Jurnal Riset Multidisiplin Edukasi
https://journal.hasbaedukasi.co.id/index.php/jurmie
Halaman : 1216 - 1230

ANALISIS PENGATURAN HUKUM TINDAK PIDANA CYBER CRIME PHISING DI INDONESIA BERDASARKAN PRESPEKTIF HUKUM RESPONSIF

Fajrotul Lailiyah[1], Syarifuddin[2], Fathorrahman[3]
Fakultas Ilmu Sosial Dan Humaniora Universitas Ibrahimy Situbondo [1,2,3]
Email: lylandreanna@gmail.com

Informasi

Volume : 3
Nomor : 1
Bulan : Januari
Tahun : 2026
E-ISSN : 3062-9624

Abstract

Phishing is a type of cybercrime that continues to develop with diverse methods, aiming to manipulate victims for the perpetrators' personal gain. Its complexity raises legal issues, particularly regarding the alignment of phishing definitions within the framework of cybercrime and the applicable legal norms in Indonesia. This study seeks to analyze the concept of phishing from a cybercrime perspective and to evaluate the extent to which Indonesian legal norms—particularly the Electronic Information and Transactions Law (UU ITE)—accommodate phishing practices. It also examines the effectiveness of existing regulations, including the Criminal Code (KUHP), the Personal Data Protection Law (UU PDP), and sectoral regulations issued by the Financial Services Authority (OJK), the Ministry of Communication and Information Technology (Kominfo), and Bank Indonesia (BI). The research method employed is a literature study, drawing on primary legal sources such as legislation, secondary sources such as scholarly works, and court rulings, including Decision No. 28/Pid.Sus/2021/PN Semapura. The findings indicate that the regulation of phishing in Indonesia is still fragmented and lacks comprehensiveness. Provisions in the ITE Law, such as Article 28(1), are often used to prosecute offenders but do not adequately cover the full scope of modern phishing practices. Similarly, the KUHP, PDP Law, and sectoral regulations focus more on system and consumer protection but do not provide clear legal certainty in addressing phishing. Therefore, regulatory reform—particularly amendments to the ITE Law—is necessary to explicitly and comprehensively regulate phishing in order to ensure legal certainty and stronger protection for society.

Keyword: *phishing, cybercrime, ITE Law, legal regulation in Indonesia*

Abstrak
Phising merupakan salah satu bentuk kejahatan cyber yang mengalami perkembangan pesat, memiliki beragam modus operandi, serta bertujuan memperoleh keuntungan pribadi melalui penipuan dan manipulasi korban di ruang elektronik. Kompleksitas kejahatan ini menimbulkan persoalan hukum, terutama terkait kesesuaian makna phising dalam kerangka konsep kejahatan cyber dengan norma hukum yang berlaku. Penelitian ini menganalisis masalah makna phising dalam perspektif kejahatan cyber serta menilai sejauh mana norma hukum di Indonesia, khususnya Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), dapat mengakomodasi praktik phising. Metode yang digunakan adalah penelitian kepustakaan dengan menelaah bahan hukum primer berupa peraturan perundang-undangan, bahan hukum sekunder berupa literatur ilmiah, serta studi dokumen putusan pengadilan, khususnya Putusan Nomor 28/Pid.Sus/2021/PN Semapura. Hasil penelitian menunjukkan bahwa pengaturan mengenai tindak pidana phising di Indonesia belum diatur secara spesifik dan menyeluruh. Beberapa ketentuan dalam UU ITE, seperti Pasal 28 ayat (1), kerap dijadikan dasar untuk menjerat pelaku, namun belum mampu mencakup seluruh bentuk dan variasi kejahatan phising modern. Demikian pula, KUHP, UU PDP, serta regulasi sektoral dari OJK, Kominfo, dan BI lebih menekankan pada perlindungan sistem dan konsumen, tetapi masih belum memberikan kepastian hukum yang tegas dalam penanggulangan phising. Dengan demikian, diperlukan pembaruan regulasi, khususnya dalam UU ITE, agar dapat mengatur tindak pidana phising secara eksplisit dan komprehensif demi menjamin kepastian hukum dan perlindungan optimal bagi masyarakat.

Kata Kunci: *phising, cyber crrime, pengaturan hukum di Indonesia*

A. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang berlangsung sangat pesat telah membawa perubahan besar dalam hampir seluruh aspek kehidupan manusia, termasuk dalam bidang ekonomi, sosial, dan hukum. Digitalisasi yang semakin masif memberikan kemudahan dalam melakukan berbagai aktivitas, seperti transaksi keuangan, pertukaran data, serta komunikasi jarak jauh tanpa batas ruang dan waktu. Namun, di balik manfaat tersebut, kemajuan teknologi juga menghadirkan tantangan serius berupa meningkatnya kejahatan berbasis teknologi informasi atau yang dikenal sebagai kejahatan siber (cyber crime). Fenomena kejahatan siber berkembang seiring dengan meningkatnya ketergantungan masyarakat terhadap sistem elektronik, sehingga ruang digital menjadi lahan baru bagi pelaku kejahatan untuk melakukan berbagai bentuk tindak pidana.

Salah satu bentuk kejahatan siber yang paling sering terjadi dan menimbulkan kerugian signifikan bagi masyarakat adalah tindak pidana phising. Phising merupakan metode kejahatan berbasis digital yang bertujuan untuk memperoleh data atau informasi sensitif milik korban, seperti data pribadi, informasi perbankan, maupun akun digital, melalui cara-cara penipuan. Kejahatan ini tidak hanya mengandalkan kecanggihan teknologi, tetapi juga mengeksploitasi kelemahan psikologis manusia melalui teknik manipulasi sosial (social engineering). Pelaku phising memanfaatkan kepercayaan, ketidaktahuan, serta kondisi emosional korban agar

secara sukarela menyerahkan informasi penting tanpa menyadari bahwa dirinya sedang menjadi target kejahatan.

Phising pada dasarnya merupakan kejahatan yang mengombinasikan manipulasi sosial dengan eksploitasi sistem elektronik, sehingga menjadikannya sulit untuk dikenali, baik oleh korban maupun oleh aparat penegak hukum. Modus operandi phising terus mengalami perkembangan, mulai dari pengiriman email palsu yang menyerupai institusi resmi, pembuatan situs web tiruan, penyebaran tautan berbahaya melalui pesan singkat, hingga penggunaan teknologi kecerdasan buatan (artificial intelligence/AI) untuk meniru identitas seseorang secara meyakinkan. Keragaman teknik ini menunjukkan bahwa phising merupakan kejahatan yang bersifat dinamis dan adaptif terhadap perkembangan teknologi, sehingga memerlukan pengaturan hukum yang responsif dan komprehensif.

Dalam konteks hukum pidana nasional, tindak pidana phising sering kali dikualifikasikan sebagai tindak penipuan sebagaimana diatur dalam Pasal 378 Kitab Undang-Undang Hukum Pidana (KUHP), karena mengandung unsur tipu muslihat dan rangkaian kebohongan. Namun, ketentuan tersebut pada dasarnya dirancang untuk mengatur penipuan dalam bentuk konvensional yang tidak berbasis teknologi informasi. Sementara itu, pengaturan utama terkait kejahatan siber di Indonesia terdapat dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 dan Undang-Undang Nomor 1 Tahun 2024. Meskipun demikian, hingga saat ini Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) belum secara eksplisit mendefinisikan atau menyebut tindak pidana phising sebagai delik tersendiri.

Ketiadaan pengaturan yang spesifik mengenai phising dalam UU ITE menimbulkan ketidaklengkapan norma (uncompletly of norm) yang berdampak pada lemahnya kepastian hukum dalam proses penegakan hukum. Aparat penegak hukum, khususnya jaksa penuntut umum dan hakim, terpaksa melakukan penafsiran ekstensif terhadap pasal-pasal yang ada untuk menjerat pelaku phising. Secara normatif, ketentuan yang paling mendekati unsur-unsur phising dapat ditemukan dalam Pasal 28 ayat (1), Pasal 30 ayat (1), Pasal 32 ayat (1), Pasal 35, dan Pasal 36 ayat (1) UU ITE. Pasal-pasal tersebut memuat unsur penyebaran informasi menyesatkan, akses tanpa izin, manipulasi data elektronik, serta perbuatan yang menimbulkan kerugian, yang secara substansi berkaitan dengan praktik phising.

Penerapan pasal-pasal tersebut dalam kasus konkret sering kali menghadapi kendala. Hal ini dapat dilihat dalam Putusan Pengadilan Negeri Semapura Nomor 28/Pid.Sus/2021/PN SRP, di mana penuntut umum menggunakan Pasal 28 ayat (1) UU ITE sebagai dakwaan alternatif

terhadap pelaku phising. Pasal tersebut mengatur larangan penyebaran berita bohong dan menyesatkan yang merugikan konsumen dalam transaksi elektronik. Dari perspektif keamanan siber, pasal ini memang berkaitan dengan teknik manipulasi sosial yang digunakan dalam phising. Namun, unsur "kerugian konsumen dalam transaksi elektronik" menjadi problematik ketika phising dilakukan tanpa adanya hubungan hukum antara pelaku dan korban sebagai pelaku usaha dan konsumen.

Penggunaan Pasal 28 ayat (1) UU ITE dalam putusan tersebut menunjukkan keterbatasan pilihan pasal yang tersedia dalam sistem hukum positif Indonesia. Jaksa penuntut umum tetap menggunakan pasal tersebut karena belum adanya ketentuan khusus yang secara eksplisit mengatur phising dalam segala bentuknya, baik yang melibatkan transaksi elektronik maupun yang tidak. Regulasi lain, seperti Undang-Undang Perlindungan Data Pribadi (UU PDP), peraturan Otoritas Jasa Keuangan (OJK), serta kebijakan Bank Indonesia (BI), pada prinsipnya lebih menitikberatkan pada aspek perlindungan data, pencegahan, dan keamanan sistem, bukan pada pengkualifikasian tindak pidana phising secara komprehensif.

Kondisi ini berbeda dengan beberapa negara lain yang telah mengatur phising secara jelas dalam peraturan perundang-undangan terkait kejahatan siber, sehingga memberikan kepastian hukum yang lebih kuat dalam penegakan hukum. Oleh karena itu, diperlukan pembaruan hukum yang menyeluruh melalui perumusan norma yang secara eksplisit mengatur tindak pidana phising, termasuk unsur, bentuk, dan sanksinya. Pengaturan yang komprehensif diharapkan mampu menjawab kompleksitas kejahatan phising yang semakin berkembang serta memberikan perlindungan hukum yang efektif bagi masyarakat dalam ruang digital.

Penelitian ini bertujuan untuk menjawab permasalahan yang telah dirumuskan dan memberikan kontribusi konseptual maupun praktis dalam pengembangan ilmu hukum pidana cyber, khususnya terkait dengan tindak pidana phising. Penelitian ini bertujuan untuk menyusun pemahaman konseptual yang utuh mengenai definisi phising, unsur- unsurnya, serta bagaimana konstruksi hukumnya dapat dipahami dalam sistem hukum pidana nasional melalui pendekatan interpretatif terhadap ketentuan yang tersedia. Sebagai tambahan, penelitian ini membandingkan pengaturan tindak pidana phising di Indonesia dengan beberapa negara yang memuat pengaturan terhadap kejahatan phising untuk memahami cara negara lain menyelesaikan masalah yang sama. Tujuan selanjutnya dari penelitian ini adalah untuk mengkaji bagaimana penegakan hukum terhadap tindak pidana phising sesuai dengan kasus yang ada dalam masyarakat ditinjau dari putusan pengadilan nomor

28/Pid.Sus/2021/PN SRP. Penelitian ini bertujuan untuk memahami bagaimana aparat penegak hukum mengonstruksikan pengaturan phising sesuai dengan perbuatan pidana phising yang terjadi.

B. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif yuridis, yaitu penelitian yang menitikberatkan pada pengkajian norma hukum tertulis dengan cara menelaah peraturan perundang-undangan serta menganalisis penerapannya dalam praktik penegakan hukum. Pendekatan ini digunakan untuk menilai sejauh mana ketentuan hukum yang berlaku mampu mengakomodasi tindak pidana cyber crime phising, termasuk mengidentifikasi adanya kekosongan norma, ketidakjelasan pengaturan, atau multitafsir dalam penerapannya. Penelitian ini berfokus pada analisis bahan hukum primer dan sekunder yang dikaji secara konseptual dan teoritis untuk memahami konstruksi hukum tindak pidana phising dalam sistem hukum positif Indonesia. Pendekatan penelitian yang digunakan meliputi pendekatan perundang-undangan (statute approach), dengan menelaah Undang-Undang Informasi dan Transaksi Elektronik beserta perubahannya, Kitab Undang-Undang Hukum Pidana (KUHP), Kitab Undang-Undang Hukum Acara Pidana (KUHAP), Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, serta peraturan dari Otoritas Jasa Keuangan, Bank Indonesia, dan Kementerian Komunikasi dan Informatika. Selain itu, penelitian ini juga menggunakan pendekatan kasus (case approach) melalui analisis Putusan Pengadilan Negeri Nomor 28/Pid.Sus/2021/PN SRP yang berkaitan dengan tindak pidana phising.

Sumber bahan hukum dalam penelitian ini terdiri atas bahan hukum primer, sekunder, dan tersier. Bahan hukum primer meliputi peraturan perundang-undangan terkait, putusan pengadilan, serta panduan atau laporan resmi dari Badan Siber dan Sandi Negara (BSSN). Bahan hukum sekunder berupa buku teks hukum, artikel jurnal ilmiah nasional dan internasional, serta hasil seminar yang relevan dengan kejahatan siber dan phising. Adapun bahan hukum tersier mencakup direktori putusan dan indeks hukum untuk menunjang penelusuran bahan hukum. Teknik pengumpulan data dilakukan melalui studi kepustakaan dengan menelusuri peraturan, putusan pengadilan, buku, dan jurnal ilmiah baik secara cetak maupun digital. Data yang terkumpul kemudian dianalisis menggunakan analisis isi (content analysis) dan analisis komparatif untuk membandingkan norma hukum dengan praktik penerapannya, yang selanjutnya dijadikan dasar dalam penarikan simpulan dan perumusan

rekomendasi terkait penanggulangan tindak pidana phising.

C. HASIL DAN PEMBAHASAN

Hasil Penelitian

Penelitian ini menggunakan berbagai bahan hukum primer dan sekunder yang relevan untuk menganalisis tindak pidana phising dalam perspektif hukum pidana dan hukum siber. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya menjadi dasar hukum utama dalam menilai sejauh mana perbuatan phising diakomodasi secara normatif dalam sistem hukum Indonesia. Selain itu, Kitab Undang-Undang Hukum Pidana (KUHP) dan Kitab Undang-Undang Hukum Acara Pidana (KUHAP) digunakan sebagai instrumen pendukung dalam menganalisis aspek pemidanaan serta praktik penegakan hukum di pengadilan. Penelitian ini juga mengacu pada Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, peraturan Otoritas Jasa Keuangan (OJK), serta peraturan Bank Indonesia yang berfokus pada keamanan sistem keuangan dan perlindungan nasabah.

Laporan dan pedoman teknis dari Badan Siber dan Sandi Negara (BSSN) dimanfaatkan untuk memahami kebijakan pengamanan siber dan pencegahan kejahatan phising, meskipun BSSN tidak memiliki kewenangan pembentukan norma pidana yang bersifat represif. Sebagai data pendukung perbandingan hukum, penelitian ini juga mengkaji Cybercrimes (Prohibition, Prevention, etc.) Act 2015 Nigeria, EU Artificial Intelligence Act, AI Executive Order 2023 Amerika Serikat, Interim Measures for Generative AI Services Tiongkok, serta Artificial Intelligence and Data Act Kanada.

Selain bahan normatif, penelitian ini didukung oleh data kasus dan tinjauan teoritis. Putusan Pengadilan Nomor 28/Pid.Sus/2021/PN SRP dijadikan objek kajian untuk menilai penerapan hukum pidana terhadap tindak pidana phising dalam praktik peradilan, di mana terdakwa dipidana bukan semata-mata sebagai penadah, melainkan sebagai pihak yang turut serta dalam melancarkan tindak pidana cyber crime phising. Analisis teoritis dalam penelitian ini menggunakan teori keamanan siber yang menjelaskan kerangka konseptual perlindungan terhadap ancaman digital, sebagaimana dikemukakan oleh David S. Wall bahwa kejahatan siber merupakan transformasi kejahatan di era informasi (David S. Wall, 2007,). Selanjutnya, teori subsumsi hukum digunakan untuk menentukan apakah perbuatan konkret dapat dimasukkan ke dalam rumusan norma hukum yang bersifat umum dan abstrak, sebagaimana dijelaskan oleh Satjipto Rahardjo bahwa penegakan hukum dilakukan dengan mencocokkan fakta dengan

unsur-unsur norma hukum (Satjipto Rahardjo, 2021). Penelitian ini juga mengacu pada teori perumusan tindak pidana yang menekankan pentingnya kejelasan dan kepastian norma pidana sesuai asas lex certa, serta teori hukum responsif yang menegaskan bahwa hukum harus adaptif terhadap perkembangan teknologi dan kebutuhan perlindungan masyarakat (Satjipto Rahardjo, 2021).

Pembahasan

Analisis Kesesuaian Makna Phising Dalam Konsep Kejahatan Cyber Dan Norma Hukum

Perkembangan teknologi informasi dan komunikasi telah membawa dampak signifikan terhadap pola interaksi sosial dan ekonomi masyarakat modern. Di satu sisi, kemajuan digital memberikan kemudahan dalam berbagai aspek kehidupan, namun di sisi lain juga melahirkan bentuk-bentuk kejahatan baru yang semakin kompleks, salah satunya adalah tindak pidana phising. Dalam konteks kejahatan siber (cyber crime), phising merupakan bentuk kejahatan yang memanfaatkan rekayasa sosial (social engineering) untuk menipu korban agar secara sukarela menyerahkan data pribadi, informasi keuangan, atau kredensial digital. Oleh karena itu, phising membutuhkan respons hukum yang spesifik dan adaptif agar dapat dijadikan dasar yang kuat dalam proses penegakan hukum. Tanpa pengaturan yang eksplisit, aparat penegak hukum akan mengalami kesulitan dalam mengkualifikasikan perbuatan tersebut ke dalam norma hukum yang ada, sehingga berpotensi menghambat tercapainya keadilan dan kepastian hukum.

Dalam sistem hukum Indonesia, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 (UU ITE) merupakan regulasi utama yang digunakan untuk menanggulangi kejahatan siber. Istilah phising tidak disebutkan maupun dijelaskan secara eksplisit dalam UU ITE. Pasal-pasal yang terdapat dalam undang-undang tersebut pada umumnya bersifat umum dan lebih menitikberatkan pada perbuatan teknis seperti akses tanpa izin, manipulasi data, atau penyebaran informasi bohong. Kondisi ini menunjukkan adanya ketidaklengkapan norma (incompleteness of norm) yang berpotensi menimbulkan ketidakpastian hukum dalam penerapan pasal-pasal UU ITE terhadap kasus phising (Tulus Widjanarko, 2018). Ketidaklengkapan norma tersebut menjadi problematik karena karakteristik phising tidak selalu melibatkan peretasan sistem secara langsung, melainkan lebih sering menggunakan manipulasi psikologis dan penipuan berbasis komunikasi digital.

Secara konseptual beberapa pasal dalam UU ITE masih dapat dikaitkan dengan teknik phising, meskipun dengan berbagai keterbatasan. Salah satu pasal yang sering digunakan

adalah Pasal 28 ayat (1) UU ITE yang mengatur perbuatan menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik. Pasal ini memuat unsur "setiap orang", "dengan sengaja dan tanpa hak", "menyebarkan berita bohong dan menyesatkan", serta "mengakibatkan kerugian konsumen dalam transaksi elektronik" (UU ITE, Pasal 28 ayat (1)). Unsur "setiap orang" mencakup individu maupun badan hukum sebagai subjek hukum yang dapat dimintai pertanggungjawaban pidana, sedangkan unsur "dengan sengaja" menunjukkan adanya kehendak dan kesadaran pelaku atas akibat perbuatannya, bukan sekadar kelalaian (Roeslan Saleh, 2018).

Kelemahan mendasar dari Pasal 28 ayat (1) terletak pada pembatasan korban sebagai "konsumen dalam transaksi elektronik". Artinya, agar pasal ini dapat diterapkan, harus dibuktikan adanya hubungan transaksi elektronik antara korban dan pelaku. Dalam praktik phising, korban sering kali bukan konsumen dalam arti sempit, melainkan pengguna layanan digital atau individu yang tertipu melalui pesan singkat, email, atau media sosial tanpa adanya transaksi ekonomi secara langsung. Akibatnya, ketika posisi korban tidak dapat dikualifikasikan sebagai konsumen, unsur pasal tersebut tidak terpenuhi meskipun korban mengalami kerugian nyata. Kondisi ini menciptakan celah hukum yang serius dan mengurangi efektivitas perlindungan hukum bagi korban phising.

Selain Pasal 28 ayat (1), Pasal 30 ayat (1) UU ITE juga sering dikaitkan dengan tindak pidana phising. Pasal ini mengatur perbuatan mengakses komputer dan/atau sistem elektronik milik orang lain secara sengaja dan tanpa hak atau melawan hukum. Unsur-unsur dalam pasal ini mencakup subjek "setiap orang", unsur kesengajaan, sifat melawan hukum, perbuatan mengakses sistem elektronik orang lain, serta frasa "dengan cara apa pun" (UU ITE, Pasal 30 ayat (1)). Secara konseptual, pasal ini memang relevan untuk menjerat perbuatan pembobolan sistem atau peretasan (hacking). Namun, dalam konteks phising, pasal ini memiliki kelemahan normatif karena lebih berorientasi pada serangan teknis terhadap sistem keamanan digital, bukan pada manipulasi sosial yang menjadi ciri utama phising. Banyak kasus phising tidak melibatkan akses langsung ke sistem korban, melainkan memanfaatkan kelengahan korban untuk menyerahkan data secara sukarela.

Keterbatasan serupa juga terlihat pada Pasal 32 ayat (1) UU ITE yang mengatur perbuatan mengubah, menambah, mengurangi, mentransmisikan, merusak, menghilangkan, memindahkan, atau menyembunyikan informasi elektronik atau dokumen elektronik milik orang lain. Pasal ini menitikberatkan pada manipulasi data yang sudah ada dalam suatu sistem elektronik. Dalam praktik phising, pelaku justru lebih sering menciptakan sarana palsu seperti

situs web tiruan atau pesan palsu untuk memperoleh data baru dari korban, bukan memanipulasi data yang sudah tersimpan dalam sistem korban. Selain itu, unsur penipuan (fraudulent scheme) sebagai inti dari phising tidak secara eksplisit diakomodasi dalam pasal ini, sehingga menyulitkan pembuktian dalam praktik penegakan hukum.

Pasal 35 UU ITE juga sering dianggap paling mendekati karakteristik phising karena mengatur perbuatan manipulasi informasi elektronik agar seolah-olah data yang otentik. Pasal ini mencakup perbuatan membuat atau memanipulasi informasi elektronik sehingga tampak sah dan meyakinkan. Meskipun demikian, fokus pasal ini masih cenderung pada manipulasi teknis terhadap data atau dokumen elektronik, bukan pada aspek manipulasi psikologis terhadap pengguna. Dalam banyak kasus phising modern, pelaku tidak perlu mengubah data pada sistem elektronik korban atau pihak ketiga, melainkan cukup menipu korban agar memberikan informasi sensitif secara sukarela melalui media yang tampak meyakinkan (Sulistyo & Wicaksono, 2024). Dengan demikian, cakupan pasal ini masih belum sepenuhnya responsif terhadap variasi modus phising yang berkembang.

Keterbatasan pengaturan dalam UU ITE semakin terlihat seiring berkembangnya teknologi kecerdasan buatan (artificial intelligence). Modus phising kini tidak hanya dilakukan melalui email atau situs palsu, tetapi juga melalui deepfake dan voice cloning yang memanfaatkan AI untuk meniru wajah, suara, atau identitas seseorang secara sangat meyakinkan. Modus ini memungkinkan pelaku untuk menciptakan video atau rekaman suara palsu tokoh agama, pejabat publik, atau pimpinan perusahaan untuk menipu korban agar memberikan dana atau informasi sensitif. Fenomena ini menunjukkan bahwa phising telah berevolusi menjadi kejahatan siber yang jauh lebih kompleks dan berbahaya (Itsna Hidayatul Husna et al., 2019).

UU ITE belum memiliki definisi yuridis mengenai deepfake, synthetic media, atau voice cloning sebagai sarana kejahatan siber. Selain itu, tidak terdapat pengakuan normatif bahwa pembuatan dan distribusi konten manipulatif berbasis AI untuk tujuan menyesatkan atau memperoleh keuntungan merupakan perbuatan melawan hukum secara spesifik. Ketiadaan pengaturan ini menimbulkan hambatan serius dalam proses penegakan hukum, karena pasal-pasal konvensional seperti Pasal 378 KUHP tentang penipuan atau Pasal 263 KUHP tentang pemalsuan masih berorientasi pada objek fisik atau dokumen konvensional, bukan konten digital berbasis AI.

Dalam konteks perbandingan hukum, beberapa negara telah menunjukkan langkah progresif dalam mengatur kejahatan siber dan penyalahgunaan AI. Uni Eropa, melalui EU

Artificial Intelligence Act, mengklasifikasikan sistem AI berdasarkan tingkat risikonya dan melarang penggunaan AI untuk manipulasi sosial dan penipuan, termasuk phising. Regulasi ini juga menekankan tanggung jawab penyedia teknologi terhadap potensi penyalahgunaan AI (EU Artificial Intelligence Act, 2024). Amerika Serikat, melalui AI Executive Order 2023, menekankan transparansi, etika, dan mitigasi risiko AI dalam keamanan siber, termasuk ancaman deepfake dan voice cloning (AI Executive Order, 2023). Tiongkok dan Kanada juga telah mengadopsi pendekatan regulasi yang secara tegas mengatur konten AI dan potensi penipuan digital.

Di Indonesia, regulasi pendukung seperti Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta peraturan Kominfo, OJK, dan Bank Indonesia pada dasarnya bertujuan untuk meningkatkan keamanan sistem dan melindungi data pengguna. Namun, regulasi-regulasi tersebut masih didominasi oleh sanksi administratif dan pendekatan preventif, tanpa menyediakan mekanisme perlindungan dan pemulihan yang konkret bagi korban phising. UU Perlindungan Data Pribadi, misalnya, lebih menekankan asas-asas umum tanpa mengatur secara rinci hak korban atas kompensasi atau pemulihan ketika terjadi pelanggaran data akibat phising (UU PDP, Pasal 2 ayat (2)).

Pengaturan hukum phising di Indonesia masih bersifat parsial dan belum mampu menjawab tantangan kejahatan siber yang terus berkembang. Ketergantungan pada pasal-pasal umum dalam UU ITE menyebabkan ketidakpastian hukum dan lemahnya perlindungan terhadap korban. Oleh karena itu, diperlukan pembaruan hukum nasional yang secara eksplisit mengatur phising, baik dari segi definisi, unsur perbuatan, maupun teknik-teknik yang digunakan, termasuk yang berbasis AI. Pembentukan pasal khusus mengenai phising akan memberikan kepastian hukum, meningkatkan efektivitas penegakan hukum, serta mewujudkan perlindungan hukum yang adil dan responsif terhadap masyarakat digital Indonesia, sejalan dengan asas kepastian hukum dan keadilan substantif (Nyoman Gde Remaja, 2014).

Analisis Pengaturan Tindak Pidana Phising Terhadap Praktik Penegakan Hukumnya

Pengaturan mengenai tindak pidana phising dalam hukum positif Indonesia saat ini masih bertumpu pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024 (UU ITE). Namun demikian, regulasi tersebut belum mampu mengakomodasi teknik phising secara komprehensif karena tidak menyebut maupun mendefinisikan phising secara eksplisit.

Salah satu ketentuan yang kerap digunakan untuk menjerat perbuatan phising adalah Pasal 28 ayat (1) UU ITE yang mengatur larangan bagi setiap orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik (Indonesia, UU No. 11 Tahun 2008 jo. UU No. 19 Tahun 2016, Pasal 28 ayat (1)). Secara normatif, pasal ini dimaksudkan untuk melindungi konsumen dalam aktivitas transaksi elektronik, bukan secara khusus untuk menanggulangi kejahatan siber berbasis penipuan digital seperti phising.

Keterbatasan tersebut dapat dilihat secara konkret dalam Putusan Pengadilan Nomor 28/Pid.Sus/2021/PN Srp. Dalam perkara ini, terdakwa Kadek Edi Mudita Yasa alias Kenyot ditangkap pada 12 Februari 2021 dan didakwa oleh jaksa penuntut umum dengan dakwaan alternatif, di mana dakwaan alternatif kesatu menggunakan Pasal 28 ayat (1) UU ITE. Berdasarkan fakta persidangan, terdakwa bersama Peda Diduhu Wau alias Cokro (DPO) secara sadar dan terencana melakukan penipuan melalui media elektronik dengan cara meretas akun Instagram milik korban Ni Kadek Septia Cahyani, kemudian menyamar sebagai pemilik akun untuk menghubungi pihak lain yang memiliki hubungan dekat dengan korban, yaitu Made Candra Ayustina. Modus ini dilakukan untuk memperoleh keuntungan finansial melalui manipulasi sosial, yang oleh ahli dinyatakan sebagai bentuk phising.

Apabila dianalisis secara yuridis, penerapan Pasal 28 ayat (1) UU ITE dalam perkara tersebut menimbulkan persoalan hukum yang mendasar. Unsur utama pasal ini mensyaratkan adanya "kerugian konsumen dalam transaksi elektronik", sedangkan dalam fakta perkara tidak terdapat hubungan hukum antara pelaku dan korban dalam posisi sebagai pelaku usaha dan konsumen. Korban bukanlah konsumen dalam suatu transaksi elektronik, melainkan individu yang menjadi sasaran penipuan berbasis rekayasa sosial. Dengan demikian, unsur delik dalam Pasal 28 ayat (1) tidak terpenuhi secara utuh, sehingga penerapan pasal tersebut berpotensi bertentangan dengan asas legalitas dan kepastian hukum.

Dalam hukum pidana, asas lex certa merupakan bagian tidak terpisahkan dari asas legalitas (nullum crimen, nulla poena sine lege), yang menghendaki agar rumusan tindak pidana disusun secara jelas, tegas, dan tidak multitafsir. Asas ini bertujuan agar setiap orang dapat mengetahui secara pasti perbuatan apa yang dilarang dan sanksi apa yang dapat dijatuhkan oleh negara (Nyoman Gde Remaja, 2014). Ketika suatu pasal digunakan untuk menjerat perbuatan yang secara karakteristik tidak sepenuhnya sesuai dengan rumusan normanya, maka hukum pidana kehilangan fungsi prediktabilitas dan keadilannya, serta membuka ruang penyalahgunaan kewenangan dalam penegakan hukum.

Selain lex certa, asas lex stricta juga menghendaki agar hukum pidana ditafsirkan secara ketat dan tidak diperluas melalui analogi. Artinya, meskipun suatu perbuatan secara substansial merugikan dan bersifat menipu, aparat penegak hukum tidak dibenarkan untuk memaksakan penerapan pasal pidana apabila unsur-unsurnya tidak terpenuhi secara normatif. Dalam konteks phising, kondisi ini menyebabkan aparat penegak hukum sering kali berada pada posisi dilematis, karena harus memilih antara melindungi korban atau tetap berpegang pada ketentuan hukum yang rumusannya tidak dirancang untuk menghadapi kejahatan digital modern. Hal ini juga bertentangan dengan teori subsumsi hukum yang menuntut adanya kesesuaian antara fakta konkret dengan norma hukum yang bersifat umum dan abstrak (Satjipto Rahardjo, 2000).

Perbandingan hukum menunjukkan bahwa permasalahan tersebut tidak dialami oleh semua negara. Nigeria, misalnya, telah mengatur tindak pidana phising secara eksplisit melalui Cybercrimes (Prohibition, Prevention, etc.) Act 2015. Undang-undang ini secara tegas mendefinisikan phising sebagai proses kriminal dan penipuan yang bertujuan memperoleh informasi sensitif, seperti nama pengguna, kata sandi, dan data kartu kredit, dengan cara menyamar sebagai entitas terpercaya dalam komunikasi elektronik (Nigeria, Cybercrimes Act, 2015). Definisi tersebut secara jelas merepresentasikan karakteristik phising sebagai kejahatan siber berbasis manipulasi sosial dan penipuan digital.

Nigeria juga mengatur sanksi pidana secara spesifik bagi pelaku phising dalam Section 32 Cybercrimes Act 2015, yang menyatakan bahwa setiap orang yang dengan sengaja melakukan digital phising dapat dipidana dengan penjara paling lama tiga tahun atau denda, atau kedua-duanya sekaligus (Nigeria, Cybercrimes Act, 2015, Section 32). Kejelasan redaksional ini memberikan kepastian hukum bagi aparat penegak hukum, memudahkan proses pembuktian unsur delik, serta menjamin konsistensi dalam penanganan perkara phising.

Di Indonesia hingga saat ini belum terdapat satu pun ketentuan peraturan perundang-undangan yang secara eksplisit menyebut atau mendefinisikan phising, baik dalam UU ITE maupun regulasi turunannya. Dalam praktik, aparat penegak hukum terpaksa menggunakan pasal-pasal yang bersifat umum, seperti Pasal 28 ayat (1), Pasal 30 ayat (1), atau Pasal 35 UU ITE. Meskipun pasal-pasal tersebut secara substansi dapat dikaitkan dengan beberapa unsur perbuatan phising, ketiadaan pengaturan khusus menimbulkan permasalahan serius dalam hal kepastian hukum, konsistensi putusan pengadilan, dan efektivitas perlindungan hukum bagi korban. Kondisi ini menunjukkan perlunya pembaruan hukum nasional yang secara eksplisit

mengatur phising sebagai tindak pidana siber, agar hukum pidana Indonesia mampu bersikap responsif dan adaptif terhadap perkembangan kejahatan digital modern.

D. KESIMPULAN

Phising dalam ranah kejahatan cyber memiliki cakupan yang sangat luas karena mencakup berbagai metode penipuan mulai dari voice phising, pharming, spoofing, domain, hijacking, hingga deepfake atau voice cloning dari artificial intelligent AI, dan berdasarkan phising secara norma relevan dengan undang-undang informasi dan transaksi elektronik, antara lain pasal 28 ayat 1, pasal 30 ayat 1, pasal 35, dan 36 yang mengatur mengenai penyebaran informasi elektronik yang menyesatkan,manipulasi data dan tindakan yang merugikan pihak lain secara digital akan tetapi berdasarkan phising secara norma dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) belum mampu menjangkau phising secara makna yang sangat beragam. Dalam peraturan yang ada di Indonesia PP No.71 tahun 2019, UU PDP, Kominfo, OJK, BI juga tidak mampu menjangkau kejahatan phising secrara kompleks. Dalam praktik penegakan hukumnya, Undang- Undang Informasi dan Transaksi Elektronik (UU ITE) belum sepenuhnya mampu mengakomodasi tindak pidana phising secara memadai. Hal ini dapat dilihat dari Putusan Pengadilan Nomor 28/Pid.Sus/2021/PN Sempura, di mana jaksa penuntut umum menggunakan dakwaan alternatif terhadap terdakwa. Pada dakwaan alternatif pertama, jaksa mendakwakan terdakwa berdasarkan Pasal 28 ayat (1) UU ITE. Namun, apabila ditinjau dari kronologi perkara, penggunaan pasal tersebut kurang tepat, karena norma dalam Pasal 28 ayat (1) lebih relevan untuk kasus yang melibatkan konsumen dalam hubungan transaksi elektronik. Sedangkan dalam perkara ini, hubungan antara korban dan pelaku tidak dilandasi oleh transaksi atau jasa apapun, melainkan murni merupakan tindak manipulasi digital tanpa ikatan konsumen.

E. DAFTAR PUSTAKA

Danuri, Muhammad. “Perkembangan Dan Transformasi Teknologi Digital”. Managemen Informatika, AMIK Jakarta, Vol. 1. Semarang: Teknologi Cipta Semarang, 2019.

Sarputra. Ardi. “Cyber Crime Dalam Bentuk Phising Berdasarkan Undang- Undang Informasi Dan Transaksi Eletronik”, Vol.1 Jakarta: Pampas, 2020.

Zahra. Artanti. “Perlindungan Hukum Terhadap Korban Phising Terkiat Penhgiriman File Apk”, Vol.10. Jakarta: Jutisi Fakultas Hukum Universitas Pembangunan Nasional Veteran, 2024.

Irfan. Rizal. “Mengurai Permasalahan Peraturan Perundang-Undangan di Indonesia”, Vol.4.

Surakarta: Jurnal Hukum Universitas Sebelas Maret Surakarta, 2020.

Nigeria, Cybercrimes Prohibition, Prevention, etc. Act, 2015.

Malunsenge Leticia. "Penegakan Hukum Terhadap Pelaku Dan Korban Tindak Pidana Cyber Crime Berbentuk Phising di Indonesia", Bandung: jurnal hukum, Vol.11.

Ratna Sari Devi. "Perlindungan Hukum Terhadap Korban Kejahatan Cyber: Studi Kasus Phising", Vol 51. Depok: Jurnal hukum dan Pembangunan Fakultas Hukum Universitas Indonesia, 2021.

Raharjo. Sajipto. Penegakan hukum: suatu tinjauan sosiaologis. Yogyakarta: Genta Publishing, 2009.

Wall. David. Cybercrime: The Trnsformation of crime in the information age,Cambridge: Polity Press, 2007.

Andi Hamzah. Asas-Asas Hukum Pidana. Jakarta: Rineka Cipta, 2008). Sudarto. Hukum dan Hukum Pidana. Bandung: Alumni, 1986

Gunarso. Teknik Menyusun Naskah Akademik dan Rancangan Peraturan Perundang-undangan, Jakarta: Sinar Grafika, 2014.

Nonet. Philippe. law and society in transition: toward responsive law. New York: Haeper & Row, 1978.

Sulistyo. Ananda. "Strategi Penanggulangan Serangan Phising Di Media Sosial", Seminar Nasional Teknologi Informasi Dan Bisnis (SENATIB) Fakultas Ilmu Komputer Universitas Duta Bangsa Surakarta, 2024.

Badan Siber dan Negara (BSSN), BESTI Edisi 40: Tips jaga keamnan digital saat perjalanan lebaran, edisi, 2024

Aziz. Lutfi. "Phising Di Era Media Sosial: Identifikasi Dan Pencegahan Ancaman di Platform Sosial", Vol. 1. Jurnal Internet Software Engineering, 2024.

Badan Siber dan Negara (BSSN), BESTI Edisi 16: Tips jaga keamnan digital saat perjalanan lebaran, edisi, 2024.

Hidayatul. Itsna. "Deepfake, Tantangan Baru Untuk Netizen", Vol.5. Jurnal PROMEDIA, 2019.

Indonesia, "Undang-Undang nomor 11 tahun 2008 jo Undang-Undang nomor 19 tahun 2016 28 ayat 1" LN no. 58, TLN no 4843

Indonesia, "Undang-Undang nomor 11 tahun 2008 jo Undang-Undang nomor 19 tahun 2016 30 ayat 1" LN no. 58, TLN no 4843

Indonesia, Undang-Undang Nomor 11 Tahun 2016 Tentang Informasi dan Transaksi Eletronik, Pasal 35 Ayat 1. LN 251, TLN Tahun 2024 No 5952

Feri Sulianta, Trik Mudah Menjebol Sekaligus Mengamankan Password. Bandung: Penerbit Andi, 2015.

Uni Eropa, EU Artificial Intelegent Act, 2024. United States, AI Executive Order, 2023.

Tiongkok, Interim Measures for Generative AI Service, 2023.

Kanada, Artificial Intelligent and Data Act, 2022.

Nyoman Gde Remaja, "Makna Hukum dan Kepastian Hukum". Vol.2, Jurnal Hukum, 2014.