KUALIFIKASI YURIDIS *PHISHING* SEBAGAI KEJAHATAN MANIPULASI INFORMASI ELEKTRONIK DAN PEROLEHAN DATA PRIBADI SECARA MELAWAN HUKUM

Agus Setyawan[1] dan Vita Mahardhika[2]

[1]Fakultas Hukum, Universitas Negeri Surabaya, Surabaya, Indonesia, agus.22108@mhs.unesa.ac.id
[2]Fakultas Hukum, Universitas Negeri Surabaya, Surabaya, Indonesia, vitamahardhika@unesa.ac.id

Abstrak

The development of digital technology has encouraged the emergence of various forms of cybercrime, one of which is phishing conducted through the manipulation of electronic information to unlawfully obtain victims' personal data. The urgency of this study lies in the limited legal approach to phishing crimes, particularly the use of provisions oriented toward illegal access under Article 30 of the Electronic Information and Transactions Law (ITE Law), which has not fully addressed the characteristics and modus operandi of phishing. This study aims to analyze the application of Article 35 of the ITE Law and Article 65 paragraph (1) of the Personal Data Protection Law (PDP Law) to phishing crimes, as well as the element of intent in phishing as a form of electronic information manipulation and unlawful acquisition of personal data. This study employed a normative juridical method using statutory, and conceptual approaches. The findings indicate that phishing constitutes an intentional act (dolus directus) involving electronic information manipulation and unlawful acquisition of personal data. Therefore, Article 35 of the ITE Law and Article 65 paragraph (1) of the PDP Law are more appropriate for prosecuting phishing offenders in Indonesia.
***Kata kunci**: phishing, concursus realis, ITE Law, criminal liability*

A. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang pesat membawa dampak signifikan terhadap seluruh aspek kehidupan masyarakat, termasuk di bidang hukum. Di satu sisi, digitalisasi memberikan kemudahan akses layanan publik dan swasta, namun di sisi lain membuka celah bagi munculnya berbagai modus kejahatan siber yang semakin canggih. Salah satu bentuk kejahatan siber yang paling banyak merugikan masyarakat Indonesia adalah *phishing*. Kejahatan ini memanfaatkan kepercayaan pengguna sistem elektronik dengan cara memanipulasi informasi digital guna memperoleh data pribadi korban secara tidak sah (Manorek, Koesomo, and Maramis 2025).

Phishing secara etimologis berasal dari kata "fishing" yang berarti memancing, yakni sebuah upaya untuk mendapatkan informasi sensitif dengan cara menipu calon korban

melalui saluran komunikasi elektronik (Anon n.d.). Melalui data laporan IDADX, terlihat bahwa intensitas serangan *phishing* di Indonesia mengalami peningkatan yang signifikan. Pada kuartal I tahun 2023, tercatat sebanyak 26.675 laporan, dengan puncak tertinggi terjadi pada bulan Februari yang mencapai 15.050 kasus, disusul Januari sebanyak 7.665 laporan dan Maret sebesar 3.960 laporan (Bjcoid2 n.d.). Data tersebut menunjukkan bahwa *phishing* telah berkembang menjadi ancaman nyata dalam ruang digital yang tidak hanya berdampak pada kerugian ekonomi, tetapi juga menyasar keamanan data pribadi masyarakat secara luas. Kondisi ini menuntut adanya kerangka hukum yang komprehensif dan tepat dalam menangani tindak pidana *phishing*.

Dalam praktik penegakan hukum di Indonesia, tindak pidana *phishing* selama ini cenderung dijerat dengan Pasal 30 Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang mengatur mengenai akses ilegal terhadap sistem elektronik. Pendekatan ini tercermin dalam Putusan Nomor 764/Pid.Sus/2022/PN.Pbr, di mana majelis hakim mengkualifikasikan perbuatan terdakwa sebagai pelanggaran Pasal 30 jo Pasal 51 ayat (2) UU ITE dengan alasan terdakwa telah melakukan akses ilegal terhadap akun milik korban. Namun demikian, pendekatan tersebut dinilai belum sepenuhnya mencerminkan karakteristik utama tindak pidana *phishing* (Gulo, Lasmadi, and Nawawi 2021).

Phishing pada hakikatnya bukan hanya merupakan kejahatan berbasis akses ilegal, melainkan melibatkan serangkaian perbuatan yang dimulai dari manipulasi informasi elektronik untuk menyesatkan korban, diikuti dengan perolehan data pribadi secara melawan hukum. Kedua komponen perbuatan tersebut masing-masing memiliki pengaturan tersendiri dalam hukum positif Indonesia, yakni Pasal 35 UU ITE yang mengatur manipulasi informasi elektronik dan Pasal 65 ayat (1) Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) yang melarang perolehan data pribadi secara melawan hukum. Dengan demikian, penggunaan Pasal 30 UU ITE semata dalam penanganan kasus *phishing* menciptakan kondisi keterbatasan norma yang perlu dikaji secara lebih komprehensif (Wiranata et al. 2024).

Penelitian terdahulu mengenai *phishing* di Indonesia umumnya membahas *phishing* dalam kerangka UU ITE semata. Gulo, Lasmadi, dan Nawawi (2021) mengkaji *phishing* sebagai bentuk cybercrime berdasarkan UU ITE dengan menekankan bahwa *phishing* merupakan social engineering yang mengandalkan manipulasi persepsi korban. Sutarli dan Kurniawan (2023) menelaah peran UU PDP

dalam menanggulangi *phishing* tanpa menganalisis penerapan kombinasi pasal secara mendalam. Sementara Wiranata et al. (2024) mengkaji pertanggungjawaban pidana pelaku *phishing* namun belum secara spesifik menganalisis kualifikasi *concursus realis* antara UU ITE dan UU PDP. Berbeda dengan penelitian sebelumnya, artikel ini secara khusus menganalisis kualifikasi yuridis *phishing* berdasarkan Pasal 35 UU ITE dan Pasal 65 ayat (1) UU PDP serta unsur kesengajaan pelaku dalam konteks pelanggaran pelaku dalam manipulasi informasi elektronik dan perolehan data pribadi secara melawan hukum.

Berdasarkan uraian tersebut, rumusan masalah dalam penelitian ini adalah:

(1) Bagaimana kualifikasi tindak pidana *phishing* berdasarkan Pasal 35 UU ITE dan Pasal 65 ayat (1) UU PDP?

(2) Apa pertanggungjawaban pidana pelaku yang dikenakan Pasal 30 UU ITE dikaitkan dengan pelaku yang melakukan manipulasi informasi elektronik dan perolehan data pribadi secara melawan hukum dalam Putusan No. 764/Pid.Sus/2022/PN.Pbr?

Tujuan penelitian ini adalah untuk menganalisis ketepatan penerapan kedua pasal tersebut terhadap tindak pidana *phishing* serta membuktikan adanya dolus directus dalam keseluruhan rangkaian perbuatan pelaku.

B. METODE PENELITIAN

Penelitian ini menggunakan metode yuridis normatif, yakni metode penelitian hukum yang dilakukan dengan cara meneliti bahan pustaka atau data sekunder (Ismoyo 2019). Metode ini dipilih karena fokus penelitian terletak pada analisis norma hukum positif dan penerapannya terhadap permasalahan hukum yang dikaji, bukan pada fenomena sosial yang terjadi di lapangan. Pendekatan yang digunakan adalah pendekatan perundang-undangan (statute approach) dan pendekatan konseptual (conceptual approach). Pendekatan perundang-undangan dilakukan dengan menelaah seluruh peraturan perundang-undangan yang bersangkutan dengan isu hukum yang sedang ditangani, meliputi Undang-Undang Nomor 1 Tahun 2023 tentang KUHP Nasional, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU ITE, dan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Pendekatan konseptual dilakukan dengan menelaah pandangan-pandangan dan doktrin-doktrin yang berkembang dalam ilmu hukum, meliputi teori tindak pidana, teori *phishing* sebagai cybercrime, teori pertanggungjawaban pidana, dan teori *concursus* sebagai kerangka analisis perbarengan tindak pidana.

Sumber bahan hukum terdiri atas bahan hukum primer berupa peraturan perundang-undangan dan putusan pengadilan, khususnya Putusan No. 764/Pid.Sus/2022/PN Pbr yang digunakan sebagai contoh kasus konkret. Bahan hukum sekunder meliputi literatur ilmiah, jurnal hukum, dan doktrin yang relevan. Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan dengan mengumpulkan, mengidentifikasi, dan mengklasifikasikan bahan hukum yang relevan dengan permasalahan yang dikaji. Analisis bahan hukum dilakukan secara preskriptif dengan cara mengidentifikasi fakta hukum, mengidentifikasi isu hukum, mengumpulkan bahan hukum yang relevan, dan mengevaluasi penyelesaian isu hukum berdasarkan argumen yang dikembangkan dari bahan hukum yang tersedia.

C. HASIL DAN PEMBAHASAN

1. Kualifikasi Tindak Pidana *Phishing* sebagai Pelanggaran Pasal 35 UU ITE dan Pasal 65 Ayat (1) UU PDP dalam Kerangka *Concursus Realis*

Phishing merupakan bentuk kejahatan siber yang mengeksploitasi kepercayaan pengguna sistem elektronik untuk memperoleh data pribadi atau informasi rahasia secara melawan hukum. Dalam perspektif hukum pidana, *phishing* tidak dapat dipahami secara sederhana sebagai penipuan konvensional karena memiliki karakteristik khusus yang membedakannya dari tindak pidana penipuan dalam Pasal 492 KUHP Nasional. Perbedaan mendasar terletak pada modus operandi dan objek kejahatan. Penipuan konvensional umumnya dilakukan melalui interaksi langsung atau komunikasi verbal yang menyesatkan korban untuk menyerahkan barang atau memberikan hutang. Sementara itu, *phishing* dilakukan melalui manipulasi sistem elektronik dan memanfaatkan celah kepercayaan terhadap teknologi digital (Putri Ramadhani Rangkuti et al. 2025).

Berdasarkan fakta-fakta yang terungkap dalam persidangan Putusan No. 764/Pid.Sus/2022/PN.Pbr, mekanisme *phishing* terdiri atas beberapa tahapan sistematis. Pertama, tahap persiapan dan perencanaan, di mana pelaku mempelajari metode *phishing* secara autodidak melalui internet, mempersiapkan infrastruktur berupa domain dan server, serta merancang email dengan header dan tampilan identik dengan platform resmi yang menjadi target tiruan. Kedua, tahap pembuatan dan penyampaian umpan, di mana pelaku menyusun pesan elektronik palsu menggunakan logo dan alamat pengirim yang dimanipulasi agar tampak resmi, kemudian disebarkan secara massal kepada calon korban. Ketiga, tahap manipulasi

psikologis dan aksi korban, di mana korban yang terkecoh mengklik tautan palsu menuju halaman login tiruan yang identik dengan tampilan aslinya. Keempat, tahap pengumpulan data, di mana setiap input kredensial korban langsung terekam ke server pelaku. Kelima, tahap eksploitasi data, di mana pelaku menggunakan kombinasi data yang diperoleh untuk mengakses rekening atau akun digital korban dan melakukan pengalihan aset secara ilegal (Putusan Nomor 764/Pid.Sus/2022/PN Pbr 2022).

Dilihat dari penafsiran sosiologis, *phishing* berkembang seiring meningkatnya digitalisasi layanan publik dan swasta, khususnya di sektor perbankan, keuangan, dan e-commerce. Masyarakat yang semakin bergantung pada layanan digital seringkali tidak memiliki literasi digital yang memadai untuk membedakan komunikasi elektronik yang sah dengan yang palsu. Kepercayaan publik terhadap sistem elektronik ini kemudian dieksploitasi oleh pelaku *phishing* melalui rekayasa sosial (social engineering) yang mengandalkan manipulasi persepsi korban melalui peniruan identitas digital (Gulo et al. 2021). Pola ini menunjukkan bahwa *phishing* bukan hanya kejahatan yang memanfaatkan teknologi, tetapi juga kejahatan yang memanfaatkan psikologi sosial (Febrika Ardy et al. 2024).

Dalam perkara Putusan No. 764/Pid.Sus/2022/PN.Pbr, majelis hakim mengkualifikasikan perbuatan terdakwa sebagai akses ilegal berdasarkan Pasal 30 jo Pasal 51 ayat (2) UU ITE dengan pertimbangan bahwa terdakwa terbukti melakukan akses tanpa izin terhadap akun email dan akun cryptocurrency milik korban, sehingga mengakibatkan kerugian sebesar kurang lebih 148 ETH atau setara dengan Rp6.500.000.000 (enam miliar lima ratus juta rupiah). Namun demikian, pendekatan tersebut belum sepenuhnya mencerminkan karakteristik utama tindak pidana *phishing*. *Phishing* pada hakikatnya tidak diawali dengan tindakan akses, melainkan dengan proses manipulasi informasi elektronik yang dirancang untuk menyesatkan korban agar secara sukarela menyerahkan data pribadinya. Dari tindakan tersebut terlihat bahwa pelaku memperoleh data pribadi korban secara melawan hukum dengan cara membuat seolah-olah informasi elektronik yang disebarkannya merupakan informasi yang otentik (Muhammad and Harefa 2023).

Pasal 35 UU ITE menyatakan bahwa "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan,

penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik (UU ITE 2024)." Ketentuan ini secara substansial sesuai dengan modus operandi *phishing* yang pada umumnya mencoba meniru sebuah aplikasi ataupun tampilan website sebuah perusahaan atau institusi resmi. Untuk membuktikan bahwa *phishing* memenuhi unsur-unsur Pasal 35 UU ITE, perlu dilakukan analisis terhadap setiap unsur pasal tersebut (Ks et al. 2022),

1. Unsur "Setiap Orang" merujuk pada subjek hukum yang dapat dimintai pertanggungjawaban pidana. Unsur ini bersifat formal dan terpenuhi sepanjang pelaku adalah subjek hukum yang cakap untuk dimintai pertanggungjawaban pidana. Dalam kasus *phishing*, pelaku umumnya adalah orang perseorangan yang memiliki kemampuan teknis untuk memanipulasi sistem elektronik.
2. Unsur "dengan sengaja" merupakan unsur subjektif yang menunjukkan sikap batin pelaku terhadap perbuatan dan akibatnya. Dalam *phishing*, pelaku secara sadar dan terencana membuat situs web palsu atau informasi elektronik palsu melalui tahapan persiapan yang matang. Pelaku mengetahui bahwa perbuatannya akan menyesatkan korban dan menghendaki agar korban percaya bahwa informasi palsu tersebut adalah otentik. Oleh karena itu, unsur kesengajaan dalam *phishing* memenuhi kriteria kesengajaan sebagai maksud (Meliala 2020).
3. Unsur "tanpa hak atau melawan hukum" menunjukkan bahwa perbuatan dilakukan tanpa kewenangan yang sah atau bertentangan dengan hukum. Dalam konteks *phishing*, pelaku tidak memiliki hak untuk membuat situs web yang menyerupai layanan resmi suatu institusi dan tidak memiliki kewenangan untuk mengatasnamakan institusi tersebut dalam komunikasi elektronik. Sifat melawan hukum dalam *phishing* bersifat formil karena perbuatan bertentangan dengan ketentuan hukum yang berlaku, sekaligus bersifat materiil karena bertentangan dengan asas-asas kepatutan dalam masyarakat (Reyhan and Gultom 2025).
4. Unsur "melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik" merupakan unsur perbuatan bersifat alternatif. Dalam *phishing*, bentuk perbuatan yang paling relevan adalah "penciptaan" dan "manipulasi" informasi elektronik. Penciptaan terjadi ketika pelaku membuat situs web palsu, formulir elektronik

palsu, atau aplikasi palsu. Manipulasi terjadi ketika pelaku mengubah atau memodifikasi informasi elektronik yang sudah ada untuk tujuan menyesatkan korban, misalnya dengan menggunakan domain yang mirip dengan situs website resmi.

5. Unsur "dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik" merupakan unsur tujuan yang menjadi kunci untuk memahami esensi dari Pasal 35 UU ITE. Dalam *phishing*, tujuan ini sangat jelas terlihat. Pelaku berusaha keras agar situs palsu yang dibuat tidak dapat dibedakan dari situs asli, dengan menggunakan logo resmi, bahasa formal yang mirip dengan komunikasi resmi institusi, bahkan kadang menggunakan sertifikat SSL palsu agar situs terlihat aman. Tujuan akhir dari semua upaya ini adalah agar korban percaya bahwa mereka sedang berinteraksi dengan institusi yang sah, sehingga dengan sukarela memasukkan data pribadi mereka (Gulo et al. 2021).

Dari analisis di atas, dapat disimpulkan bahwa tindak pidana *phishing* memenuhi seluruh unsur Pasal 35 UU ITE, meliputi pelaku sebagai subjek hukum yang cakap, perbuatan dilakukan dengan sengaja dan terencana, perbuatan dilakukan tanpa hak dan melawan hukum, pelaku menciptakan/memanipulasi informasi elektronik, dan tujuan perbuatan adalah agar informasi palsu dianggap otentik. Terpenuhinya seluruh unsur ini menunjukkan bahwa *phishing* secara mandiri merupakan tindak pidana berdasarkan Pasal 35 UU ITE. Meskipun demikian, Pasal 35 hanya berfokus pada manipulasi atau rekayasa informasi elektronik tanpa menjangkau dimensi perolehan data pribadi sebagai tujuan utama *phishing*, sehingga perlu dilengkapi dengan ketentuan lain (Lokapala, Nurfauzi, and Widowaty n.d.).

Untuk melengkapi keterbatasan pengaturan dalam Pasal 35 UU ITE, pengaturan mengenai perolehan data pribadi dapat ditemukan dalam Pasal 65 ayat (1) UU PDP yang menyatakan bahwa "Setiap Orang dilarang secara melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi (UU PDP 2022)." Dalam konteks *phishing*, pelaku melakukan manipulasi informasi elektronik sebagai sarana untuk mendapatkan data pribadi korban, seperti username, password, data biometrik, dan informasi keuangan (Asherli and Wiraguna 2025).

Analisis terhadap unsur-unsur Pasal 65 ayat (1) UU PDP dalam tindak pidana *phishing* menunjukkan hasil sebagai berikut:

1. Unsur "Setiap Orang" terpenuhi karena pelaku adalah subjek hukum yang cakap dimintai pertanggungjawaban.
2. Unsur "dengan sengaja" dalam konteks Pasal 65 ayat (1) UU PDP merujuk pada sikap batin pelaku terhadap perbuatan memperoleh atau mengumpulkan data pribadi. Dalam *phishing*, pelaku secara sadar merancang skema untuk memperoleh data pribadi korban, bahkan perolehan data pribadi adalah tujuan utama dari seluruh skema *phishing*, sehingga kesengajaan ini lebih kuat dibandingkan kesengajaan dalam manipulasi sistem elektronik (Wuwungan, Massie, and Pinori 2024).
3. Unsur "melawan hukum" dalam perolehan data pribadi dapat dilihat dari dua aspek. Dari aspek formal, perolehan data pribadi dalam *phishing* dilakukan tanpa persetujuan yang sah dari subjek data karena korban memberikan datanya berdasarkan informasi yang menyesatkan, sedangkan Pasal 16 ayat (2) huruf d UU PDP menegaskan bahwa pemrosesan data pribadi harus dilakukan dengan tidak menyesatkan subjek data pribadi. Dari aspek materiil, perolehan data pribadi melalui tipu daya dan manipulasi jelas bertentangan dengan norma kepatutan dalam masyarakat.
4. Unsur "memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya" terpenuhi karena seluruh data yang diperoleh pelaku merupakan milik korban sebagai subjek data, yang meliputi data identitas (nama, nomor KTP, tanggal lahir), data keuangan (nomor rekening, PIN), serta data akses (username, password, OTP). Pelaku tidak memiliki hak kepemilikan atau hak akses terhadap data tersebut.
5. Unsur "dengan maksud untuk menguntungkan diri sendiri atau orang lain" terpenuhi karena data pribadi yang diperoleh digunakan pelaku untuk melakukan transaksi finansial tanpa hak, seperti transfer dana dari rekening korban, transaksi menggunakan akun digital korban, serta pengalihan aset kripto ke dompet digital milik pelaku, sebagaimana terbukti dalam perkara Putusan No. 764/Pid.Sus/2022/PN.Pbr di mana pelaku berhasil menguasai 148 ETH milik korban. Keenam, unsur "yang dapat mengakibatkan kerugian Subjek Data Pribadi" terpenuhi baik melalui kerugian materiil (kehilangan aset finansial) maupun kerugian immateriil (hilangnya kendali atas data pribadi,

potensi penyalahgunaan identitas, dan gangguan psikologis). Frasa "dapat mengakibatkan" menunjukkan bahwa tidak perlu dibuktikan adanya kerugian aktual, cukup dibuktikan bahwa perbuatan tersebut berpotensi menimbulkan kerugian (Maramis, Doodoh, and L.Lambonan 2025).

Dari analisis unsur-unsur di atas, tindak pidana *phishing* juga memenuhi seluruh unsur Pasal 65 ayat (1) UU PDP. Pemenuhan ganda terhadap dua ketentuan pidana yang berbeda ini membuka ruang bagi penerapan lebih dari satu ketentuan pidana terhadap pelaku *phishing*, yang dalam doktrin hukum pidana Indonesia dikenal sebagai *concursus* atau perbarengan tindak pidana. Dalam hal ini, *phishing* secara normatif dapat dikualifikasikan sebagai *concursus realis* karena melibatkan dua perbuatan pidana yang berbeda dan masing-masing berdiri sendiri: manipulasi informasi elektronik (melanggar Pasal 35 UU ITE) dan perolehan data pribadi secara melawan hukum (melanggar Pasal 65 ayat (1) UU PDP). Sebagaimana diatur dalam Pasal 127-128 KUHP Nasional (KUHP 2023), *concursus realis* mensyaratkan adanya beberapa perbuatan yang masing-masing merupakan tindak pidana berdiri sendiri dan diperiksa sekaligus dalam satu proses peradilan (Sri, Fence, and Mohamad Taufiq 2023).

Kemandirian masing-masing tindak pidana dalam *phishing* dapat dilihat dari dua sudut pandang. Dari sudut waktu, manipulasi sistem elektronik telah terpenuhi ketika pelaku membuat atau menciptakan sistem elektronik palsu, tanpa harus menunggu adanya korban yang memasukkan data pribadi. Sebaliknya, tindak pidana dalam Pasal 65 ayat (1) UU PDP baru terpenuhi ketika pelaku benar-benar memperoleh atau mengumpulkan data pribadi secara melawan hukum. Dari sudut objek perlindungan hukum (rechtsgoed theorie), Pasal 35 UU ITE berorientasi pada perlindungan integritas dan kepercayaan terhadap sistem elektronik sebagai kepentingan umum, sedangkan Pasal 65 ayat (1) UU PDP berorientasi pada perlindungan hak individual atas data pribadi sebagai bagian dari hak privasi. Perbedaan objek perlindungan ini mempertegas bahwa tidak terdapat hubungan penyerapan (absorptie) atau hubungan lex specialis antara kedua ketentuan tersebut, sehingga pertanggungjawaban pidana atas kedua delik tidak bertentangan dengan asas kepastian hukum (Dhyaksa, Thalib, and Ramadani 2025).

Berdasarkan uraian tersebut, kualifikasi tindak pidana *phishing* sebagai *concursus realis* didasarkan pada kemandirian masing-masing tindak pidana, adanya beberapa perbuatan yang dapat dibedakan secara jelas, terpenuhinya seluruh

unsur delik secara terpisah, serta perbedaan objek perlindungan hukum dari masing-masing ketentuan. Dengan demikian, penggunaan Pasal 35 UU ITE dan Pasal 65 ayat (1) UU PDP secara bersamaan memberikan konstruksi hukum yang lebih komprehensif dibandingkan dengan hanya menggunakan Pasal 30 UU ITE yang berfokus semata pada aspek akses ilegal sebagai akibat akhir dari rangkaian kejahatan *phishing*. Penerapan *concursus realis* ini memungkinkan pelaku *phishing* dijerat dengan ancaman pidana berlapis sesuai Pasal 127 KUHP Nasional yang mengatur sistem absorpsi yang dipertajam (hukuman terberat ditambah sepertiganya).

2. Unsur Kesengajaan dalam Tindak Pidana *Phishing* sebagai Dasar Pertanggungjawaban Pidana Pelaku

Dalam hukum pidana dikenal asas geen straf zonder schuld atau tidak ada pidana tanpa kesalahan. Asas ini menegaskan bahwa seseorang hanya dapat dimintai pertanggungjawaban pidana apabila terdapat hubungan antara perbuatan yang dilakukan dengan kesalahan pada diri pelaku. Kesalahan tersebut dalam hukum pidana pada dasarnya terdiri atas kesengajaan (dolus) dan kealpaan (culpa). Dalam tindak pidana *phishing*, bentuk kesalahan yang paling relevan adalah kesengajaan, mengingat *phishing* merupakan tindak pidana yang dilakukan melalui tahapan perencanaan, rekayasa informasi elektronik, serta tindakan yang secara sadar diarahkan untuk memperoleh data pribadi korban (Chandra 2022).

Sistem pertanggungjawaban pidana yang dipilih tidak disebutkan secara jelas dalam KUHP. Roeslan Saleh menyampaikan bahwa istilah kesengajaan dan kelalaian sering digunakan dalam definisi tindak pidana, tetapi tanpa memahami apa yang diisyaratkannya (Utoyo and Afriani 2020). Dalam Pasal 35 UU ITE terdapat frasa "dengan sengaja dan tanpa hak atau melawan hukum" yang secara eksplisit mensyaratkan adanya unsur kesengajaan. Adapun dalam Pasal 65 ayat (1) UU PDP, unsur kesengajaan diisyaratkan secara tersirat melalui ketentuan "dengan maksud untuk menguntungkan diri sendiri atau orang lain", yang menunjukkan adanya kehendak batin yang terarah pada suatu tujuan tertentu. Dengan demikian, unsur kesengajaan merupakan syarat esensial dalam pertanggungjawaban pidana atas kedua pasal tersebut. Unsur kesalahan dalam hukum pidana merupakan keadaan batin pelaku yang menghubungkan antara perbuatan, akibat, dan sifat melawan hukum yang dapat berbentuk kesengajaan (*dolus*) maupun kealpaan

(*culpa*). Keberadaan unsur kesalahan menjadi parameter utama dalam menentukan pertanggungjawaban pidana seseorang. Dengan demikian, untuk menilai pertanggungjawaban pidana pelaku *phishing*, perlu dianalisis bentuk kesengajaan yang melatarbelakangi tindakan manipulasi informasi elektronik dan perolehan data pribadi korban (Mahardhika 2021).

Dalam teori hukum pidana kesengajaan sendiri dibedakan menjadi tiga jenis: kesengajaan sebagai maksud (dolus directus), kesengajaan sebagai kepastian (dolus indirectus), dan kesengajaan sebagai kemungkinan (dolus eventualis). Dolus directus terjadi ketika pelaku dengan sengaja melakukan tindakan yang ditujukan tepat untuk mewujudkan akibat melawan hukum, di mana pelaku menghendaki terjadinya perbuatan, mengetahui akibat dari perbuatannya, serta akibat yang dihasilkan menjadi tujuan utama. Berdasarkan fakta yang terungkap dalam Putusan No. 764/Pid.Sus/2022/PN.Pbr, tindak pidana *phishing* yang dilakukan terdakwa memenuhi kualifikasi dolus directus karena seluruh rangkaian perbuatan dilakukan secara sadar, terencana, dan sistematis dengan tujuan yang jelas untuk memperoleh keuntungan pribadi melalui penguasaan data dan aset milik korban secara melawan hukum (Prasetyo 2016).

Berdasarkan fakta yang terungkap dalam Putusan No. 764/Pid.Sus/2022/PN.Pbr, perbuatan terdakwa dalam melakukan *phishing* tidak dilakukan secara spontan, melainkan melalui rangkaian tindakan yang menunjukkan perencanaan dan kesengajaan yang matang. Pada sekitar bulan Agustus 2021, terdakwa secara aktif mempelajari metode *phishing* melalui media internet, termasuk dengan mengakses berbagai konten dan tutorial yang menjelaskan teknik memperoleh data korban secara ilegal. Setelah memahami metode tersebut, terdakwa kemudian menyiapkan sarana yang diperlukan, seperti daftar email calon korban serta perangkat lunak pendukung berupa SMTP, validator, dan sender. Selanjutnya, terdakwa membuat dan menggunakan email serta halaman elektronik palsu yang dirancang menyerupai sistem resmi dengan tujuan menciptakan kesan bahwa informasi yang ditampilkan merupakan informasi yang sah dan dapat dipercaya (Putusan Nomor 764/Pid.Sus/2022/PN Pbr 2022).

Rangkaian perbuatan tersebut membuktikan bahwa tindakan terdakwa dilakukan secara bertahap, dimulai dari proses pembelajaran, persiapan sarana, pelaksanaan aksi, hingga pemanfaatan hasil kejahatan. Dengan demikian, perbuatan tersebut tidak dapat dikategorikan sebagai tindakan spontan ataupun kelalaian,

melainkan merupakan perbuatan yang dilakukan dengan kesadaran penuh. Unsur kesengajaan dalam konteks manipulasi informasi elektronik juga terlihat dari adanya tindakan terdakwa yang secara sadar membuat tampilan elektronik menyerupai institusi resmi guna menciptakan kesan keaslian (appearance of authenticity). Tindakan membuat website tiruan, penggunaan email palsu, serta penyusunan pesan elektronik yang meyakinkan tidak dapat dipandang sebagai kelalaian, melainkan bentuk rekayasa elektronik yang dilakukan secara sadar dan terencana (Utoyo and Afriani 2020).

Tindakan terdakwa menunjukkan adanya hubungan batin antara pelaku dengan akibat yang ditimbulkan (willens en wetens), yakni pelaku mengetahui dan menghendaki akibat dari perbuatannya. Hal tersebut terlihat dari adanya tindakan terdakwa yang secara sadar merancang website palsu, menyusun email *phishing*, serta mengarahkan korban menuju media elektronik yang telah dimanipulasi sebelumnya. Terdakwa tidak hanya menyadari bahwa informasi elektronik yang dibuat merupakan informasi palsu, tetapi juga menghendaki agar korban mempercayainya sebagai informasi yang otentik sehingga bersedia menyerahkan data pribadinya. Dalam persidangan pun majelis hakim mengakui adanya frasa "dengan sengaja" yang terbukti dari keseluruhan tindakan terdakwa (Putusan Nomor 764/Pid.Sus/2022/PN Pbr 2022).

Phishing sebagai bentuk ancaman keamanan siber yang sangat berbahaya merupakan tindak pidana rekayasa sosial yang dilakukan dengan kesengajaan. Pelaku tidak hanya mengetahui bahwa perbuatannya melawan hukum, tetapi juga secara aktif menghendaki terjadinya akibat dari perbuatan tersebut. Bukti kesengajaan dalam manipulasi informasi elektronik terlihat dari: (a) pembuatan infrastruktur *phishing* yang rumit berupa domain palsu, server, dan situs web tiruan; (b) penyusunan pesan yang dirancang khusus untuk menyesatkan korban; (c) persiapan mekanisme untuk mengumpulkan dan menyimpan data yang diperoleh; serta (d) rencana untuk menggunakan data tersebut demi keuntungan pribadi. Dengan itu, terlihat bahwa pelaku dalam Putusan No. 764/Pid.Sus/2022/PN.Pbr melakukan manipulasi informasi elektronik dengan kesengajaan dalam bentuk dolus directus, karena pelaku mengetahui, menghendaki, dan menjadikan keberhasilan pengelabuan korban sebagai tujuan utama dari perbuatannya.

Tujuan utama pelaku *phishing* dalam Putusan No. 764/Pid.Sus/2022/PN.Pbr adalah membuat orang-orang yang mendapatkan informasi elektronik palsu

terkecoh dan memasukkan data pribadi mereka ke media *phishing* yang telah disiapkan. Manipulasi informasi elektronik yang dilakukan terdakwa melalui penggunaan identitas palsu perusahaan BaseCoin pada dasarnya merupakan sarana untuk mencapai tujuan utama, yaitu memperoleh data pribadi korban. Hal ini menunjukkan bahwa tindakan terdakwa sejak awal telah diarahkan pada upaya memperoleh akses terhadap informasi pribadi korban melalui cara-cara yang melawan hukum (Wiranata et al. 2024).

Perolehan data pribadi dalam tindak pidana *phishing* menunjukkan adanya kehendak (willens en wetens) dari pelaku untuk menguasai data milik orang lain secara melawan hukum. Hal tersebut terlihat dari tindakan terdakwa yang tidak hanya menciptakan media *phishing*, tetapi juga secara aktif mengarahkan korban agar memasukkan data akun berupa username dan password ke dalam sistem palsu yang telah disiapkan sebelumnya. Dengan demikian, terdakwa mengetahui bahwa data yang diperoleh bukan merupakan haknya dan secara sadar menghendaki penguasaan atas data tersebut sebagai sarana memperoleh keuntungan pribadi. Terdakwa pun terbukti secara konkret memanfaatkan data tersebut untuk mengakses dan menguasai 148 ETH atau setara Rp6.500.000.000 milik korban.

Meskipun dalam Putusan No. 764/Pid.Sus/2022/PN.Pbr majelis hakim mengkualifikasikan perbuatan terdakwa sebagai akses ilegal berdasarkan Pasal 30 jo Pasal 51 ayat (2) UU ITE, pendekatan tersebut belum sepenuhnya mencerminkan karakteristik utama tindak pidana *phishing*. *Phishing* pada hakikatnya tidak semata-mata bertumpu pada tindakan akses tanpa hak, melainkan diawali dengan manipulasi informasi elektronik yang dirancang untuk menyesatkan korban, dilanjutkan dengan perolehan data pribadi secara melawan hukum. Pelaku *phishing* secara sadar menciptakan atau merekayasa tampilan sistem elektronik yang menyerupai sistem resmi agar korban mempercayai keaslian informasi tersebut, yang secara normatif lebih tepat dikualifikasikan berdasarkan Pasal 35 UU ITE dan Pasal 65 ayat (1) UU PDP daripada sekadar Pasal 30 UU ITE (Handoyo et al. 2024).

Unsur kesengajaan juga diperkuat oleh tidak ditemukannya keadaan yang dapat menghapuskan pertanggungjawaban pidana pelaku. Dalam perkara ini, terdakwa berada dalam kondisi mental yang sehat, memahami konsekuensi dari perbuatannya, serta melakukan seluruh rangkaian tindakan tanpa adanya paksaan, ancaman, ataupun keadaan darurat tertentu. Tidak ditemukan adanya alasan pembenar maupun alasan pemaaf yang dapat menghapuskan pertanggungjawaban

pidana terdakwa. Oleh sebab itu, unsur kemampuan bertanggung jawab dan kesalahan dalam bentuk kesengajaan telah terpenuhi, sehingga terdakwa secara hukum dapat dimintai pertanggungjawaban pidana atas tindakan manipulasi informasi elektronik dan perolehan data pribadi secara melawan hukum (Sari 2022).

Pertanggungjawaban pidana pelaku dalam perkara *phishing* tidak hanya dapat dipahami dari akibat akhir berupa akses ilegal, melainkan juga harus dilihat dari adanya kesengajaan dalam melakukan manipulasi informasi elektronik dan memperoleh data pribadi korban secara melawan hukum. Dengan demikian, pelaku memiliki kemampuan bertanggung jawab, melakukan perbuatan dengan sengaja (dolus directus), serta tidak memiliki alasan pemaaf, sehingga secara hukum dapat dimintai pertanggungjawaban pidana atas keseluruhan rangkaian perbuatannya. Penerapan *concursus realis* memungkinkan pelaku dijerat dengan ancaman pidana berlapis dari UU ITE dan UU PDP dengan pemidanaan menggunakan sistem absorpsi yang dipertajam sebagaimana Pasal 127 KUHP Nasional, yakni hukuman pidana terberat ditambah sepertiganya dari keseluruhan ancaman pidana yang ada.

D. PENUTUP

KESIMPULAN

Berdasarkan hasil analisis yang telah diuraikan, terdapat dua kesimpulan utama dalam penelitian ini. Pertama, tindak pidana *phishing* merupakan rangkaian perbuatan yang tidak hanya berupa akses ilegal terhadap sistem elektronik, tetapi juga melibatkan manipulasi informasi elektronik dan perolehan data pribadi korban secara melawan hukum. Penggunaan Pasal 30 UU ITE dalam perkara *phishing* sebagaimana terlihat dalam Putusan No. 764/Pid.Sus/2022/PN.Pbr cenderung hanya menjangkau akibat akhir berupa akses tanpa hak, sehingga belum sepenuhnya mencerminkan karakteristik utama tindak pidana *phishing*. Pasal 35 UU ITE lebih tepat diterapkan karena unsur-unsurnya mencerminkan tindakan manipulasi, penciptaan, atau rekayasa informasi elektronik agar dianggap seolah-olah otentik. Pasal 65 ayat (1) UU PDP relevan diterapkan karena *phishing* pada hakikatnya bertujuan memperoleh data pribadi korban secara melawan hukum. Kedua ketentuan tersebut secara bersama-sama membentuk kualifikasi yuridis *phishing* sebagai *concursus realis* karena masing-masing perbuatan dapat berdiri sendiri sebagai delik yang independen dengan objek perlindungan hukum yang berbeda.

Kedua, unsur kesengajaan dalam tindak pidana *phishing* terbukti dalam bentuk dolus directus melalui tindakan pelaku yang dilakukan secara sadar, terencana, dan

sistematis sejak tahap persiapan hingga pelaksanaan kejahatan. Kesengajaan pelaku tercermin dari adanya proses pembelajaran teknik *phishing*, persiapan perangkat pendukung, pembuatan email dan website palsu, penyebaran informasi elektronik yang menyerupai institusi resmi, serta pemanfaatan data korban untuk kepentingan pribadi. Pelaku secara sadar menghendaki menciptakan situasi palsu agar korban memasukkan data pribadi, sehingga data tersebut dapat digunakan untuk mengakses akun korban dan memperoleh keuntungan. Dengan demikian, unsur kesengajaan dalam tindak pidana *phishing* tidak hanya terletak pada tindakan akses terhadap akun korban, tetapi telah dimulai sejak tahap manipulasi informasi elektronik dan upaya memperoleh data pribadi secara melawan hukum, yang menuntut penerapan Pasal 35 UU ITE dan Pasal 65 ayat (1) UU PDP sebagai instrumen hukum yang lebih tepat

SARAN

1. Bagi legislatif, diperlukan penguatan dan harmonisasi pengaturan hukum terkait tindak pidana *phishing*, khususnya dalam mengintegrasikan ketentuan UU ITE dan UU PDP agar terdapat kejelasan konstruksi norma yang secara eksplisit mengakomodasi karakteristik *phishing* sebagai kejahatan yang melibatkan dua komponen tindak pidana yang berbeda.
2. Bagi aparat penegak hukum, disarankan untuk tidak hanya berfokus pada aspek akses ilegal berdasarkan Pasal 30 UU ITE, tetapi juga mempertimbangkan penerapan Pasal 35 UU ITE dan Pasal 65 ayat (1) UU PDP secara bersamaan dalam kerangka *concursus realis*, agar penegakan hukum menjangkau seluruh rangkaian perbuatan pelaku secara komprehensif dan menghasilkan putusan yang lebih mencerminkan keadilan.
3. Bagi masyarakat, diperlukan peningkatan literasi digital dan kewaspadaan terhadap risiko *phishing*, khususnya dengan tidak mudah mempercayai tautan, situs web, email, atau notifikasi elektronik yang meminta data pribadi, informasi keuangan, atau kredensial akun.

REFRENSI

Buku

Chandra, Tofik Yanuar. 2022. *Hukum Pidana*. edited by Y. Putera. PT. Sangir Multi Usaha.

Prasetyo, Teguh. 2016. Hukum Pidana. Edisi Revi. Jakarta: Rajawali Pers.

Artikel Ilmiah

Asherli, Bella Fistya, and Sidi Ahyar Wiraguna. 2025. "Perlindungan Keamanan Data Pribadi Di Era Digital Menghadapi Serangan *Phishing* Ditinjau Dari Undang-Undang Pelindungan Data Pribadi Nomor 27 Tahun 2022." *Jurnal Hukum, Administrasi Publik* ... 2(4):01–14.

Dhyaksa, MuhDhirga, Hambali Thalib, and Rizki Ramadani. 2025. "Analisis Hukum *Concursus* Terhadap Tindak Pidana Pengancaman, Pengrusakan, Dan Penggunaan Senjata Tajam." *Legal Dialogica* 1(1):31–44.

Febrika Ardy, Lutfi Aziz, Iklima Istiqomah, Angga Eben Ezer, and Shelvie Nidya Neyman. 2024. "*Phishing* Di Era Media Sosial: Identifikasi Dan Pencegahan Ancaman Di Platform Sosial." *Journal of Internet and Software Engineering* 1(4):11. doi: 10.47134/pjise.v1i4.2753.

Gulo, Ardi Saputra, Sahuri Lasmadi, and Khabib Nawawi. 2021. "Cyber Crime Dalam Bentuk Phising Berdasarkan Undang-Undang Informasi Dan Transaksi Elektronik." *PAMPAS: Journal of Criminal Law* 1(2):68–81. doi: 10.22437/pampas.v1i2.9574.

Handoyo, Budi, Husamuddin MZ, Ida Rahma, and Asy'ari. 2024. "Tinjaun Yuridis Penegakkan Hukum Kejahatan Cyber Crime Studi Implementasi Undang-Undang Nomor 11 Tahun 2008." *MAQASIDI: Jurnal Syariah Dan Hukum* 4(1):40–55. doi: 10.47498/maqasidi.v4i1.2966.

Ismoyo, Jarot Didgo. 2019. *Metodologi Penelitian Hukum Mendapatkan Kebenaran Berdasarkan Konsep Hukum*. Ed. 1, Cet. edited by A. Avia. Jakarta: PT RajaGrafindo Persada.

Ks, Yolanda Sari, Madiasa Ablisar, Mahmud Mulyadi, and Jelly Leviza. 2022. "Analisis Yuridis Terhadap Tindak Pidana Manipulasi InformasiPengguna E-CommerceMenurut Undang-Undang Nomor 11 Tahun2008 Tentang Informasi Dan Transaksi Elektronik(Studi Putusan No. 542/Pid.Sus/2019/PN.Mlg)." *Locus: Jurnal Konsep Ilmu Hukum* 2(June):53–67.

Lokapala, Yazid Haikal, Fuad Januar Nurfauzi, and Yeni Widowaty. n.d. "Tindak Pidana Kejahatan Phising Dalam Dunia Cybercrime Ditinjau Menurut Aspek Yuridis Indonesia." *Indonesian Journal of Criminal Law and Criminology (IJCLC)*.

Mahardhika, Vita. 2021. "Pencegahan Korupsi Pengadaan Barang / Jasa Pemerintah."

Hukum 16:140–55.

Manorek, Bonaventuran Deogratia, Adi Tirto Koesomo, and Meylan Maramis. 2025. "Penegakan Hukum Pidana Dalam Memberantas Kejahatan Pencurian Data Elektronik (*Phishing*)." *Lex Privatum* 15(02).

Maramis, Aprilia Violita, Marthin Doodoh, and Marthin L.Lambonan. 2025. "Tinjauan Yuridis Terhadap Perlindungan Data Pribadi Dalam Mengatasi Cybercrime Pada Kasus *Phishing*." *Lex Privatum Jurnal Fakultas Hukum, UNSRAT* 15(2):2.

Muhammad, Faiz Emery, and Beniharmoni Harefa. 2023. "Pengaturan Tindak Pidana Bagi Pelaku Penipuan Phisning Berbasis Web." *Jurnal Usm Law Review* 6(1):226–41. doi: 10.26623/julr.v6i1.6649.

Laman

Anon. n.d. "*Phishing* (Noun)." *Merriam-Webster*. Retrieved (https://www.merriam webster.com/dictionary/*phishing*).

Bjcoid2. n.d. *Serangan Phishing Di Indonesia Terus Meningkat, Berikut Data Lengkapnya*.

Meliala, Nefa Claudia. 2020. "Beberapa Catatan Mengenai Unsur 'Sengaja' Dalam Hukum Pidana." *Hukum Online.Com*. Retrieved January 11, 2026 (https://www.hukumonline.com/berita/a/beberapa-catatan-mengenai-unsur-sengaja-dalam-hukum-pidana-oleh--nefa-claudia-meliala-lt5ee99dda4a3d2/?page=2).

Peraturan perundang-undangan

Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Transaksi Elektronik.

Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi.

Putusan Nomor 764/Pid.Sus/2022/PN Pbr.