

BAB I PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi informasi telah mengubah pola interaksi masyarakat dalam berbagai aspek kehidupan, termasuk komunikasi digital.¹ 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.² 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

¹ Herman Herman, “Pengaruh Komunikasi Digital Terhadap Pola Komunikasi Pada Nilai-Nilai Budaya Masyarakat Modern,” *Professional: Jurnal Komunikasi Dan Administrasi Publik* 11, No. 2 (2024): 505–10.

² Republik Indonesia, “Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik,” Database Peraturan Bpk § (2008), <https://Peraturan.Bpk.Go.Id/Details/37589/Uu-No-11-Tahun-2008>.

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.

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.³ 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

³ Tim Detikoto, "Masih Ada Penipuan Modus Tilang Elektronik Di Whatsapp, Jangan Asal Klik Link," *Detikoto*, 2025, <https://Oto.Detik.Com/Berita/D-8364091/Masih-Ada-Penipuan-Modus-Tilang-Elektronik-Di-Watsapp-Jangan-Asal-Klik-Link>.

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.⁵ Prinsip tersebut ditegaskan dalam Pasal 1 ayat (3) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 yang menyatakan bahwa Indonesia adalah negara hukum, sehingga segala tindakan penyelenggaraan negara harus berorientasi pada perlindungan hak warga negara berdasarkan hukum. Jaminan perlindungan tersebut diperkuat dalam Pasal 28D ayat (1) UUD 1945 yang menegaskan bahwa setiap orang berhak atas pengakuan, jaminan, perlindungan, dan kepastian hukum yang adil, serta Pasal 28G ayat (1) UUD 1945 yang menyatakan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, harta benda, serta rasa aman dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.

Perlindungan hukum dalam konteks kejahatan digital terhadap penyalahgunaan teknologi informasi diatur dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, khususnya Pasal 30 mengenai larangan

⁴ Detikoto.

⁵ Rahma Agri Firdaus, "Perlindungan Hukum Dan Pencegahan Kejahatan Siber Di Era Digital Dalam Sistem Hukum Di Indonesia," *Staatsrecht: Jurnal Hukum Kenegaraan Dan Politik Islam* 4, No. 1 (2024): 79–104.

akses tanpa hak terhadap sistem elektronik dan Pasal 35 mengenai larangan manipulasi informasi elektronik dengan tujuan agar data tersebut dianggap otentik. Selain itu, perlindungan terhadap data pribadi korban diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, khususnya Pasal 65 ayat (1) yang melarang setiap orang memperoleh atau mengumpulkan data pribadi yang bukan miliknya secara melawan hukum. Adapun unsur penipuan dalam tindak pidana *phishing* juga dapat dijerat berdasarkan Pasal 378 Kitab Undang-Undang Hukum Pidana, yaitu perbuatan dengan maksud menguntungkan diri sendiri atau orang lain secara melawan hukum dengan menggunakan nama palsu, tipu muslihat, atau rangkaian kebohongan. Dengan demikian, sistem hukum di Indonesia secara normatif telah menyediakan landasan hukum bagi perlindungan warga negara terhadap tindak pidana *phishing*, baik melalui instrumen hukum pidana umum maupun melalui regulasi khusus di bidang teknologi informasi dan perlindungan data pribadi.

Pengaturan hukum dalam Undang-Undang Informasi dan Transaksi Elektronik maupun Kitab Undang-Undang Hukum Pidana masih belum secara spesifik mengatur tindak pidana *phishing*, terutama yang dilakukan melalui pengiriman *URL* atau file dokumen palsu melalui aplikasi WhatsApp. Tidak adanya definisi normatif mengenai *phishing* menyebabkan kekaburan norma dalam menentukan ruang lingkup perbuatan, pertanggungjawaban pidana pelaku, serta bentuk perlindungan hukum bagi korban. Kondisi ini menunjukkan bahwa perkembangan kejahatan digital berlangsung lebih cepat dibandingkan perkembangan regulasi yang ada.

Ditinjau dari asas hukum, perlindungan terhadap korban tindak pidana *phishing* seharusnya didasarkan pada asas kepastian hukum, asas keadilan, dan asas perlindungan hukum. Asas kepastian hukum menghendaki adanya aturan yang jelas mengenai larangan dan sanksi terhadap perbuatan *phishing*.⁶ Asas keadilan menuntut agar korban mendapatkan pemulihan atas kerugian yang dialami,⁷ sedangkan asas perlindungan hukum menegaskan kewajiban negara untuk melindungi hak korban dari ancaman penyalahgunaan teknologi.⁸ Namun dalam praktiknya, perlindungan terhadap korban masih lemah karena regulasi yang ada lebih menitikberatkan pada pemberian sanksi terhadap pelaku dibandingkan pemulihan hak korban.

Philipus M. Hadjon menjelaskan secara teoritis, perlindungan hukum merupakan perlindungan terhadap harkat dan martabat, serta pengakuan terhadap hak-hak asasi manusia yang dimiliki oleh subjek hukum berdasarkan ketentuan hukum dari tindakan kesewenang-wenangan. Philipus M. Hadjon juga menjelaskan bahwa perlindungan hukum bagi masyarakat terdiri atas dua bentuk, yaitu perlindungan hukum preventif dan perlindungan hukum represif. Perlindungan hukum preventif diberikan untuk mencegah terjadinya pelanggaran melalui pengaturan dan pengawasan, sedangkan perlindungan hukum represif diberikan setelah terjadi pelanggaran melalui penyelesaian sengketa dan penegakan hukum.⁹

⁶ Kaharuddin, *Ilmu Peraturan Perundang-Undangan: Pemahaman Dasar Dan Struktur Hukum* (Prenada Media, 2025), <https://books.google.co.id/books?id=Qzwmqaaqbaj>.Hlm.29.

⁷ Syarifuddin, *Prinsip Keadilan Dalam Mengadili Perkara Tindak Pidana Korupsi: Implementasi Perma Nomor 1 Tahun 2020* (Prenada Media, 2020), <https://books.google.co.id/books?id=Bxrneaaqbaj>.Hlm 200.

⁸ H Fardiansyah Et Al., *Pengantar Ilmu Hukum* (Cv. Intelektual Manifes Media, 2023), <https://books.google.co.id/books?id=Gei9eaaqbaj>.Hlm 150.

⁹ M. Hajon Dalam Abdul Rasyid Thalib And P.T.C.A. Bakti, *Wewenang Mahkamah Konstitusi & Implikasinya Dalam Sistem Ketatanegaraan Ri* (Citra Aditya Bakti, 2006),

Perlindungan preventif diwujudkan melalui regulasi yang jelas untuk mencegah terjadinya kejahatan, sedangkan perlindungan represif dilakukan melalui penegakan hukum dan pemberian pemulihan kepada korban. Kejadian dalam kasus *phishing* melalui aplikasi WhatsApp, perlindungan preventif belum optimal karena belum ada pengaturan khusus yang mendefinisikan dan mengatur karakteristik tindak pidana *phishing*. Di sisi lain, perlindungan represif juga belum sepenuhnya efektif karena korban sering kali hanya menjadi pihak yang dirugikan tanpa mekanisme pemulihan yang memadai.

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. Penelitian berjudul “*Pertanggungjawaban Pidana Pelaku Phishing dan Efektivitas Penegakan Hukum Berdasarkan UU Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik*” karya Fauzan Mahdi Irawan, Muhammad Zibran Al Habsy, dan Asmak Ul Hosnah lebih menitikberatkan pada efektivitas penegakan hukum terhadap pelaku *phishing*.¹⁰ Penelitian lain berjudul “*Pertanggungjawaban Pidana Terhadap Penyebaran Link Phishing di Media Sosial Berdasarkan Peraturan Perundang-Undangan*” karya Agustinus Pandapotan Silalahi juga berfokus pada pertanggungjawaban pidana pelaku penyebaran *link phishing*.¹¹ Selain itu, penelitian “*Pertanggungjawaban Pidana Terhadap Kejahatan Siber Phishing Dalam Sistem Hukum Indonesia Berdasarkan Putusan Pengadilan Banjarbaru*” karya Khairul Saleh Harahap, Achmad Yusuf, dan Dimas Arya Aziza lebih membahas penerapan pertanggungjawaban pidana berdasarkan putusan pengadilan.¹² Penelitian lain yang berjudul “*Pengaturan Tindak Pidana bagi Pelaku Penipuan Phising Berbasis Web*” karya Faiz Emery Muhammad juga lebih.¹³

¹⁰ Fauzan Irawan, Muhammad Habsy, And Asmak Hosnah, “Pertanggungjawaban Pidana Pelaku Phishing Dan Efektivitas Penegakan Hukum Berdasarkan Uu Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik,” *Jurnal Komputer, Informasi Dan Teknologi* 5, No. 2 Se-Articles (October 29, 2025): 11, <https://doi.org/10.53697/jkomitek.V5i2.3159>.

¹¹ Agustinus Pandapotan Silalahi, “Pertanggungjawaban Pidana Terhadap Penyebaran Link Phishing Di Media Sosial Berdasarkan Peraturan Perundang-Undangan” (Universitas Jambi, 2025), <https://repository.unja.ac.id/79553/>.

¹² Khairul Saleh Harahap, Achmad Yusuf, And Dimas Arya Aziza, “Pertanggungjawaban Pidana Terhadap Kejahatan Siber Phishing Dalam Sistem Hukum Indonesia Berdasarkan Putusan Pengadilan Banjarbaru,” *Krisna Law : Jurnal Mahasiswa Fakultas Hukum Universitas Krisnadwipayana* 8, No. 1 Se-Articles (March 10, 2026): 121–38, <https://doi.org/10.37893/krisnalaw.V8i1.1314>.

¹³ Faiz Emery Muhammad, “Pengaturan Tindak Pidana Bagi Pelaku Penipuan Phising Berbasis Web,” *Jurnal Usm Law Review* 6, No. 1 (2023): 226–41,

Penelitian-penelitian sebelumnya belum secara khusus mengkaji perlindungan hukum terhadap korban tindak pidana *phishing* melalui aplikasi WhatsApp dengan modus pengiriman *URL* atau file dokumen palsu, padahal modus ini merupakan salah satu bentuk kejahatan digital yang semakin sering terjadi di masyarakat. Penelitian ini difokuskan pada bentuk perlindungan hukum terhadap korban tindak pidana *phishing* melalui aplikasi WhatsApp, khususnya yang dilakukan dengan modus pengiriman *URL* atau file dokumen palsu, serta pada mekanisme pemulihan hak dan kerugian korban berdasarkan peraturan perundang-undangan yang berlaku di Indonesia. 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.”

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang di atas, dapat dirumuskan permasalahan sebagai berikut: Berpijak pada latar belakang sebagaimana telah diuraikan di atas, dapat dirumuskan permasalahan sebagai berikut :

Bagaimana bentuk Perlindungan Hukum Korban Tindak Pidana Penipuan Elektronik *Phishing* Melalui Aplikasi Whatsapp dalam Bentuk *Uniform Resource Locator* (*URL*) atau File Palsu?

1.3 Tujuan Penelitian

Penelitian ini bertujuan untuk menganalisa dan mengetahui bentuk perlindungan hukum korban tindak pidana *phishing* melalui aplikasi WhatsApp dalam bentuk *Uniform Resource Locator (URL)* atau file palsu berdasarkan ketentuan hukum dan peraturan perundang-undangan yang berlaku di Indonesia.

1.4 Manfaat Penelitian

Manfaat secara teoritis hasil penelitian ini diharapkan dapat memperkaya khazanah ilmu pengetahuan di bidang hukum, khususnya dalam kajian hukum pidana dan hukum teknologi informasi, serta dapat dijadikan sebagai bahan referensi atau acuan bagi penelitian-penelitian selanjutnya yang membahas topik serupa terkait kejahatan siber.¹⁴

Manfaat praktis penelitian ini adalah meningkatkan pemahaman dan kesadaran hukum masyarakat mengenai hak-hak yang dimiliki sebagai korban, serta menjadi masukan yang konstruktif bagi aparat penegak hukum dalam upaya menindaklanjuti dan menyelesaikan kasus *phishing* dengan lebih optimal dan efektif.¹⁵

1.5 Metode Penelitian

Penulisan laporan ilmiah memerlukan suatu strategi atau tahapan dalam menganalisa data agar dapat memperoleh kebenaran ilmiah. Untuk memperoleh kebenaran ilmiah, seorang peneliti dituntut untuk berpikir secara logis dan tepat. Mengenai studi ini, penulis menerapkan berbagai metode seperti pendekatan

¹⁴ “Tinjauan Yuridis Perlindungan Data Pribadi,” *Lex Privatum*, 2022, 12, <https://ejournal.unsrat.ac.id/index.php/lexprivatum/search?query=tinjauan+yuridis+perlindungan+data+pribadi>.

¹⁵ “Tinjauan Yuridis Perlindungan Data Pribadi.”

masalah, jenis penelitian, sumber bahan hukum, analisis bahan hukum.

1.5.1 Pendekatan Penelitian

- 1). Pendekatan peraturan perundang-undangan (*Statute Approach*), dilakukan dengan menelaah seluruh peraturan perundang-undangan yang berkaitan dengan isu hukum yang diteliti. Pendekatan ini digunakan untuk mengidentifikasi norma hukum yang mengatur perlindungan terhadap korban tindak pidana phishing melalui aplikasi WhatsApp dalam bentuk URL atau file dokumen palsu.¹⁶

Pendekatan dalam penelitian ini, akan menganalisis berbagai ketentuan hukum yang relevan, antara lain Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Kitab Undang-Undang Hukum Pidana, 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 Pelindungan Data Pribadi, serta Undang-Undang Nomor 31 Tahun 2014 tentang Perlindungan Saksi dan Korban. Pendekatan ini bertujuan untuk mengetahui sejauh mana peraturan perundang-undangan tersebut memberikan perlindungan hukum terhadap korban serta mengatur pertanggungjawaban pidana terhadap pelaku phishing.

- 2). Pendekatan konseptual (*Conseptual Approach*) dilakukan dengan mengkaji konsep-konsep, asas-asas hukum, dan doktrin para ahli yang

¹⁶ Kusnandar And P Adab, *Putusan Mk Dan Masa Depan Sertifikat Jaminan Fidusia Di Indonesia* (Penerbit Adab, 2025), Hlm.22 https://Books.Google.Co.Id/Books?Id=R_Jjeqaaqbaj.

berkaitan dengan objek penelitian, pendekatan konseptual digunakan untuk memahami konsep perlindungan hukum, konsep korban, konsep tindak pidana *phishing*, serta asas-asas hukum yang mendasari perlindungan terhadap korban kejahatan siber.¹⁷

Pendekatan dalam penelitian ini, menggunakan teori perlindungan hukum yang dikemukakan oleh Philipus M. Hadjon, khususnya mengenai perlindungan hukum preventif dan represif.¹⁸ Pendekatan ini juga digunakan untuk menganalisis asas kepastian hukum, asas keadilan, dan asas perlindungan hukum sebagai dasar dalam menilai kecukupan regulasi terhadap perlindungan korban tindak pidana *phishing*.¹⁹ Pendekatan konseptual dalam penelitian ini memungkinkan analisis yang lebih mendalam terhadap kekosongan norma serta kelemahan pengaturan hukum yang ada.

1.5.2 Jenis Penelitian

Jenis penelitian yang diterapkan adalah penelitian hukum normatif (*yuridis normatif*). Penelitian hukum normatif difokuskan pada telaah tentang bahan hukum primer, bahan hukum sekunder.²⁰ Penelitian ini bersifat kualitatif karena tidak melibatkan data statistik, tetapi justru bergantung pada penalaran hukum dan interpretasi norma untuk menjawab

¹⁷ Kusnandar And Adab Hlm.22-23.

¹⁸ Philipus M Hadjon, *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).

¹⁹ John Rawls, *A Theory Of Justice* (Cambridge: Harvard University Press, 1971).

²⁰ Peter Mahmud Marzuki, *Penelitian Hukum* (Jakarta: Kencana, 2021), <https://books.google.co.id/books?id=Ckzadwaaqbaj>.

rumusan persoalan.²¹ Metode ini dipilih karena sesuai untuk menganalisis permasalahan hukum secara mendalam dan sistematis berdasarkan ketentuan peraturan yang berlaku serta doktrin hukum.

Penelitian hukum normatif dilakukan dengan mempelajari bahan pustaka atau data sekunder, yang mencakup peraturan perundang-undangan, literatur, dan hasil penelitian sebelumnya.²² Tujuan dari penelitian hukum normatif adalah untuk menemukan prinsip-prinsip hukum, kaidah hukum, dan peraturan hukum positif yang berlaku.²³ Abdulkadir Muhammad berpendapat bahwa penelitian hukum normatif menggunakan pendekatan perundang-undangan, konseptual, dan kasus dalam menjawab permasalahan hukum yang dikaji.²⁴

1.5.3 Bahan Hukum

1.5.3.1. Bahan Hukum Primer

Bahan hukum primer merujuk kepada sumber hukum yang utama dan menjadi pedoman normatif dalam suatu penelitian. Dalam studi ini, bahan hukum primer meliputi:

- 1). Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
- 2). Kitab Undang-Undang Hukum Pidana.
- 3). Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas

²¹ Soerjono Soekanto And Sri Mamudji, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat* (Jakarta: Rajawali Pers, 2015), <https://books.google.co.id/books?id=Tj8meaaqbaj>.

²² Soekanto, Soerjono & Mamudji, Sri, 2015, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Raja Grafindo Persada, Jakarta, Hal. 15

²³ Marzuki, Peter Mahmud, 2017, *Penelitian Hukum*, Kencana, Jakarta, Hal. 35

²⁴ Muhammad, Abdulkadir, 2014, *Hukum Dan Penelitian Hukum*, Citra Aditya Bakti, Bandung, Hal. 101–103

Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan.

- 4). Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- 5). Undang-Undang Nomor 31 Tahun 2014 tentang Perlindungan Saksi dan Korban.
- 6). Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
- 7). Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016 tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi oleh Bank Umum.
- 8). Putusan pengadilan yang berkaitan dengan tindak pidana *phishing* atau penipuan berbasis elektronik, apabila tersedia.

Bahan hukum primer mencakup peraturan perundang-undangan, dokumentasi resmi pembuatan undang-undang, dan keputusan hakim, yang memiliki sifat autoritatif dan mengikat.²⁵

1.5.3.2 Bahan Hukum Sekunder

Bahan hukum sekunder adalah bahan hukum yang memberikan penjelasan mengenai bahan hukum primer, berupa literatur hukum, hasil penelitian, jurnal ilmiah, dan pendapat para ahli. Dalam penelitian ini, bahan hukum sekunder yang digunakan meliputi:

1. Buku-buku hukum yang membahas mengenai:

²⁵ Marzuki, Peter Mahmud, Op.Cit, Hal. 141

2. Jurnal ilmiah dan hasil penelitian terdahulu yang berkaitan dengan:
3. Pendapat para ahli hukum, seperti:
4. Artikel, berita, dan laporan resmi yang berkaitan dengan kasus *phishing* melalui WhatsApp,

Bahan hukum sekunder ini digunakan untuk memperkuat analisis terhadap efektivitas pengaturan hukum yang berlaku serta mengidentifikasi kelemahan perlindungan hukum bagi korban tindak pidana *phishing*.

1.5.4 Teknik Pengumpulan Bahan Hukum

Bahan hukum dalam penelitian ini dikumpulkan melalui studi *kepastakaan (library research)*. Teknik ini dilakukan dengan membaca, menelaah, dan menganalisis berbagai dokumen hukum, literatur ilmiah, dan sumber informasi lainnya yang relevan dengan pokok permasalahan. Pengumpulan dilakukan dengan dua cara, yaitu pencarian langsung di perpustakaan fakultas hukum dan perpustakaan umum untuk mendapatkan sumber cetak, disertai pencarian online melalui situs resmi seperti Direktori Putusan Mahkamah Agung, Jaringan Dokumentasi dan Informasi Hukum (JDIH), portal jurnal nasional Garuda, Sinta, dan Google Scholar.

Metode ini sejalan dengan pernyataan Peter Mahmud Marzuki yang menekankan bahwa penelitian hukum normatif memerlukan pencarian sistematis terhadap sumber hukum primer sebagai dasar analisis,²⁶ serta pandangan Soerjono Soekanto dan Sri Mamudji yang menyatakan bahwa sumber hukum sekunder memiliki fungsi untuk menjelaskan sumber hukum

²⁶ Marzuki, Peter Mahmud, Op.Cit, Hal. 181

primer.²⁷

1.5.5 Teknik Analisis Bahan Hukum

Teknik untuk menganalisis bahan hukum dalam studi ini mengadopsi metode analisis deskriptif-kualitatif yang dilakukan dengan cara membahas, menginterpretasikan, dan mengaitkan sumber hukum primer, dan sekunder secara terstruktur guna menjawab pertanyaan penelitian. Selanjutnya, analisis kualitatif dilakukan dengan menginterpretasikan norma-norma tersebut berdasar teori dan doktrin hukum dari sumber hukum sekunder untuk mencari kesesuaian atau perbedaan antara norma dan aplikasinya. Analisis dalam penelitian hukum normatif dilakukan dengan mempelajari isi (*content*) dan makna (*meaning*) dari aturan hukum, serta sudut pandang para ahli untuk merumuskan argumen hukum yang rasional.²⁸ Pernyataan lain yaitu penelitian hukum normatif memerlukan penalaran hukum (*legal reasoning*) yang menghubungkan fakta hukum dengan ketentuan peraturan untuk menghasilkan kesimpulan yang bisa dipertanggungjawabkan.²⁹

²⁷ Soekanto, Soerjono & Mamudji, Sri, Op.Cit, Hal. 23

²⁸ Ibrahim, Johnny, Op.Cit, Hal. 300

²⁹ Marzuki, Peter Mahmud, Op.Cit, Hal. 171

