JURNAL MEDIA AKADEMIK (JMA)
Vol.3, No.4 April 2025
e-ISSN: 3031-5220; DOI: 10.62281, Hal XX-XX
PT. Media Akademik Publisher
AHU-084213.AH.01.30.Tahun 2023

ANALISIS YURIDIS TERHADAP PENANGGULANGAN KEJAHATAN SIBER PHISHING DI INDONESIA

Oleh:

Immanuel Wurangian[1]
Steven Sanjaya Putra[2]
Leslie Glori Julio Mandibondibo[3]
Shera Aurelia Kusoy[4]
Nanda Natazia Lenggu[5]

Universitas Pelita Harapan Kampus Surabaya
Alamat: JL. Raya Kedung Baruk No.26-28, Kedung Baruk, Kec. Rungkut, Surabaya, Jawa Timur (60298).
Korespondensi Penulis: 02051230017@student.uph.edu, 02051230018@student.uph.edu, 02051230030@student.uph.edu, 02051230041@student.uph.edu, 02051230039@student.uph.edu.

Abstract. *Phishing is one of the fastest-growing forms of cybercrime, coinciding with the rapid advancement of information technology. In Indonesia, several legal instruments have been established to address phishing crimes, including the Electronic Information and Transactions Law (ITE Law), the Criminal Code (KUHP), and regulations governing electronic commerce systems. This research employs a normative juridical approach to assess the effectiveness of these regulations in combating phishing activities. Legislative analysis and case studies reveal that although Indonesia possesses a relatively comprehensive legal framework, its implementation encounters several barriers. These include low levels of digital literacy among the public, limited law enforcement capacity, and the ever-evolving techniques used by cybercriminals. The study highlights the urgent need for regulatory updates that can keep pace with technological developments, alongside efforts to increase public awareness and education on cybersecurity. Furthermore, enhancing cooperation among law enforcement agencies and cybersecurity*

Received April 15, 2025; Revised April 24, 2025; April 30, 2025
*Corresponding author: 02051230017@student.uph.edu

stakeholders is essential to improve the overall effectiveness of phishing countermeasures in Indonesia.

Keywords: *Cybercrime, Phishing, Regulation, Indonesian Law, Countermeasures.*

Abstrak. Phishing merupakan salah satu bentuk kejahatan siber yang berkembang pesat seiring dengan kemajuan teknologi informasi. Di Indonesia, berbagai instrumen hukum telah dibentuk untuk mengatasi kejahatan phishing, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Kitab Undang-Undang Hukum Pidana (KUHP), serta regulasi terkait sistem perdagangan elektronik. Penelitian ini menggunakan pendekatan yuridis normatif untuk menilai efektivitas regulasi dalam menanggulangi kejahatan phishing. Berdasarkan analisis peraturan perundang-undangan dan studi kasus, ditemukan bahwa meskipun Indonesia memiliki kerangka hukum yang cukup komprehensif, pelaksanaan dan penegakannya menghadapi berbagai hambatan. Tantangan tersebut mencakup rendahnya literasi digital masyarakat, keterbatasan sumber daya penegak hukum, serta cepatnya perkembangan modus operandi pelaku phishing. Penelitian ini menekankan perlunya pembaruan regulasi yang lebih adaptif terhadap perkembangan teknologi, serta peningkatan edukasi masyarakat tentang keamanan siber. Selain itu, penguatan kerja sama antar lembaga penegak hukum dan pemangku kepentingan keamanan siber sangat penting guna meningkatkan efektivitas penanggulangan phishing di Indonesia.

Kata Kunci: Kejahatan Siber, Phishing, Regulasi, Hukum Indonesia, Penanggulangan.

LATAR BELAKANG

Dalam arus deras transformasi era digital, berbagai sektor kehidupan mulai dari ekonomi, pendidikan, hingga pelayanan publik mengalami perubahan fundamental. Ketersediaan akses internet yang luas dan eksploitasi teknologi informasi telah membuka gerbang inovasi dan pertumbuhan. Akan tetapi, di balik peluang tersebut tersembunyi tantangan serius berupa eskalasi tindak kejahatan siber. Salah satu bentuk ancaman yang menonjol adalah phishing. Phishing adalah praktik penipuan di ranah maya yang bertujuan membajak informasi sensitif korban dengan berpura-pura sebagai entitas resmi dan tepercaya. Metodenya kini berkembang pesat, meliputi penyebaran email tipuan, pembuatan situs palsu, hingga manipulasi psikologis melalui media sosial (rekayasa

sosial). Kerugian yang diakibatkan tidak hanya bersifat finansial, tetapi juga menggerus kepercayaan publik terhadap keamanan dunia digital.

Dengan populasi pengguna internet yang luar biasa besar, Indonesia menjadi ladang empuk bagi pelaku phishing. Berbagai laporan mencatat lonjakan kasus phishing tiap tahunnya, mengincar baik individu maupun institusi negara serta korporasi. Fenomena ini menuntut bukan hanya kehadiran regulasi yang kokoh di atas kertas, melainkan juga penerapan yang efektif di lapangan untuk menjaga masyarakat dari serangan siber. Pemerintah Indonesia telah mengantisipasi tantangan ini melalui produk hukum seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta revisinya dalam Undang-Undang Nomor 19 Tahun 2016, Kitab Undang-Undang Hukum Pidana (KUHP), serta regulasi teknis terkait transaksi elektronik dan proteksi data pribadi. Aturan-aturan tersebut menjadi landasan hukum untuk menjerat pelaku phishing dan memitigasi kerugian korban. Namun, di tataran praktis, berbagai hambatan membayangi efektivitas penegakan hukum terhadap kejahatan phishing. Rendahnya literasi digital masyarakat memperbesar peluang kejahatan ini, sementara kapasitas penegak hukum dalam memahami dinamika kejahatan berbasis teknologi juga masih membutuhkan penguatan. Ditambah lagi, strategi pelaku phishing yang terus berevolusi seringkali menyalip kemampuan adaptasi regulasi yang cenderung statis.

Realitas ini mencerminkan adanya celah antara idealisme hukum (*das Sollen*) dan kenyataan implementasi di masyarakat (*das Sein*). Oleh karena itu, diperlukan langkah-langkah konkret berupa penyempurnaan regulasi yang lebih adaptif, peningkatan kesadaran digital masyarakat, dan kolaborasi multisektor dalam melawan kejahatan siber. Dengan pendekatan yuridis normatif, penelitian ini berupaya mengevaluasi efektivitas kerangka hukum yang ada dalam memberantas phishing di Indonesia, mengidentifikasi kendala-kendala dalam aplikasinya, serta merumuskan rekomendasi strategis untuk memperkuat perlindungan hukum bagi pengguna internet. Harapannya, hasil penelitian ini dapat memperkaya upaya penguatan sistem hukum nasional di tengah dinamika era digital yang kian kompleks.

KAJIAN TEORITIS

Teori Perlindungan Hukum

Kejahatan siber merupakan bentuk tindak pidana yang memanfaatkan teknologi informasi untuk memperoleh data seperti informasi akun perbankan atau identitas pribadi secara ilegal dengan cara menyamar sebagai pihak terpercaya. Dalam konteks ini, kejahatan phishing diatur melalui berbagai instrumen hukum, antara lain Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) beserta perubahannya, yang mengatur larangan penyebaran informasi palsu serta manipulasi data elektronik, serta pasal-pasal terkait dalam Kitab Undang-Undang Hukum Pidana (KUHP) mengenai penipuan. Upaya penanggulangan phishing meliputi tindakan preventif seperti edukasi keamanan siber kepada masyarakat, penggunaan teknologi proteksi data, hingga tindakan represif berupa penegakan hukum terhadap pelaku kejahatan. Namun demikian, karakteristik phishing yang bersifat lintas negara, kesulitan dalam pembuktian digital, dan rendahnya literasi digital masyarakat menjadi tantangan serius dalam upaya pemberantasan kejahatan ini.

METODE PENELITIAN

Penelitian ini menggunakan metode yuridis normatif di mana analisis difokuskan pada studi terhadap norma hukum positif yang berlaku, seperti Undang-Undang ITE, KUHP, dan regulasi terkait perlindungan data pribadi dalam konteks kejahatan phishing. Data diperoleh melalui studi kepustakaan, dengan bahan hukum primer berupa peraturan perundang-undangan, bahan hukum sekunder berupa literatur ilmiah, serta bahan hukum tersier seperti kamus dan ensiklopedia hukum. Teknik analisis yang digunakan adalah analisis kualitatif, yaitu dengan menginterpretasikan ketentuan hukum untuk menggambarkan secara sistematis bagaimana regulasi di Indonesia mengatur dan menanggulangi kejahatan phishing serta menilai efektivitas penerapannya di praktik.

HASIL DAN PEMBAHASAN

Analisis Yuridis Terhadap Penanggulangan Kejahatan Siber Phishing di Indonesia

Era digital yang semakin berkembang pesat memunculkan berbagai peluang, namun juga membawa beragam ancaman baru, salah satunya adalah kejahatan siber seperti phishing. Kejahatan phishing adalah tindakan penipuan yang dilakukan dengan tujuan memperoleh informasi pribadi korban, seperti nomor kartu kredit, akun perbankan, atau data sensitif lainnya, dengan cara yang tidak sah dan manipulatif. Teknik yang

digunakan oleh pelaku sering kali sangat canggih, di mana mereka berpura-pura menjadi entitas yang dapat dipercaya, seperti bank, perusahaan besar, atau lembaga pemerintah, untuk mengelabui korban agar memberikan data pribadi mereka melalui email, pesan teks, atau tautan yang tampaknya sah. Phishing merupakan salah satu bentuk kejahatan siber yang sangat merugikan baik secara finansial maupun emosional bagi korban. Di Indonesia, dengan jumlah pengguna internet yang terus meningkat, ancaman ini semakin nyata. Berdasarkan data terbaru, jumlah pengguna internet di Indonesia mencapai 185,3 juta orang pada tahun 2024, dan hampir setengah dari jumlah tersebut aktif menggunakan media sosial. Seiring dengan pertumbuhan pesat penggunaan internet, praktik kejahatan siber juga mengalami peningkatan, dan phishing menjadi salah satu ancaman terbesar yang harus dihadapi oleh pengguna internet di Indonesia. Kejahatan ini tidak hanya menyerang individu dewasa, namun juga dapat menimpa anak-anak dan remaja yang rentan terhadap tipu daya di dunia maya. Salah satu alasan mengapa phishing menjadi masalah yang semakin kompleks adalah cara pelaku beroperasi. Kejahatan ini sering kali dilakukan dengan teknik yang sangat sulit untuk dideteksi oleh korban. Pelaku phishing menggunakan berbagai metode untuk menciptakan pesan atau situs web yang sangat mirip dengan yang asli, sehingga korban merasa aman ketika diminta untuk memasukkan informasi pribadi mereka. Hal ini menjadi lebih berbahaya ketika pelaku menggunakan identitas palsu atau berpura-pura menjadi seseorang yang sudah dikenal korban. Misalnya, pelaku dapat mengirimkan email yang terlihat seolah-olah berasal dari bank atau perusahaan yang sudah sering dihubungi korban. Jika korban tidak memiliki kewaspadaan yang cukup, mereka dapat dengan mudah terjebak dalam jebakan phishing ini. Dari segi hukum, kejahatan phishing di Indonesia diatur oleh sejumlah peraturan perundang-undangan yang memberikan dasar hukum untuk menanggulangi kejahatan siber tersebut. Salah satu dasar hukum yang paling utama adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Undang-Undang ini mengatur berbagai jenis kejahatan siber, termasuk phishing, dan memberikan dasar hukum untuk menghukum pelaku yang melakukan tindak pidana ini. Pasal 26 UU ITE misalnya, mengatur bahwa setiap orang yang dengan sengaja dan tanpa hak mengakses informasi elektronik yang dikuasai oleh orang lain dapat dikenakan sanksi pidana. Namun meskipun UU ITE memberikan landasan hukum untuk menanggulangi phishing,

kenyataannya praktik penegakan hukum terhadap kejahatan siber, khususnya phishing, belum sepenuhnya efektif.

Phishing sering kali dilakukan dengan cara yang sangat canggih dan sulit dideteksi, apalagi dengan adanya perkembangan teknologi yang memungkinkan pelaku untuk beroperasi tanpa terdeteksi. Banyak pelaku phishing yang menggunakan perangkat lunak atau alat-alat tertentu, seperti VPN (*Virtual Private Network*) dan proxy, untuk menyembunyikan lokasi mereka dan menyamarkan identitas mereka. Hal ini menyulitkan aparat penegak hukum dalam melacak dan menangkap pelaku. Selain itu, banyak pelaku phishing yang beroperasi di luar negeri, yang menambah kerumitan dalam penegakan hukum. Oleh karena itu, selain adanya dasar hukum yang kuat, diperlukan juga upaya yang lebih intensif dalam hal penegakan hukum terhadap pelaku phishing. Di Indonesia, meskipun terdapat sejumlah aturan yang mengatur tentang kejahatan siber, implementasi dan penegakan hukum terhadap kasus phishing masih menghadapi sejumlah kendala. Salah satunya adalah kurangnya pemahaman yang mendalam tentang kejahatan siber, baik di kalangan aparat penegak hukum maupun di masyarakat umum. Banyak aparat penegak hukum yang belum memiliki keterampilan yang memadai untuk menangani kasus kejahatan siber secara efektif. Ini menjadi salah satu faktor yang memperburuk situasi, karena tanpa pemahaman yang memadai, aparat tidak dapat menanggapi kasus phishing dengan cepat dan tepat. Dalam banyak kasus, bahkan ketika korban melapor, penyelidikan yang dilakukan tidak cukup menyeluruh untuk menemukan pelaku dan memberikan sanksi yang pantas.Selain itu, masalah lain yang dihadapi adalah kurangnya kesadaran masyarakat mengenai bahaya phishing. Banyak orang yang belum tahu bagaimana cara mengenali tanda-tanda phishing atau bagaimana cara melaporkan kejadian tersebut. Hal ini terutama berlaku untuk masyarakat yang tidak memiliki latar belakang pendidikan di bidang teknologi informasi atau keamanan siber. Banyak korban yang merasa bingung atau bahkan enggan untuk melapor karena mereka tidak tahu kepada siapa mereka harus mengadukan kasus tersebut. Beberapa dari mereka bahkan merasa bahwa proses hukum yang panjang dan rumit tidak sebanding dengan kerugian yang mereka alami, yang akhirnya membuat mereka memilih untuk diam. Padahal, dampak yang ditimbulkan oleh phishing bisa sangat besar, baik dalam hal kerugian finansial maupun dampak psikologis. Sebagai upaya untuk menanggulangi kejahatan phishing dengan lebih efektif, pendidikan dan peningkatan literasi digital di kalangan

masyarakat sangat penting. Pemerintah, lembaga pendidikan, dan organisasi non-pemerintah perlu bekerja sama untuk memberikan edukasi mengenai bahaya phishing dan bagaimana cara melindungi diri dari serangan siber ini. Salah satu langkah penting dalam upaya ini adalah meningkatkan kesadaran masyarakat tentang pentingnya menjaga informasi pribadi mereka, serta cara mengenali tanda-tanda phishing, seperti email atau pesan yang mencurigakan yang meminta data pribadi. Dengan pengetahuan yang cukup, masyarakat akan lebih mudah untuk mengidentifikasi potensi ancaman phishing dan mengambil langkah pencegahan yang tepat. Di sisi lain, aparat penegak hukum juga perlu diberikan pelatihan khusus mengenai kejahatan siber dan bagaimana cara menangani kasus phishing secara efektif. Pelatihan ini harus mencakup aspek teknis dalam penyelidikan kejahatan digital, serta pemahaman yang lebih mendalam mengenai peraturan-peraturan yang ada. Hal ini penting agar mereka dapat menangani kasus phishing dengan lebih profesional dan efisien. Selain itu, pemerintah juga perlu meningkatkan kapasitas sumber daya manusia di bidang teknologi informasi dan keamanan siber, sehingga aparat penegak hukum dapat lebih siap dalam menghadapi tantangan kejahatan digital. Di tingkat internasional, kerja sama antarnegara juga sangat penting dalam mengatasi kejahatan phishing. Mengingat banyaknya pelaku phishing yang beroperasi lintas negara, kerja sama internasional antara lembaga penegak hukum di berbagai negara akan mempercepat proses penyelidikan dan penuntutan. Negara-negara di dunia, termasuk Indonesia, perlu memperkuat jaringan kerja sama internasional di bidang kejahatan siber untuk mengatasi masalah ini dengan lebih efektif. Beberapa langkah yang bisa dilakukan antara lain adalah memperkuat mekanisme pelaporan internasional, pertukaran informasi intelijen, dan penegakan hukum secara lintas negara. Selain itu, pemerintah Indonesia juga perlu memperkuat regulasi mengenai kejahatan siber, khususnya phishing, dengan mengadaptasi peraturan yang lebih relevan dengan perkembangan teknologi. Hal ini termasuk memperbarui UU ITE untuk memasukkan ketentuan yang lebih spesifik mengenai penanggulangan phishing. Peraturan yang lebih jelas dan komprehensif akan mempermudah aparat penegak hukum dalam menangani kasus phishing dan memberikan kejelasan bagi korban tentang hak-hak mereka.

Selain UU ITE, Kitab Undang-Undang Hukum Pidana (KUHP) juga mengatur tentang tindakan pidana yang berkaitan dengan kejahatan siber, termasuk phishing. Dalam Pasal 310 KUHP, misalnya, diatur tentang pencemaran nama baik, yang juga

dapat dijadikan dasar untuk menuntut pelaku phishing yang melakukan fitnah atau penghinaan melalui media elektronik. Namun, meskipun KUHP memberikan dasar hukum, pelaksanaannya dalam kasus phishing masih terbatas. Oleh karena itu, perlu ada penyesuaian dalam peraturan-peraturan tersebut agar dapat memberikan perlindungan yang lebih baik terhadap korban phishing. Dengan langkah-langkah yang lebih terkoordinasi dan peningkatan pemahaman di semua lapisan masyarakat serta aparat penegak hukum, diharapkan kejahatan phishing dapat ditekan dan korban dapat memperoleh perlindungan yang memadai. Masyarakat yang teredukasi dan aparat yang lebih terlatih akan dapat menciptakan ruang digital yang lebih aman bagi semua orang, terutama anak-anak dan remaja yang sering kali menjadi sasaran utama dalam kejahatan siber. Upaya ini akan menciptakan sistem perlindungan yang tidak hanya reaktif, tetapi juga proaktif dalam menjaga keamanan informasi pribadi masyarakat di dunia maya.

KESIMPULAN DAN SARAN

Kesimpulan

Phishing merupakan salah satu bentuk kejahatan siber yang berkembang sangat pesat seiring meningkatnya penggunaan teknologi informasi di Indonesia. Dalam praktiknya penanggulangan kejahatan phishing masih menghadapi tantangan yang signifikan. Rendahnya tingkat literasi digital masyarakat menyebabkan banyak individu menjadi korban phishing tanpa memahami risiko yang mereka hadapi. Selain itu, keterbatasan sumber daya manusia dalam penegak hukum, baik dari sisi jumlah maupun kompetensi teknis, menghambat upaya penyelidikan dan penuntutan terhadap pelaku phishing. Penegakan hukum yang baik membutuhkan kerangka hukum yang kuat dan perubahan regulasi untuk menyesuaikan diri dengan perkembangan teknologi serta penguatan kapasitas lembaga penegak hukum. Kejahatan phishing akan terus berkembang dan berpotensi merugikan semakin banyak orang, baik dari segi finansial maupun keamanan data pribadi, jika tidak ada upaya kolektif dari sektor pemerintah, swasta, lembaga pendidikan, dan masyarakat umum. Oleh karena itu, untuk meningkatkan perlindungan hukum dan ketahanan siber Indonesia, diperlukan rencana nasional yang lebih komprehensif dan terintegrasi.

Tantangan utama yang dihadapi adalah bagaimana mempercepat proses adaptasi regulasi seiring laju inovasi teknologi yang sangat dinamis. Hukum positif di Indonesia

harus mampu bertransformasi untuk mengantisipasi metode-metode baru yang digunakan pelaku kejahatan siber. Selain memperbarui substansi hukum, perlu juga diperhatikan efektivitas implementasi di lapangan melalui penyederhanaan prosedur pelaporan, peningkatan respons aparat penegak hukum, serta optimalisasi penggunaan teknologi digital dalam proses penyelidikan. Selain itu, kesadaran masyarakat tentang pentingnya perlindungan data pribadi harus menjadi prioritas utama dalam program-program edukasi nasional. Peningkatan literasi digital akan memperkuat ketahanan individu terhadap berbagai bentuk serangan phishing yang semakin canggih. Tanpa dukungan masyarakat yang sadar dan waspada, upaya hukum formal akan sulit membendung pertumbuhan kejahatan ini. Dengan kolaborasi antara pemerintah, sektor swasta, dunia pendidikan, dan masyarakat umum, diharapkan dapat tercipta sebuah ekosistem digital yang aman, adaptif, dan tahan terhadap berbagai ancaman kejahatan siber di masa depan.

Namun demikian, penting untuk disadari bahwa regulasi yang ada saat ini, seperti UU ITE dan KUHP, meskipun memberikan dasar hukum umum, belum secara spesifik mengatur tindak pidana phishing secara terpisah dan mendetail. Dengan semakin kompleks dan variatifnya teknik phishing modern, diperlukan pembentukan atau revisi undang-undang baru yang secara eksplisit mengatur tentang kejahatan phishing, termasuk definisi, jenis-jenis modus phishing, mekanisme pelaporan cepat, bentuk perlindungan bagi korban, serta ancaman pidana yang lebih jelas dan terukur. Regulasi yang spesifik tersebut menjadi kebutuhan mendesak agar proses penegakan hukum lebih efektif, pelaku dapat dihukum dengan adil, dan korban memperoleh perlindungan maksimal. Pemerintah Indonesia diharapkan segera merancang instrumen hukum baru yang komprehensif tentang kejahatan phishing, atau setidaknya melakukan amandemen pada UU ITE agar lebih responsif terhadap tantangan ini. Hukum yang spesifik tidak hanya akan memberikan kepastian hukum, tetapi juga menjadi instrumen preventif yang kuat untuk menekan laju kejahatan phishing di masa depan. Dengan demikian, penguatan aspek regulatif yang sejalan dengan penguatan edukasi, teknologi, dan kerja sama internasional menjadi pilar utama dalam menciptakan ruang digital yang aman, produktif, dan terpercaya di Indonesia.

Mengingat kompleksitas dan kecepatan perkembangan kejahatan phishing Pemerintah perlu terus mendorong inovasi di bidang keamanan siber dan meningkatkan investasi di sektor ini. Dunia pendidikan pun memiliki peran strategis dalam membekali

generasi muda dengan keterampilan dan pengetahuan tentang ancaman siber. Kampanye nasional tentang keamanan data, seminar rutin tentang literasi digital, serta simulasi penanganan insiden siber harus lebih sering dilakukan. Dengan demikian, ketahanan nasional di bidang siber dapat terbangun dari akar rumput hingga ke tingkat strategis nasional. Jika seluruh elemen bangsa berkomitmen memperkuat perlindungan terhadap kejahatan phishing, Indonesia akan lebih siap menghadapi era digital dengan lebih aman, cerdas, dan berdaya saing tinggi.

Saran

Berdasarkan berbagai paparan dan analisis di atas, dapat disimpulkan bahwa kejahatan phising merupakan ancaman serius dalam dunia siber yang memerlukan penanganan lebih komprehensif, adaptif, dan sistematis. Meskipun Indonesia telah memiliki berbagai landasan hukum seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Kitab Undang-Undang Hukum Pidana (KUHP), kenyataan di lapangan menunjukkan bahwa regulasi yang ada belum sepenuhnya mampu menjawab tantangan phishing modern yang terus berkembang. Pemerintah perlu memperbaharui UU ITE agar lebih adaptif terhadap modus phishing modern, meningkatkan literasi digital masyarakat, memperkuat kapasitas aparat penegak hukum, dan mempererat kerja sama internasional untuk menghadapi phishing yang bersifat lintas negara. Kompleksitas modus operandi para pelaku, rendahnya literasi digital masyarakat, keterbatasan kapasitas penegakan hukum, serta kurangnya regulasi yang secara spesifik mengatur phishing, menjadi hambatan utama dalam upaya pemberantasan kejahatan ini. Fenomena ini menuntut adanya langkah-langkah strategis yang tidak hanya berfokus pada aspek hukum, tetapi juga menyentuh aspek sosial, edukasi, teknologi, dan kerja sama internasional. Regulasi yang lebih rinci dan spesifik mengenai phishing sangat diperlukan untuk menciptakan kepastian hukum dan memperjelas mekanisme perlindungan terhadap korban. Selain itu, pemberdayaan masyarakat melalui pendidikan literasi digital dan peningkatan kapasitas aparat penegak hukum juga harus menjadi prioritas nasional.

Oleh karena itu, dalam bagian saran ini, Diharapkan dapat memperkuat upaya pencegahan, penanganan, dan penanggulangan kejahatan phishing di Indonesia. Saran-saran ini disusun dengan mempertimbangkan kebutuhan akan regulasi yang lebih adaptif, pentingnya peningkatan edukasi publik, perlunya pelatihan teknis bagi aparat penegak

hukum, serta dorongan untuk memperkuat kerja sama lintas sektor dan internasional. Dengan implementasi saran-saran ini, diharapkan Indonesia mampu menghadapi ancaman phishing secara lebih efektif, membangun ruang digital yang lebih aman, dan menjaga kepercayaan publik terhadap sistem teknologi informasi nasional.

DAFTAR REFERENSI

Undang-Undang

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik(UUITE)https://peraturan.bpk.go.id/details/37589/uu-no-11-tahun-200

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) https://peraturan.bpk.go.id/Details/37582/uu-no-19-tahun-2016

Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak. Pidana Pencucian Uang (UU PTPPU) https://peraturan.bpk.go.id/Details/38547/uu-no-8-tahun-2010

Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi https://peraturan.bpk.go.id/Details/45357/uu-no-36-tahun-1999

Undang-Undang Nomor 1 Tahun 2008 tentang Penyebaran Informasi Melalui Teknologi https://peraturan.bpk.go.id/Download/26683/UU%20Nomor%2011%20Tahun%202008.pdf

Jurnal

Adnan, A. J., Putriyana, D., Wibowo, H. A., & Ramada, S. (2024). Perlindungan Hukum terhadap Anak Sebagai Korban Tindak Pidana Cyberbullying. Indonesian Journal of Criminal Law and Criminology (IJCLC), 5(1), 25–33. https://doi.org/10.18196/ijclc.v5i1.20935

Burhanuddin, A. H., Suryanto, S., Alqadri, A. R., & Novianti, L. (2024). Pengalaman Pengungkapan Diri Di Akun Kedua Instagram. Psyche: Jurnal Psikologi, 6(2), 252–270. https://doi.org/10.36269/psyche.v6i2.2579

Rachmayanti, A., & Candrasari, Y. (2022). Perilaku Cyberbullying Di Instagram . Linimasa: Jurnal Ilmu Komunikasi, 5(1), 1–12. https://doi.org/10.23969/linimasa.v5i1.4291

Kementerian Komunikasi dan Informatika Republik Indonesia. (2023). Survei Penetrasi Internet Indonesia 2023. Diakses dari: https://kominfo.go.id/

Komisi Perlindungan Anak Indonesia (KPAI). (2023). Laporan Tahunan KPAI 2023. Diakses dari: https://www.kpai.go.id/

The Conversation Indonesia. (2023). Tiap Hari Polisi Terima 25 Laporan Perundungan Siber. Diakses dari: https://theconversation.com/

Artikel

Mengatasi Ancaman Phishing di Era Digital: Tantangan dan Upaya di Indonesia
https://kbr.id/berita/ragam/mengatasi-ancaman-phishing-di-era-digital-tantangan-d. an-upaya-di-indonesia

Sinergi antara UU ITE dan Kebijakan Keamanan Digital https://ulilalbabinstitute.id/index.php/PESHUM/article/view/8311/6317

Aspek Yuridis Kejahatan Phishing dalam Ketentuan Hukum di Indonesia, Indonesian Journal of Criminal Law and Criminology, diakses dari https://journal.umy.ac.id/index.php/ijclc/article/download/19853/9270

Kajian Sosiologi Kriminal terhadap Penanggulangan Kejahatan Cyber Phishing, Jurnal Darussalam, diakses dari https://ejournal.stisdarussalam.ac.id/index.php/jd/article/download/4/3 .

Muhammad Bagas Putra, "Analisis Yuridis Tindak Pidana Cyber Crime Phishing di Bidang Perbankan dalam Perspektif Peraturan Perundang-Undangan di Indonesia," Skripsi, Universitas Jambi, 2023, diakses dari https://repository.unja.ac.id/72416/