Jurnal Komputer, Informasi dan Teknologi Vol: 5, No 2, 2025, Page: 1-11

Pertanggungjawaban Pidana Pelaku *Phishing* dan Efektivitas Penegakan Hukum Berdasarkan UU Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik

Fauzan Mahdi Irawan*, Muhammad Zibran AL Habsy, Asmak Ul Hosnah

Universitas Pakuan

Abstrak: Perkembangan teknologi informasi telah memunculkan berbagai kejahatan siber, seperti *phishing*, yang mengalami peningkatan signifikan di Indonesia, dengan lebih dari 400 juta insiden siber tercatat pada tahun 2023. Penelitian ini bertujuan untuk menganalisis pertanggungjawaban pidana pelaku *phishing* dan mengevaluasi efektivitas penegakan hukum sesuai dengan UU Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Metode penelitian yang digunakan adalah normatif yuridis dengan pendekatan perundang-undangan dan pendekatan kasus, menggunakan bahan hukum primer seperti UU ITE, UU Perlindungan Data Pribadi, dan KHUP, serta bahan hukum sekunder seperti jurnal ilmiah dan putusan pengadilan. Hasil penelitian menunjukkan bahwa kerangka hukum untuk pertanggungjawaban pidana pelaku *phishing* cukup komprehensif, mencakup Pasal 28 ayat (1), Pasal 30, dan Pasal 35 UU ITE. Hukuman pidana dikenakan denda hingga Rp12 miliar dan penjara hingga 12 tahun. Namun, implementasi penegakan hukum terus menghadapi tantangan berupa kesulitan dalam mengumpulkan bukti elektronik, masalah yurisdiksi lintas negara, dan kurangnya kapasitas forensik digital. Rendahnya literasi digital masyarakat dan ketidakhadiran mekanisme restitusi yang jelas juga mengakibatkan perlindungan hukum yang kurang optimal bagi korban. Penelitian ini menyimpulkan bahwa reformasi sistemik diperlukan untuk meningkatkan efektivitas penegakan hukum dan melindungi korban *phishing* di Indonesia.

Kata kunci: *Phishing*, Kejahatan Siber, UU ITE

DOI: https://doi.org/10.53697/jkomitek.v5i2.3159
Correspondence: Fauzan Mahdi Irawan
Email: zibranals31@gmail.com

Received: 22-10-2025
Accepted: 22-11-2025
Published: 22-12-2025

Abstract: *The development of information technology has given rise to various cybercrimes, such as phishing, which has seen a significant increase in Indonesia, with more than 400 million cyber incidents recorded in 2023. This study aims to analyze the criminal liability of phishing perpetrators and evaluate the effectiveness of law enforcement in accordance with Law Number 19 of 2016 concerning Electronic Information and Transactions. The research method used is normative juridical with a legislative and case approach, using primary legal materials such as the ITE Law, the Personal Data Protection Law, and the Criminal Code, as well as secondary legal materials such as scientific journals and court decisions. The results of the study show that the legal framework for the criminal liability of phishing perpetrators is quite comprehensive, covering Article 28 paragraph (1), Article 30, and Article 35 of the ITE Law. Criminal penalties include fines of up to IDR 12 billion and imprisonment of up to 12 years. However, law enforcement continues to face challenges in the form of difficulties in collecting electronic evidence, cross-border jurisdiction issues, and a lack of digital forensic capacity. Low digital literacy among the public and the absence of clear restitution mechanisms also result in suboptimal legal protection for victims. This study concludes that systemic reform is needed to improve the effectiveness of law enforcement and protect victims of phishing in Indonesia.*

Keywords: *Phishing, Cybercrime, ITE Law*

Pendahuluan

Perkembangan teknologi informasi dan komunikasi telah secara signifikan mengubah berbagai aspek masyarakat *modern*. Komunikasi, transaksi, dan interaksi *online* menjadi lebih efisien berkat digitalisasi layanan publik dan privat serta kemudahan akses internet. Namun, kemajuan ini juga disertai dengan munculnya berbagai bentuk kejahatan baru yang memanfaatkan kelemahan dalam sistem keamanan digital, termasuk *phishing*. *Phishing* adalah bentuk penipuan digital yang melibatkan penggunaan media elektronik palsu untuk menipu korban agar memberikan informasi pribadi, termasuk nomor rekening, *username*, dan *password* (Putra, 2021). Modus operandi *phishing* terus berubah seiring dengan kemajuan teknologi, sehingga semakin sulit bagi individu dengan literasi digital terbatas untuk mengidentifikasinya.

Dalam beberapa tahun terakhir, jumlah kasus *phishing* di Indonesia mengalami peningkatan yang signifikan. Selama tahun 2023, Badan Siber dan Sandi Nasional (BSSN) melaporkan bahwa masyarakat mengalami lebih dari 400 juta insiden siber, dengan *phishing* menjadi bentuk serangan yang paling umum (BSSN, 2023). Kerugian yang ditimbulkan tidak hanya berupa kerugian material, seperti kehilangan dana di akun atau penipuan kartu kredit, tetapi juga kerugian immaterial, seperti kebocoran data pribadi yang dapat dimanfaatkan untuk kegiatan kriminal lebih lanjut. Jumlah kasus *phishing* yang signifikan menunjukkan bahwa ancaman kejahatan siber ini telah berkembang menjadi masalah serius yang memerlukan perhatian berbagai pemangku kepentingan, terutama aparat penegak hukum dan pembuat kebijakan.

Peningkatan insiden *phishing* menunjukkan bahwa kejahatan siber telah menjadi masalah yang tidak dapat diabaikan. Data dari *Anti-Phishing Working Group* (APWG) menunjukkan bahwa serangan *phishing* secara global meningkat sebesar 46% pada kuartal pertama 2018 dibandingkan dengan periode sebelumnya. *Phishing* diperkirakan menyebabkan kerugian finansial sebesar miliaran rupiah setiap tahun di Indonesia, selain kerugian non-materiil seperti trauma psikologis dan penurunan kepercayaan publik terhadap sistem digital. Kondisi ini menyoroti pentingnya kerangka hukum yang kuat dan penegakan hukum yang konsisten untuk melindungi kepentingan masyarakat luas dalam perjuangan melawan *phishing* di luar kesadaran individu.

Sebagai tanggapan terhadap fenomena ini, Indonesia telah menetapkan kerangka hukum yang mengatur kejahatan siber. Kerangka hukum ini tertuang dalam Undang-Undang Nomor 19 Tahun 2016, yang mengubah Undang-Undang Nomor 11 Tahun 2008, yang berkaitan dengan informasi elektronik dan transaksi elektronik. *Phishing* diklasifikasikan sebagai tindak pidana dalam Undang-Undang ITE dan diatur oleh beberapa pasal, termasuk Pasal 28 ayat (1) mengenai penyebaran berita palsu yang menyesatkan, Pasal 30 mengenai akses ilegal ke sistem elektronik, dan Pasal 35 mengenai manipulasi data elektronik (Gulo et al, 2021). Selain itu, tujuan utama *phishing* adalah untuk memperoleh data atau harta benda korban secara ilegal. Dengan demikian, pelaku *phishing* dapat dijerat dengan ketentuan Kitab Undang-Undang Hukum Pidana (KUHP), seperti Pasal 378 tentang penipuan dan Pasal 362 tentang pencurian.

Meskipun regulasi telah ada, penegakan hukum terhadap pelaku *phishing* masih menghadapi berbagai kendala. Tantangan utama dalam proses penuntutan adalah keterbatasan kapasitas penyidik dalam menguasai teknologi forensik digital, masalah

yurisdiksi karena pelaku sering berlokasi di luar Indonesia, dan tantangan dalam memperoleh bukti elektronik (Supanto, 2016). Selain itu, perlindungan hukum yang diberikan kepada korban *phishing* masih kurang optimal karena tidak adanya peraturan khusus mengenai restitusi dan ganti rugi dalam UU ITE. Oleh karena itu, penelitian ini bertujuan untuk melakukan analisis komprehensif mengenai pertanggungjawaban pidana pelaku *phishing* dan mengevaluasi efektivitas penegakan hukum sesuai dengan UU Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.

Metodologi

Penelitian ini menggunakan metode yuridis normatif dengan pendekatan perundang-undangan (*statute approach*) dan pendekatan kasus (*case approach*). Bahan hukum primer meliputi Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang ITE, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, dan KUHP. Bahan hukum sekunder berupa jurnal ilmiah, artikel, dan putusan pengadilan yang berkaitan dengan kasus *phishing*. Data dikumpulkan melalui studi kepustakaan (*library research*) dengan menelaah dokumen hukum dan literatur akademik. Analisis dilakukan menggunakan metode kualitatif-deskriptif untuk menggambarkan ketentuan hukum yang berlaku dan mengevaluasi efektivitas penerapannya dalam praktik penegakan hukum terhadap *phishing* di Indonesia.

Penggunaan bahan hukum primer dan sekunder dalam penelitian ini bertujuan untuk memberikan analisis yang komprehensif terhadap peraturan yang relevan dan implementasinya dalam praktik peradilan. Landasan normatif ditetapkan oleh bahan hukum primer berupa undang-undang, sementara putusan pengadilan digunakan sebagai studi kasus untuk menyelidiki penerapan hukum secara tepat. Tahap pertama analisis kualitatif-deskriptif melibatkan identifikasi dan inventarisasi ketentuan hukum yang relevan dengan *phishing*. Tahap kedua melibatkan analisis unsur-unsur pidana dan tanggung jawab pelaku sesuai dengan pasal-pasal yang relevan Tahap ketiga melibatkan evaluasi efektivitas penegakan hukum dengan menganalisis hambatan yang dihadapi dalam praktik. Metodologi ini memungkinkan peneliti tidak hanya menggambarkan lanskap hukum saat ini, tetapi juga mengidentifikasi ketidaksesuaian antara regulasi dan implementasinya di lapangan.

Hasil dan Pembahasan

Konsep dan Modus Operandi *Phishing* sebagai Kejahatan Siber

1. Definisi dan Karakteristik *Phishing*

Istilah "*phishing*" berasal dari kata dalam bahasa Inggris "*fishing*," yang merujuk pada metode yang digunakan pelaku kejahatan untuk memancing korban agar mengungkapkan informasi rahasia mereka (Gulo et al., 2021). *Phishing* adalah upaya sistematis untuk memperoleh data pribadi, termasuk *username*, *password*, nomor rekening, dan informasi kartu kredit, melalui penipuan identitas digital dalam konteks kejahatan siber. *Phishing* diklasifikasikan sebagai kejahatan siber karena bergantung pada teknologi informasi, berbeda dengan kejahatan tradisional yang memerlukan kehadiran fisik.

Karakteristik utama *phishing* adalah penggunaan rekayasa sosial (*social engineering*) yang canggih. Pelaku menciptakan situasi yang mendorong korban untuk bertindak tanpa melakukan verifikasi yang cukup. Teknik ini memanfaatkan kelemahan psikologis manusia, termasuk rasa ingin tahu, keserakahan, dan rasa takut (Wibowo & Fatimah, 2017). Misalnya, korban mungkin menerima email dari institusi perbankan yang tampak seolah-olah berasal dari institusi tersebut, memberitahu mereka bahwa akun mereka akan ditangguhkan jika tidak segera memperbarui data mereka. Korban dibujuk untuk memberikan kredensial login mereka melalui email tersebut, yang berisi tautan ke situs web palsu yang tampak identik dengan situs web resmi bank.

2. Jenis-Jenis Phishing

Seiring kemajuan teknologi digital, telah terjadi peningkatan bentuk *phishing* yang semakin kompleks. Bentuk *phishing* klasik adalah email *phishing*, di mana pelaku mengirim surat elektronik palsu yang tampak berasal dari lembaga terpercaya (Putra Y, 2021). *Website phishing* melibatkan pembuatan situs tiruan dengan domain yang mirip dengan situs asli, dengan perbedaan huruf kecil minor yang seringkali terlewatkan oleh pengguna (Diniyah, 2022). Kemungkinan penipuan berhasil meningkat dengan *spear phishing*, yang menargetkan individu atau organisasi tertentu dengan informasi pribadi dan spesifik. Di sisi lain, *whaling* merupakan bentuk serangan yang menggunakan isu strategis sebagai umpan untuk menargetkan eksekutif tingkat tinggi atau pejabat penting.

3. Tahapan Modus Operandi Pelaku *Phishing*

Tahapan operandi *phishing* umumnya dengan fase persiapan, di mana pelaku mengumpulkan informasi tentang target potensial dari media sosial atau sumber terbuka. Tahap berikutnya melibatkan pembuatan media penipuan, seperti email palsu, situs web tiruan, atau pesan manipulatif lainnya yang dirancang untuk terlihat kredibel (Aprilianti, 2025). Pelaku kemudian menyebarkan jebakan ini ke target yang telah ditentukan, sering kali menggunakan teknik *mass mailing* untuk menjangkau sebanyak mungkin korban. Data segera direkam dalam *database* pelaku ketika korban menerima umpan dan memasukkan informasi mereka. Tahap akhir adalah eksploitasi, di mana informasi tersebut digunakan untuk mengakses rekening, melakukan transaksi ilegal, atau dijual di *dark web*.

4. Dampak Kerugian Materiil dan Immateriil bagi Korban

Kerugian finansial bukanlah satu-satunya dampak dari *phishing*. Korban juga mengalami kerugian psikologis, termasuk kecemasan, ketegangan, dan penurunan kepercayaan mereka terhadap sistem digital (Muhammad & Harefa, 2023). Reputasi organisasi dapat tercemar dan kepercayaan publik dapat mengalami penurunan signifikan dalam kasus yang melibatkan institusi. Selain itu, data yang disalahgunakan dapat digunakan untuk melakukan berbagai kejahatan berlapis, termasuk penipuan identitas, pencucian uang, dan terorisme (Mansur & Gultom, 2010). Fenomena ini menunjukkan bahwa *phishing* bukan hanya masalah keamanan digital teknis, tetapi telah berkembang menjadi ancaman serius bagi stabilitas ekonomi dan keamanan nasional.

Kompleksitas modus operandi *phishing* menuntut pemahaman komprehensif dari berbagai pihak Untuk mengidentifikasi indikator *phishing*, seperti domain mencurigakan, kesalahan tata bahasa dalam email, atau permintaan informasi sensitif yang tidak lazim, pengguna internet harus memiliki literasi digital yang memadai. Institusi pengelola data diharuskan menerapkan protokol keamanan berlapis, yang meliputi enkripsi data, autentikasi dua faktor, dan pembaruan sistem secara berkala. Namun, untuk mengidentifikasi pelaku yang sering menggunakan teknologi penyamaran, seperti VPN atau *proxy server*, aparat penegak hukum memerlukan kemampuan forensik digital.

Kerangka Hukum Pertanggungjawaban Pidana Pelalu *Phishing*

1. Pengaturan *Phishing* dalam Perspektif KUHP

Tindak pidana *phishing* ditangani melalui interpretasi yang luas terhadap ketentuan dalam Kitab Undang-Undang Hukum Pidana (KUHP) sebelum diberlakukannya regulasi khusus mengenai teknologi informasi. Pasal 378 KUHP tentang penipuan menjadi acuan utama karena *phishing* pada dasarnya merupakan bentuk penipuan yang dilakukan melalui media elektronik (Gulo et al., 2021). Pasar tersebut merumuskan unsur-unsur memperoleh keuntungan secara ilegal bagi diri sendiri atau orang lain, menggunakan nama atau martabat palsu, penipuan atau serangkaian kebohongan, serta meyakinkan orang lain untuk menyerahkan suatu benda. Dalam konteks *phishing*, pelaku menggunakan identitas palsu berupa situs atau email yang menyerupai institusi resmi untuk memancing korban agar memberikan data pribadi, yang kemudian dimanfaatkan untuk keuntungan pelaku.

Dalam kasus *phishing*, Pasal 263 KUHP yang berkaitan dengan pemalsuan surat juga relevan, karena pelaku membuat atau memalsukan dokumen elektronik yang tampak asli (Putra Y, 2021). Pembuatan email atau situs web palsu oleh pelaku dapat diklasifikasikan sebagai bentuk pemalsuan, karena tujuannya adalah menipu orang lain agar percaya pada keasliannya. Sementara itu, Pasal 362 KUHP, yang berkaitan dengan pencurian, dapat diterapkan, karena *phishing* melibatkan pengambilan aset digital atau data milik orang lain tanpa izin. Namun, penerapan KUHP terhadap kejahatan siber sangat dibatasi oleh fakta bahwa norma-norma dalam KUHP ditujukan untuk kejahatan konvensional yang memiliki karakteristik berbeda dari *cybercrime*.

2. Pengaturan *Phishing* dalam UU ITE

Kesadaran dan keterbatasan KUHP mendorong lahirnya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang kemudian diubah melalui Undang-Undang Nomor 19 Tahun 2016. Peraturan perundang-undangan ini menetapkan kerangka hukum yang komprehensif untuk penuntutan berbagai kejahatan siber, seperti *phishing*. Penyebaran informasi palsu dan menyesatkan yang mengakibatkan kerugian bagi konsumen dalam transaksi elektronik dilarang berdasarkan Pasal 28 ayat (1) Undang-Undang ITE, sebagaimana diatur dalam Pasal 45A ayat (1) (Muhammad & Harefa, 2023). Hukuman maksimal untuk pelanggaran tersebut adalah denda hingga satu miliar rupiah dan enam tahun penjara. *Phishing*, yang sering menggunakan informasi menyesatkan untuk memikat korban, secara khusus diatur dalam ketentuan ini.

Larangan akses ilegal ke sistem elektronik dengan tujuan memperoleh informasi atau dengan melanggar sistem pengamanan diatur dalam Pasal 30 ayat 2 dan 3 UU ITE (Awawangi, 2014). Ketentuan ini jelas dilanggar oleh pelaku *phishing* yang berhasil mengakses akun korban menggunakan kredensial yang diperoleh secara curang. Sesuai dengan Pasal 46 ayat 2 dan 3, sanksi pidana sangat berat, termasuk hukuman penjara maksimal delapan tahun dan denda hingga delapan ratus juta rupiah. Ketentuan ini menunjukkan komitmen legislator untuk mencegah pelaku kejahatan siber merugikan masyarakat luas. Manipulasi, penciptaan, perubahan, atau perusakan informasi elektronik dengan niat menciptakan kesan keaslian dilarang oleh Pasal 35 UU ITE. Pasal ini khususnya relevan dengan kasus *phishing*, di mana pelaku membuat situs web atau email palsu yang sangat mirip dengan aslinya. Hukuman penjara maksimal adalah dua belas tahun, dan hukuman pidana diatur dalam Pasal 51 ayat 1 dengan denda hingga dua belas miliar rupiah. Keparahan hukuman pidana ini menunjukkan bahwa pemalsuan data elektronik dianggap sebagai kejahatan serius yang berpotensi merusak kepercayaan publik terhadap sistem digital.

3. Penguatan Regulasi melalui UU Perlindungan Data Pribadi

Undang-Undang Nomor 1 Tahun 2024, yang berkaitan dengan Perubahan Kedua Undang-Undang ITE, memperkuat kewenangan penyidik PPNS di bidang ITE untuk sementara waktu memblokir akses ke akun media sosial, rekening bank, uang elektronik, atau aset digital milik pelanggar (Santoso et al., 2024). Inovasi ini sangat penting dalam konteks penanganan *phishing* karena memungkinkan pemblokiran cepat akses pelaku untuk mencegah kerugian yang lebih besar. Namun, kewenangan ini harus digunakan dengan hati-hati untuk mencegah penyalahgunaan yang dapat melanggar hak asasi manusia, khususnya hak privasi dan kebebasan berekspresi. Pengesahan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi telah memperluas kerangka hukum perlindungan terhadap kejahatan *phishing*. Perlindungan data pribadi merupakan hak fundamental yang diakui oleh undang-undang ini (Maulana et al., 2024). Sesuai dengan Pasal 67 Undang-Undang PDP, individu yang memproses data pribadi secara ilegal dapat dikenakan sanksi pidana, yang dapat meliputi penjara dan denda yang signifikan. Prinsip validitas pemrosesan data, sebagaimana diatur dalam Pasal 20 Undang-Undang PDP, jelas dilanggar oleh pelaku yang mengumpulkan dan menggunakan data pribadi korban tanpa persetujuan mereka dalam konteks *phishing*. Transparansi, pembatasan tujuan, minimisasi data, dan pertanggungjawaban merupakan prinsip-prinsip UU PDP yang harus dipatuhi oleh pengendali data. Pengendali data diwajibkan untuk segera memberitahukan subjek data dan otoritas pengawas dalam hal terjadi pelanggaran data akibat serangan *phishing*, sebagaimana diatur dalam Pasal 46 UU PDP. Sanksi administratif dan pidana dapat dikenakan atas ketidakpatuhan terhadap kewajiban ini. Dengan demikian, UU PDP tidak hanya melindungi korban *phishing* tetapi juga mendorong institusi pengelolaan data untuk menetapkan protokol keamanan yang ketat.

Implementasi Penegakan Hukum terhadap Pelaku *Phishing*

1. Proses Penyidikan dan Peran Dittipidsiber

Penegakan hukum terhadap pelaku *phishing* di Indonesia dihadapkan pada berbagai tantangan kompleks yang melibatkan aspek teknis, hukum, dan koordinasi kelembagaan. Tahap awal proses penyelidikan *phishing* melibatkan pengumpulan bukti elektronik melalui tahap identifikasi dan analisis forensik digital. Informasi elektronik dan dokumen elektronik yang secara hukum sah dianggap sebagai bukti berdasarkan UU ITE. Namun, pengumpulan bukti digital sering terhalang oleh kendala teknis dalam praktiknya, karena pelaku sering menggunakan teknik enkripsi atau menghapus jejak digital, yang mempersulit proses pelacakan. Bareskrim Polri melalui Direktorat Tindak Pidana Siber (Dittipidsiber), memainkan peran strategis dalam penindakan kejahatan *phishing*. Dittipidsiber bertanggung jawab atas penerimaan laporan masyarakat, pelaksanaan analisis forensik digital, identifikasi pelaku melalui pemantauan IP *address*, dan koordinasi dengan pihak terkait, termasuk bank dan penyedia layanan internet. Proses penyelidikan melibatkan pengumpulan bukti berupa catatan transaksi elektronik yang mencurigakan, email palsu, dan situs web tiruan. Setelah cukup banyak unsur pidana teridentifikasi, penyidik dapat mengidentifikasi tersangka sesuai dengan Pasal 28 ayat (1), Pasal 45A ayat (1), dan Pasal 35 junto Pasal 51 ayat (1) UU ITE.

2. Hambatan Teknis dan Yuridis

Hambatan utama dalam penegakan hukum *phishing* adalah potensi pelaku untuk memanipulasi atau menghapus bukti elektronik. Lokasi kejahatan (*locus delicti*) dan waktu kejahatan (*tempus delicti*) sulit untuk ditentukan secara akurat karena sifat virtual kejahatan siber. Penyelidik kesulitan menentukan yurisdiksi hukum yang tepat karena pelaku dapat mengubah pengaturan lokasi dan waktu pada perangkat digital mereka. Kompleksitas masalah yurisdiksi semakin diperparah oleh fakta bahwa *phishing* adalah kejahatan transnasional yang melampaui batas geografis, karena pelaku berada di luar negeri.

3. Analisis Putusan Pengadilan

Secara umum, pelaku *phishing* didakwa dengan beberapa tuduhan berdasarkan UU ITE, sebagaimana terlihat dari analisis putusan pengadilan. Dalam kasus di Pengadilan Distrik Sengkang dengan nomor putusan 30/Pid.Sus/2019/PN.Skg, terdakwa terbukti telah memanipulasi data elektronik dengan membuat *website* palsu yang menyerupai situs internet *banking* resmi. *Website* tersebut dirancang untuk memancing korban agar memberikan informasi pribadi mereka. Pasal 35, Pasal 51 ayat (1) UU ITE, dan Pasal 55 ayat (1) KUHP digunakan untuk mendakwa terdakwa. Hukuman maksimal untuk tindak pidana ini adalah 12 tahun penjara dan denda hingga Rp12 miliar. Putusan ini menunjukkan bahwa pengadilan menerapkan sistem hukuman kumulatif yang lebih ringan, dengan syarat hukuman tidak melebihi hukuman maksimal ditambah sepertiga. Keputusan ini juga menunjukkan bahwa meskipun terdapat instrumen hukum yang tersedia, proses pembuktian kasus *phishing* memerlukan keahlian khusus dalam forensik digital, termasuk analisis *log serve*r, IP *address*, dan metadata dokumen elektronik.

Perlindungan Hukum terhadap Korban *Phishing*

Perlindungan hukum bagi korban *phishing* di Indonesia terus terkendala oleh berbagai kelemahan sistemik. Bareskrim Polri, BSSN, serta lembaga keuangan terkait merupakan saluran yang dapat digunakan untuk menerapkan mekanisme pelaporan. Namun, dalam praktiknya, sejumlah besar korban tidak mengetahui prosedur pelaporan yang tepat atau menganggap prosesnya terlalu birokratis. Banyak kasus *phishing* tidak dilaporkan karena kurangnya kesadaran mengenai hak-hak korban, yang memungkinkan pelaku terus beroperasi tanpa terdeteksi. Undang-Undang Informasi dan Transaksi Elektronik (ITE) dan Kitab Undang-Undang Hukum Pidana (KUHP) saat ini belum mengatur mekanisme restitusi bagi korban *phishing* dalam hal hak korban untuk mendapatkan ganti rugi. Penerapan Undang-Undang Perlindungan Saksi dan Korban (LPSK), yang mengatur restitusi, masih bersifat fakultatif dan bergantung pada keputusan LPSK. Proses memperoleh ganti rugi bagi korban *phishing* memakan waktu dan biaya, karena mereka diharuskan mengajukan gugatan perdata terpisah. Hal ini menimbulkan ketidakadilan, karena sistem peradilan pidana lebih fokus pada hukuman bagi pelaku daripada kerugian materiil yang dialami korban.

Computer Security Incident Response Team (CSIRT) merupakan fungsi preventif BSSN, yang bertanggung jawab atas keamanan siber nasional. BSSN mengadakan kampanye literasi keamanan siber untuk masyarakat, memantau lalu lintas siber, mendeteksi aktivitas mencurigakan, dan memberikan peringatan dini. Upaya edukasi mencakup publikasi panduan yang memberikan petunjuk tentang identifikasi modus *phishing*, keamanan kredensial, dan tindakan yang tepat jika menjadi korban. Namun demikian, rendahnya tingkat literasi digital di kalangan masyarakat Indonesia terus menghambat efektivitas pendidikan. Penerapan UU ITE merupakan indikasi yang jelas akan adanya kesenjangan antara perlindungan normatif dan praktik. Terlepas dari kenyataan bahwa undang-undang tersebut mengatur hak-hak subjek data dan tanggung jawab pengendali data, korban *phishing* menghadapi tantangan yang signifikan dalam memperoleh ganti rugi karena tidak adanya otoritas perlindungan data pribadi yang berfungsi secara optimal. Perlindungan hukum menjadi tidak efektif akibat ketidakhadiran sistem pengaduan terintegrasi dan ketidakjelasan mengenai lembaga yang bertanggung jawab untuk menyelesaikan masalah korban. Situasi ini menunjukkan bahwa keberadaan norma hukum tidak menjamin keadilan substansial bagi korban kejahatan siber di Indonesia.

Simpulan

Penelitian ini menganalisis pertanggungjawaban pidana pelaku *phishing* dan efektivitas penegakan hukum sesuai dengan UU Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Hasil pembahasan menunjukkan bahwa *phishing* merupakan kejahatan siber yang canggih dengan modus operandi dinamis yang memanfaatkan teknik rekayasa sosial untuk memperoleh informasi pribadi korban secara ilegal. Di Indonesia, kerangka hukum mengenai pertanggungjawaban pidana pelaku *phishing* sangat komprehensif, mencakup ketentuan dalam Kitab Undang-Undang Hukum Pidana (Pasal 378 tentang penipuan, Pasal 263 tentang pemalsuan surat, dan Pasal 362 tentang pencurian)

serta Undang-Undang ITE, yang secara khusus mengatur penyebaran berita palsu (Pasal 28 ayat 1), akses ilegal ke sistem elektronik (Pasal 30), dan manipulasi data elektronik (Pasal 35). Meskipun demikian, implementasi penegakan hukum masih dihadapkan pada tantangan yang signifikan sepertibsifat transnasional kejahatan, keterbatasan kemampuan forensik digital, dan kemampuan pelaku kejahatan untuk menghapus jejak digital. Undang-Undang ITE tidak memiliki mekanisme restitusi yang jelas, proses pelaporan birokratis, dan rendahnya literasi digital di kalangan masyarakat, menunjukkan bahwa perlindungan hukum bagi korban *phishing* belum optimal.

Berdasarkan temuan penelitian menunjukkan bahwa sejumlah langkah strategis diperlukan untuk memperkuat pertahanan penegak hukum terhadap serangan *phishing*. Pertama, pemerintah diharuskan segera membentuk otoritas perlindungan data pribadi yang independen dan berfungsi, sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022. Kedua, sangat penting untuk meningkatkan kemampuan aparat penegak hukum dengan menyediakan infrastruktur teknologi yang diperlukan dan mengadakan pelatihan forensik digital secara berkelanjutan. Ketiga, peraturan turunannya Undang-Undang ITE atau revisi undang-undang tersebut harus secara eksplisit mengatur mekanisme ganti rugi bagi korban *phishing*. Keempat, diperlukan sinergi yang lebih kuat antara sektor swasta, BSSN, Polri, dan OJK untuk menetapkan sistem pelaporan dan respons insiden siber yang terintegrasi. Penelitian ini membuka peluang untuk penelitian lanjutan di berbagai bidang. Pertama, perlu dilakukan analisis komparatif terhadap praktik penegakan hukum *phishing* di negara-negara dengan sistem hukum yang berbeda guna mengidentifikasi strategi paling efektif yang dapat diterapkan di Indonesia. Kedua, diperlukan penelitian empiris untuk mengembangkan strategi pencegahan yang lebih tepat dengan mengkaji efektivitas program literasi digital dalam mengurangi insiden korban *phishing*. Ketiga, sangat penting untuk melakukan pemeriksaan komprehensif terhadap model kompensasi dan restitusi bagi korban kejahatan siber yang dapat diintegrasikan ke dalam sistem peradilan pidana Indonesia guna mewujudkan keadilan restoratif. Hal ini memungkinkan realisasi perlindungan hukum yang lebih efektif dan berkelanjutan bagi masyarakat dari ancaman *phishing*.

Daftar Pustaka

Aprilianti, A. (2025). Efektivitas dan Implementasi Undang-Undang Informasi dan Transaksi Elektronik sebagai Hukum Siber di Indonesia: Tantangan dan Solusi. Begawan Abioso, 15(1), 41–50. https://doi.org/10.37893/abioso.v15i1.1002

Awawangi, R. V. (2014). Pencemaran Nama Baik Dalam KUHP dan Menurut UU NO. 11 TAHUN 2008 Tentang Informasi dan Transaksi Elektronik. Lex Crimen, 3(4), 112–123.

Blinova, H. (2023). Legal Regulation of the Ratio of Criminal and Administrative Liability as to Countering Offenses in the Sphere of Trafficking of Narcotic Drugs, Psychotropic Substances, their Analogues and Precursors. Journal of Drug and Alcohol Research, 12(8), ISSN 2090-8334, https://doi.org/10.4303/JDAR/236257

Bodnaruk, O. (2025). The role of criminal liability for illegal possession of a vehicle. Salud Ciencia Y Tecnologia Serie De Conferencias, 4, ISSN 2953-4860, https://doi.org/10.56294/sctconf20251315

Bodnaruk, O. (2025). The role of criminal liability for illegal possession of a vehicle. Salud Ciencia Y Tecnologia Serie De Conferencias, 4, ISSN 2953-4860, https://doi.org/10.56294/sctconf20251315

BSSN. (2023). Laporan Tahunan Keamanan Siber Nasional. Jakarta: BSSN.

Chegwe, E.N. (2025). Criminal liability for copyright infringement: Analysis of the law in Nigeria and South Africa. Journal of World Intellectual Property, ISSN 1422-2213, https://doi.org/10.1111/jwip.12357

Diniyah, K. J. (2022). Perlindungan Hukum Bagi Korban Tindak Pidana Cyber Crime Phishing. DINAMIKA, 28(5), 3756–3775.

Gulo, A. S., Lasmadi, S., & Nawawi, K. (2021). Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. PAMPAS: Journal of Criminal Law, 1(2), 68–81. https://doi.org/10.22437/pampas.v1i2.9574

Kaushik, N. (2024). Email Traceback: Securing Systems from Phishing and Malicious Link Prevention. Proceedings IEEE 2024 1st International Conference on Advances in Computing Communication and Networking Icac2n 2024, 647-652, https://doi.org/10.1109/ICAC2N63387.2024.10895717

Khaleefah, R.S. (2025). Criminal Liability Of Automobile Manufacturers For Traffic Accidents In Iraq: An Overview. Malaysian Journal of Syariah and Law, 13(1), 236-248, ISSN 1985-7454, https://doi.org/10.33102/mjsl.vol13no1.1100

Mansur, D. M. A., & Gultom, E. (2010). Cyber Law Aspek Hukum Teknologi Informasi. Bandung: PT. Refika Aditama.

Manullang, H. (2025). Blockchain and Corporate Criminal Liability: Law Reform and the Technological Revolution in Corporate Accountability. Journal of Law and Legal Reform, 6(3), 1411-1450, ISSN 2715-0941, https://doi.org/10.15294/jllr.v6i3.22472

Maulana, N., Laurens, T., Faiz, D. H. A., & Patrianti, T. (2024). Manajemen Krisis PT. BSI Tbk Pasca Peretasan Data Nasabah. Inovative: Journal Of Social Science Research , 4(1), 8244–8258.

Moussa, A.F. (2025). Criminal Liability For The Use Of Performance-Enhancing Drugs In Sports: A Comparative And Analytical Study Under International And Middle Eastern Criminal Law. Access to Justice in Eastern Europe, 8(2), ISSN 2663-0575, https://doi.org/10.33327/AJEE-18-8.2-r000102

Muhammad, F. E., & Harefa, B. (2023). Pengaturan Tindak Pidana Bagi Pelaku Penipuan Phisning Berbasis Web. JURNAL USM LAW REVIEW, 6(1), 226–241. https://doi.org/10.26623/julr.v6i1.6649

Putra Y, V. F. (2021). Modus Operandi Tindak Pidana Phising Menurut UU ITE. Jurist-Diction, 4(6), 2525–2548. https://doi.org/10.20473/jd.v4i6.31857

Santoso, I., Syahrin, A., Mulyadi, M., & Agusmidah, A. (2024). Kebijakan Hukum Pidana Terhadap Perbuatan Melawan Hukum Dalam UU ITE Pasca Berlakunya Pedoman Implementasi Pasal - Pasal Tertentu UU ITE. Locus Journal of Academic Literature Review, 3(4), 329–335. https://doi.org/10.56128/ljoalr.v3i4.312

Supanto. (2016). Perkembangan Kejahatan Teknologi Informasi (Cyber Crime) Dan Antisipasinya Dengan Penal Policy. Yustisia Jurnal Hukum, 5(1), 52–70. https://doi.org/10.20961/yustisia.v5i1.8718

Wibowo, M. H., & Fatimah, N. (2017). Ancaman Phishing Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime. JOEICT(Jurnal of Education and Information Communication Technology), 1(1), 1–5.

Yuspin, W. (2024). Digital Banking Security: Internet Phishing Attacks, Analysis and Prevention of Fraudulent Activities. International Journal of Safety and Security Engineering, 14(6), 1699-1706, ISSN 2041-9031, https://doi.org/10.18280/ijsse.140605