Jurnal ILMU HUKUM • FAKULTAS HUKUM • UNIVERSITAS RIAU
ISSN (P) : 2087-8591
ISSN (O) : 2654-3761

Fakultas Hukum Universitas Riau, Jalan Pattimura Nomor 9 Gobah, Kel. Cinta Raja, Kec. Sail, Pekanbaru, Riau, Kode Pos 28127. Telp: (+62761)-22539, Fax : (+62761)-21695
E-mail: jihfhur@gmail.com / jih.fh@unri.ac.id
Website: https://jih.ejournal.unri.ac.id/index.php/JIH/index

Phishing Berbasis AI sebagai Serangan *Social Engineering*: Ancaman Baru di Dunia Keamanan Siber

Uffi Novitasari [a*],

[a] Fakultas Hukum, Universitas Islam Indonesia, Email: 24912045@students.uii.ac.id

Article Info

Article History:
Received : 22-07-2025
Revised : 12-08-2025
Accepted : 20-08-2025
Published : 30-08-2025

Keywords:
AI-based Phishing
Social Engineering
Cyber Crime
Legal Reform

Abstract

AI-based phishing is a relatively new digital crime in the dangerous and difficult-to-recognize cyber world that utilizes artificial intelligence (AI) as its attack. Phishing is also part of a social engineering attack that has a mode of manipulating victims. The existence of phishing has been regulated in the Criminal Code, the ITE Law, and the PDP Law, although the regulations are still complex and not specific. This study uses a normative legal method with a legislative approach, case studies, and accompanied by literature studies. The results of the analysis show that AI-based phishing is able to imitate human communication realistically by utilizing machine learning and natural language processing and the psychological weaknesses of the victim. Although phishing already has regulations, these regulations still do not explicitly regulate phishing as a criminal act. The Criminal Code is still general in nature, while the ITE Law and the PDP Law only regulate it implicitly. Therefore, criminal law reform is needed through revision of relevant articles, strengthening digital literacy in society, and expanding international cooperation, as well as adaptive legal policy arrangements.

Informasi Artikel

Histori Artikel:
Diterima : 22-07-2025
Direvisi : 12-08-2025
Disetujui : 20-08-2025
Diterbitkan : 30-08-2025

Kata Kunci:
Phishing berbasis AI
Social Engineering
Kejahatan Siber
Reformasi Hukum

Abstrak

Phishing berbasis AI merupakan kejahatan digital yang tergolong baru dalam dunia siber yang berbahaya dan sulit dikenali yang memanfaatkan kecerdasan buatan (AI) sebagai serangannya. Phishing juga merupakan bagian dari serangan *social engineering* yang memiliki modus memanipulasi korban. Keberadaan phishing telah diatur dalam KUHP, UU ITE, dan UU PDP, meskipun pengaturannya masih kompleks dan belum spesifik Penelitian ini menggunakan metode yuridis normatif dengan pendekatan perundang-undangan, studi kasus, dan disertai studi literatur. Hasil analisis menunjukan bahwa phishing berbasis AI mampu meniru kominukasi manusia secara realistis dengan memanfaatkan *machine learning* dan *natural language processing* dan kelemahan psikologis korban. Meskipun phishing telah memiliki regulasi, namun regulasi tersebut masih belum secara eksplisit mengatur phishing sebagai tindak pidana. KUHP masih bersifat umum, sementara UU ITE dan UU PDP hanya mengatur secara implisit. Oleh karena itu, diperlukan reformasi hukum pidana melalui revisi pasal-pasal yang relevan, penguatan literasi digital masyarakat, dan memperluas kerja sama internasional, serta pengaturan kebijakan hukum yang adaptif

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi saat ini berlangsung sangat pesat dan memiliki peran strategis dalam membentuk tatanan kehidupan masyarakat yang baru. Teknologi tersebut telah menghapus batas-batas geografis, ruang, dan waktu, sehingga mempengaruhi berbagai aspek kehidupan, termasuk pola interaksi sosial, sistem ekonomi, budaya, serta spek pertahanan dan keamanan dunia digital. Namun, kemajuan ini juga membuka celah bagi lahirnya bentuk-bentuk kejahatan baru yang bersifat lebih kompleks dan sulit dideteksi. Salah satu bentuk kejahatan tersebut adalah *phishing,* yaitu tindakan penipuan yang dilakukan melalui sarana digital dengan tujuan memperoleh informasi pribadi atau rahasia secara melawan hukum.[1]

Pelaku *phishing* biasanya menyamar sebagai pihak atau lembaga yang terlihat sah dan terpercaya, seperti bank, perusahaan e-commerce, atau instansi pemerintah. Modus yang digunakan umunya berupa pesan elektronik, SMS, atau situs web palsu yang dibuat sedemikian rupa agar secara sukarela memberikan data penting seperti kata sandi, nomor kartu kredit, atau informasi keuangan lainnya. Tindakan ini tergolong sebagai kejahatan digital, karena dapat digunakan untuk pencurian identitas, penipuan finansial, atau untuk mendapatkan akses illegal ke akun dan sistem miliki korban.[2] Dalam konteks ini, *phishing* tidak lagi dapat dipandang sebagai bentuk penipuan tradisonal semata, melainkan telah berkembang menjadi bagian dari strategi rekayasa sosial digital yang memanfaatkan kerentanan psikologis dengan kecanggihan teknologi. Serangan seperti ini menjadi semakin sulit dikenali karena kecerdasan buatan (AI) mampu meyesuaikan pendekatan dan metode penipuan secara dinamis berdasarkan respons atu perilaku korban secara real-time.

Phishing merupakan salah satu bentuk kejahatan siber (cybercrime) modern yang tergolong baru dalam praktik tindak pidana di Indonesia. Sebelum diberlakukannya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), belum tersedia ketentuan hukum yang secara khusus dapat menjerat pelaku tindak pidana di ranah digital, termasuk pelaku phishing. Meskipun UU ITE telah diundangkan, pengaturannya masih dianggap belum memadai untuk menindak pelaku phishing secara efektif, karena dalam

[1] Siswanto Sunarso, Hukum Informasi dan Transaksi Elektronik, Studi Kasus Prita Mulyasari, PT. Rineka Cipta, Jakarta, 2009. Hal. 39.
[2] Irma Yurita et al., "Pengaruh Kemajuan Teknologi Terhadap Perkembangan Tindak Pidana Cybercrime," *Jurnal Hukum Legalita* 5, no. 2 (2023): 144–55, https://jurnal.umko.ac.id/index.php/legalita/article/view/995.

undang-undang tersebut tidak terdapat definisi atau rumusan norma yang secara eksplisit menyebutkan phishing.

Di Indonesia, phishing merupakan serangan digital yang berbahaya dan merupakan bentuk serangan *social engineering* yang paling umum. *Social engineering* adalah serangkaian teknik manipulasi psikologis yang dimanfaatkan penyerang untuk mengelabuhi dan memanipulasi korban agar secara sukarela memberikan informasi sensitif atau melakukan tindakan tertentu yang merugikan dirinya. Melihat pada pengertian phishing, maka phishing secara spesifik adalah salah satu bentuk serangan *social engineering* yang paling umum, dimana *phisher* (pelaku phishing) menggunakan email, pesan teks, atau situs web palsu untuk menipu korban agar memberikan data pribadi seperti password, nomor kartu kredit, atau informasi penting lainnya.

Berdasarkan data pada kuartal I tahun 2023, Indonesia mengalami lonjakan signifikan serangan phishing dengan jumlah 26.675 kasus, meningkat sekitar 220% disbanding kuartal IV 2022 yang hanya 6.106 laporan, dengan puncak tertinggi pada Februari 2023 mencapai 15.050 kasus. Media sosial menjadi target utama (45%), diikuti lembaga keuangan (31%) dan ritel/e-commerce (20%). Pada kuartal I 2025, lebih dari 3 juta ancaman siber berbasis web berhasil diblokir, menjadikan Indonesia negara kedua dengan serangan siber tertinggi di Asia Tenggara. Laporan IBM X-Force Threat Index 2025 mencatat lonjakan serangan email phishing sebesar 180% sejak 2023, didorong oleh pemanfaatan AI yang membuat phishing semakin murah, masif, dan menguntungkan bagi pelaku kejahatan siber.[3]

Fenomena tersebut mencerminkan adanya ketimpangan antara perkembangan teknologi digital yang sangat pesat dengan kemampuan hukum dalam merespons dinamika tersebut secara efektif, khususnya jika aturan-aturan tersebut dihadapkan pada kejahatan *phishing* berbasis AI. Kita melihat saat ini bahwa regulasi yang ada seperti KUHP, UU ITE, dan UU PDP belum secara spesifik mengatur bentuk-bentuk kejahatan siber yang menggunakan teknologi canggih seperti AI, terutama dalam kejahatan *phishing.* Ketimpangan seperti ini menimbulkan kekhawatiran serius mengenai timbulnya celah hukum (*legal vacuum*) yang menyulitkan penegakan hukum yang efektif, yaitu situasi dimana tidak adanya suatu aturan hukum yang jelas untuk mneyelsaikan suatu permasalahan tertentu. Sehingga permasalahan

[3]https://bankjombang.co.id/serangan-phishing-di-indonesia-terus-meningkat-berikut-data-lengkapnya/#:~:text=Serangan%20phishing%20capai%2026.675%20kasus%20pada%20kuartal%20I%202023&text=Tercatat%2C%20IDADX%20menerima%20sebanyak%2026.675,kenaikan%20sebanyak%2020.569%20laporan%20phishing.

utama dalam menghadapi kejahatan phishing berbasis kecerdasan buatan (AI) terletak pada ketidakseimbangan antara kecepatan perkembangan teknologi dengan lambatnya pembaruan regulasi hukum. Teknologi AI terus berkembang dalam waktu singkat bahkan dalam hitungan bulan, sementara proses pembentukan undang-undang atau revisi peraturan hukum sering kali memerlukan waktu bertahun-tahun. Ketimpangan ini menyebabkan sistem hukum selalu berada dalam posisi tertinggal dalam merespons kejahatan phishing yang semakin canggih dan terotomatisasi. Kondisi ini memberikan ruang leluasa bagi pelaku kejahatan untuk terus mengeksploitasi celah hukum dan kelemahan regulasi yang ada, sementara aparat penegak hukum dan perangkat perundang-undangan masih berusaha mengejar ketertinggalan tersebut.[4]

Pada beberapa penelusuran, penulis menemukan ada beberapa tulisan yang juga membahas tentang isu yang sama dengan penulis, yang pertama ada dari Hendri Ahmadian dkk, yang berjudul "Teknik Penyerangan Phishing Pada Social Engineering Menggunakan Set dan Pencegahannya", tulisannya membahas tentang bagaimana penyerang phishing (phisher) memanfaatkan perilaku manusia dengan teknik phishing sebagai social engineering dengan menggunakan SET sebagai modus operandinya.[5] Kedua, ada penelitian milik Yazid Haikal Lokapala dkk, yang berjudul "Aspek Yuridis Kejahatan Phishing dalam Ketentuan Hukum di Indonesia", tulisannya membahas tentang tindak pidana phishing dalam dunia cybercrime dalam aspek yuridis, bahwa phishing dapat dijerat Pasal 378 dan 372 KUHP, serta Pasal 28 ayat (1) dan Pasal 45 ayat (1) UU ITE yang penerapannya belum maksimal sehingga menurut penulis tersebut perlu upaya preventif dan represif.[6] Ketiga, ada penelitian milik Maria Rosanti dkk yang berjudul "Implementasi Sistem Keamanan Suber Berbasis Artificial Intelligence untuk Mengatasi Serangan Phishing", tulisannya membahas tentang sangat efektifnya adanya sistem keamanan siber berupa kecerdasan buatan (AI) dalam mendeteksi phishing khususnya

[4] Hary Abdul Hakim, Chrisna Bagus Edhita Praja, and Sung Ming-Hsi, "AI in Law: Urgency of the Implementation of Artificial Intelligence on Law Enforcement in Indonesia," *Jurnal Hukum Novelty* 14, no. 1 (2023): 122–34, https://doi.org/10.26555/novelty.v14i1.a25943.

[5] Hendri Ahmadian and Aulia Sabri, "Teknik Penyerangan Phishing Pada Social Engineering Menggunakan Set Dan Pencegahannya," *Djtechno: Jurnal Teknologi Informasi* 2, no. 1 (2021): 13–20, https://doi.org/10.46576/djtechno.v2i1.1251.

[6] Yazid Haikal Lokapala, Fuad Januar Nurfauzi, and Yeni Widowaty, "Aspek Yuridis Kejahatan Phishing Dalam Ketentuan Hukum Di Indonesia," *Indonesian Journal of Criminal Law and Criminology (IJCLC)* 5, no. 1 (2024): 19–24, https://doi.org/https://doi.org/10.18196/ijclc.v5i1.19853.

melalui algoritma machine leraning, sekaligus meinimalkan kesalahan deteksi (*false positive* dan *false negative*).[7]

Dari beberapa penulis diatas, terdapat beberapa persamaan dengan apa yang akan ditulis oleh penulis dalam tulisan ini yaitu, sama-sama menyoroti tentang bagaimana serangan kejahatan phishing dalam dunia keamanan siber dan dalam perkembangan dunia digital, serta bahaya nya phishing dalam memanipulasi dan mengancam keamanan data pribadi korban. Namun, terdapat perbedaan yang signifikan yaitu, dalam tulisan ini penulis mengkritik terkait regulasi kejahatan phishing dalam hukum pidana (KUHP, UU ITE, dan UU PDP) yang masing-masing mengatur phishing yang tidak secara eksplisit, dan penulis dalam tulisan ini lebih fokus pada phishing yang berbasis AI dibandingkan dengan phishing tradisional atau konvensional serta bagaimana seharusnya kebijakan hukum yang solutif dalam menangani regulasi hukum yang belum efektif serta menanggulangi tantangannya munculnya serangan phishing tersebut.

Oleh karena itu penting mengkaji dan mengkritisi hal tersebut guna memastikan bahwa hukum bergerak maju menanggulangi kejahatan phishing, khususnya mengenali modus operandinya dalam sistem AI, dan memastikan bahwa penegakan hukum ditegakkan dengan baik serta sesuai dengan regulasi dan unsur-unsur nya secara benar. Dengan demikian perlu pembahasan lebih mendalam terkait bagaimana penanganan, regulasi, dan tranformasi hukumnya dalam menghadapi perkembangan *phishing* berbasis AI yang dapat mengancam keamanan siber. Penelitian ini akan menggunakan metode yuridis normatif dengan pendekatan yang mengacu pada analisa terhadap kasus konkrit guna menganalisis pola serangan, teknik manipulasi sosial yang digunakan, dan respons undang-undang terhadap kejahatan tersebut, serta diperkuat dengan telaah literatur sebagai landasan teoritik dalam memahami bentuk kejahatannya dan menafsirkan ketentuan hukum yang berlaku.

ANALISIS DAN PEMBAHASAN

Bentuk dan Modus Operandi Phishing Berbasis AI sebagai Serangan *Social Engineering*

Phishing berbasis AI adalah bentuk serangan siber yang memanfaatkan teknologi kecerdasan buatan untuk membuat pesan phishing yang sangat realistis, personal, dan sulit dikenali sebagai penipuan. Berbeda dengan phishing tradisional yang biasanya menggunakan

[7] Maria Rosanti, Yusrodi, and Agatha Elisabet, "IMPLEMENTASI SISTEM KEAMANAN SIBER BERBASIS ARTIFICIAL INTELLIGENCE UNTUK MENGATASI SERANGAN PHISHING," *Aisyah Journal of Informatics and Electrical Engineering* 7, no. 1 (2025).

pesan generik dan massal, phishing berbasis AI mampu mengotomatisasi pembuatan ribuan email atau pesan yang disesuaikan dengan profil korban berdasarkan data yang dikumpulkan dari media sosial dan sumber terbuka lainnya. AI menggunakan teknik seperti *machine learning* dan *natural language processing* (NLP) untuk meniru gaya bahasa, nada, dan pola komunikasi yang meyakinkan, sehingga pesan phishing tersebut tampak seperti benar-benar berasal dari institusi resmi, seperti bank atau perusahaan besar. Berbeda dengan phishing tradisional, phishing tradisional biasanya dilakukan secara massal dengan menggunakan template email atau pesan generik yang ditujukan ke banyak orang sekaligus. Ciri khasnya adalah penggunaan bahasa yang cenderung kaku, sering terdapat kesalahan tata bahasa, alamat email pengirim yang mencurigakan, serta permintaan yang tidak relevan atau terlalu umum. Karena sifatnya yang kurang personal dan seringkali mudah dikenali, banyak pengguna yang dapat mengidentifikasi dan menghindari serangan phishing jenis ini.

Penipuan digital melalui tautan phishing bertujuan untuk memancing korban agar mengunduh virus atau mengakses situs berbahaya, sehingga korban secara tidak sadar dapat memberikan informasi penting seperti nomor kartu kredit, data pribadi, memberikan informasi login atau akun untuk situs web tertentu. Dampak yang ditimbulkan terhadap korban bervariasi tergantung pada tingkat eksploitasi setelah tautan diklik. Pertama, peretas dapat mengumpulkan informasi tentang korban secara otomatis, seperti data perangkat, lokasi perkiraan, serta informasi lainnya yang mungkin diberikan korban tanpa disadari. Kedua, terdapat risiko terinstalnya malware pada perangkat korban. Perangkat lunak berbahaya seperti virus atau spyware dapat diunduh secara diam-diam dan kemudian digunakan untuk mengakses atau mencuri data rahasia dari perangkat tersebut. Ketiga, peretas dapat mengeksploitasi jaringan dan daftar kontak korban, misalnya dengan mengirimkan pesan phishing lanjutan ke kontak korban, atau dalam situasi terburuk, mengakses perangkat korban secara jarak jauh untuk melakukan tindakan yang lebih merugikan.[8]

Dalam melancarkan aksinya, pelaku phishing (phisher) menggunakan berbagai teknik untuk menjebak korban. Di antaranya adalah sebagai berikut:[9]

1. Email Spoofing. Teknik ini digunakan dengan cara mengirimkan email yang tampak seolah-olah berasal dari lembaga resmi. Email tersebut biasanya berisi permintaan agar

[8] Afifah. Rosmalinda Sahfitri, "PENIPUAN DIGITAL MELALUI TAUTAN PHISHING," *Jurnal Dialektika Hukum* 6, no. 2 (2024): 92–107.
[9] Devi Anjheli, "Privasi Digital Dan Kejahatan Phishing Di Indonesia : Evaluasi Kritis Terhadap Efektivitas UU ITE Dan UU PDP," *STAATSRECHT: Jurnal Hukum Kenegaraan Dan Politik Islam Vol.* 4, no. 1 (2024).

penerima memberikan informasi sensitif seperti nomor kartu kredit, kata sandi, atau mengunduh formulir tertentu yang berbahaya.

2. Internet Submission. Merupakan salah satu metode phishing yang tergolong paling kompleks. Dalam metode ini, pelaku bertindak sebagai "*man-in-the-middle*", yaitu menjadi perantara tersembunyi antara situs web resmi dan pengguna, sehingga dapat menyadap data yang dikirimkan tanpa diketahui korban.
3. Pesan Instan (Chat/IM Phishing). Teknik ini melibatkan pengiriman pesan melalui aplikasi perpesanan yang berisi tautan mencurigakan, yang jika diklik akan mengarahkan pengguna ke situs phishing palsu yang dirancang menyerupai situs resmi.
4. Manipulasi Tautan (Link Manipulation). Dalam metode ini, phisher mengirimkan tautan yang tampak sah, tetapi sebenarnya telah dimodifikasi untuk mengalihkan pengguna ke situs web phishing. Tampilan awal tautan bisa menyerupai alamat resmi, namun setelah diklik, korban diarahkan ke situs palsu yang digunakan untuk mencuri informasi.

Phishing adalah salah satu bentuk serangan siber yang dilakukan dengan cara menyamar sebagai individu atau pihak yang tampak terpercaya guna memperoleh informasi penting dari korban, seperti data pribadi atau kredensial akun. Serangan ini umumnya dilakukan pada tahap awal untuk mengakses kredensial target (informasi rahasia atau sensitif milik korban yang menjadi sasaran utama untuk dicuri oleh pelaku phishing), seperti nama pengguna dan kata sandi. Salah satu contohnya adalah penggunaan situs palsu yang tampak identik dengan situs resmi, namun memiliki URL berbeda. Peretas kemudian mengirimkan tautan situs palsu tersebut kepada korban dan mendorongnya untuk login, tanpa menyadari bahwa informasi login tersebut langsung dikirimkan ke pelaku. Dalam praktiknya, phishing juga kerap menggunakan metode rekayasa sosial (social engineering), yaitu pendekatan manipulatif berbasis psikologis atau sosial. Taktik ini dapat berupa pengiriman pesan singkat (SMS) yang berisi penipuan, misalnya informasi palsu mengenai hadiah, dana pinjaman, atau notifikasi dari bank, yang bertujuan untuk membuat korban memberikan data pribadinya secara sukarela.

Dalam dunia digital, serangan *social engineering* merupakan salah satu ancaman paling serius dalam keamanan siber. Meskipun serangan ini bisa dikenali, namun menghentikan serangan tersebut sangat sulit dilakukan. *Social engineering* bekerja dengan memanipulasi korban agar memberikan informasi penting yang kemudian dapat digunakan untuk berbagai tujuan seperti dijual di pasar gelap, penipuan atau mengakses data pribadi. Dengan kemajuan big data, para pelaku kini memanfaatkan data dalam skala besar untuk keuntungan pribadi.

Mereka mengemas dan mengolah data sehingga menjadi komoditas yang sangat berharga di era digital saat ini.[10] Melihat pada bagaimana serangan *social engineering* dalam dunia siber, serangan phishing secara jelas merupakan bagian integral dari *social engineering* karena keduanya memiliki kesamaan teknik penyerangan dengan mengandalkan psikologis untuk mengeksploitasi korban dan memperoleh informasi penting.

Sebagaimana yang telah dijelaskan, social engineering adalah ancaman serius dalam keamanan siber yang sulit dihentikan sepenuhnya karena berfokus pada kelemahan manusia, bukan hanya celah teknis. Phishing memanfaatkan teknik ini dengan menyamar sebagai entitas terpercaya melalui email, pesat, atau situs palsu untuk menipu korban agar secara sukarela menyerahkan data sensitif seperti kata sandi, nomor kartu kredit, atau informasi pribadi lainnya. Modus tersebut tentu bagian dari social engineering dikarenakan adanya unsur phishing yaitu ketidaksadaran korban untuk mneyerahkan data pribadi secara sukarela dimana pelaku memanfaatkan kondisi emosional dan psikologis korban untuk mempengaruhi keputusan dan tindakan mereka tanpa disadari. Dalam phishing, biasanya pelaku mengirimkan email, atau SMS dari institusi terpercaya dengan tujuan menimbulkan rasa percaya, urgensi, atau ketakutan pada korban. Manipulasi tersebut efektif karena pelaku menggunakan elemen psikologis seperti rasa takut, kepercayaan, rasa ingin membentu, atau tekanan waktu agar korban bertindak tanpa berfikir kritis. Dengan kata lain, phishing adalah bentuk social engineering yang memanfaatkan kelemahan manusia melalui trik psikologis untuk mendapatkan akses ilegal ke informasi penting.[11]

Regulasi Kejahatan Phishing di Indonesia

Phishing merupakan salah satu bentuk cybercrime yang baru di dunia digital. Dalam KUHP, kejahatan *phishing* tidak ada penjelasan secara eksplisit menyebutkan istilah tersebut, namun *phishing* dapat dikualifikasikan sebagai tindak pidana penipuan, sebagaimana yang tercantum dalam Pasal 378 KUHP. Dalam Pasal tersebut secara eksplisit menjelaskan bahwa seorang pelaku yang melakukan tipu muslihat atau kebohongan untuk memperoleh keuntungan dari korban. Namun, ketentuan tersebut masih tergolong umum dan belum mampu

[10] Slamet, "Pertahanan Pencegahan Serangan Social Engineering Menggunakan Two Factor Authentication (2FA) Berbasis SMS (Short Message System)," *Jurnal Spirit* 14, no. 2 (2022): 23–29, https://doi.org/10.53567/spirit.v14i2.260.

[11] Lutfi Aziz Febrika Ardy et al., "Phishing Di Era Media Sosial: Identifikasi Dan Pencegahan Ancaman Di Platform Sosial," *Journal of Internet and Software Engineering* 1, no. 4 (2024): 11, https://doi.org/10.47134/pjise.v1i4.2753.

mengakomodasi modus operandi *phishing* yang berbasis teknologi, khususnya yang berbasis AI.[12] Dalam Pasal 378 KUHP adalah sebagai berikut:

> "Barang siapa yang dengan niat untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, menggunakan nama palsu atau identitas yang tidak benar, dengan tipu muslihat, atau serangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang, memberikan pinjaman, atau menghapuskan piutang, dapat dikenakan ancaman pidana penjara dengan maksimum hukuman selama empat tahun".

Berdasarkan unsur-unsur yang tercantum dalam Pasal 378 KUHP, dapat disimpulkan bahwa subjek hukum dalam ketentuan ini adalah pelaku yang melakukan tindak pidana penipuan. Unsur niat untuk menguntungkan diri sendiri atau orang lain mencerminkan adanya unsur kesengajaan (opzet) dalam tindakannya. Tindakan tersebut juga dilakukan secara melawan hukum, menunjukkan bahwa pelaku tidak memiliki hak atas keuntungan yang diperoleh dari penipuan tersebut. Dalam praktiknya, pelaku kerap menggunakan identitas palsu yang diketahui atau dipercayai oleh korban, serta mengangkat status sosial atau jabatan palsu, misalnya mengaku sebagai tokoh agama atau figur terhormat. Pelaku menggunakan tipu daya atau rangkaian kebohongan, seperti menjanjikan pembelian barang murah atau mengaku memiliki koneksi dengan pihak tertentu untuk mendapatkan kepercayaan korban. Selanjutnya, pelaku meminta sejumlah uang dengan alasan tertentu, padahal tujuannya semata-mata untuk memperoleh keuntungan dari korban.[13]

Tindakan "menggerakkan orang lain" di sini diartikan sebagai usaha pelaku untuk mempengaruhi korban agar menyerahkan barang, uang, atau hak tertentu. Hal ini juga mencakup pemberian pinjaman atau penghapusan utang, yang menjadi bagian dari inti delik penipuan. Menurut Nico Keijzer, Pasal 378 KUHP memang relevan untuk menjerat pelaku yang melakukan manipulasi demi memperoleh keuntungan, namun pasal ini tidak mencakup unsur digital, seperti informasi elektronik atau dokumen elektronik yang dipalsukan atau digunakan secara tidak sah. Dengan demikian, ketika kejahatan penipuan dilakukan melalui sarana teknologi informasi seperti dalam kasus phishing berbasis file APK, maka pengaturan hukumnya lebih tepat menggunakan Undang-Undang Informasi dan Transaksi Elektronik (UU

[12] Lokapala, Nurfauzi, and Widowaty, "Aspek Yuridis Kejahatan Phishing Dalam Ketentuan Hukum Di Indonesia."
[13] Anjheli, "Privasi Digital Dan Kejahatan Phishing Di Indonesia : Evaluasi Kritis Terhadap Efektivitas UU ITE Dan UU PDP."

ITE). Hal ini selaras dengan prinsip "*lex specialis derogat legi generali*", yaitu asas hukum yang menyatakan bahwa peraturan khusus mengesampingkan peraturan umum dalam hal terjadi konflik norma. Oleh karena itu, dalam konteks kejahatan siber, UU ITE sebagai regulasi khusus lebih relevan dan efektif diterapkan dibandingkan KUHP yang bersifat umum.

Selanjutnya, pengaturan mengenai kejahatan *phishing* perlu memiliki pengaturan yang lebih eksplisit yang mengatur terkait istilah tersebut. Oleh karena itu UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) Jo UU Nomor 19 Tahun 2016 menjadi regulasi yang lebih relevan. Dalam UU ITE tersebut, kejahatan *phishing* sebagai bentuk kejahatan rekayasa sosial saat ini di Indonesia dimungkinkan dapat dikenai Pasal 35 Jo Pasal 51 ayat (1) UU ITE, karena pelaku membuat sistus palsu yang tampilannya menyerupai situs resmi dengan tujuan menipu pengguna. Dalam hal ini, pelaku secara sengaja memanipulasi sistem elektronik agar terlihat sah, padahal sebenernya palsu, sehingga dapat menimbulkan kerugian bagi orang lain. Selain itu, kejahatan *phishing* juga dapat dikenai Pasal 28 ayat (1) Jo Pasal 45a ayat (1) UU ITE, karena pelaku menyebarkan informasi palsu atau menyesatkan yang dapat merugikan orang lain. dalam praktinya, korban diarahkan untuk mengakses tautan yang tampak resmi, lalu diminta mengisi atau memperbarui data pribadinya di situs tersebut. Data ini kemudian disalahgunakan oleh pelaku untuk memperoleh keuntungan atau menyebabkan kerugian pada korban. Dengan demikian, *phishing* merupakan bentuk penipuan digital yang memanfaatkan manipulasi informasi elektronik untuk mencuri data pribadi secara melawan hukum.[14] Pada saat ini perbuatan phising tersebut diatur pada Pasal 35 jo Pasal 51 ayat (1), yang dirumuskan sebagai berikut:

Pasal 35

> "Setiap Orang dengan sengaja, dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik".

[14] Ardi Saputra Gulo, Sahuri Lasmadi, and Khabib Nawawi, "Cyber Crime Dalam Bentuk Phising Berdasarkan Undang-Undang Informasi Dan Transaksi Elektronik," *PAMPAS: Journal of Criminal Law* 1, no. 2 (2020): 68–81, https://doi.org/10.22437/pampas.v1i2.9574.

Pasal 51

> "Setiap Orang yang memenuhi unsur sebagaimana dimaksdu dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp 12.000.000.000,00 (dua belas miliar rupiah). Unsur-unsur yang terdapat di dalam Pasal 35, yaitu: - Setiap Orang - Dengan sengaja dan tanpa hak atau melawan hukum - Melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik - Dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik".

Kejahatan *phishing* tidak hanya terbatas pada pembuatan situs palsu yang menyerupai situs resmi, tetapi juga mencakup tindakan penipuan atau kebohongan yang bertujuan untuk menyesatkan orang lain, sehingga korban secara tidak sadar memberikan informasi pribadi yang bersifat rahasia. Akibat dari tindakan tersebut, korban dapat mengalami kerugian, baik secara materil maupun immaterial karena data pribadinya berhasil diakses dan disalahgunakan oleh pelaku kejahatan siber. Oleh karena itu, kejahatan *phishing* dapat dijerat dengan Pasal 28 ayat (1) Jo Pasal 45a ayat (1) UU ITE, karena perbuatan tersebut mengandung unsur penyebaran informasi bohong atau menyesatkan yang mengakibatkan kerugian bagi orang lain. Pasal 28 ayat (1) jo Pasal 45A ayat (1) dirumuskan sebagai berikut:

Pasal 28 ayat (1)

> "Setiap Orang dengan sengaja, dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik".

Pasal 45a ayat (1)

> "Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik sebagaimana dimaksud dalam Pasal 28 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah)".

Dapat disimpulkan, bahwa phishing dapat dipahami sebagai tindakan yang dilakukan oleh seseorang untuk memancing korban agar secara sukarela memasukkan data pribadi yang bersifat rahasia ke dalam sebuah situs palsu. Situs tersebut sebelumnya telah dimodifikasi (*deface*) agar menyerupai situs resmi, dan umumnya diakses melalui tautan yang dikirimkan

lewat email. Tujuan dari tindakan ini adalah untuk memperoleh informasi pribadi milik orang lain secara tidak sah. Berdasarkan hal tersebut, timbul pertanyaan penting: apakah penanganan kejahatan siber berupa phishing di Indonesia cukup hanya dengan menerapkan Pasal 35 juncto Pasal 51 ayat (1) dan Pasal 28 ayat (1) juncto Pasal 45A ayat (1) UU Nomor 19 Tahun 2016 tentang Perubahan atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, ataukah perlu pula mempertimbangkan ketentuan pasal-pasal lain dalam UU ITE maupun ketentuan pidana yang terdapat di luar UU ITE, seperti dalam (KUHP) atau UU Perlindungan Data Pribadi (UU PDP), karena jika ditelaah lebih lanjut, UU ITE tidak secara eksplisit mengatur unsur-unsur phishing secara lengkap, melainkan hanya memuat ketentuan yang mendekati karakteristik tindak pidana tersebut. Kondisi ini dapat menimbulkan ketidakpastian hukum dalam penerapannya. Namun, karena phishing termasuk dalam kategori kejahatan siber (cybercrime), maka penanganannya tetap mengacu pada UU Nomor 19 Tahun 2016 sebagai lex specialis yang secara khusus mengatur kejahatan berbasis teknologi informasi.

Selanjutnya, dalam upaya menanggulangi kejahatan siber seperti phishing, Undang-Undang Perlindungan Data Pribadi (UU PDP) menetapkan sanksi administratif maupun pidana. Pelaku phishing dapat dijerat dengan sanksi pidana berupa hukuman penjara paling lama 5 tahun dan/atau denda paling banyak sebesar 5 miliar rupiah, sebagaimana diatur dalam Pasal 67 UU PDP. Pemberian sanksi ini bertujuan untuk memberikan efek jera kepada pelaku serta mencegah terulangnya tindak kejahatan siber di masa mendatang.[15] Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) memang tidak secara eksplisit menyebut atau mengatur perbuatan phishing sebagai tindak pidana tersendiri. Hal ini disebabkan karena UU PDP tidak secara khusus mengatur bentuk pelanggaran yang terjadi dalam interaksi person to person, yaitu komunikasi bersifat pribadi antara dua pihak dalam ruang yang tertutup. Meskipun demikian, tindakan phishing tetap dapat dijerat menggunakan ketentuan dalam UU PDP, khususnya pada Pasal 65 ayat (1) dan (3) yang mengatur larangan mengakses dan memperoleh data pribadi secara melawan hukum. Ancaman sanksi pidananya tercantum dalam Pasal 67 ayat (1) dan (3). Selain itu, penggunaan identitas atau akun palsu dalam modus phishing, termasuk yang dilakukan dengan teknologi berbasis AI, juga dapat dikualifikasikan sebagai pemalsuan data pribadi untuk keuntungan pribadi dan merugikan

[15] Potler Reyhan, Edlin. Gultom, "Perlindungan Hukum Terhadap Pengguna Sosial Media Terkait Cyber Crime Phising Berdasarkan Undang- Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik," *Lex Laguens: Jurnal Kajian Hukum Dan Keadilan* 3, no. 1 (2025): 111–24.

orang lain, sebagaimana diatur dalam Pasal 66, dengan sanksi pidana sebagaimana diatur dalam Pasal 68 UU PDP.[16]

Tantangan dan Kebijakan Hukum dalam Menanggulangi Phishing Berbasis AI

Phishing merupakan bentuk kejahatan siber yang dilakukan dengan cara menyamarkan identitas pelaku sebagai pihak yang seolah-olah terpercaya guna memperoleh data pribadi korban, seperti kata sandi sandi atau informasi keuangan melalui media elektronik atau situs web palsu. Dalam konteks penegakan hukum, kejahatan ini menghadirkan sejumlah tantangan yang signifikan.

Pertama, rendahnya tingkat literasi digital dan kesadaran hukum masyarakat terhadap modus kejahatan siber menjadikan individu rentan menjadi korban. Kedua, terbatasnya kapasitas sumber daya manusia yang memiliki kompetensi forensik digital dan pemahaman mendalam terhadap tindak pidana siber menghambat efektivitas deteksi dan penindakan. Ketiga, keterbatasan sarana dan prasarana teknologi pada aparat penegak hukum menyebabkan sulitnya mengidentifikasi dan melacak pelaku yang menggunakan teknik penyamaran digital yang semakin canggih. Keempat, apabila tindak pidana *phidhing* melibatkan yurisdiksi lintas negara, proses penegakan hukum menjadi kompleks, terutama dalam pengumpulan alat bukti elektronik yang tunduk pada hukum negara lain. Kelima, ketidakjelasan norma hukum positif, khususnya yang berkaitan dengan yurisdiksi dan pengaturan lintas negara menyebakan ketidakpastian hukum dan menjerat pelaku *phishing* secara efektif.[17]

Untuk menjawab tantangan tersebut, diperlukan penguatan regulasi nasional yang komprehensif dan adaptif terhadap dinamika kejahatan siber, peningkatan kapasitas kelembagaan dan sumber daya manuisa seperti aparat penegak hukum, edukasi publik secara massif mengenai keamanan data pribadi, serta penguatan kerjasama internasional melalui instrument hukum multilateral dalam rangka penanggulangan kejahatan siber lintas batas.

Jika melihat pada tantangan yang hadir ketika munculnya kejahatan *phishing,* maka Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sampai saat ini belum secara

[16] Dewana Saputra and Zaid Alfauza Marpaung, "Analisis Yuridis Penanggulangan Penyalahgunaan Data Pribadi Dalam Bentuk Phising Yang Dilakukan Oleh Paid Verified Account Di Media Sosial Menurut Undang-Undang Perlindungan Data Pribadi," *Uneslaw Review* 5, no. 4 (2023): 4764–75, https://doi.org/https://doi.org/10.31933/unesrev.v5i4.

[17] Lokapala, Nurfauzi, and Widowaty, "Aspek Yuridis Kejahatan Phishing Dalam Ketentuan Hukum Di Indonesia."

eksplisit merumuskan atau memberikan definisi yuridis terkait tindak pidana *phishing*. Kekosongan norma ini menimbulkan persoalan hukum, khususnya dalam hal pemidanaan terhadap pelaku kejahatan siber (*cybercrime*) yang menggunakan modus *phishing*, mengingat belum adanya kepastian hukum mengenai unsur-unsur tindakannya.

Oleh karena itu, dibutuhkan adanya kebijakan hukum represif terhadap UU ITE dengan cara memperjelas konsep *phishing* dalam norma hukum positif serta melakukan perubahan terhadap ketentuan Pasal 35. Hal ini dikarenakan Pasal 35 memiliki kedekatan substansi dengan karakteristik tindak pidana *phishing*, namun belum secara lengkap mencakup seluruh unsur perbuatan tersebut, sehingga menimbulkan kekaburan norma (*vagueness of norm*) yang dapat menghambat penegakan hukum. Sebagaimana prinsip *nullum crimen sine lege certa*, suatu perbuatan tidak dapat dikualifikasi sebagai tindak pidana tanpa adanya rumusan norma hukum yang tegas dan jelas. Ketidakjelasan norma akan berimplikasi pada multitafsir dan menyebabkan ketidakpastian hukum (*rechts onzekerheid*), sehingga pelaku *phishing* tidak dapat dipertanggungjawabkan secara pidana secara sah dan meyakinkan.[18]

Berdasarkan hal tersebut, berikut usulan kebijakan hukum:

1. Perumusan Konsep *Phishing*

   Didefinisikan sebagai perbuatan yang dilakukan dengan sengaja, tanpa hak, atau melawan hukum, berupa manipulasi, penciptaan, atau perubahan atas Informasi Elektronik dan/atau Dokumen Elektronik sehingga menimbulkan kesan seolah-olah data tersebut otentik. Tindakan tersebut dilakukan melalui media berbasis jaringan internet, dengan menggunakan nama domain tertentu untuk memancing pihak lain agar secara sukarela memberikan data atau identitas pribadi yang bersifat rahasia, dan akibatnya pihak tersebut mengalami kerugian.

2. Perubahan Pasal 35 UU ITE:

   Dirumuskan ulang sebagai berikut: *"Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan phishing yang mengakibatkan kerugian bagi orang lain."* Dengan pengaturan tersebut, Pasal 35 menjadi memiliki kekuatan hukum yang lebih jelas dan operasional dalam menjerat pelaku kejahatan *phishing*.

Selain itu, perlu dicatat bahwa kejahatan *phishing* belum dirumuskan dalam Rancangan Kitab Undang-Undang Hukum Pidana (RKUHP), yang kemungkinan besar disebabkan oleh

[18] Gulo, Lasmadi, and Nawawi, "Cyber Crime Dalam Bentuk Phising Berdasarkan Undang-Undang Informasi Dan Transaksi Elektronik."

karakteristiknya yang bersifat teknologi tinggi (*technology-based crime*), sehingga pengaturannya lebih tepat dimuat dalam UU sektoral seperti UU ITE.

Selanjutnya, jika melihat pada KUHP, khususnya dalam Pasal 378 KUHP, kejahatan *phishing* termasuk dalam bentuk penipuan. Dalam Pasal 378 KUHP mengatur bahwa setiap orang yang dengan sengaja menggunakan tipu muslihat, rangkaian kebohongan, nama palsu, atau keadaan palsu dengan maksud menguntungkan diri sendiri atau orang lain secara melawan hukum, dan berhasil membujuk korban untuk menyerahkan barang, membuat utang, atau menghapuskan piutang, dapat dipidana penjara paling lama empat tahun. Dalam konteks phishing, pelaku biasanya menyamar sebagai pihak tertentu (misalnya institusi keuangan) dan menggunakan situs web atau email palsu untuk memperdaya korban agar menyerahkan data pribadi atau informasi rahasia, sehingga unsur-unsur penipuan dalam Pasal 378 KUHP dapat terpenuhi. Dalam penerapanyya berdasarkan pasal tersebut, dalam kasus *phishing* bahwa perbuatan pelaku jelas memenuhi unsur subjektif, yaitu adanya niat menguntungkan diri sendiri atau orang lain secara melawan hukum, dan unsur objektif berupa penggunaan tipu muslihat atau rangkaian kebohongan untuk memperoleh sesuatu dari korban secara tidak sah. Namun, terdapat kelemahan dalam kebijakan ini, karena KUHP merupakan produk hukum lama yang belum secara spesifik mengantisipasi perkembangan kejahatan siber seperti phishing. Sehingga perlu dilakukan transformasi hukum yang lebih progresif dan spesifik.

Selanjutnya, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) merupakan instrumen hukum penting dalam menghadapi kejahatan siber, khususnya phishing, di Indonesia. UU ini menetapkan kewajiban hukum bagi setiap pihak yang mengelola data pribadi untuk melindungi dan menjaga kerahasiaan data tersebut, serta mengatur sanksi tegas terhadap pelanggaran, baik berupa sanksi administratif maupun pidana. Pemerintah memiliki kewajiban hukum untuk menegakkan ketentuan dalam UU PDP melalui lembaga yang berwenang, termasuk memperkuat koordinasi antar institusi seperti Kepolisian Republik Indonesia, Badan Siber dan Sandi Negara (BSSN), dan Komisi Perlindungan Anak Indonesia (KPAI). Salah satu elemen penting dalam pelaksanaan UU ini adalah pembentukan Lembaga Otoritas Perlindungan Data Pribadi (LOPDP) yang telah dibentuk oleh pemerintah sebagai bentuk pertanggungjawaban pemerintah terhadap perlindungan data pribadi sebagaimana diatur dalam Pasal 58, yang memiliki fungsi regulatif, pengawasan, dan penegakan hukum terhadap pengelolaan data pribadi. LOPDP wajib bekerja secara independen, akuntabel, tidak tumpang

tindih dengan lembaga negara lainnya, dan mampu menjalin kerjasama internasional, guna menghadapi ancaman lintas batas.[19]

Tindak pidana phishing, sebagai bentuk penipuan daring yang bertujuan memperoleh data pribadi dengan cara melawan hukum, termasuk ke dalam pelanggaran terhadap ketentuan Pasal 67 UU PDP, dengan ancaman pidana penjara paling lama 5 tahun dan/atau denda paling banyak Rp5.000.000.000,00. Selain pidana, pelaku juga dapat dikenai sanksi administratif berupa teguran, peringatan tertulis, denda, pembekuan atau pencabutan izin usaha. Pencegahan kejahatan ini memerlukan sinergi antara pemerintah, pelaku usaha sektor digital seperti marketplace, e-commerce, dan jasa ekspedisi, serta media massa dalam mendidik masyarakat mengenai perlindungan data pribadi. UU PDP juga mewajibkan setiap badan usaha atau entitas yang mengumpulkan, memproses, dan menyimpan data pribadi untuk memenuhi standar perlindungan yang ditentukan. Dengan adanya perangkat hukum yang memadai, kolaborasi multisektor, dan sosialisasi berkelanjutan, keberadaan UU PDP diharapkan mampu menurunkan insiden phishing secara signifikan serta memperkuat sistem keamanan siber nasional yang adaptif terhadap ancaman digital di era transformasi teknologi.

KESIMPULAN

Phishing berbasis kecerdasan buatan (AI) merupakan bentuk kejahatan siber modern yang memanfaatkan teknologi seperti machine learning dan natural language processing untuk menciptakan serangan manipulatif yang sangat meyakinkan dan sulit dikenali, dengan cara menyamar sebagai institusi terpercaya guna memperoleh data pribadi korban. Sehingga phishing dapat dikatakan sebagai social engineering karena memiliki unsur memanipulasi korban. Kejahatan ini tidak hanya berdampak pada kerugian individu, tetapi juga mengancam keamanan nasional akibat lemahnya literasi digital masyarakat, keterbatasan penegak hukum dalam teknologi forensik digital, serta kekosongan norma hukum yang secara eksplisit mengatur phishing sebagai tindak pidana. Saat ini, pengaturan hukum Indonesia masih mengandalkan ketentuan umum dalam KUHP (Pasal 378), UU ITE (Pasal 28 ayat (1), Pasal 35 jo Pasal 51), dan UU PDP (Pasal 65–68), yang belum sepenuhnya mengakomodasi kompleksitas phishing berbasis AI. Oleh karena itu, dibutuhkan kebijakan hukum yang adaptif

[19] Ananta Fadli Sutarli and Shelly Kurniawan, "Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi Dalam Menanggulangi Phising Di Indonesia," *INNOVATIVE: Journal Of Social Science Research* 3, no. 2 (2023), https://doi.org/10.5040/9781635577068-0537.

melalui reformulasi Pasal 35 UU ITE agar secara tegas mengatur konsep phishing, penguatan peran Lembaga Otoritas Perlindungan Data Pribadi (LOPDP), serta sinergi antara pemerintah, sektor swasta, dan masyarakat untuk memperkuat literasi digital, mempercepat respon hukum, serta memperluas kerja sama internasional guna menjawab tantangan global kejahatan siber yang semakin kompleks dan lintas batas.

DAFTAR PUSTAKA

Ahmadian, Hendri, and Aulia Sabri. "Teknik Penyerangan Phishing Pada Social Engineering Menggunakan Set Dan Pencegahannya." *Djtechno: Jurnal Teknologi Informasi* 2, no. 1 (2021): 13–20. https://doi.org/10.46576/djtechno.v2i1.1251.

Anjheli, Devi. "Privasi Digital Dan Kejahatan Phishing Di Indonesia : Evaluasi Kritis Terhadap Efektivitas UU ITE Dan UU PDP." *STAATSRECHT: Jurnal Hukum Kenegaraan Dan Politik Islam Vol.* 4, no. 1 (2024).

Fadli Sutarli, Ananta, and Shelly Kurniawan. "Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi Dalam Menanggulangi Phising Di Indonesia." *INNOVATIVE: Journal Of Social Science Research* 3, no. 2 (2023). https://doi.org/10.5040/9781635577068-0537.

Febrika Ardy, Lutfi Aziz, Iklima Istiqomah, Angga Eben Ezer, and Shelvie Nidya Neyman. "Phishing Di Era Media Sosial: Identifikasi Dan Pencegahan Ancaman Di Platform Sosial." *Journal of Internet and Software Engineering* 1, no. 4 (2024): 11. https://doi.org/10.47134/pjise.v1i4.2753.

Gulo, Ardi Saputra, Sahuri Lasmadi, and Khabib Nawawi. "Cyber Crime Dalam Bentuk Phising Berdasarkan Undang-Undang Informasi Dan Transaksi Elektronik." *PAMPAS: Journal of Criminal Law* 1, no. 2 (2020): 68–81. https://doi.org/10.22437/pampas.v1i2.9574.

Hakim, Hary Abdul, Chrisna Bagus Edhita Praja, and Sung Ming-Hsi. "AI in Law: Urgency of the Implementation of Artificial Intelligence on Law Enforcement in Indonesia." *Jurnal Hukum Novelty* 14, no. 1 (2023): 122–34. https://doi.org/10.26555/novelty.v14i1.a25943.

Lokapala, Yazid Haikal, Fuad Januar Nurfauzi, and Yeni Widowaty. "Aspek Yuridis Kejahatan Phishing Dalam Ketentuan Hukum Di Indonesia." *Indonesian Journal of Criminal Law and Criminology (IJCLC)* 5, no. 1 (2024): 19–24. https://doi.org/https://doi.org/10.18196/ijclc.v5i1.19853.

Reyhan, Edlin. Gultom, Potler. "PERLINDUNGAN HUKUM TERHADAP PENGGUNA SOSIAL MEDIA TERKAIT CYBER CRIME PHISING BERDASARKAN UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 19 TAHUN 2016 TENTANG PERUBAHAN ATAS UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK Komputer Da." *Lex Laguens: Jurnal Kajian Hukum Dan Keadilan* 3, no. 1 (2025): 111–24.

Rosanti, Maria, Yusrodi, and Agatha Elisabet. "IMPLEMENTASI SISTEM KEAMANAN SIBER BERBASIS ARTIFICIAL INTELLIGENCE UNTUK MENGATASI

SERANGAN PHISHING." *Aisyah Journal of Informatics and Electrical Engineering* 7, no. 1 (2025).

Sahfitri, Afifah. Rosmalinda. "PENIPUAN DIGITAL MELALUI TAUTAN PHISHING." *Jurnal Dialektika Hukum* 6, no. 2 (2024): 92–107.

Saputra, Dewana, and Zaid Alfauza Marpaung. "Analisis Yuridis Penanggulangan Penyalahgunaan Data Pribadi Dalam Bentuk Phising Yang Dilakukan Oleh Paid Verified Account Di Media Sosial Menurut Undang-Undang Perlindungan Data Pribadi." *Uneslaw Review* 5, no. 4 (2023): 4764–75. https://doi.org/https://doi.org/10.31933/unesrev.v5i4.

Slamet. "Pertahanan Pencegahan Serangan Social Engineering Menggunakan Two Factor Authentication (2FA) Berbasis SMS (Short Message System)." *Jurnal Spirit* 14, no. 2 (2022): 23–29. https://doi.org/10.53567/spirit.v14i2.260.

Yurita, Irma, M Kevin Ramadhan, M Candra, and Universitas Muhammadiyah Kotabumi. "Pengaruh Kemajuan Teknologi Terhadap Perkembangan Tindak Pidana Cybercrime." *Jurnal Hukum Legalita* 5, no. 2 (2023): 144–55. https://jurnal.umko.ac.id/index.php/legalita/article/view/995.