https://journaledutech.com/index.php/great
Global Research and Innovation Journal (GREAT)
Volume 2, Nomor 2, 2026, Hal. 1450-1460
e-ISSN : 3090-3289

PERLINDUNGAN HUKUM KORBAN TINDAK PIDANA PENIPUAN ELEKTRONIK *PHISHING* MELALUI APLIKASI WHATSAPP DALAM BENTUK *UNIFORM RESOURCE LOCATOR* (URL) ATAU FILE PALSU

Dinar Trisnaputri[1], Aris Yuni Pawestri[2]
Fakultas Hukum, Universitas Muhammadiyah Jember, Jember
E-mail: dinartrisnaputri@gmail.com[1]

ABSTRAK

Perkembangan teknologi juga membuka peluang munculnya kasus penipuan elektronik dan/atau kejahatan siber, termasuk *phishing*, yaitu penipuan digital melalui manipulasi *URL* atau file dokumen elektronik palsu. Istilah *phishing* memang belum diatur secara eksplisit dalam Undang-Undang Informasi dan Transaksi Elektronik maupun Kitab Undang-Undang Hukum Pidana. Namun, praktik *phishing* berkaitan erat dengan aspek keamanan sistem elektronik dan perlindungan data nasabah dalam kegiatan perbankan. Tingginya intensitas penggunaan WhatsApp di kalangan masyarakat menjadikan aplikasi tersebut sebagai salah satu sarana yang kerap dimanfaatkan oleh pelaku untuk melakukan tindak pidana penipuan elektronik "*phishing*". Pelaku biasanya mengirim pesan yang menyerupai pemberitahuan resmi dari instansi tertentu, disertai *URL* atau file dokumen yang tampak meyakinkan. Ketika korban membuka *URL* tersebut dan memasukkan data pribadi, pelaku dapat mengambil alih akses akun korban atau memperoleh informasi penting yang kemudian digunakan untuk tindakan penipuan lanjutan

Kata kunci **Perlindungan Hukum, Korban, Penipuan Elektronik *Phising***

ABSTRACT

Technological developments have also opened up opportunities for electronic fraud and/or cybercrime, including phishing, a digital fraud scheme involving the manipulation of URLs or fake electronic document files. The term phishing is not explicitly regulated in the Electronic Information and Transactions Law or the Criminal Code. However, phishing practices are closely related to the security of electronic systems and the protection of customer data in banking activities. The high level of WhatsApp usage among the public has made the application a frequent tool for perpetrators to commit electronic phishing fraud. Perpetrators typically send messages that resemble official notices from certain agencies, accompanied by a seemingly convincing URL or document file. When the victim opens the URL and enters personal data, the perpetrator can gain access to the victim's account or obtain important information that is then used for further fraudulent activities.

Keywords ***Legal Protection, Victims, Electronic Phishing Fraud***

1. PENDAHULUAN

Perkembangan teknologi informasi telah mengubah pola interaksi masyarakat dalam berbagai aspek kehidupan, termasuk komunikasi digital. Perubahan tersebut secara yuridis diakui dalam konsideran Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya di sebut UU ITE) yang menegaskan bahwa pemanfaatan teknologi informasi memberikan kontribusi

bagi peningkatan kesejahteraan dan peradaban masyarakat (Herman, 2024 :10). Salah satu bentuk pemanfaatannya adalah Penggunaan aplikasi komunikasi elektronik seperti WhatsApp termasuk dalam sistem elektronik sebagaimana dimaksud dalam Pasal 1 angka 5 UU ITE, karena memungkinkan pengiriman dan penyebaran informasi elektronik berupa pesan, dokumen, dan tautan sebagaimana diatur dalam Pasal 1 angka 1 dan angka 4 UU ITE.

Perkembangan teknologi juga membuka peluang munculnya kasus penipuan elektronik dan/atau kejahatan siber, termasuk *phishing*, yaitu penipuan digital melalui manipulasi *URL* atau file dokumen elektronik palsu. Istilah *phishing* memang belum diatur secara eksplisit dalam Undang-Undang Informasi dan Transaksi Elektronik maupun Kitab Undang-Undang Hukum Pidana. Namun, praktik *phishing* berkaitan erat dengan aspek keamanan sistem elektronik dan perlindungan data nasabah dalam kegiatan perbankan. Dalam Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan, khususnya Pasal 29 ayat (4), ditegaskan bahwa untuk kepentingan nasabah, bank wajib menyediakan informasi mengenai kemungkinan timbulnya risiko kerugian sehubungan dengan transaksi nasabah yang dilakukan melalui bank. Ketentuan tersebut menunjukkan adanya kewajiban perlindungan terhadap keamanan transaksi dan data nasabah dalam sistem perbankan. Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum, khususnya Pasal 1 angka 12, dijelaskan bahwa risiko keamanan merupakan risiko akibat kegagalan menjaga kerahasiaan, keutuhan, dan ketersediaan sistem informasi dan data bank. Ketentuan ini berkaitan dengan praktik *phishing* yang dilakukan melalui penyalahgunaan teknologi informasi untuk memperoleh data rahasia nasabah secara melawan hukum.

Praktiknya, *phishing* dilakukan dengan cara pelaku menyamar sebagai bank atau lembaga resmi melalui pesan elektronik seperti SMS, email, maupun WhatsApp untuk memperoleh data rahasia nasabah, seperti nomor rekening, PIN, password, OTP, dan kode keamanan, guna mengambil alih akun atau memperoleh keuntungan secara melawan hukum. Tindakan *phishing* melalui pengiriman *URL* atau file dokumen elektronik palsu dapat dikualifikasikan sebagai perbuatan melawan hukum karena memenuhi unsur manipulasi informasi elektronik sebagaimana diatur dalam Pasal 35 Undang-Undang Informasi dan Transaksi Elektronik, unsur akses tanpa hak terhadap sistem elektronik sebagaimana diatur dalam Pasal 30 Undang-Undang Informasi dan Transaksi Elektronik, serta unsur penipuan sebagaimana diatur dalam Pasal 378 Kitab Undang-Undang Hukum Pidana, yakni perbuatan dengan maksud menguntungkan diri sendiri atau orang lain secara melawan hukum melalui tipu muslihat atau rangkaian kebohongan.

Tingginya intensitas penggunaan WhatsApp di kalangan masyarakat menjadikan aplikasi tersebut sebagai salah satu sarana yang kerap dimanfaatkan oleh pelaku untuk melakukan tindak pidana penipuan elektronik "*phishing"*. Pelaku biasanya mengirim pesan yang menyerupai pemberitahuan resmi dari instansi tertentu, disertai *URL* atau file dokumen yang tampak meyakinkan. Ketika korban membuka *URL* tersebut dan memasukkan data pribadi, pelaku dapat mengambil alih akses akun korban atau memperoleh informasi penting yang kemudian digunakan untuk tindakan penipuan lanjutan (Detik Oto, 2025). Fenomena tersebut semakin nyata dengan meningkatnya kasus penipuan digital berbasis tautan palsu di Indonesia. Salah satu modus yang marak terjadi adalah pengiriman tautan palsu tilang elektronik melalui aplikasi WhatsApp. Pelaku mengirim pesan seolah-olah berasal dari sistem tilang elektronik resmi,

kemudian mengarahkan korban untuk membuka tautan tertentu. Setelah korban membuka tautan tersebut, data pribadi korban dapat diambil dan disalahgunakan oleh pelaku. Selain itu, terdapat korban yang mengalami kerugian materiil hingga jutaan rupiah akibat memasukkan data ke dalam situs palsu yang dikirim melalui pesan elektronik.[4] Fakta ini menunjukkan bahwa *phishing* tidak hanya mengancam keamanan data pribadi, tetapi juga menimbulkan kerugian ekonomi nyata bagi korban. Kondisi tersebut menegaskan bahwa negara memiliki kewajiban untuk memberikan perlindungan hukum kepada setiap warga negara dari segala bentuk ancaman dan kejahatan, termasuk kejahatan siber, sebagai perwujudan prinsip negara hukum (Rahma Agri Firdaus, 2024 : 9).

Berdasarkan fakta dan ketentuan hukum yang ada, terdapat beberapa kesenjangan hukum *(legal gap)* dalam pengaturan tindak pidana *phishing*. Pertama, belum adanya definisi khusus mengenai phishing dalam peraturan perundang-undangan menyebabkan kekosongan norma terhadap bentuk kejahatan ini. Kedua, perlindungan hukum terhadap korban masih lemah karena fokus pengaturan lebih diarahkan pada sanksi pelaku. Ketiga, Undang-Undang Informasi dan Transaksi Elektronik memang mengatur kejahatan berbasis teknologi, tetapi belum secara spesifik mengatur penipuan melalui *URL* atau file palsu. Keempat, Kitab Undang-Undang Hukum Pidana lebih mengatur penipuan konvensional sehingga belum cukup relevan untuk menjawab kompleksitas *phishing* berbasis digital. Berdasarkan uraian tersebut, diperlukan kajian yuridis mengenai bentuk perlindungan hukum terhadap korban tindak pidana penipuan elektronik "*phishing*" melalui aplikasi WhatsApp dalam bentuk URL atau file dokumen palsu. Meskipun telah terdapat beberapa penelitian yang membahas tindak pidana *phishing* dan perlindungan hukum dalam kejahatan siber, sebagian besar penelitian tersebut masih berfokus pada aspek pertanggungjawaban pidana pelaku dan pengaturan kejahatan siber secara umum. Berdasarkan beberapa hal tersebut di atas penulis mengidentifikasikan permasalahan yaitu ; Bagaimana bentuk Perlindungan Hukum Korban Tindak Pidana Penipuan Elektronik *Phishing* Melalui Aplikasi Whatsapp dalam Bentuk *Uniform Resource Locator* (URL) atau File Palsu?

Kajian ini penting untuk menilai sejauh mana regulasi yang ada mampu memberikan perlindungan hukum bagi korban, sekaligus menjadi dasar untuk merumuskan penguatan norma hukum yang lebih adaptif terhadap perkembangan kejahatan digital. Berdasarkan permasalahan tersebut, penelitian ini mengangkat judul "Perlindungan Hukum Korban Tindak Pidana Penipuan Elektronik *Phishing* Melalui Aplikasi Whatsapp dalam Bentuk *Uniform Resource Locator* (URL) atau File Palsu."

2. METODE PENELITIAN

Tipe penelitian yang digunakan adalah tipe penelitian yuridis empiris, dengan pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conseptual approarch*). Bahan hukum yang dipergunakan adalah bahan hukum primer dan bahan hukum sekunder. Metode analisis yang dipergunakan dalam penyusunan skripsi ini adalah analisa sumber data deduktif, yaitu suatu metode penelitian berdasarkan konsep atau teori yang bersifat umum diaplikasikan untuk menjelaskan tentang seperangkat data, atau menunjukkan komparasi atau hubungan seperangkat data dengan seperangkat data yang lain dengan sistematis berdasarkan kumpulan sumber data yang diperoleh, ditambahkan pendapat para sarjana yang mempunyai hubungan dengan bahan kajian sebagai bahan komparatif.

3. PEMBAHASAN

Perkembangan teknologi informasi dan komunikasi telah melahirkan berbagai bentuk kejahatan siber (*cyber crime*) yang memanfaatkan media elektronik sebagai sarana melakukan tindak pidana. Salah satu bentuk kejahatan siber yang semakin sering terjadi adalah tindak pidana *phishing*. *Phishing* merupakan bentuk penipuan elektronik yang dilakukan dengan cara memanipulasi korban melalui pesan, tautan, atau dokumen palsu agar korban memberikan data pribadi secara sukarela. Data tersebut kemudian digunakan pelaku untuk memperoleh keuntungan secara melawan hukum, seperti mengambil alih akun, mengakses layanan perbankan, atau melakukan transaksi tanpa izin pemilik akun (Hasanudin, 2025) Secara praktiknya, tindak pidana *phishing* sering dilakukan melalui pengiriman *Uniform Resource Locator* (URL) atau file dokumen palsu. (URL) *Uniform Resource Locator* merupakan alamat atau tautan yang digunakan untuk mengakses suatu halaman atau sumber daya di internet. Pelaku biasanya membuat URL yang menyerupai situs resmi milik bank, instansi pemerintah, atau platform digital tertentu agar korban percaya dan membuka tautan tersebut. Selain menggunakan URL palsu, pelaku juga sering mengirim file dokumen palsu dalam bentuk PDF, APK, atau dokumen elektronik lain yang tampak meyakinkan. File tersebut umumnya mengandung malware atau mengarahkan korban menuju situs palsu yang digunakan untuk mencuri data pribadi korban. (Dharani, Indrayanti, 2025)

Penggunaan WhatsApp sebagai media komunikasi elektronik turut mempermudah terjadinya tindak pidana *phishing*. WhatsApp merupakan aplikasi berbasis internet yang memungkinkan pengguna mengirim pesan, dokumen, gambar, video, maupun tautan elektronik secara cepat dan luas. Tingginya penggunaan WhatsApp di masyarakat menjadikan aplikasi ini sering dimanfaatkan pelaku kejahatan siber untuk menyebarkan tautan palsu dan dokumen elektronik palsu. Kemudahan komunikasi digital melalui WhatsApp membuat pelaku lebih mudah menjangkau korban tanpa harus bertemu secara langsung. Tindak pidana *phishing* memiliki karakteristik yang termasuk dalam kategori kejahatan siber (*cyber crime*). Kejahatan siber merupakan tindak pidana yang memanfaatkan sistem elektronik, jaringan internet, dan teknologi informasi sebagai sarana melakukan perbuatan melawan hukum. Karakteristik utama kejahatan siber terletak pada penggunaan media elektronik, sifatnya yang dapat dilakukan tanpa batas wilayah, serta sulitnya identifikasi pelaku karena memanfaatkan identitas digital dan teknologi jaringan internet. Kondisi tersebut menyebabkan tindak pidana *phishing* menjadi salah satu bentuk kejahatan yang sulit dicegah dan ditangani (Risma Novia : 2024)

Modus operandi *phishing* melalui WhatsApp dilakukan dengan berbagai cara untuk mengelabui korban. Pelaku biasanya mengirim pesan yang menyerupai pemberitahuan resmi dari bank, marketplace, jasa pengiriman, atau instansi pemerintah tertentu. Pesan tersebut disertai tautan palsu yang mengarahkan korban menuju situs tiruan. Pelaku juga sering mengirim file APK atau dokumen palsu yang apabila dibuka dapat mengambil data dalam perangkat korban. Modus lain dilakukan dengan meminta kode OTP, PIN, atau password melalui pesan elektronik. Data tersebut kemudian digunakan pelaku untuk mengambil alih akun korban, mengakses layanan perbankan digital, atau melakukan transaksi ilegal menggunakan identitas korban (Risma Novia : 2025)

Tindak pidana *phishing* menimbulkan berbagai dampak bagi korban, baik secara materiil maupun nonmateriil. Korban dapat mengalami kerugian ekonomi akibat hilangnya saldo rekening atau penyalahgunaan akun digital. Penyalahgunaan data pribadi juga dapat mengancam privasi dan keamanan korban karena data yang diperoleh pelaku dapat digunakan untuk tindak pidana lain. Kondisi tersebut menimbulkan hilangnya rasa

aman dalam penggunaan teknologi digital, terutama dalam aktivitas komunikasi dan transaksi elektronik melalui internet. Kondisi tersebut menunjukkan bahwa tindak pidana *phishing* tidak hanya menimbulkan kerugian ekonomi, tetapi juga mengancam keamanan dan perlindungan data pribadi masyarakat dalam penggunaan teknologi digital (Rahmanto, 2025). Permasalahan tersebut kemudian mendorong pentingnya pengaturan hukum yang mampu memberikan perlindungan terhadap korban tindak pidana *phishing* melalui media elektronik.

Pengaturan hukum terhadap tindak pidana *phishing* di Indonesia pada dasarnya tersebar dalam beberapa peraturan perundang-undangan yang mengatur mengenai perlindungan hak warga negara, penggunaan teknologi informasi, perlindungan data pribadi, serta tindak pidana penipuan. Pengaturan tersebut menjadi dasar hukum dalam memberikan perlindungan terhadap korban tindak pidana *phishing* yang dilakukan melalui media elektronik, termasuk melalui aplikasi WhatsApp. Pengaturan lebih khusus mengenai tindak pidana *phishing* terdapat dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang- Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pasal 30 mengatur mengenai larangan akses tanpa hak terhadap komputer atau sistem elektronik milik orang lain. Ketentuan tersebut berkaitan dengan tindakan pelaku *phishing* yang memperoleh akses terhadap akun atau data korban secara melawan hukum. Pasal 35 mengatur larangan manipulasi, penciptaan, perubahan, penghilangan, atau perusakan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi tersebut dianggap seolah-olah data yang autentik. Ketentuan tersebut relevan dengan modus *phishing* yang menggunakan tautan atau dokumen palsu untuk mengelabui korban. Pasal 5 menyatakan bahwa informasi elektronik, dokumen elektronik, dan hasil cetaknya merupakan alat bukti hukum yang sah. Ketentuan tersebut memberikan dasar hukum penggunaan bukti digital dalam proses pembuktian tindak pidana *phishing*.

Pengaturan mengenai unsur penipuan dalam tindak pidana *phishing* juga terdapat dalam Kitab Undang-Undang Hukum Pidana. Pasal 378 KUHP menyebutkan bahwa setiap orang yang dengan maksud menguntungkan diri sendiri atau orang lain secara melawan hukum menggunakan nama palsu, tipu muslihat, atau rangkaian kebohongan untuk menggerakkan orang lain menyerahkan barang, memberi utang, atau menghapus piutang dapat dipidana karena penipuan. Ketentuan tersebut berkaitan dengan modus *phishing* yang dilakukan melalui penyamaran identitas, pengiriman pesan palsu, dan manipulasi informasi elektronik

Perlindungan terhadap data pribadi korban diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Undang-undang ini memberikan perlindungan terhadap data pribadi setiap individu dari penyalahgunaan secara melawan hukum. Pasal 65 ayat (1) menyatakan bahwa setiap orang dilarang memperoleh atau mengumpulkan data pribadi yang bukan miliknya secara melawan hukum. Ketentuan tersebut berkaitan dengan tindakan pelaku *phishing* yang mengambil data pribadi korban melalui tautan atau dokumen elektronik palsu. Perlindungan data pribadi menjadi penting karena tindak pidana *phishing* umumnya bertujuan memperoleh informasi pribadi korban untuk digunakan secara ilegal. Pengaturan mengenai hak korban tindak pidana diatur dalam Undang-Undang Nomor 31 Tahun 2014 tentang Perlindungan Saksi dan Korban. Pasal 5 ayat (1) memberikan hak kepada korban untuk memperoleh perlindungan atas keamanan pribadi, keluarga, dan harta bendanya, serta hak untuk memberikan keterangan tanpa tekanan dalam proses peradilan pidana. Pasal 7A ayat (1) juga mengatur bahwa korban tindak pidana berhak memperoleh restitusi berupa ganti kerugian atas kehilangan kekayaan atau penghasilan, penderitaan yang

ditimbulkan akibat tindak pidana, dan/atau biaya perawatan medis maupun psikologis.

Ketentuan tersebut menunjukkan bahwa korban tindak pidana *phishing* berhak memperoleh perlindungan hukum, pendampingan selama proses hukum, serta pemulihan atas kerugian yang dialaminya. Restitusi diberikan sebagai bentuk ganti kerugian yang dibebankan kepada pelaku tindak pidana untuk memulihkan hak-hak korban yang telah dirugikan akibat perbuatan tersebut. Pengaturan mengenai perlindungan data nasabah dan keamanan sistem perbankan diatur dalam Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan dan Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016. Pasal 40 ayat (1) UU Perbankan mewajibkan bank merahasiakan keterangan mengenai nasabah penyimpan dan simpanannya. Sehingga data nasabah memperoleh perlindungan hukum dari penyalahgunaan oleh pihak yang tidak berwenang.

Perlindungan terhadap data nasabah dan keamanan sistem perbankan diperkuat melalui POJK Nomor 38/POJK.03/2016 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum. Pasal 2 ayat (1) mewajibkan bank menerapkan manajemen risiko dalam penggunaan teknologi informasi, sedangkan Pasal 19 mengatur kewajiban bank menjaga kerahasiaan, integritas, dan ketersediaan data serta informasi. Pengaturan tersebut bertujuan mencegah risiko penyalahgunaan teknologi informasi, termasuk tindak pidana *phishing* yang dapat mengakibatkan pencurian data pribadi, pengambilalihan akun, dan kerugian finansial bagi nasabah. Menurut Philipus M. Hadjon, upaya pencegahan melalui pengaturan dan pengawasan merupakan bentuk perlindungan preventif yang bertujuan melindungi hak masyarakat sebelum terjadi pelanggaran. Pengaturan dalam POJK tersebut merupakan salah satu bentuk perlindungan preventif terhadap nasabah dari ancaman *phishing* dan kejahatan siber lainnya.

Risiko keamanan digital yang ditimbulkan oleh tindak pidana *phishing* menunjukkan bahwa perlindungan hukum terhadap korban masih menjadi persoalan penting dalam perkembangan kejahatan siber. Pengaturan hukum mengenai tindak pidana *phishing* di Indonesia pada dasarnya telah tersebar dalam beberapa peraturan perundang-undangan. Kondisi tersebut belum sepenuhnya mampu memberikan perlindungan hukum yang optimal terhadap korban. Perkembangan kejahatan digital berlangsung lebih cepat dibanding perkembangan regulasi yang ada, sehingga masih ditemukan berbagai kelemahan pengaturan dan hambatan dalam penegakan hukum terhadap tindak pidana *phishing* melalui aplikasi WhatsApp.

Kelemahan pertama terletak pada belum adanya definisi khusus mengenai *phishing* dalam peraturan perundang-undangan di Indonesia. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik maupun Kitab Undang-Undang Hukum Pidana tidak memberikan pengertian secara eksplisit mengenai tindak pidana *phishing*. Kondisi tersebut menyebabkan kekaburan norma dalam menentukan ruang lingkup perbuatan, karakteristik tindak pidana, serta bentuk pertanggungjawaban pidana pelaku. Penegak hukum akhirnya menggunakan ketentuan umum mengenai akses ilegal, manipulasi informasi elektronik, dan penipuan untuk menjerat pelaku *phishing*.

Kekaburan norma juga terlihat dalam pengaturan mengenai URL atau file dokumen palsu sebagai sarana kejahatan. Regulasi yang ada belum secara spesifik mengatur penggunaan tautan palsu, file APK berbahaya, maupun dokumen elektronik palsu dalam tindak pidana *phishing*. Pasal 35 UU ITE memang mengatur manipulasi informasi elektronik agar dianggap autentik, namun ketentuan tersebut belum

menjelaskan secara rinci bentuk dan karakteristik kejahatan berbasis URL atau file palsu yang berkembang di masyarakat digital. Pengaturan dalam UU ITE masih bersifat umum terhadap kejahatan berbasis teknologi informasi. Pasal 30 mengatur akses tanpa hak terhadap sistem elektronik, sedangkan Pasal 35 mengatur manipulasi informasi elektronik.

Ketentuan tersebut belum secara khusus mengatur modus *phishing* yang dilakukan melalui penyamaran identitas, pengiriman tautan palsu, maupun pencurian OTP melalui aplikasi pesan elektronik. Kondisi tersebut menunjukkan bahwa pengaturan hukum belum sepenuhnya adaptif terhadap perkembangan modus kejahatan siber. Kelemahan lain terdapat dalam pengaturan Kitab Undang-Undang Hukum Pidana yang masih berorientasi pada penipuan konvensional. Pasal 378 KUHP mengatur penipuan melalui tipu muslihat dan rangkaian kebohongan untuk memperoleh keuntungan secara melawan hukum. Ketentuan tersebut lebih ditujukan pada kejahatan yang dilakukan secara langsung atau konvensional. Karakteristik tindak pidana *phishing* memiliki kompleksitas berbeda karena dilakukan melalui sistem elektronik, jaringan internet, serta identitas digital yang sulit dilacak.

Perlindungan hukum terhadap korban juga masih tergolong lemah karena regulasi lebih banyak berfokus pada pemberian sanksi terhadap pelaku dibanding pemulihan hak korban. Pengaturan mengenai restitusi, kompensasi, dan pemulihan kerugian korban belum berjalan optimal dalam praktik. Korban tindak pidana *phishing* sering mengalami kesulitan memperoleh kembali kerugian materiil akibat lambatnya proses hukum dan sulitnya pelacakan aset pelaku. Hambatan lain dalam penegakan hukum terletak pada sulitnya pelacakan pelaku kejahatan siber. Pelaku *phishing* umumnya menggunakan identitas palsu, jaringan virtual, akun anonim, dan sistem elektronik lintas wilayah. Kondisi tersebut menyebabkan aparat penegak hukum mengalami kesulitan dalam melakukan identifikasi dan penangkapan pelaku. Karakteristik kejahatan siber yang tidak mengenal batas wilayah juga mempersulit proses penegakan hukum apabila pelaku berada di luar yurisdiksi Indonesia.

Rendahnya literasi digital masyarakat turut menjadi hambatan dalam pencegahan tindak pidana *phishing*. Banyak pengguna teknologi digital yang belum memahami bentuk tautan palsu, file APK berbahaya, maupun modus pencurian data pribadi melalui media elektronik. Kondisi tersebut menyebabkan masyarakat mudah menjadi korban penipuan digital karena kurang berhati-hati dalam membuka tautan atau memberikan data pribadi kepada pihak lain. Lemahnya pemulihan kerugian korban juga menjadi salah satu kelemahan perlindungan hukum terhadap tindak pidana *phishing*. Korban sering mengalami kerugian materiil berupa hilangnya saldo rekening, penyalahgunaan akun digital, maupun pencurian data pribadi. Proses pengembalian kerugian korban sering tidak berjalan efektif karena pelaku sulit ditemukan atau aset hasil kejahatan telah dipindahkan melalui sistem elektronik.

Berbagai kelemahan dan hambatan tersebut menunjukkan adanya kesenjangan hukum (*legal gap*) dalam pengaturan tindak pidana *phishing* di Indonesia. Kondisi tersebut memperlihatkan bahwa regulasi yang ada belum sepenuhnya mampu memberikan perlindungan hukum yang optimal terhadap korban tindak pidana *phishing* melalui WhatsApp dalam bentuk URL atau file dokumen palsu. Keadaan ini menjadi alasan penting perlunya kajian hukum yang lebih mendalam mengenai bentuk perlindungan hukum terhadap korban kejahatan digital berbasis *phishing*. Perlindungan hukum terhadap korban masih menjadi persoalan penting dalam perkembangan kejahatan siber. Pengaturan hukum mengenai tindak pidana *phishing* di Indonesia pada dasarnya telah tersebar dalam beberapa peraturan perundang-undangan. Kebutuhan

pembaruan hukum tersebut menunjukkan bahwa perlindungan hukum terhadap korban tindak pidana *phishing* tidak hanya memerlukan pengaturan yang jelas, tetapi juga mekanisme perlindungan yang efektif bagi korban kejahatan digital.

Perlindungan hukum terhadap korban tindak pidana *phishing* melalui aplikasi WhatsApp pada dasarnya dilakukan melalui dua bentuk perlindungan,yaitu perlindungan hukum preventif dan perlindungan hukum represif. Konsep tersebut sejalan dengan teori perlindungan yang dikemukakan oleh Philipus M. Hadjon yang membedakan perlindungan hukum menjadi perlindungan preventif dan perlindungan represif. Perlindungan preventif bertujuan mencegah terjadinya pelanggaran hukum, sedangkan perlindungan represif bertujuan menyelesaikan sengketa dan memberikan perlindungan setelah terjadinya pelanggaran.

a. Perlindungan Hukum Preventif

Perlindungan hukum preventif merupakan bentuk perlindungan yang dilakukan sebelum terjadinya tindak pidana. Perlindungan ini bertujuan mencegah masyarakat menjadi korban phishing melalui pengawasan, pengamanan sistem elektronik, serta peningkatan kesadaran digital masyarakat. Bentuk perlindungan preventif menjadi penting karena tindak pidana phishing berkembang melalui pemanfaatan teknologi informasi dan kelemahan keamanan digital pengguna. Pengawasan terhadap sistem elektronik menjadi salah satu bentuk perlindungan preventif dalam mencegah tindak pidana phishing. Pengawasan tersebut dilakukan oleh pemerintah, penyelenggara sistem elektronik, lembaga perbankan, serta penyedia layanan digital untuk menjaga keamanan sistem dari akses tanpa hak, manipulasi data, dan penyalahgunaan informasi elektronik. Pasal 16 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024 mengatur bahwa penyelenggara sistem elektronik wajib menyelenggarakan sistem elektronik secara andal, aman, dan bertanggung jawab. Kewajiban tersebut diwujudkan melalui penerapan sistem keamanan, pemantauan aktivitas mencurigakan, serta pembaruan sistem secara berkala guna mencegah penyalahgunaan teknologi informasi. Perlindungan data pribadi pengguna juga menjadi bentuk perlindungan preventif terhadap korban phishing. Perlindungan tersebut dilakukan oleh pengendali data pribadi dan pemroses data pribadi melalui pengamanan informasi pengguna agar tidak diperoleh, digunakan, atau disebarluaskan secara melawan hukum. Pasal 65 ayat (1) Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi melarang setiap orang memperoleh atau mengumpulkan data pribadi yang bukan miliknya secara melawan hukum. Data berupa nomor telepon, nomor rekening, password, PIN, dan kode OTP merupakan informasi yang paling sering menjadi sasaran pelaku phishing sehingga memerlukan perlindungan yang memadai.

Edukasi dan literasi digital masyarakat memiliki peran penting dalam mencegah tindak pidana phishing. Upaya tersebut dilakukan oleh pemerintah, lembaga perbankan, penyelenggara sistem elektronik, serta berbagai lembaga terkait melalui sosialisasi mengenai ciri-ciri tautan palsu, file APK berbahaya, pesan penipuan yang mengatasnamakan instansi resmi, serta bahaya memberikan data pribadi kepada pihak lain. Peningkatan literasi digital bertujuan agar masyarakat mampu mengenali modus phishing sejak awal dan menghindari tindakan yang dapat menimbulkan kerugian. Pemblokiran tautan atau situs palsu juga menjadi bagian dari perlindungan preventif terhadap korban phishing. Pemerintah melalui kementerian yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika bersama penyelenggara sistem elektronik dapat melakukan pemutusan akses terhadap situs atau URL yang terindikasi digunakan untuk penipuan atau pencurian data pribadi. Tindakan tersebut

bertujuan mengurangi penyebaran tautan berbahaya serta mencegah munculnya korban baru akibat tindak pidana phishing.

Kewajiban penyelenggara sistem elektronik menjaga keamanan data pengguna menjadi bentuk perlindungan preventif lainnya. Penyelenggara sistem elektronik wajib menjaga kerahasiaan, keutuhan, dan ketersediaan data pengguna yang berada dalam penguasaannya. Pengamanan tersebut dilakukan melalui penggunaan teknologi enkripsi, autentikasi berlapis, sistem verifikasi identitas pengguna, serta pemantauan aktivitas mencurigakan dalam sistem elektronik. Tanggung jawab tersebut merupakan bagian dari upaya memberikan rasa aman kepada masyarakat dalam menggunakan layanan digital.

Pencegahan penyalahgunaan akun dan kode OTP juga menjadi bagian penting dalam perlindungan preventif terhadap tindak pidana phishing. Bank dan penyelenggara layanan digital umumnya menggunakan OTP sebagai bentuk autentikasi tambahan untuk memastikan bahwa transaksi dilakukan oleh pemilik akun yang sah. Penyalahgunaan OTP dapat menyebabkan pelaku mengambil alih akun korban dan mengakses layanan elektronik secara ilegal. Pencegahan dilakukan melalui edukasi kepada masyarakat agar tidak memberikan kode OTP, PIN, password, maupun informasi perbankan kepada pihak lain karena informasi tersebut sering digunakan pelaku untuk mengambil alih akun dan melakukan transaksi tanpa izin pemiliknya. Uraian tersebut menunjukkan bahwa perlindungan hukum preventif terhadap korban tindak pidana phishing tidak hanya menjadi tanggung jawab negara, tetapi juga melibatkan penyelenggara sistem elektronik, lembaga perbankan, dan masyarakat sebagai pengguna teknologi digital. Pendekatan tersebut sejalan dengan teori perlindungan hukum preventif menurut Philipus M. Hadjon yang menempatkan pencegahan sebagai langkah utama untuk menghindari terjadinya pelanggaran dan kerugian sebelum sengketa atau tindak pidana terjadi. Upaya preventif tidak hanya dilakukan melalui pengamanan sistem elektronik dan perlindungan data pribadi, tetapi juga melalui penyediaan mekanisme pelaporan dini terhadap dugaan tindak pidana phishing. Pengguna yang menerima pesan mencurigakan berupa URL, file dokumen, atau permintaan kode OTP dianjurkan untuk tidak membuka tautan maupun memberikan data pribadi kepada pihak yang tidak dikenal. Bukti berupa tangkapan layar percakapan, nomor telepon pelaku, tautan elektronik, maupun dokumen yang diterima perlu disimpan sebagai langkah antisipatif apabila tindak pidana benar-benar terjadi. Masyarakat dapat melaporkan nomor telepon, tautan, atau situs yang diduga digunakan untuk melakukan phishing kepada penyelenggara sistem elektronik, penyedia layanan perbankan, maupun instansi pemerintah yang berwenang. Pelaporan dini memungkinkan dilakukan pemblokiran terhadap nomor, akun, maupun situs yang digunakan pelaku sehingga potensi kerugian terhadap masyarakat dapat diminimalkan. Mekanisme tersebut merupakan bentuk perlindungan preventif karena bertujuan mencegah timbulnya korban baru akibat tindak pidana phishing.

b. Perlindungan Hukum Represif

Perlindungan hukum represif merupakan bentuk perlindungan yang diberikan setelah terjadinya tindak pidana phishing. Perlindungan ini diwujudkan melalui penegakan hukum terhadap pelaku, pemberian sanksi pidana, perlindungan terhadap korban selama proses peradilan, serta pemulihan hak dan kerugian korban. Konsep tersebut sejalan dengan teori perlindungan represif menurut Philipus M. Hadjon yang menempatkan penyelesaian sengketa melalui mekanisme hukum sebagai sarana untuk mengembalikan hak pihak yang dirugikan akibat suatu pelanggaran hukum. Upaya represif diawali dengan tindakan penyelidikan dan penyidikan oleh Kepolisian Negara Republik Indonesia terhadap dugaan tindak pidana phishing yang dilakukan melalui aplikasi WhatsApp. Proses tersebut dilanjutkan dengan penuntutan oleh kejaksaan dan

pemeriksaan perkara oleh pengadilan sampai diperoleh putusan yang berkekuatan hukum tetap.

Rangkaian proses tersebut bertujuan memberikan kepastian hukum bagi korban sekaligus menjatuhkan pertanggungjawaban pidana kepada pelaku tindak pidana phishing. Penegakan hukum terhadap pelaku phishing dilakukan melalui penerapan ketentuan pidana dalam beberapa peraturan perundang-undangan. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik digunakan untuk menjerat pelaku yang melakukan akses ilegal terhadap sistem elektronik dan manipulasi informasi elektronik.

Pasal 30 mengatur larangan mengakses komputer dan sistem elektronik milik orang lain tanpa hak atau melawan hukum. Pasal 35 mengatur larangan melakukan manipulasi, penciptaan, perubahan, penghilangan, atau perusakan informasi elektronik dan dokumen elektronik dengan tujuan agar data tersebut dianggap seolah-olah autentik. Penerapan sanksi pidana terhadap pelaku phishing juga dapat menggunakan Kitab Undang-Undang Hukum Pidana, khususnya Pasal 378 mengenai tindak pidana penipuan. Ketentuan tersebut berkaitan dengan penggunaan nama palsu, tipu muslihat, maupun rangkaian kebohongan untuk memperoleh keuntungan secara melawan hukum. Penyalahgunaan data pribadi korban dapat dijerat menggunakan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi karena pelaku memperoleh dan menggunakan data pribadi milik korban tanpa hak dan secara melawan hukum. Perlindungan terhadap korban selama proses peradilan menjadi bagian penting dalam perlindungan represif. Undang-Undang Nomor 31 Tahun 2014 tentang Perlindungan Saksi dan Korban memberikan hak kepada korban untuk memperoleh perlindungan atas keamanan pribadi, keluarga, dan harta bendanya serta hak memperoleh pendampingan dan bantuan selama proses hukum berlangsung.

4. KESIMPULAN

Berdasarkan uraian di bab pembahasan maka dapat disimpulkan sebagai berikut: Bentuk perlindungan hukum terhadap korban tindak pidana phishing melalui aplikasi WhatsApp dalam bentuk URL atau file dokumen palsu terdiri atas perlindungan hukum preventif dan perlindungan hukum represif. Perlindungan preventif diwujudkan melalui pengamanan sistem elektronik, perlindungan data pribadi, penerapan manajemen risiko teknologi informasi, edukasi dan literasi digital masyarakat, serta pemblokiran tautan atau situs palsu yang berpotensi digunakan dalam tindak pidana phishing. Perlindungan represif diwujudkan melalui pelaporan kepada aparat penegak hukum, penegakan hukum terhadap pelaku, pemberian sanksi pidana, penggunaan alat bukti elektronik dalam proses pembuktian, perlindungan korban selama proses peradilan, serta pemulihan kerugian melalui mekanisme restitusi dan kompensasi. Namun, perlindungan tersebut belum optimal karena belum terdapat pengaturan khusus mengenai tindak pidana phishing dan perlindungan korban masih lebih berorientasi pada penghukuman pelaku daripada pemulihan hak korban.

Berdasarkan hasil penelitian, pemerintah perlu membentuk pengaturan yang lebih spesifik mengenai tindak pidana *phishing* guna memberikan kepastian hukum dan perlindungan yang lebih optimal bagi korban. Aparat penegak hukum perlu meningkatkan efektivitas penegakan hukum terhadap kejahatan siber melalui penguatan kemampuan investigasi digital. Penyelenggara sistem elektronik dan sektor perbankan perlu memperkuat keamanan sistem serta meningkatkan edukasi kepada pengguna. Masyarakat juga perlu meningkatkan literasi digital dan kehati-hatian dalam penggunaan

teknologi informasi untuk mencegah menjadi korban tindak pidana *phishing*.

5. DAFTAR PUSTAKA

A.Z Nasution, Perkembangan Hukum Perlindungan Konsumen di Indonesia, Rajawali Grafindo Persada, Jakarta, 2006

Abdul Rasyid Thalib, S.H.M.H., and P.T.C.A. BAKTI. *Wewenang Mahkamah Konstitusi & Implikasinya Dalam Sistem Ketatanegaraan RI*. Citra Aditya Bakti, 2006. https://books.google.co.id/books?id=JgUrDwAAQBAJ.

H. M. Syarifuddin, S.H.M.H. *Prinsip Keadilan Dalam Mengadili Perkara Tindak Pidana Korupsi: Implementasi PERMA Nomor 1 Tahun 2020*. Prenada Media, 2020. https://books.google.co.id/books?id=bxRNEAAAQBAJ

Kaharuddin, M H. *Ilmu Peraturan Perundang-Undangan: Pemahaman Dasar Dan Struktur Hukum*. Prenada Media, 2025. https://books.google.co.id/books?id=QZWMEQAAQBAJ.

Fardiansyah, H, N D Rizkia, M S Is, F F Busroh, F N Lobo, F M Pratama, A Triyono, A Wau, and F Khairo. *PENGANTAR ILMU HUKUM*. CV. Intelektual Manifes Media, 2023. https://books.google.co.id/books?id=GEi9EAAAQBAJ.

Fuady, Munir. *Hukum Internet Indonesia*. Jakarta: Citra Aditya Bakti, 2006. https://books.google.com/books?q=Munir+Fuady+Hukum+Internet+Indones ia.

Hadjon, Philipus M. *Perlindungan Hukum Bagi Rakyat Di Indonesia: Sebuah Studi Tentang Prinsip-Prinsipnya, Penanganannya Oleh Pengadilan Dalam Lingkungan Peradilan Umum Dan Pembentukan Peradilan Administrasi Negara. Surabaya: Bina Ilmu, 1987.*

Harahap, M Yahya. Hukum Acara Pidana. Jakarta: Sinar Grafika, 2010. https://books.google.com/books?q=M.+Yahya+Harahap+Hukum+Acara+Pid ana.

Muladi. Hak-Hak Korban Kejahatan. Semarang: UNDIP, 2001. https://books.google.com/books?q=Muladi+Hak-Hak+Korban+Kejahatan.

Hadjon, Philipus M. Perlindungan Hukum Bagi Rakyat Di Indonesia: Sebuah Studi Tentang Prinsip-Prinsipnya, Penanganannya Oleh Pengadilan Dalam Lingkungan Peradilan Umum Dan Pembentukan Peradilan Administrasi Negara. Surabaya: Bina Ilmu, 1987.

Prof. RA. Retno Murni, S.H.M.H., P Kolega, and D M Pustaka. Pemikiran Komprehensif Hukum Bisnis: Menjawab Tantangan Digitalisasi. Divya Media Pustaka, 2025. https://books.google.co.id/books?id=juGzEQAAQBAJ.