Al-Zayn: Jurnal Ilmu Sosial & Hukum e-ISSN 3026-2917
https://ejournal.yayasanpendidikandzurriyatulquran.id/index.php/AlZyn p-ISSN 3026-2925
Volume 4 Number 2, 2026
DOI: https://doi.org/10.61104/alz.v4i2.4739

Analisis Yuridis Tindak Pidana Phising Sebagai Cyber Enabled Crime

(Studi Putusan PN Banjarbaru Nomor 85/Pid.Sus/2022/PN Bjb)

Laela Kuwayyis Wijaya[1], Nasya Nadhira Rahma[2], Keisha Nadine Sastraatmaja[3], Tyazza Amaranila Ghifari[4], Pietro Grassio Eko Yulio[5]
Program Studi Hukum, Universitas Pelita Harapan, Indonesia[1-5]
Email Korespondensi: Laelakwys@gmail.com

Article received: 01 Januari 2026, Review process: 12 Januari 2026
Article Accepted: 22 Februari 2026, Article published: 01 Maret 2026

ABSTRACT

Phishing has emerged as a significant form of cyber-enabled crime as the traditional offense of fraud increasingly relies on electronic systems and digital communication technologies. This research aims to analyze the juridical construction of phishing as regulated under Indonesian law through an examination of Decision of the Banjarbaru District Court Number 85/Pid.Sus/2022/PN Bjb. The study employs a normative legal research method with statutory and case approaches, focusing on the application of the Electronic evidence in judicial reasoning. The findings indicate that the court applied the relevant provisions of the ITE law by emphasizing the fulfillment of criminal elements and the validity of electronic evidence, while the decision also reflects challenges in addressing broader impacts of phishing crimes, particularly regarding victim protection and the evolving nature of cyber-enabled offenses.

Keywords: *Phishing, Cyber-enabled Crime, Electronic Evidence, ITE Law, Court Decision.*

ABSTRAK

Phishing merupakan bentuk kejahatan yang berkembang seiring dengan meningkatnya penggunaan sistem elektronik dan teknologi informasi dalam aktivitas masyarakat, terutama dalam transaksi keuangan dan komunikasi digital. Penelitian ini bertujuan untuk menganalisis konstruksi yuridis tindak pidana Phishing sebagai cyber enabled crime melalui studi Putusan Pengadilan Negeri Banjarbaru Nomor 85/Pid.Sus/2022/PN Bjb. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan dan pendekatan kasus yang menitikberatkan pada penerapan Undang-Undang Informasi dan Transaksi Elektronik serta penilaian terhadap alat bukti elektronik. Hasil penelitian menunjukan bahwa hakim telah menerapkan ketentuan hukum yang relevan dengan menilai pemenuhan unsur tindak pidana dan keabsahan alat bukti elektronik, namun putusan tersebut juga menunjukkan adanya keterbatasan dalam menjangkau dimensi perlindungan korban dan kompleksitas kejahatan phishing yang terus berkembang.

Kata Kunci: Phishing, Cyber enabled Crime, Alat Bukti Elektronik, Undang-Undang ITE, Putusan Pengadilan.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan mendasar dalam cara masyarakat melakukan aktivitas ekonomi, komunikasi, dan transaksi keuangan melalui sarana elektronik yang semakin terintegrasi dalam kehidupan sehari-hari. Kondisi ini sejalan dengan meningkatnya tindak pidana penipuan berbasis teknologi, sebagaimana tercermin dari data Indonesia Anti-Scam Centre yang mencatat lebih dari 432.000 laporan penipuan digital sejak November 2024 hingga Januari 2026 dengan total kerugian masyarakat mencapai sekitar Rp9,1 triliun. Angka tersebut menunjukan bahwa penipuan melalui media elektronik telah berkembang menjadi permasalahan serius yang berdampak langsung pada kerugian finansial individu serta menurunnya rasa aman dalam penggunaan layanan digital. Salah satu bentuk penipuan yang dominan dalam laporan tersebut adalah phishing, yakni perbuatan yang dilakukan dengan cara memanipulasi kepercayaan korban melalui pesan elektronik dan tautan palsu untuk memperoleh data pribadi atau menguasai akses ke rekening dan sistem pembayaran korban.

Fenomena phishing juga terlihat dalam skala global dengan tingkat kejadian yang sangat tinggi dan berlangsung secara berkelanjutan, sebagaimana dilaporkan oleh Anti-Phishing Working Group yang mencatat lebih dari satu juta serangan phishing selama periode Januari hingga Maret 2025. Data tersebut memperlihatkan bahwa sektor keuangan dan sistem pembayaran menempati posisi paling rentan terhadap serangan phishing, yang menunjukkan adanya orientasi kejahatan pada perolehan keuntungan ekonomi melalui penyalahgunaan teknologi digital. Modus operandi phishing terus mengalami perkembangan dengan menggunakan pesan singkat, media sosial, kode QR, dan situs tiruan yang menyerupai layanan resmi sehingga meningkatkan keberhasilan pelaku dalam mengecoh korban. Keadaan ini menunjukkan bahwa teknologi digital berperan sebagai sarana yang mempercepat penyebaran kejahatan penipuan dan memperluas cakupan korban dalam waktu yang relatif singkat.

Situasi di Indonesia semakin kompleks dengan tingginya aktivitas mencurigakan di ruang siber, sebagaimana tercerminnya dalam laporan Badan Siber dan Sandi negara yang mencatat ratusan juta trafik anomali sepanjang tahun 2023. Sepanjang tahun 2023. Aktivitas tersebut seringkali berkaitan dengan upaya penipuan, pencurian data, dan penyalahgunaan sistem elektronik yang diawali melalui teknik phishing dan rekayasa sosial. Kondisi ini menggambarkan bahwa phishing berfungsi sebagai pintu masuk bagi berbagai bentuk kejahatan siber lain yang saling berkaitan dalam satu rangkaian perbuatan melawan hukum. Realitas tersebut menghadirkan tantangan besar bagi penegakan hukum, khususnya dalam mengidentifikasi pelaku, menelusuri alur kejahatan, dan mengamankan bukti yang sebagian besar berbentuk data elektronik.

Dalam perspektif hukum pidana, phishing dapat dipahami sebagai cyber enabled crime karena perbuatan penipuan yang telah lama dikenal memperoleh karakteristik baru melalui pemanfaatan teknologi informasi sebagai sarana utama pelaksanaan kejahatan. Ketergantungan pada sistem elektronik, jaringan internet,

dan kepercayaan pengguna layanan digital menjadikan phishing memiliki kompleksitas tersendiri dalam aspek pembuktian dan pertanggungjawaban pidana. Pembuktian tindak pidana phishing sangat bergantung pada alat bukti elektronik seperti rekam komunikasi digital, data transaksi keuangan, dan jejak aktivitas sistem yang memerlukan penilaian hukum secara sistematis. Keadaan ini menuntut peran aktif aparat penegak hukum dan hakim dalam memahami karakteristik kejahatan siber agar penerapan hukum dapat berjalan secara tepat dan adil.

Putusan Pengadilan Negeri Banjarbaru Nomor 85/Pid Sus/2022/PN Bjb memberikan gambaran konkret mengenai bagaimana tindak pidana phishing diproses dalam sistem peradilan pidana Indonesia. Perkara tersebut menunjukan penerapan Undang-Undang Informasi dan Transaksi Elektronik dalam menilai perbuatan terdakwa serta penggunaan alat bukti elektronik sebagai dasar pembuktian di persidangan. Pertimbangan hakim dalam putusan ini mencerminkan upaya pengadilan dalam menyesuaikan norma hukum pidana dengan karakteristik kejahatan yang dilakukan melalui sarana digital. Analisis terhadap putusan tersebut menjadi penting untuk menilai konsistensi penerapan unsur tindak pidana, kekuatan pembuktian elektronik, serta relevansi konsep cyber crime dalam praktik peradilan.

Berdasarkan fenomena dan data empiris tersebut, kajian yuridis terhadap tindak pidana phishing sebagai cyber enabled crime memiliki urgensi akademik dan praktis yang tinggi. Penelitian terhadap putusan Pengadilan Negeri Banjarbaru memungkinkan pengkajian mendalam mengenai bagaimana hukum positif merespons kejahatan penipuan berbasis teknologi serta sejauh mana perlindungan hukum terhadap korban dapat diwujudkan. Pendekatan yuridis normatif dengan studi putusan memberikan ruang analisis terhadap konstruksi hukum yang digunakan hakim dalam menilai perbuatan phishing dan alat bukti elektronik yang diajukan di persidangan. Melalui penelitian ini diharapkan dapat diperoleh pemahaman yang lebih komprehensif mengenai penegakan hukum terhadap tindak pidana phishing serta kontribusinya bagi pengembangan hukum pidana siber di Indonesia.

METODE

Penelitian ini menggunakan metode penelitian hukum normatif yang berfokus pada pengkajian norma hukum positif yang mengatur tindak pidana phishing serta penerapannya dalam praktik peradilan pidana. Pendekatan yang digunakan adalah pendekatan perundang-undangan dan pendekatan kasus dengan menelaah ketentuan Undang-undangan Informasi dan Transaksi Elektronik serta putusan Pengadilan Negeri Banjarbaru Nomor 85/Pid Sus/2022/PN Bjb sebagai objek kajian utama. Pendekatan tersebut digunakan untuk mengkaji kesesuaian antara norma hukum yang berlaku dengan pertimbangan hukum hakim dalam memutus perkara tindak pidana phishing. Melalui pendekatan ini, penelitian diarahkan untuk memahami konstruksi yuridis

phishing sebagai cyber enabled crime serta penerapan unsur-unsur tindak pidana dan alat bukti elektronik dalam putusan pengadilan.

Jenis dan sumber bahan hukum yang digunakan dalam penelitian ini terdiri atas bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier yang saling melengkapi dalam proses analisis. Bahan hukum primer meliputi peraturan perundang-undangan yang relevan dan putusan Pengadilan Negeri Banjarbaru Nomor 85/Pid Sus/2022/PN Bjb, sementara bahan hukum sekunder mencakup buku teks, hukum, jurnal ilmiah, dan publikasi resmi yang membahas hukum pidana siber serta kejahatan phishing. Bahan hukum tersier digunakan sebagai penunjang untuk memberikan pemahaman konseptual dan terminologis terhadap istilah-istilah hukum yang digunakan dalam penelitian. Keseluruhan bahan hukum tersebut dikumpulkan melalui studi kepustakaan dengan cara menelusuri dan menelaah sumber-sumber hukum yang relevan secara sistematis. Teknik analisis bahan hukum dalam penelitian ini dilakukan secara kualitatif dengan menggunakan metode analisis deskriptif-analitif untuk menguraikan dan menilai fakta hukum, norma hukum, serta pertimbangan hakim dalam putusan yang dikaji. Analisis dilakukan dengan cara menghubungkan ketentuan hukum pidana siber dengan fakta-fakta yang terungkap dalam putusan pengadilan, termasuk modus phishing, alat bukti elektronik, dan pemenuhan unsur tindak pidana. Proses analisis tersebut diarahkan untuk menilai kekuatan pembuktian elektronik serta konsistensi penerapan konsep cyber enabled crime dalam praktik peradilan. Hasil analisis kemudian disusun secara sistematis untuk memberikan gambaran menyeluruh mengenai penegakan hukum terhadap tindak pidana phishing dalam kerangka hukum pidana Indonesia.

HASIL DAN PEMBAHASAN

Kronologi dan Fakta Hukum Perkara Phishing

Perkara tindak pidana di bidang teknologi informasi ini diperiksa dan diputus oleh Pengadilan Negeri Banjarbaru melalui Putusan Nomor 85/Pid.Sus/2022/PN Bjb tanggal 14 Juli 2022. Perkara ini berkaitan dengan kejahatan siber berupa pembuatan dan penjualan perangkat lunak phishing yang digunakan untuk mencuri data pribadi dan data keuangan secara ilegal melalui media elektronik.

Terdakwa dalam perkara ini adalah Riswanda Noor Saputra, yang diketahui mengoperasikan platform daring bernama 16shop.vip, sebuah situs yang menyediakan layanan Phishing-as-a-Service (PaaS), yaitu penyediaan perangkat phishing kepada pihak lain dengan imbalan tertentu. Berdasarkan hasil penyelidikan yang melibatkan kerja sama internasional, platform tersebut teridentifikasi oleh FBI dan NCB INTERPOL sebagai salah satu penyedia phishing toolkit yang beroperasi dari Indonesia. Terdakwa ditangkap pada 19 November 2021 di kediamannya di Kalimantan Selatan.

Secara kronologis, perbuatan terdakwa dimulai pada Desember 2017, ketika terdakwa mulai membuat perangkat lunak yang meniru tampilan situs-situs

populer seperti Apple, Amazon, dan PayPal. Pada awalnya terdakwa mengaku tidak mengetahui secara pasti tujuan penggunaan perangkat tersebut.

Namun, sejak tahun 2018, terdakwa telah menyadari bahwa perangkat lunak tersebut digunakan untuk mencuri data identitas dan informasi kartu kredit milik korban. Meskipun demikian, terdakwa tetap melanjutkan kegiatannya dengan menyempurnakan perangkat phishing tersebut dan pada Desember 2019 meluncurkan situs 16shop.vip sebagai sarana penjualan. Setiap unit phishing toolkit dijual dengan harga sekitar Rp1.000.000,00, dan tercatat sekitar 400 pembeli telah menggunakan layanan tersebut.

Modus operandi yang dilakukan terdakwa bersifat teknis dan terstruktur. Terdakwa menggunakan perangkat lunak XAMPP dan Sublime Text untuk memodifikasi desain situs asli dengan bahasa pemrograman HTML, PHP, JavaScript, dan CSS. Perangkat lunak tersebut dirancang untuk merekam data sensitif korban, seperti kredensial akun, informasi kartu pembayaran, serta data pendukung lainnya.

Dalam pelaksanaannya, para pembeli phishing toolkit menyebarkan email palsu secara massal kepada calon korban, yang berisi tautan menuju halaman situs palsu buatan terdakwa. Ketika korban memasukkan data pribadinya, data tersebut secara otomatis tersimpan dalam basis data yang dapat diakses oleh pelaku.

Akibat perbuatan tersebut, korban mengalami kerugian nyata. Salah satu korban, Mari Ramadhan Alvianto, mengalami transaksi ilegal pada akun PayPal miliknya setelah menerima email konfirmasi palsu pada tahun 2021. Selain merugikan korban, kejahatan ini juga memberikan keuntungan finansial yang besar bagi terdakwa. Berdasarkan hasil analisis PPATK, terdapat aliran dana masuk ke rekening terdakwa sebesar Rp1.702.383.118,00 dalam periode Agustus 2019 hingga November 2021, yang kemudian digunakan untuk memenuhi kebutuhan pribadi dan pembelian aset bernilai tinggi.

Dalam persidangan, Penuntut Umum mengajukan dakwaan kumulatif yang mencakup pelanggaran ketentuan Undang-Undang Informasi dan Transaksi Elektronik serta Undang-Undang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang. Penuntut Umum menuntut terdakwa dengan pidana penjara selama 1 (satu) tahun. Namun, Majelis Hakim Pengadilan Negeri Banjarbaru memiliki pertimbangan tersendiri dengan menilai bahwa perbuatan terdakwa telah menimbulkan keresahan di masyarakat luas dan dilakukan secara berkelanjutan dengan memperoleh keuntungan dalam jumlah besar.

Berdasarkan pertimbangan tersebut, Majelis Hakim menjatuhkan pidana penjara selama 2 (dua) tahun dan 6 (enam) bulan serta denda sebesar Rp500.000.000,00. Selain itu, Majelis Hakim memerintahkan perampasan aset-aset yang diperoleh dari hasil tindak pidana untuk dirampas oleh negara, serta pemusnahan sarana elektronik yang digunakan dalam pelaksanaan kejahatan tersebut.

Penerapan Pasal-Pasal UU ITE dalam Putusan PN Banjarbaru

Dalam Putusan Nomor 85/Pid.Sus/2022/PN Bjb, Pengadilan Negeri Banjarbaru menerapkan ketentuan pidana dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) terhadap perbuatan terdakwa. Pasal yang digunakan sebagai dasar pemidanaan adalah Pasal 50 jo. Pasal 34 ayat (1) huruf a UU ITE, sedangkan dakwaan alternatif berupa Pasal 51 jo. Pasal 35 UU ITE tidak dipilih oleh Majelis Hakim.

Pasal 34 ayat (1) huruf a UU ITE mengatur larangan bagi setiap orang untuk memproduksi, menjual, atau menyediakan perangkat keras atau perangkat lunak komputer yang dirancang atau dikembangkan secara khusus untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33 UU ITE. Dalam perkara ini, Majelis Hakim mengkualifikasikan perbuatan terdakwa sebagai tindak pidana penyalahgunaan perangkat (misuse of device), karena fokus perbuatan terdakwa terletak pada pembuatan perangkat lunak dengan fungsi teknis tertentu yang memungkinkan terjadinya kejahatan siber.

Dalam menilai pemenuhan unsur "setiap orang", Majelis Hakim memandang terdakwa sebagai subjek hukum perorangan yang cakap dan mampu mempertanggungjawabkan perbuatannya secara hukum. Oleh karena itu, unsur tersebut dinyatakan terpenuhi. Terhadap unsur "dengan sengaja dan tanpa hak atau melawan hukum", Majelis Hakim menilai bahwa terdakwa mengetahui sifat terlarang dari perbuatan yang dilakukannya dan tetap melanjutkan perbuatan tersebut tanpa memiliki hak atau kewenangan hukum.Sikap batin tersebut dipandang telah memenuhi unsur kesengajaan sekaligus unsur tanpa hak.

Unsur "memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki" dinilai bersifat alternatif, sehingga pemenuhan salah satu perbuatan sudah cukup untuk memenuhi unsur ini. Majelis Hakim menyimpulkan bahwa terdakwa terbukti melakukan perbuatan memproduksi dan menjual perangkat lunak komputer, sehingga unsur tersebut telah terpenuhi.

Sementara itu, unsur "perangkat keras atau perangkat lunak komputer yang dirancang atau dikembangkan secara khusus untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33" dinilai sebagai unsur yang paling menentukan. Majelis Hakim menilai bahwa perangkat lunak yang dibuat terdakwa tidak bersifat netral, melainkan secara khusus dirancang untuk memfasilitasi perbuatan yang dilarang dalam UU ITE, khususnya perbuatan sebagaimana diatur dalam Pasal 32 ayat (2) UU ITE.

Berdasarkan penilaian terhadap seluruh unsur tersebut, Majelis Hakim menyimpulkan bahwa perbuatan terdakwa telah memenuhi seluruh unsur Pasal 34 ayat (1) huruf a UU ITE, sehingga dakwaan kesatu dinyatakan terbukti secara sah dan meyakinkan. Sebaliknya, Majelis Hakim tidak menerapkan Pasal 35 UU ITE dengan pertimbangan bahwa pasal tersebut menitikberatkan pada pemalsuan informasi atau dokumen elektronik, sedangkan perbuatan terdakwa lebih tepat dikualifikasikan sebagai pembuatan perangkat lunak dengan fungsi teknis yang

memfasilitasi kejahatan siber. Dengan demikian, penerapan Pasal 34 ayat (1) huruf a UU ITE dalam putusan ini dinilai telah sesuai dengan karakter perbuatan terdakwa dan tujuan pengaturan tindak pidana di bidang teknologi informasi.

Pembuktian Alat Bukti Elektronik dalam Kasus Phishing

Berdasarkan telaah hukum terhadap Putusan Nomor 85/Pid.Sus/2022/PN Bjb, terlihat bahwa Majelis Hakim memanfaatkan berbagai bentuk alat bukti elektronik yang saling berkaitan untuk membuktikan kesalahan Terdakwa Riswanda Noor Saputra. Alat bukti tersebut tidak berdiri sendiri, tetapi saling menguatkan satu sama lain sehingga membentuk rangkaian pembuktian yang utuh. Salah satu alat bukti yang digunakan adalah percakapan digital yang ditemukan melalui pemeriksaan ahli digital forensik terhadap barang bukti berupa satu unit iPhone 11 Pro milik Terdakwa. Dari hasil pemeriksaan tersebut, ditemukan adanya komunikasi aktif antara Terdakwa dengan beberapa nomor telepon yang datanya sesuai dengan hasil penyidikan terkait penjualan Phishing Tool Kit. Percakapan ini menunjukkan adanya keterkaitan langsung antara Terdakwa sebagai penyedia sarana dengan pihak-pihak yang membeli alat tersebut.

Selain itu, pengadilan juga menghadirkan bukti berupa mutasi rekening PT Bank Central Asia (BCA) atas nama Terdakwa dengan periode transaksi Agustus 2019 sampai November 2021. Dari mutasi rekening tersebut, terdeteksi adanya aliran dana sekitar Rp1,7 miliar. Meskipun Terdakwa beralasan bahwa uang tersebut berasal dari jasa pembuatan web design, Majelis Hakim menilai bahwa pola transaksi tersebut berkaitan dengan rangkaian alat bukti elektronik lainnya yang diajukan di persidangan. Bukti lainnya berupa lembaran struk transfer ATM BCA sebesar Rp900.329,00 yang masuk ke rekening Terdakwa. Di samping itu, ditemukan pula riwayat pembayaran digital melalui Payment Gateway OVO yang digunakan untuk membayar layanan hosting di IDCloudhost. Hosting tersebut digunakan untuk menjalankan operasional website phishing 16shop, Bukti ini memperlihatkan keterkaitan antara sistem pembayaran elektronik dengan operasional website phishing yang dijalankan Terdakwa.

Untuk memastikan keabsahan alat bukti elektronik tersebut, pengadilan juga mendasarkan pada Berita Acara Pemeriksaan Barang Bukti Digital Nomor: 524-XII-2021-SIBER. Pemeriksaan oleh ahli digital forensik memastikan bahwa pada laptop dan handphone Terdakwa ditemukan file berformat PHP, HTML, SQL, dan ZIP yang berkaitan dengan sistem 16shop. Hal ini menjadi dasar bagi Majelis Hakim untuk menerima hasil pemeriksaan tersebut sebagai alat bukti elektronik yang sah sebagaimana diatur dalam Pasal 5 ayat (1) UU ITE. Pertimbangan hakim dalam perkara ini juga menunjukkan bahwa pembuatan website phishing yang menyerupai tampilan resmi Apple dan PayPal merupakan bagian dari perbuatan yang didakwakan kepada Terdakwa berdasarkan UU ITE. Melalui rangkaian alat bukti elektronik tersebut, Majelis Hakim menilai bahwa Terdakwa secara sadar dan aktif menjalankan sistem elektronik yang digunakan untuk melakukan kejahatan serta menerima pembayaran atas penjualan software tersebut melalui sistem

elektronik. Jejak transaksi elektronik juga menjadi bagian penting dalam pembuktian, terutama dalam kaitannya dengan Tindak Pidana Pencucian Uang (TPPU). Ditemukan aktivitas transaksi pada akun Indodax milik Terdakwa dengan username Devilscream. Majelis Hakim mempertimbangkan perubahan pola transaksi tersebut sebagai bagian dari rangkaian perbuatan yang berkaitan dengan Tindak Pidana Pencucian Uang.

Dalam putusan ini, penerapan Pasal 5 UU ITE terlihat jelas sebagai dasar legalitas penggunaan alat bukti elektronik, Pasal 5 ayat (1) UU ITE menyatakan bahwa Informasi Elektronik, Dokumen Elektronik, maupun hasil cetaknya merupakan alat bukti hukum yang sah. Oleh karena itu, Majelis Hakim menerima berbagai hasil cetak seperti tangkapan layar (screen capture) website 16shop, akun PayPal, mutasi rekening bank, dan mutasi akun indodax sebagai alat bukti yang sah dalam hukum acara.

Phishing sebagai Cyber Enabled Crime dalam Putusan Ini

Berdasarkan pertimbangan hukum Majelis Hakim dalam Putusan Nomor 85/Pid.Sus/2022/PN Bjb, perbuatan phishing yang dilakukan oleh Terdakwa dipahami sebagai tindak pidana yang pelaksanaannya secara langsung bergantung pada pemanfaatan sistem dan teknologi informasi. Majelis Hakim menilai bahwa substansi perbuatan Terdakwa pada dasarnya merupakan penipuan, namun dilakukan melalui sarana elektronik berupa pembuatan dan pengoperasian perangkat lunak serta website palsu yang menyerupai tampilan layanan resmi pihak lain, sehingga memungkinkan penguasaan data pribadi dan keuangan korban secara melawan hukum. Pertimbangan tersebut menunjukkan bahwa kejahatan yang diperiksa bukan merupakan jenis kejahatan baru, melainkan bentuk penipuan konvensional yang pelaksanaannya diperluas dan dimungkinkan secara efektif melalui penggunaan teknologi informasi dan sistem elektronik sebagaimana diatur dalam Undang-Undang Informasi dan Transaksi Elektronik.

Majelis Hakim secara tegas mengaitkan perbuatan Terdakwa dengan ketentuan Pasal 34 ayat (1) huruf a Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016, dengan menilai bahwa Terdakwa telah memproduksi dan menjual perangkat lunak komputer yang secara khusus dirancang dan dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33 UU ITE. Dalam pertimbangannya, Majelis Hakim menekankan bahwa perangkat lunak phishing yang dibuat dan diperdagangkan oleh Terdakwa tidak bersifat netral, melainkan memiliki fungsi teknis tertentu yang secara langsung ditujukan untuk melakukan kejahatan melalui sistem elektronik. Dengan demikian, teknologi informasi tidak sekadar menjadi sarana pendukung, tetapi menjadi instrumen utama yang memungkinkan terjadinya perbuatan pidana secara sistematis dan berkelanjutan.

Lebih lanjut, Majelis Hakim juga menilai bahwa penggunaan sistem elektronik dalam perkara ini menyebabkan dampak perbuatan menjadi lebih luas dan masif, sebagaimana tercermin dari banyaknya korban serta besarnya aliran

dana hasil kejahatan yang masuk ke rekening Terdakwa. Pertimbangan tersebut diperkuat dengan pembuktian berupa alat bukti elektronik, antara lain percakapan digital, mutasi rekening bank, riwayat transaksi pembayaran elektronik, serta temuan hasil pemeriksaan forensik digital terhadap perangkat yang digunakan Terdakwa. Rangkaian alat bukti tersebut menunjukkan bahwa teknologi informasi memungkinkan perbuatan penipuan dilakukan secara lintas wilayah, berulang, dan dengan jangkauan korban yang jauh lebih besar dibandingkan penipuan konvensional.

Relevansi Putusan Pengadilan Negeri Banjarbaru Nomor 85/Pid.Sus/2022/PN Bjb dengan konsep cyber enabled crime tercermin dari cara Majelis Hakim mengkualifikasikan perbuatan Terdakwa sebagai penipuan yang difasilitasi dan diperkuat oleh sistem elektronik, serta dari pilihan penerapan pasal-pasal UU ITE yang secara khusus mengatur penyalahgunaan teknologi informasi. Tanpa menciptakan delik baru, Majelis Hakim menempatkan teknologi informasi sebagai faktor krusial yang memperluas skala, efektivitas, dan dampak kejahatan penipuan tersebut. Dengan demikian, putusan ini menunjukkan penerapan hukum pidana yang sejalan dengan karakteristik cyber enabled crime, yaitu kejahatan konvensional yang dalam pelaksanaannya sangat bergantung pada teknologi informasi sehingga menimbulkan kompleksitas pembuktian dan dampak yang lebih besar dalam ruang siber.

Implikasi Putusan terhadap Penegakan Hukum Cyber Crime di Indonesia

Putusan Nomor 85/Pid.Sus/2022/PN Bjb membawa implikasi yang signifikan terhadap perlindungan korban penipuan online dalam konteks penegakan hukum cyber crime di Indonesia. Dalam pertimbangan hukumnya, Majelis Hakim secara tegas mengakui adanya kerugian nyata yang dialami oleh para korban sebagai akibat langsung dari perbuatan phishing yang dilakukan oleh Terdakwa, yang dibuktikan melalui aliran dana hasil kejahatan ke rekening Terdakwa penggunaan data korban tanpa hak. Pengakuan terhadap kerugian korban ini menunjukkan bahwa kejahatan siber tidak dipandang sebagai kejahatan yang bersifat abstrak atau semata-mata teknis, melainkan sebagai perbuatan yang menimbulkan dampak konkret terhadap hak dan kepentingan individu. Dengan menerima dan menilai alat bukti elektronik sebagai alat bukti yang sah dan menentukan, Majelis Hakim secara tidak langsung memperkuat posisi korban dalam perkara penipuan online, khususnya dalam hal pembuktian kerugian yang timbul dari penyalahgunaan sistem elektronik.

Dari perspektif penegakan hukum cyber crime, putusan ini memperlihatkan kelebihan yang penting, yaitu kejelasan penerapan Undang-Undang Informasi dan Transaksi Elektronik dalam menjerat perbuatan phishing. Majelis Hakim secara konsisten membangun konstruksi hukum berdasarkan Pasal 34 ayat (1) huruf a UU ITE dengan menitikberatkan pada perbuatan Terdakwa yang memproduksi dan memperjualbelikan perangkat lunak yang secara khusus dirancang untuk memfasilitasi kejahatan melalui sistem elektronik. Pendekatan ini menunjukkan pemahaman hakim bahwa kejahatan siber tidak hanya dilakukan oleh pelaku yang

secara langsung menipu korban, tetapi juga oleh pihak-pihak yang menyediakan sarana teknis yang memungkinkan kejahatan tersebut terjadi. Kejelasan penerapan pasal ini memberikan arah yang jelas bagi aparat penegak hukum dalam menangani perkara serupa, sekaligus mencegah kerancuan dalam mengkualifikasikan perbuatan phishing antara penipuan konvensional dan tindak pidana di bidang teknologi informasi.

Namun demikian, di balik kelebihan tersebut, putusan ini juga memperlihatkan kelemahan yang patut dicermati secara kritis, khususnya terkait dengan orientasi pemidanaan yang masih berfokus pada pelaku. Pertimbangan Majelis Hakim lebih banyak diarahkan pada pembuktian unsur tindak pidana, peran dan kesalahan Terdakwa, serta pemenuhan syarat pertanggungjawaban pidana, sementara aspek pemulihan korban belum mendapatkan perhatian yang memadai. Meskipun kerugian korban diakui sebagai akibat dari perbuatan pidana, putusan ini belum secara maksimal menggali mekanisme pengembalian kerugian atau pemulihan hak korban sebagai bagian dari tujuan penegakan hukum. Hal ini mencerminkan bahwa dalam praktik peradilan cyber crime, orientasi retributif masih lebih dominan dibandingkan pendekatan restoratif yang berfokus pada kepentingan korban.

Implikasi lebih lanjut dari putusan ini menunjukkan bahwa penegakan hukum cyber crime tidak dapat hanya bertumpu pada pendekatan penal semata, tetapi perlu didukung oleh upaya pencegahan yang bersifat struktural dan edukatif. Fakta bahwa modus phishing dalam perkara ini berhasil menjangkau banyak korban menunjukkan adanya keterbatasan literasi digital masyarakat dalam mengenali risiko penyalahgunaan data dan transaksi elektronik. Selain itu, meskipun perkara ini diproses berdasarkan UU ITE, karakter kejahatan yang melibatkan pengumpulan dan penyalahgunaan data pribadi korban menunjukkan adanya irisan yang kuat dengan rezim perlindungan data pribadi. Dengan demikian, putusan ini secara implisit menegaskan pentingnya sinergi antara penegakan UU ITE dengan kebijakan perlindungan data pribadi, agar penanganan cyber crime tidak hanya berorientasi pada penghukuman pelaku, tetapi juga pada pencegahan kejahatan dan perlindungan hak korban secara lebih komprehensif.

SIMPULAN

Berdasarkan hasil pembahasan terhadap Putusan Pengadilan Negeri Banjarbaru Nomor 85/Pid.Sus/2022/PN Bjb, dapat dipahami bahwa tindak pidana phishing dalam perkara ini merupakan bentuk penipuan yang dilakukan dengan memanfaatkan sistem elektronik. Perkembangan teknologí membuat cara melakukan penipuan menjadi lebih luas jangkauannya, lebih cepat, dan lebih sulit dilacak dibandingkan penipuan dengan cara biasa. Dalam putusan ini, Majelis Hakim telah menerapkan ketentuan UU ITE dengan menilai terpenuhinya unsur tindak pidana serta menerima berbagai alat bukti elektronik yang saling berkaitan untuk membuktikan kesalahan terdakwa. Alat bukti elektronik seperti percakapan digital, mutasi rekening bank, riwayat pembayaran elektronik, dan jejak transaksi kripto menunjukkan peran penting data elektronik dalam proses pembuktian di

persidangan. Pemeriksaan digital forensik juga memastikan bahwa data yang digunakan tetap asli dan tidak mengalami perubahan, sehingga memiliki kekuatan pembuktian yang dapat dipertanggungjawabkan.

Hal ini memperlihatkan bahwa pembuktian dalam perkara kejahatan siber sangat bergantung pada kemampuan penegak hukum dalam membaca dan menilai jejak digital yang ditinggalkan pelaku. Di sisi lain, putusan ini memperlihatkan bahwa pertimbangan hakim masih lebih berfokus pada pembuktian kesalahan pelaku dan penjatuhan pidana, sementara pembahasan mengenai kondisi dan pemulihan korban belum menjadi perhatian utama. Dalam tindak pidana phishing, kerugian korban tidak hanya berupa kehilangan uang, tetapi juga menyangkut keamanan data pribadi yang berpotensi disalahgunakan kembali. Hal ini menunjukkan bahwa penanganan kejahatan siber tidak hanya berkaitan dengan penghukuman pelaku, tetapi juga perlu memperhatikan perlindungan korban dan kesadaran masyarakat dalam menggunakan sistem elektronik.

DAFTAR RUJUKAN

Pengadilan Negeri Banjarbaru. (2022). *Putusan Nomor 85/Pid.Sus/2022/PN Bjb*. Pengadilan Negeri Banjarbaru.

Republik Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58. Sekretariat Negara.

Republik Indonesia. (2010). *Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang*. Lembaran Negara Republik Indonesia Tahun 2010 Nomor 122.

Republik Indonesia. (2016). *Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251. Sekretariat Negara.

Arief, B. N. (2016). *Tindak pidana mayantara: Perkembangan kajian cyber crime di Indonesia*. RajaGrafindo Persada.

Chazawi, A., & Ferdian, A. (2015). *Tindak pidana informasi & transaksi elektronik: Penyerangan terhadap kepentingan hukum pemanfaatan teknologi informasi dan transaksi elektronik*. Media Nusa Creative.

INTERPOL. (2021). *NCB INTERPOL communication number CAR-21-0074-ID regarding phishing toolkit investigation*. INTERPOL.

Lamintang, P. A. F. (2014). *Dasar-dasar hukum pidana Indonesia*. Citra Aditya Bakti.

Pusat Pelaporan dan Analisis Transaksi Keuangan. (2021). *Laporan analisis transaksi keuangan mencurigakan*. PPATK.

Sitompul, J. (2012). *Cyberspace, cybercrimes, cyberlaw: Tinjauan aspek hukum pidana*. Tatanusa.

Suhariyanto, B. (2013). *Tindak pidana teknologi informasi (cybercrime): Urgensi pengaturan dan celah hukumnya*. RajaGrafindo Persada.

Yanuar, M. A. (2015). *Tindak pidana pencucian uang dan perampasan aset*. Prenadamedia Group.

Kepolisian Negara Republik Indonesia. (2021). *Berita Acara Pemeriksaan Barang Bukti Digital Nomor: 524-XII-2021-SIBER*.

Pengadilan Negeri Banjarbaru. (2022). *Putusan Nomor 85/Pid.Sus/2022/PN Bjb: Keterangan Ahli Digital Forensik Muhamad Asep Saputra, S.T.*

Pengadilan Negeri Banjarbaru. (2022). Putusan Nomor 85/Pid.Sus/2022/PN Bjb: Keterangan Ahli ITE Denden Imadudin Soleh, S.H., M.H., CLA.

Pengadilan Negeri Banjarbaru. (2022). Putusan Nomor 85/Pid.Sus/2022/PN Bjb: Keterangan Ahli PPATK Dhira Gulista Sudjaja, S.H., L.L.M. terkait analisis mutasi rekening dan transaksi kripto.

Mia Haryati Wibowo dan Nur Fatimah, "Ancaman phishing terhadap pengguna sosial media dalam dunia cyber crime," JOEICT(jurnal Educ. Inf. Commun. Technol., vol. 1, pp. 1–5, 2017, [Online].Available: http://jurnal.stkippgritulungagung.ac.id/index.php/joeict/article/view/69

D. Rachmawati, "Phising Sebagai Salah Satu Bentuk Ancaman Dalam Dunia Cyber," J. Ilm. Saintikom, Univ. Sumatera Utara, Medan, vol. 1978–6603, pp. 209–216, 2014.N. Abdelhamid, "Multi-label rules for phishing classification," Appl. Comput. Informatics, vol. 11, no. 1

M. Junger, L. Montoya, and F.-J. Overink, "Priming and warnings are not effective to prevent social engineering attacks," Comput. Human Behav., vol. 66, pp. 75–87, 2017