama kegiatan

¹ Loughlin, "The Rule of Law: A Slogan in Search of a Concept."

² Pattiruhu, *Pendidikan Kewarganegaraan*.

³ Fredman, "Substantive Equality Revisited."

⁴ Kosasih dan Haykal, *Kasus Hukum Notaris di Bidang Kredit Perbankan*

⁵ Hermansyah, *Hukum Perbankan Nasional Indonesia*

⁶ Sulistyandari et al., "Implementation of Prudential Banking Principles: State Responsibility in Combating Banking Crimes in Indonesia."

⁷ Basel Committee on Banking Supervision, *Core Principles for Effective Banking Supervision*.

operasional perbankan, keberlangsungan dan stabilitas sektor perbankan memiliki pengaruh yang sangat besar terhadap pembangunan ekonomi nasional.⁸

Perkembangan teknologi informasi dan komunikasi yang berlangsung sangat pesat pada era digital telah mengubah berbagai aspek kehidupan masyarakat, termasuk dalam bidang ekonomi dan jasa keuangan. Teknologi berbasis internet kini menjadi kebutuhan fundamental yang memungkinkan masyarakat melakukan komunikasi, pertukaran informasi, dan berbagai aktivitas transaksi secara lebih cepat, mudah, serta tanpa dibatasi oleh ruang dan waktu. Kemajuan tersebut juga mendorong lahirnya berbagai inovasi aplikasi komunikasi digital, salah satunya WhatsApp, yang saat ini menjadi media komunikasi yang lebih banyak digunakan dibandingkan layanan pesan singkat (*Short Message Service* atau SMS) karena menawarkan kemudahan penggunaan serta hanya memerlukan koneksi internet.⁹

Di samping memberikan berbagai manfaat, perkembangan teknologi informasi juga menimbulkan konsekuensi berupa meningkatnya berbagai bentuk kejahatan siber (*cybercrime*), khususnya yang menyasar sektor perbankan.¹⁰ Fenomena ini menjadi perhatian serius mengingat meningkatnya berbagai modus kejahatan digital, seperti *phishing*, yaitu tindakan penipuan yang dilakukan melalui surat elektronik, pesan digital, maupun situs web palsu dengan tujuan memperoleh data pribadi korban, antara lain kata sandi, nomor kartu kredit, data rekening bank, maupun informasi identitas lainnya.¹¹ Selain itu, terdapat pula modus penipuan melalui panggilan telepon maupun media sosial yang dilakukan dengan cara memberikan tekanan psikologis atau menimbulkan rasa takut kepada korban agar bersedia menyerahkan uang ataupun informasi pribadi. Salah satu modus yang paling sering ditemukan adalah panggilan atau pesan yang mengatasnamakan petugas bank dengan dalih adanya transaksi mencurigakan, kemudian meminta korban memberikan data pribadi beserta kode *One Time Password* (OTP). Informasi tersebut selanjutnya digunakan pelaku untuk mengakses rekening korban sehingga mengakibatkan kerugian finansial. Kejahatan semacam ini tidak hanya merugikan nasabah secara individual, tetapi juga berpotensi menurunkan tingkat kepercayaan masyarakat terhadap sistem dan lembaga perbankan.

Terhadap tindak kejahatan perbankan yang memanfaatkan WhatsApp sebagai sarana komunikasi, terdapat berbagai ketentuan hukum yang dapat diterapkan kepada pelaku. Salah satunya adalah Pasal 28 ayat (1) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Ketentuan tersebut melarang setiap orang dengan sengaja menyebarkan informasi yang tidak benar atau menyesatkan yang dapat menimbulkan kerugian bagi konsumen dalam transaksi elektronik. Dalam praktiknya, bentuk pelanggaran yang sering terjadi antara lain pelaku yang mengaku sebagai pihak bank, mengirimkan tautan palsu (*phishing link*), maupun menyebarkan informasi yang menyesatkan dengan tujuan memperoleh data pribadi dan menguasai rekening korban secara melawan hukum.

Kejahatan siber hingga saat ini masih terus berkembang seiring meningkatnya penggunaan media komunikasi digital. Berbagai bentuk kejahatan tersebut memanfaatkan jaringan internet sebagai sarana untuk menyebarkan perangkat lunak berbahaya (*malware*),

⁸ Aini, "Perlindungan Hukum Nasabah dalam Kasus Pembobolan Rekening Bank di Indonesia."

⁹ Lestari, Dewi, and Mahaputra, "Penerapan Undang-Undang Nomor 11 Tahun 2008 tentang ITE dalam Tindak Pidana Penipuan *Love Scam*."

¹⁰ Cele and Kwenda, "Do Cybersecurity Threats and Risks Have an Impact on the Adoption of Digital Banking? A Systematic Literature Review."

¹¹ Waliullah et al., "Assessing the Influence of Cybersecurity Threats and Risks on the Adoption and Growth of Digital Banking: A Systematic Literature Review."

virus komputer, data ilegal, maupun konten yang bertentangan dengan hukum, serta melakukan serangan terhadap berbagai perangkat yang terhubung ke jaringan internet, seperti komputer dan telepon pintar. Dampak yang ditimbulkan tidak hanya berupa gangguan terhadap sistem informasi, tetapi juga kerugian finansial yang signifikan melalui serangan *ransomware*, penipuan daring, pencurian identitas, serta pengambilan data keuangan, termasuk informasi rekening bank maupun kartu kredit milik korban.¹²

Berdasarkan uraian tersebut, perkembangan teknologi digital yang diikuti dengan meningkatnya berbagai modus kejahatan siber melalui aplikasi WhatsApp menimbulkan persoalan hukum yang memerlukan kajian secara komprehensif. Oleh karena itu, penelitian ini difokuskan pada dua permasalahan utama, yaitu: (1) bagaimana pengaturan hukum mengenai penyelenggaraan komunikasi pesan digital melalui WhatsApp yang berkaitan dengan kejahatan siber dalam sektor perbankan; dan (2) bagaimana penegakan hukum terhadap pelaku kejahatan siber yang menggunakan pesan digital WhatsApp sehingga mengakibatkan kerugian bagi nasabah dalam sektor perbankan.

2. Metode dan Bahan Hukum

Penelitian ini menggunakan metode penelitian hukum normatif (*normative legal research*), yang dalam literatur juga dikenal sebagai penelitian hukum doktrinal (*doctrinal legal research*) atau penelitian kepustakaan (*library research*).¹³ Penelitian hukum normatif berfokus pada pengkajian norma-norma hukum yang tertuang dalam peraturan perundang-undangan, doktrin, serta berbagai sumber hukum lainnya sebagai dasar untuk menganalisis permasalahan hukum yang menjadi objek penelitian.

Pendekatan yang digunakan dalam penelitian ini meliputi pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Pendekatan perundang-undangan dilakukan melalui penelaahan secara sistematis terhadap berbagai peraturan perundang-undangan yang berlaku dan memiliki relevansi dengan isu hukum yang dikaji, sehingga dapat diketahui kesesuaian maupun hubungan antar norma hukum yang mengatur permasalahan tersebut. Sementara itu, pendekatan konseptual digunakan untuk mengidentifikasi, menjelaskan, serta menganalisis konsep-konsep, asas-asas, doktrin, dan teori hukum yang berkembang dalam literatur hukum guna memperoleh pemahaman yang lebih komprehensif terhadap permasalahan penelitian.

Bahan hukum yang digunakan dalam penelitian ini terdiri atas bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Bahan hukum primer meliputi Undang-Undang Dasar Negara Republik Indonesia Tahun 1945; Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana; Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi; Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan beserta perubahannya; serta Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Bahan hukum sekunder terdiri atas buku-buku hukum, artikel jurnal ilmiah, hasil penelitian, pendapat para ahli, dan doktrin yang membahas hukum siber, hukum perbankan, perlindungan data pribadi, serta penegakan hukum terhadap tindak pidana siber. Bahan hukum tersier meliputi kamus hukum, ensiklopedia hukum, serta sumber referensi lainnya

¹² Sitorus dan Astono, "Aplikasi *Whatsapp* Bajakan sebagai Ancaman Kejahatan Siber di Indonesia."

¹³ Syahrur, *Pengantar Metodologi Penelitian Hukum: Kajian Penelitian Normatif, Empiris, Penulisan Proposal, Laporan Skripsi dan Tesis*.

yang memberikan penjelasan dan mendukung interpretasi terhadap bahan hukum primer dan bahan hukum sekunder.

Seluruh bahan hukum tersebut dikumpulkan melalui studi kepustakaan (*library research*) dan dianalisis secara kualitatif menggunakan metode penafsiran hukum (*legal interpretation*), yang meliputi penafsiran gramatikal, sistematis, dan konseptual terhadap ketentuan peraturan perundang-undangan. Analisis dilakukan untuk memperoleh pemahaman yang komprehensif mengenai norma hukum yang mengatur penyelenggaraan komunikasi digital melalui WhatsApp dalam sektor perbankan serta penegakan hukum terhadap pelaku kejahatan siber, sehingga dapat disusun argumentasi hukum yang logis, sistematis, dan dapat dipertanggungjawabkan secara ilmiah.

3. Hasil dan Pembahasan

3.1 Pengaturan Hukum Penyelenggaraan Komunikasi Pesan Digital WhatsApp Terkait Kejahatan Siber Sektor Perbankan

Kejahatan siber (*cybercrime*) merupakan setiap perbuatan melawan hukum yang dilakukan dengan memanfaatkan teknologi informasi dan komunikasi melalui jaringan komputer maupun internet dengan tujuan memperoleh keuntungan secara melawan hukum atau menimbulkan kerugian bagi pihak lain, baik dalam bentuk kerugian finansial, penyalahgunaan data, maupun gangguan terhadap keamanan sistem elektronik.¹⁴ Perkembangan teknologi digital yang semakin pesat telah memperluas ruang lingkup tindak kejahatan siber, termasuk berbagai modus yang menyasar sektor perbankan sebagai salah satu sektor yang sangat bergantung pada sistem elektronik dan teknologi informasi.

Salah satu bentuk kejahatan siber yang saat ini banyak ditemukan dalam praktik adalah *sniffing*. Kejahatan *sniffing* merupakan modus kejahatan siber yang dilakukan dengan memanfaatkan aplikasi pesan instan, khususnya WhatsApp, sebagai media untuk mengirimkan berkas berbahaya kepada korban, misalnya berupa undangan pernikahan digital dalam format aplikasi (*Android Package Kit* atau APK).¹⁵ Melalui modus tersebut, pelaku berupaya mengelabui korban agar mengunduh dan memasang berkas yang dikirimkan sehingga perangkat korban dapat diakses atau terhubung dengan sistem yang telah dipersiapkan oleh pelaku. Kondisi tersebut memungkinkan pelaku melakukan penyadapan terhadap data pribadi maupun informasi keuangan korban, termasuk data yang berkaitan dengan layanan perbankan digital. Oleh karena itu, *sniffing* dapat dikategorikan sebagai salah satu bentuk kejahatan siber yang memiliki tingkat prevalensi tinggi, khususnya yang memanfaatkan platform WhatsApp sebagai sarana untuk melancarkan tindak pidana.¹⁶

Berkaitan dengan pengaturan hukum mengenai penyelenggaraan komunikasi digital melalui aplikasi WhatsApp dalam sistem hukum Indonesia, terdapat sejumlah peraturan perundang-undangan yang menjadi dasar hukum dalam mengatur penggunaan teknologi informasi, perlindungan data, serta keamanan komunikasi elektronik. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik merupakan landasan hukum utama yang mengatur penyelenggaraan teknologi informasi dan komunikasi elektronik, termasuk

¹⁴ Butarbutar, "Kejahatan Siber Terhadap Individu: Jenis, Analisis, dan Perkembangannya."

¹⁵ Bupu, Medan, dan Amalo, "Analisis Yuridis *Cyber Crime* Pembobolan Dana Nasabah pada Aplikasi *Mobile Banking* dengan Modus Pembobolan Jalur Undangan Pernikahan Palsu."

¹⁶ Sutarli dan Kurniawan, "Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi dalam Menanggulangi *Phishing* di Indonesia."

penggunaan aplikasi pesan instan seperti WhatsApp. Undang-undang ini memberikan dasar hukum terhadap berbagai aktivitas komunikasi elektronik serta menetapkan prinsip-prinsip yang harus dipenuhi dalam penyelenggaraan sistem elektronik sebagaimana tercantum dalam Pasal 1 ayat (1). Di samping pengaturan normatif tersebut, WhatsApp sebagai penyedia layanan komunikasi digital juga menerapkan mekanisme keamanan berupa teknologi *end-to-end encryption*, yaitu sistem enkripsi yang memastikan bahwa isi komunikasi hanya dapat diakses oleh pihak pengirim dan penerima pesan.¹⁷ Penerapan teknologi tersebut mencerminkan adanya komitmen dalam menjaga kerahasiaan, integritas, dan keamanan komunikasi digital para pengguna sebagai bagian dari perlindungan terhadap data elektronik.

Selanjutnya, Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana memberikan pengakuan terhadap eksistensi data dan informasi elektronik sebagai objek yang memperoleh perlindungan hukum. Dalam ketentuan tersebut ditegaskan bahwa informasi elektronik mencakup setiap data yang dibuat, disimpan, dikirimkan, diterima, atau diproses melalui sistem elektronik dalam berbagai bentuk, seperti tulisan, suara, gambar, foto, video, simbol, kode, maupun kode akses lainnya. Agar memperoleh makna hukum, informasi elektronik harus memiliki nilai informasi yang dapat dipahami oleh pihak yang mengaksesnya, sehingga keberadaannya tidak hanya dipandang sebagai data digital semata, melainkan juga sebagai objek hukum yang dapat menimbulkan hak, kewajiban, maupun akibat hukum.

Perlindungan terhadap data pribadi pengguna komunikasi digital selanjutnya diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Undang-undang ini mendefinisikan data pribadi sebagai setiap data mengenai individu yang teridentifikasi atau dapat diidentifikasi, baik secara langsung maupun tidak langsung, melalui sistem elektronik maupun non-elektronik. Data pribadi tersebut dapat berbentuk dokumen fisik maupun data elektronik yang dikombinasikan dengan informasi lain, seperti gambar, suara, video, atau informasi identitas lainnya. Lebih lanjut, Pasal 4 ayat (1), ayat (2), dan ayat (3) membedakan data pribadi ke dalam dua kategori, yaitu data pribadi yang bersifat spesifik dan data pribadi yang bersifat umum. Pengaturan tersebut memberikan dasar hukum yang kuat dalam menjamin perlindungan terhadap data pribadi pengguna layanan komunikasi digital, termasuk pengguna aplikasi WhatsApp.

Selain itu, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik mengatur penyelenggaraan sistem elektronik oleh penyelenggara layanan digital. Berdasarkan karakteristik layanan yang disediakan, WhatsApp dapat dikualifikasikan sebagai Penyelenggara Sistem Elektronik (PSE) Lingkup Privat karena menyediakan layanan komunikasi berbasis internet yang memungkinkan pengguna melakukan pertukaran pesan, panggilan suara, panggilan video, pengiriman dokumen, serta berbagai bentuk komunikasi elektronik lainnya melalui sistem elektronik. Sebagai Penyelenggara Sistem Elektronik, WhatsApp memiliki kewajiban untuk menjamin keandalan, keamanan, dan perlindungan terhadap data serta informasi pengguna sesuai dengan ketentuan peraturan perundang-undangan yang berlaku.

Berdasarkan keseluruhan pengaturan tersebut, dapat dipahami bahwa penyelenggaraan komunikasi digital melalui aplikasi WhatsApp telah memiliki landasan hukum yang komprehensif dalam sistem hukum Indonesia. Pengaturan tersebut tidak hanya bertujuan

¹⁷ Bafadhal, "Komunikasi Ritual Penggunaan Aplikasi WhatsApp: Studi Konsumsi Berita Lewat Group WhatsApp."

mengatur pemanfaatan teknologi informasi dan komunikasi, tetapi juga memberikan kepastian hukum, perlindungan terhadap data pribadi, serta menjamin keamanan pengguna dalam melakukan komunikasi elektronik. Dengan demikian, keberadaan berbagai regulasi tersebut menjadi instrumen hukum yang penting dalam mencegah penyalahgunaan media komunikasi digital sekaligus mendukung upaya penanggulangan kejahatan siber, khususnya yang terjadi dalam sektor perbankan.

3.2 Penegakan Hukum terhadap Pelaku Kejahatan Siber melalui Pesan Digital WhatsApp Berakibat Kerugian Nasabah dalam Sektor Perbankan

Sanksi pidana merupakan konsekuensi hukum yang dijatuhkan oleh negara kepada seseorang yang terbukti melakukan tindak pidana sebagai bentuk pertanggungjawaban atas perbuatan yang melanggar hukum. Secara terminologis, istilah *sanksi* mengandung pengertian sebagai ancaman atau konsekuensi hukum yang dikenakan terhadap pelanggaran suatu norma hukum, sedangkan *pidana* merupakan penderitaan yang secara sengaja dijatuhkan oleh negara kepada pelaku tindak pidana berdasarkan putusan pengadilan yang telah memperoleh kekuatan hukum tetap.¹⁸ Dengan demikian, sanksi pidana berfungsi sebagai instrumen penegakan hukum yang bertujuan menjamin ditaatinya ketentuan peraturan perundang-undangan, memberikan efek jera (*deterrent effect*) kepada pelaku, serta melindungi kepentingan hukum masyarakat. Roslan Saleh menjelaskan bahwa pidana merupakan reaksi negara terhadap suatu tindak pidana yang diwujudkan dalam bentuk penderitaan yang secara sengaja dibebankan kepada pelaku sebagai konsekuensi atas perbuatannya.¹⁹ Oleh karena itu, sanksi pidana dapat dipahami sebagai ancaman hukuman, baik berupa pidana penjara maupun pidana lainnya, yang dikenakan kepada setiap orang yang secara sah dan meyakinkan terbukti melakukan perbuatan yang dilarang oleh hukum.

Dalam praktiknya, pelaku kejahatan siber yang memanfaatkan pesan WhatsApp sebagai modus operandi berupaya mengganggu, merusak, atau memperoleh akses secara melawan hukum terhadap sistem elektronik milik korban melalui pesan digital yang dikirimkan. Salah satu modus yang banyak ditemukan adalah pengiriman tautan (*malicious link*) atau berkas berbahaya yang dirancang untuk mengambil alih akses terhadap layanan *mobile banking* milik korban.²⁰ Setelah korban mengakses tautan tersebut, pelaku dapat memperoleh akses tanpa hak terhadap sistem elektronik korban sehingga sistem tidak lagi berfungsi sebagaimana mestinya dan mengakibatkan kerugian finansial bagi pemilik rekening.²¹

Terhadap perbuatan tersebut, pelaku dapat dimintai pertanggungjawaban pidana berdasarkan Pasal 45A ayat (1) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Selain itu, ketentuan pidana juga dapat diterapkan berdasarkan Pasal 492 Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP). Berdasarkan ketentuan tersebut, pelaku dapat dijatuhi pidana penjara paling lama empat tahun serta pidana denda Kategori V dengan jumlah paling banyak Rp500.000.000,00 (lima ratus juta rupiah). Pengaturan tersebut menunjukkan bahwa kejahatan siber melalui

¹⁸ Ekaputra dan Khair, *Sistem Pidana di dalam KUHP dan Pengaturannya Menurut Konsep KUHP Baru*.

¹⁹ Wulandari, Rideng, dan Suryani, "Sanksi Pidana dalam Tindak Pidana Pemilu terkait dengan Asas *Lex Specialis Derogate Legi Generali*."

²⁰ Zia dan Kalidass, "Web Phishing Net (WPN): A Scalable Machine Learning Approach for Real-Time Phishing Campaign Detection."

²¹ Putra, "Tanggungjawab Hukum Bank Terhadap Nasabah dalam Hal Terjadinya Kegagalan Transaksi pada Sistem *Mobile Banking*."

pesan WhatsApp tidak hanya menimbulkan kerugian materiil bagi korban, tetapi juga membawa konsekuensi hukum yang serius bagi pelaku berupa pidana penjara dan pidana denda sebagai bentuk perlindungan terhadap masyarakat serta upaya pencegahan terhadap terulangnya tindak pidana serupa.

Penerapan sanksi pidana terhadap pelaku kejahatan siber melalui media WhatsApp dalam sektor perbankan pada dasarnya telah memiliki landasan hukum yang memadai. Pengaturan tersebut tersebar dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Meskipun demikian, implementasi penegakan hukum terhadap tindak pidana tersebut masih menghadapi berbagai kendala. Dari aspek pembuktian, pelaku umumnya menggunakan identitas palsu, menyamarkan jejak digital, serta menghapus barang bukti elektronik sehingga menyulitkan proses pembuktian. Selain itu, perkembangan modus operandi kejahatan siber yang berlangsung sangat cepat dan rendahnya tingkat kesadaran hukum masyarakat juga menjadi faktor yang menghambat efektivitas penegakan hukum. Oleh karena itu, selain diperlukan penerapan sanksi pidana secara tegas dan konsisten, diperlukan pula peningkatan kapasitas aparat penegak hukum di bidang teknologi informasi serta penguatan edukasi dan literasi digital kepada masyarakat sebagai langkah preventif dalam meminimalkan terjadinya kejahatan siber.²² Dengan demikian, tujuan perlindungan hukum terhadap nasabah perbankan dapat diwujudkan secara lebih optimal.

Penegakan hukum terhadap kejahatan siber bermodus pesan WhatsApp pada sektor perbankan tidak hanya diwujudkan melalui penerapan sanksi pidana, tetapi juga melalui pelaksanaan mekanisme penegakan hukum sesuai dengan ketentuan peraturan perundang-undangan yang berlaku. Dalam praktiknya, proses penegakan hukum dilakukan secara bertahap, dimulai dari penyelidikan, penyidikan, penuntutan, hingga pemeriksaan dan putusan perkara oleh pengadilan. Dasar hukum pelaksanaan proses tersebut antara lain Kitab Undang-Undang Hukum Pidana (KUHP), Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024, serta berbagai ketentuan hukum lain yang berkaitan dengan sistem elektronik dan perlindungan data pribadi. Dalam proses tersebut, Kepolisian Negara Republik Indonesia memiliki kewenangan untuk melakukan penyelidikan dan penyidikan terhadap tindak pidana siber sesuai dengan ketentuan hukum acara pidana yang berlaku.

Penegakan hukum terhadap kejahatan siber bermodus pesan WhatsApp pada sektor perbankan melibatkan koordinasi berbagai lembaga penegak hukum dan instansi pemerintah.²³ Tahapan tersebut meliputi penyelidikan dan penyidikan oleh Kepolisian Negara Republik Indonesia, penuntutan oleh kejaksaan, pemeriksaan dan putusan perkara oleh pengadilan, serta tindakan administratif berupa putusan akses terhadap Informasi Elektronik atau Dokumen Elektronik yang bermuatan melanggar hukum oleh Kementerian Komunikasi dan Digital (Komdigi). Karakteristik kejahatan siber yang memanfaatkan teknologi informasi, penggunaan identitas samaran atau identitas palsu, serta sifatnya yang lintas batas (*transnational crime*) menyebabkan tindak pidana ini dapat

²² Khiaonarong dan Zheng, "The Rise of Cyber Events and Digital Fraud in the Financial Sector."

²³ INTERPOL, *Asia and South Pacific Cyberthreat Assessment Report 2024*.

dilakukan dari berbagai negara selama pelaku memiliki akses terhadap jaringan internet.²⁴ Kondisi tersebut menjadikan penegakan hukum terhadap kejahatan siber memiliki tingkat kompleksitas yang lebih tinggi dibandingkan tindak pidana konvensional. Selain itu, aparat penegak hukum juga menghadapi berbagai tantangan, antara lain kesulitan dalam melacak keberadaan pelaku, kompleksitas pembuktian berbasis alat bukti elektronik, serta keterbatasan sumber daya manusia yang memiliki kompetensi di bidang forensik digital dan teknologi informasi.²⁵ Oleh karena itu, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik merupakan instrumen hukum yang paling relevan dalam penegakan hukum terhadap kejahatan siber bermodus pesan WhatsApp pada sektor perbankan karena secara khusus mengatur berbagai perbuatan yang berkaitan dengan pemanfaatan teknologi informasi, memberikan dasar hukum terhadap pertanggungjawaban pidana pelaku, serta mengakui informasi elektronik dan dokumen elektronik sebagai alat bukti yang sah dalam proses peradilan pidana.

4. Kesimpulan

Berdasarkan hasil penelitian, dapat disimpulkan bahwa pengaturan hukum mengenai penyelenggaraan komunikasi pesan digital melalui WhatsApp yang berkaitan dengan kejahatan siber pada sektor perbankan telah memiliki landasan hukum yang relatif komprehensif, yaitu melalui Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, serta berbagai peraturan mengenai penyelenggaraan sistem elektronik. Dalam kerangka regulasi tersebut, WhatsApp dapat dikategorikan sebagai Penyelenggara Sistem Elektronik (PSE) yang memiliki kewajiban untuk menjamin keamanan sistem dan melindungi data pengguna. Meskipun demikian, perkembangan teknologi informasi juga diikuti dengan meningkatnya berbagai modus kejahatan siber, seperti *phishing*, *malware*, *sniffing*, serta penipuan yang mengatasnamakan pihak perbankan, yang masih menimbulkan kerugian bagi masyarakat, khususnya pengguna WhatsApp yang memanfaatkan layanan *mobile banking*. Penegakan hukum terhadap pelaku kejahatan siber pada sektor perbankan pada dasarnya telah diatur melalui ketentuan dalam Undang-Undang Informasi dan Transaksi Elektronik, khususnya Pasal 28 ayat (1), Pasal 30, Pasal 33, dan Pasal 45A, Pasal 492 Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Implementasi penegakan hukum dilakukan melalui tahapan penyelidikan, penyidikan, penuntutan, hingga penjatuhan sanksi pidana berupa pidana penjara dan pidana denda terhadap pelaku yang terbukti melakukan tindak pidana, sedangkan Kementerian Komunikasi dan Digital berwenang melakukan pemutusan akses terhadap informasi elektronik yang melanggar hukum. Meskipun demikian, efektivitas penegakan hukum masih menghadapi berbagai tantangan, antara lain perkembangan modus operandi kejahatan siber, kompleksitas pembuktian elektronik, serta karakteristik kejahatan yang bersifat lintas batas.

²⁴ Bruce et al., "Mapping the Global Geography of Cybercrime with the World Cybercrime Index"; Wang, "Global (Re-)Framing of Cybercrime: An Emerging Common Interest in Flux of Competing Normative Powers?"

²⁵ Marsilindo, Karo-Karo, dan Widarto, "Penggunaan Alat Bukti Digital dalam Pembuktian Tindak Pidana Siber di Pengadilan Indonesia."

Sejalan dengan temuan tersebut, diperlukan langkah-langkah strategis untuk meningkatkan efektivitas pencegahan dan penegakan hukum terhadap kejahatan siber di sektor perbankan. Pemerintah perlu terus memperkuat dan memperbarui regulasi agar mampu mengakomodasi perkembangan teknologi informasi yang berlangsung sangat cepat, disertai dengan peningkatan kapasitas aparat penegak hukum, khususnya di bidang teknologi informasi dan forensik digital, serta memperluas kerja sama internasional dalam penanggulangan kejahatan siber yang bersifat transnasional. Di sisi lain, sektor perbankan perlu memperkuat sistem keamanan informasi, meningkatkan mekanisme perlindungan terhadap data dan transaksi nasabah, serta memberikan edukasi secara berkelanjutan mengenai berbagai modus kejahatan siber yang berkembang. Selain itu, masyarakat sebagai pengguna layanan perbankan digital juga dituntut untuk meningkatkan kesadaran dan kewaspadaan dalam menggunakan teknologi komunikasi, khususnya dengan tidak membuka tautan yang mencurigakan, tidak mengunduh berkas dari sumber yang tidak dikenal, serta tidak memberikan informasi pribadi seperti *username*, *password*, PIN, alamat surat elektronik, maupun kode *One Time Password* (OTP) kepada pihak mana pun. Melalui sinergi antara pemerintah, lembaga perbankan, aparat penegak hukum, dan masyarakat, diharapkan perlindungan hukum terhadap pengguna layanan perbankan digital dapat terwujud secara lebih efektif sekaligus memperkuat keamanan ekosistem digital di Indonesia.

Acknowledgments

The authors express their sincere gratitude to the Faculty of Law, Universitas Warmadewa, Denpasar, Bali 80239, Indonesia, for providing the academic environment, institutional support, and research facilities that enabled the completion of this normative legal study. The authors also extend their appreciation to the academic supervisors for their invaluable guidance, constructive comments, and continuous support throughout the stages of legal analysis, manuscript preparation, and completion of this research. Their expertise and critical insights have significantly contributed to the quality of this manuscript.

Funding

This research received no external funding.

Conflict of Interest

The authors declare that there is no conflict of interest regarding the publication of this article.

Authors' Contributions

The first author conducted the research by identifying the legal issues, collecting and examining primary, secondary, and tertiary legal materials, performing statutory and conceptual analyses, interpreting the relevant legal norms, and preparing the manuscript. The second and third authors acted as academic supervisors by providing conceptual and methodological guidance, reviewing the legal analysis and arguments, critically revising the manuscript, and supervising the overall research process. All authors discussed the findings, contributed to the final version of the manuscript, and approved it for publication.

Statement of the use of AI

The authors declare that no artificial intelligence (AI) tools or generative AI technologies were used in the conception, preparation, writing, analysis, or revision of this manuscript.

Referensi

- Aini, Almira Qurrotul. "Perlindungan Hukum Nasabah dalam Kasus Pembobolan Rekening Bank di Indonesia." *Jurnal Multidisiplin Ilmu Akademik* 1, no. 6 (2024): 165–172. <https://doi.org/10.61722/jmia.v1i6.2891>.
- Bafadhal, Oemar Madri. "Komunikasi Ritual Penggunaan Aplikasi WhatsApp: Studi Konsumsi Berita Lewat Group WhatsApp." *Jurnal Komunikasi Indonesia* 6, no. 1 (2017): 49–56. <https://doi.org/10.7454/jki.v6i1.8628>.
- Basel Committee on Banking Supervision. *Core Principles for Effective Banking Supervision*. Basel: Bank for International Settlements, 2024.
- Bruce, Miranda, Jonathan Lusthaus, Ridhi Kashyap, Nigel Phair, and Federico Varese. "Mapping the Global Geography of Cybercrime with the World Cybercrime Index." *PLOS ONE* 19, no. 4 (2024): e0297312. <https://doi.org/10.1371/journal.pone.0297312>.
- Bupu, Angela Gabriela, Karolus Kopong Medan, and Heryanto Amalo. "Analisis Yuridis Cyber Crime Pembobolan Dana Nasabah pada Aplikasi Mobile Banking dengan Modus Pembobolan Jalur Undangan Pernikahan Palsu." *Hakim: Jurnal Ilmu Hukum dan Sosial* 2, no. 2 (2024): 367–383. <https://doi.org/10.51903/hakim.v2i2.1829>.
- Butarbutar, Russel. "Kejahatan Siber Terhadap Individu: Jenis, Analisis, dan Perkembangannya." *Technology and Economics Law Journal* 2, no. 2 (2023). <https://doi.org/10.21143/TELJ.vol2.no2.1043>.
- Cele and Kwenda. "Do Cybersecurity Threats and Risks Have an Impact on the Adoption of Digital Banking? A Systematic Literature Review." *Journal of Financial Crime* 32, no. 1 (2025): 31–48. <https://doi.org/10.1108/JFC-10-2023-0263>.
- Ekaputra, Mohammad, and Abdul Khair. *Sistem Pidana di Dalam KUHP dan Pengaturannya Menurut Konsep KUHP Baru*. Medan: USU Press, 2010.
- Fredman, Sandra. "Substantive Equality Revisited." *International Journal of Constitutional Law* 14, no. 3 (2016): 712–738. <https://doi.org/10.1093/icon/mow043>.
- Hermansyah. *Hukum Perbankan Nasional Indonesia*. 3rd ed. Jakarta: Prenada Media, 2020.
- INTERPOL. *Asia and South Pacific Cyberthreat Assessment Report 2024*. Lyon: International Criminal Police Organization, 2024.
- Khiaonarong, Tanai, and Shanyuan Zheng. "The Rise of Cyber Events and Digital Fraud in the Financial Sector." *IMF Working Papers* 2026, no. 062 (2026). <https://doi.org/10.5089/9798229043557.001>.
- Kosasih, Johannes Ibrahim, and Hassanain Haykal. *Kasus Hukum Notaris di Bidang Kredit Perbankan*. Jakarta: Sinar Grafika, 2021.
- Lestari, Desak Nyoman Ayu Melbi, Anak Agung Sagung Laksmi Dewi, and I. B. Gede Agustya Mahaputra. "Penerapan Undang-Undang Nomor 11 Tahun 2008 tentang ITE dalam Tindak Pidana Penipuan Love Scam." *Jurnal Analogi Hukum* 5, no. 1 (2023): 120–125. <https://doi.org/10.22225/ah.5.1.2023.120-125>.
- Loughlin, Martin. "The Rule of Law: A Slogan in Search of a Concept." *Hague Journal on the Rule of Law* 16 (2024): 509–523. <https://doi.org/10.1007/s40803-024-00224-5>.
- Marsilindo, Rizky Pratama Putra Karo-Karo, and Bambang Widarto. "Penggunaan Alat Bukti Digital dalam Pembuktian Tindak Pidana Siber di Pengadilan Indonesia." *Judge: Jurnal Hukum* 6, no. 8 (2026): 1527–1538. <https://doi.org/10.54209/judge.v6i08.2213>.

- Pattiruhu, Fransisca Jallie. *Pendidikan Kewarganegaraan*. Yogyakarta: Deepublish, 2024.
- Putra, I Made Aditya Mantara. "Tanggungjawab Hukum Bank Terhadap Nasabah dalam Hal Terjadinya Kegagalan Transaksi pada Sistem Mobile Banking." *Kertha Wicaksana* 14, no. 2 (2020): 132–138. <https://doi.org/10.22225/kw.14.2.1921.132-138>.
- Sitorus, Angelia Pratiwi Mastiurlani Christina, and Agustinus Astono. "Aplikasi Whatsapp Bajakan sebagai Ancaman Kejahatan Siber di Indonesia." *Arus Jurnal Sosial dan Humaniora* 4, no. 1 (2024): 157–162. <https://doi.org/10.57250/ajsh.v4i1.355>.
- Sulistiyandari, Sulistiyandari, Ulil Afwa, Putri Ayu Sutrisno, and Rohaida Nordin. "Implementation of Prudential Banking Principles: State Responsibility in Combating Banking Crimes in Indonesia." *Volkgeist: Jurnal Ilmu Hukum dan Konstitusi* 7, no. 2 (2024): 341–359. <https://doi.org/10.24090/volkgeist.v7i2.12132>.
- Sutarli, Ananta Fadli, and Shelly Kurniawan. "Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi dalam Menanggulangi *Phishing* di Indonesia." *Innovative: Journal of Social Science Research* 3, no. 2 (2023): 4208–4221. <https://j-innovative.org/index.php/Innovative/article/view/760>.
- Syahrum, Muhammad. *Pengantar Metodologi Penelitian Hukum: Kajian Penelitian Normatif, Empiris, Penulisan Proposal, Laporan Skripsi dan Tesis*. Jambi: CV. DOTPLUS Publisher, 2022.
- Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
- Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
- Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.
- Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggara Sistem dan Transaksi Elektronik.
- Waliullah, Md., Md Zahin Hossain George, Md Tarek Hasan, Md Khorshed Alam, Mosa Sumaiya Khatun Munira, and Noor Alam Siddiqui. "Assessing the Influence of Cybersecurity Threats and Risks on the Adoption and Growth of Digital Banking: A Systematic Literature Review." *arXiv* (2025). <https://doi.org/10.48550/arXiv.2503.22710>.
- Wang, Xin. "Global (Re-)Framing of Cybercrime: An Emerging Common Interest in Flux of Competing Normative Powers?" *Leiden Journal of International Law* 38, no. 2 (2025): 235–261. <https://doi.org/10.1017/S0922156524000402>.
- Wulandari, Ida Ayu Sintya, I Wayan Rideng, and Luh Putu Suryani. "Sanksi Pidana dalam Tindak Pidana Pemilu terkait dengan Asas *Lex Specialis Derogate Legi Generali*." *Jurnal Konstruksi Hukum* 4, no. 3 (2023): 354–359. <https://doi.org/10.22225/jkh.4.3.8060.354-359>.
- Zia, Muhammad Fahad, and Sri Harish Kalidass. "Web Phishing Net (WPN): A Scalable Machine Learning Approach for Real-Time Phishing Campaign Detection." *arXiv* (2025). <https://doi.org/10.48550/arXiv.2502.13171>.