Konstitusi: Jurnal Hukum, Administrasi Publik, dan Ilmu Komunikasi
Volume. 2, Nomor. 3 Juli 2025
e-ISSN: 3063-4040; p-ISSN: 3063-3877, Hal 291-305
DOI: https://doi.org/10.62383/konstitusi.v2i3.908
*Available Online at:*https://ejournal.appihi.or.id/index.php/Konstitusi

Sanksi Pidana terhadap Kejahatan Pishing Menurut Hukum Pidana Indonesia

Putri Ramadhani Rangkuti [1*], Muhammad Aldi Khoiri [2], Sumantri Ritonga [3], Putri Nabila Sitorus Pane [4]
[1-4] Universitas Islam Negeri Sumatera Utara, Indonesia
Email : putrihamdani007@gmail.com [1], muhammadaldikhoiri@gmail.com [2], mantriritonga03@gmail.com [3], nabilanabila4@icloud.com [4]*

Abstract : *This study uses a qualitative method to examine the criminal sanctions against phishing crimes under Indonesian criminal law. Phishing is a form of cybercrime committed by deceiving victims into disclosing personal or confidential information such as identity data, bank accounts, or other sensitive details. In Indonesian criminal law, phishing is not explicitly mentioned, but it can be prosecuted under several articles of the Electronic Information and Transactions Law (Law No. 19 of 2016), particularly Articles 35 and 36, which regulate manipulative acts that cause harm to others. Offenders may face imprisonment of up to 12 years and/or fines of up to 12 billion rupiah. Additionally, offenders may be charged under the Indonesian Penal Code (KUHP) if their actions meet the elements of fraud or data theft. This study highlights the need for legal reform to be more responsive to the rapid advancement of digital technology. More specific regulations are needed to ensure legal certainty and provide adequate protection for victims of phishing crimes in Indonesia.*

Keywords: *criminal sanctions, Cybercrime, data protection, EIT Law, phishing*

Abstrak : Penelitian ini menggunakan metode kualitatif untuk mengkaji sanksi pidana terhadap kejahatan phishing dalam perspektif hukum pidana di Indonesia. Phishing merupakan bentuk kejahatan siber yang dilakukan dengan cara menipu korban agar menyerahkan data pribadi atau informasi penting seperti identitas, akun bank, maupun data rahasia lainnya. Dalam konteks hukum pidana Indonesia, kejahatan ini belum memiliki pengaturan yang secara eksplisit menyebutkan istilah "phishing", namun dapat dijerat melalui beberapa pasal dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) Nomor 19 Tahun 2016, khususnya Pasal 35 dan 36, yang mengatur perbuatan manipulatif yang menimbulkan kerugian terhadap orang lain. Pelaku dapat dikenai pidana penjara maksimal 12 tahun dan/atau denda hingga Rp12 miliar. Di samping itu, pelaku juga dapat dijerat dengan Kitab Undang-Undang Hukum Pidana (KUHP) jika tindakannya memenuhi unsur penipuan atau pencurian data. Penelitian ini menekankan pentingnya pembaruan hukum agar lebih responsif terhadap perkembangan teknologi digital yang cepat. Regulasi yang lebih spesifik diperlukan untuk menjamin kepastian hukum dan perlindungan korban kejahatan phishing di Indonesia.

Kata Kunci: Kejahatan siber, perlindungan data, phishing, sanksi pidana, UU ITE

1. PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah membawa dampak positif dalam berbagai bidang kehidupan manusia, seperti pendidikan, ekonomi, pemerintahan, hingga layanan kesehatan. Namun, seiring dengan manfaatnya, teknologi juga memunculkan tantangan baru dalam bentuk kejahatan siber yang semakin kompleks. Salah satu bentuk kejahatan yang cukup meresahkan masyarakat digital adalah phishing, yakni penipuan berbasis elektronik yang bertujuan mendapatkan data pribadi korban. Kejahatan ini sering kali dilakukan melalui email, situs palsu, hingga aplikasi yang dirancang menyerupai layanan resmi. Phishing tidak hanya berdampak pada kerugian ekonomi, tetapi juga pada hilangnya kepercayaan publik terhadap sistem digital. Fenomena ini menuntut adanya respons yang

Received: Mei 31, 2025; Revised: Juni 12, 2025; Accepted: Juni 26, 2025; Online Available: Juni 28, 2025

cepat dan tegas dari sistem hukum, terutama hukum pidana yang berfungsi sebagai ultimum remedium. Oleh karena itu, pemahaman yang komprehensif mengenai pengaturan phishing dalam sistem hukum pidana Indonesia menjadi sangat penting untuk dikaji dan dianalisis secara mendalam. (Ramadhan & Widodo, 2020)

Kejahatan phishing berkembang seiring dengan kemampuan pelaku dalam mengeksploitasi kelemahan sistem dan kelengahan manusia (human error). Pelaku phishing menggunakan metode rekayasa sosial (social engineering) yang sangat efektif dalam mengelabui korban. Mereka menciptakan tampilan yang meyakinkan seolah-olah berasal dari lembaga resmi, seperti bank, e-commerce, atau institusi pemerintahan. Sasaran mereka tidak terbatas pada individu, tetapi juga institusi bisnis dan negara. Di Indonesia, kasus phishing menunjukkan peningkatan signifikan terutama sejak meningkatnya aktivitas digital pasca pandemi COVID-19. Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK) serta BSSN (Badan Siber dan Sandi Negara) telah mencatat tren ancaman siber ini sebagai kategori risiko tinggi. Namun demikian, regulasi yang mengatur kejahatan phishing masih belum bersifat spesifik dan sering kali tumpang tindih dengan tindak pidana siber lainnya. Situasi ini menciptakan celah hukum yang menguntungkan pelaku. Untuk itu, analisis terhadap kerangka hukum pidana terkait phishing menjadi sangat penting dilakukan. (Anugerah & Suryani, 2021)

Indonesia telah memiliki beberapa peraturan yang dapat dijadikan dasar dalam menjerat pelaku kejahatan phishing, terutama melalui Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Pasal-pasal yang sering digunakan dalam menjerat pelaku phishing antara lain Pasal 28 ayat (1) tentang penyebaran informasi menyesatkan dan Pasal 35 tentang manipulasi data elektronik. Meskipun begitu, tidak ada satu pun pasal dalam UU ITE yang secara eksplisit menyebut istilah phishing, sehingga penegakan hukum sering kali mengalami hambatan dalam pembuktian dan pemidanaan. Aparat penegak hukum perlu menafsirkan norma secara luas atau melalui pendekatan analogi, yang dalam konteks hukum pidana sering kali menjadi perdebatan karena bertentangan dengan asas legalitas. Ketidaktegasan ini berpotensi melemahkan posisi korban dalam menuntut keadilan dan mempersulit upaya preventif. Maka dari itu, kajian ini penting untuk melihat apakah norma yang ada cukup memberikan kepastian hukum. (Fitriani & Nugroho, 2022)

Selain UU ITE, Kitab Undang-Undang Hukum Pidana (KUHP) juga digunakan untuk menjerat pelaku phishing, khususnya dengan pasal-pasal tentang penipuan dan pencurian. Pasal 378 KUHP tentang penipuan dan Pasal 362 KUHP tentang pencurian dapat diterapkan jika phishing dianggap sebagai tindakan mengambil keuntungan secara melawan hukum dari

korban. Namun, penerapan pasal ini menghadapi kendala dalam membuktikan elemen materiil dan formil perbuatan pidana, mengingat modus phishing dilakukan secara daring dan sering kali lintas negara. Selain itu, banyak korban yang tidak melaporkan kejadian karena malu atau merasa tidak akan mendapatkan penyelesaian yang adil. Hal ini membuat kejahatan phishing menjadi "low-risk high-return" bagi pelakunya. Dalam sistem hukum pidana Indonesia, pendekatan yang komprehensif masih diperlukan agar kejahatan digital ini bisa diberantas secara efektif, tidak hanya dari sisi normatif, tetapi juga dari sisi kelembagaan dan teknis penegakan hukum. (Wijaya & Lestari, 2019)

Karakteristik kejahatan phishing yang bersifat transnasional menimbulkan tantangan tersendiri bagi penegakan hukum nasional. Kerja sama internasional menjadi kunci dalam penanganan kasus-kasus phishing lintas negara, baik dari segi pelacakan, pembuktian, hingga penindakan. Indonesia telah menjadi anggota dari beberapa konvensi dan forum internasional yang membahas kejahatan siber, seperti ASEAN Cybersecurity Cooperation dan INTERPOL. Namun, efektivitas kerja sama ini belum optimal karena belum adanya harmonisasi hukum yang jelas antar negara. Oleh karena itu, regulasi nasional harus mampu menyesuaikan diri dengan standar internasional dan mengadopsi prinsip-prinsip hukum pidana modern yang adaptif terhadap teknologi. Penguatan regulasi, kapasitas penegak hukum, dan sistem pelaporan publik menjadi kunci dalam menanggulangi phishing secara sistemik. Tanpa itu, kejahatan phishing akan terus berkembang, bahkan bisa menjadi alat dalam kejahatan yang lebih besar seperti pencucian uang atau pendanaan terorisme. (Santoso & Hidayat, 2023)

Dalam konteks perlindungan hukum terhadap korban phishing, Indonesia belum memiliki skema kompensasi yang tegas bagi kerugian yang ditimbulkan akibat tindak pidana ini. Sebagian besar korban hanya bisa mengandalkan proses pidana untuk memidanakan pelaku tanpa jaminan pemulihan kerugian secara finansial. Hal ini berbanding terbalik dengan beberapa negara lain yang telah menerapkan pendekatan restorative justice dan skema restitusi dalam menangani kejahatan siber. Ketiadaan perlindungan yang optimal terhadap korban juga berdampak pada rendahnya tingkat pelaporan kasus phishing. Ketika korban tidak merasa dilindungi, maka upaya penegakan hukum akan sulit berkembang. Oleh karena itu, perlu dipertimbangkan adanya integrasi perlindungan korban ke dalam regulasi yang lebih komprehensif, baik melalui UU ITE maupun revisi KUHP. Dengan begitu, sistem hukum pidana tidak hanya berfungsi menghukum pelaku, tetapi juga memberikan keadilan bagi korban. (Fadillah & Mulyani, 2021)

Penanggulangan phishing tidak hanya dapat mengandalkan instrumen hukum pidana, tetapi juga memerlukan sinergi dengan pendekatan preventif dan edukatif. Upaya literasi

digital kepada masyarakat merupakan langkah strategis untuk meningkatkan kewaspadaan terhadap modus-modus penipuan berbasis daring. Pemerintah, institusi pendidikan, dan sektor perbankan perlu bekerja sama dalam membentuk kesadaran masyarakat digital. Dalam praktiknya, banyak korban phishing adalah pengguna awam yang tidak memahami bagaimana membedakan situs resmi dan situs palsu, atau bagaimana menjaga keamanan data pribadi. Oleh karena itu, hukum pidana harus diposisikan sebagai instrumen pelengkap dari ekosistem pencegahan yang lebih luas. Ketika masyarakat sudah cakap secara digital, maka potensi keberhasilan phishing pun menurun signifikan. Hukum pidana perlu dikaitkan dengan agenda literasi digital nasional agar perlindungan terhadap masyarakat dapat tercapai secara holistik. (Nursalim & Wahyuni, 2020)

Dalam kerangka penegakan hukum, peran aparat penegak hukum sangat krusial dalam menangani kejahatan phishing. Namun, kenyataan di lapangan menunjukkan masih adanya keterbatasan dari segi pengetahuan, teknologi, dan koordinasi antar lembaga dalam mengusut kasus phishing secara efektif. Banyak aparat belum memiliki pelatihan khusus mengenai modus operandi phishing atau tidak memiliki akses terhadap teknologi digital yang dapat membantu proses penyelidikan. Hal ini mengakibatkan proses penanganan perkara berjalan lambat, bahkan berpotensi gagal membuktikan kesalahan pelaku di pengadilan. Maka dari itu, penguatan kapasitas sumber daya manusia di kepolisian, kejaksaan, dan kehakiman perlu menjadi prioritas dalam agenda reformasi hukum pidana siber di Indonesia. Kualitas aparat akan sangat menentukan efektivitas sistem hukum dalam merespons kejahatan phishing yang terus berkembang. (Hasibuan & Kusuma, 2023)

Akhirnya, urgensi untuk merumuskan kebijakan pidana yang spesifik terhadap kejahatan phishing semakin meningkat seiring dengan meluasnya penggunaan internet dan meningkatnya kompleksitas modus kejahatan. Ketiadaan pasal yang secara khusus mengatur phishing membuat aparat penegak hukum harus bekerja ekstra untuk menyesuaikan delik yang tersedia. Hal ini tidak hanya menyulitkan aparat, tetapi juga membuka ruang perbedaan tafsir dalam proses peradilan. Oleh karena itu, dibutuhkan formulasi hukum pidana yang lebih presisi, baik dalam bentuk pasal baru di UU ITE maupun integrasi dalam KUHP yang direvisi. Dengan regulasi yang tegas, diharapkan penanggulangan phishing tidak hanya bersifat reaktif, tetapi juga proaktif dalam melindungi masyarakat digital. Penelitian ini mencoba menggali sejauh mana sanksi pidana terhadap kejahatan phishing dapat diterapkan secara efektif di Indonesia. (Yulianto & Prasetya, 2024)

2. TINJAUAN TEORITIS

Tinjauan teoritis dalam penelitian ini membahas dasar-dasar konseptual mengenai integrasi Supply Chain Management (SCM) dalam konteks industri otomotif, yang mencakup koordinasi lintas fungsi antara manufaktur dan layanan jasa. Konsep SCM tidak lagi dipahami sebagai aliran logistik semata, melainkan sebagai sistem strategis yang menghubungkan seluruh elemen dalam rantai nilai perusahaan, mulai dari pemasok, produsen, hingga penyedia layanan purna jual. Dalam era digital dan hiperkompetitif seperti sekarang, integrasi manufaktur-jasa melalui pendekatan SCM memungkinkan perusahaan meningkatkan kecepatan respon terhadap perubahan permintaan pasar serta membangun relasi jangka panjang dengan pelanggan. Selain itu, penggunaan teknologi seperti ERP, IoT, dan SCM Analytics memperkuat visibilitas serta keterhubungan antar fungsi yang sebelumnya terpisah. Model-model seperti SCOR dan Lean Supply Chain juga memberikan kerangka yang dapat diadaptasi dalam meningkatkan efisiensi dan fleksibilitas operasional. Dengan memadukan teori dan praktik, integrasi SCM dalam industri otomotif dapat menciptakan keunggulan kompetitif yang berkelanjutan di tengah tantangan global.

Teori Kriminologi dan Kejahatan Siber

Kejahatan siber, termasuk phishing, merupakan salah satu bentuk kejahatan modern yang membutuhkan pendekatan kriminologis baru. Dalam konteks ini, teori kriminologi klasik seperti teori rasionalitas masih relevan karena pelaku kejahatan siber kerap melakukan tindakannya berdasarkan perhitungan untung rugi. Mereka menilai bahwa kejahatan phishing memiliki risiko rendah dengan potensi keuntungan tinggi, terlebih jika dilakukan secara anonim dan lintas batas negara. Selain itu, teori kontrol sosial juga menjelaskan bahwa pelaku yang tidak memiliki keterikatan sosial yang kuat lebih rentan terlibat dalam kejahatan digital. Dalam kejahatan phishing, pelaku memanfaatkan anonimitas internet untuk melakukan penipuan tanpa rasa takut terhadap sanksi sosial atau hukum.

Sementara itu, pendekatan kriminologi modern menekankan pentingnya analisis terhadap faktor-faktor struktural, seperti ketimpangan ekonomi, akses teknologi, dan lemahnya pengawasan digital. Kejahatan phishing dapat berkembang di masyarakat yang belum memiliki pemahaman digital yang memadai, dan sistem hukum yang belum adaptif terhadap teknologi. Dalam konteks ini, teori kriminologi siber (cybercriminology) menjadi kunci untuk memahami dinamika pelaku dan korban kejahatan digital. Teori ini memadukan pemahaman teknologi, psikologi pelaku, serta faktor sosial yang mendukung terjadinya kejahatan phishing. (Hutapea & Iskandar, 2021)

Asas Legalitas dalam Hukum Pidana

Asas legalitas adalah prinsip dasar dalam hukum pidana yang menyatakan bahwa tidak ada perbuatan yang dapat dipidana kecuali telah diatur dalam undang-undang sebelumnya. Dalam konteks kejahatan phishing, asas ini menjadi tantangan tersendiri karena tidak ada pasal yang secara eksplisit menggunakan istilah "phishing." Akibatnya, aparat penegak hukum harus melakukan konstruksi hukum atau analogi untuk menjerat pelaku, yang dalam praktiknya sering menimbulkan perdebatan. Meskipun Pasal 35 UU ITE dianggap relevan karena mengatur manipulasi data, penerapannya terhadap kasus phishing masih sering dikritik karena tafsirnya yang luas dan berpotensi multitafsir.

Penerapan asas legalitas yang terlalu kaku juga berisiko mengabaikan perkembangan kejahatan modern. Oleh karena itu, sebagian pakar hukum pidana mendorong penggunaan asas "analogical reasoning" atau penafsiran progresif dalam konteks cybercrime. Meskipun demikian, hal ini harus dilakukan dengan sangat hati-hati agar tidak melanggar prinsip perlindungan terhadap hak asasi pelaku. Dalam sistem hukum Indonesia yang menganut asas legalitas secara ketat, penggunaan analogi hanya diperbolehkan dalam hukum perdata, bukan pidana. Oleh karena itu, perlu pembaruan hukum yang lebih responsif terhadap kejahatan digital seperti phishing agar asas legalitas tetap dapat ditegakkan secara adil. (Lestari & Prabowo, 2020)

Teori Perlindungan Hukum bagi Korban

Dalam hukum pidana modern, perhatian tidak hanya tertuju pada pelaku kejahatan, tetapi juga pada korban yang menderita akibat perbuatan tersebut. Teori perlindungan hukum bagi korban menggarisbawahi pentingnya kehadiran negara dalam memberikan keadilan dan pemulihan kepada korban. Dalam konteks kejahatan phishing, korban umumnya adalah individu atau entitas yang mengalami kerugian materiil dan non-materiil akibat pencurian data dan penipuan. Sayangnya, sistem hukum Indonesia belum memberikan perlindungan yang komprehensif terhadap korban kejahatan siber, termasuk phishing. Korban sering kali dibiarkan berjuang sendiri tanpa ada mekanisme pemulihan yang memadai.

Ketiadaan regulasi mengenai restitusi atau kompensasi terhadap korban phishing menjadi celah dalam sistem hukum. Hal ini diperburuk oleh prosedur hukum yang panjang, rumit, dan mahal, sehingga menyulitkan korban untuk mengakses keadilan. Perlindungan korban seharusnya menjadi bagian integral dari penegakan hukum pidana, tidak hanya dalam bentuk sanksi terhadap pelaku tetapi juga dalam pemulihan hak-hak korban. Negara harus mampu menjamin kepastian hukum dan keadilan bagi semua pihak yang terdampak. Hal ini

sesuai dengan prinsip keadilan restoratif yang saat ini mulai dikembangkan dalam sistem hukum Indonesia. (Handayani & Yusuf, 2023)

Struktur Tindak Pidana dalam KUHP

Struktur tindak pidana dalam KUHP terdiri dari unsur subjektif dan objektif. Unsur subjektif mencakup niat atau kesengajaan pelaku, sedangkan unsur objektif mencakup perbuatan, akibat, dan hubungan kausalitas antara keduanya. Dalam kejahatan phishing, unsur subjektif sangat jelas terlihat karena pelaku dengan sadar dan sengaja membuat rekayasa informasi untuk menipu korban. Unsur objektif pun terpenuhi karena adanya tindakan seperti pengiriman email palsu atau pembuatan situs tiruan yang menyebabkan kerugian bagi korban. Namun, pembuktian unsur ini sering kali menemui kesulitan karena kejahatan dilakukan secara daring, tidak langsung, dan seringkali tanpa saksi.

Meskipun phishing belum diatur secara khusus dalam KUHP, pelaku dapat dijerat melalui Pasal 378 tentang penipuan, yang mensyaratkan adanya tipu muslihat untuk memperoleh keuntungan. Dalam praktiknya, aparat penegak hukum harus menunjukkan bahwa pelaku memang berniat untuk mengambil keuntungan secara tidak sah dan bahwa korban benar-benar mengalami kerugian. Proses pembuktian dalam kasus phishing kerap kali mengandalkan bukti digital yang kompleks dan membutuhkan keahlian khusus. Oleh karena itu, selain perbaikan norma hukum, sistem pembuktian juga harus disesuaikan dengan karakteristik kejahatan digital. (Saragih & Mulya, 2019)

Teori Tujuan Pemidanaan

Pemidanaan dalam hukum pidana memiliki beberapa tujuan, di antaranya adalah retributif (pembalasan), deterrent (pencegahan), dan rehabilitatif (perbaikan perilaku). Dalam kasus phishing, pemidanaan pelaku bertujuan memberikan efek jera dan mencegah terulangnya perbuatan serupa. Teori pencegahan menekankan bahwa hukuman harus cukup berat untuk menakut-nakuti pelaku potensial, sementara teori pembalasan menegaskan bahwa pelaku harus mendapatkan hukuman yang setimpal dengan perbuatannya. Dalam konteks kejahatan siber, hukuman juga perlu mempertimbangkan dampak yang ditimbulkan kepada masyarakat luas.

Namun demikian, teori pemidanaan juga tidak dapat dipisahkan dari asas proporsionalitas. Sanksi pidana terhadap pelaku phishing harus mempertimbangkan besar kecilnya kerugian korban, tingkat kesengajaan, serta skala operasi pelaku. Dalam beberapa kasus, pelaku phishing adalah bagian dari sindikat internasional yang membutuhkan pendekatan pemidanaan kolektif dan lintas yurisdiksi. Oleh karena itu, formulasi sanksi

pidana harus adaptif dan mampu merespons kompleksitas kejahatan phishing secara menyeluruh, termasuk dari sisi edukatif dan korektif. (Rahayu & Putra, 2021)

Urgensi Pembaruan Hukum Pidana Siber

Perkembangan teknologi digital mendorong kebutuhan pembaruan hukum pidana di Indonesia. UU ITE sebagai regulasi utama kejahatan siber dinilai belum memadai dalam mengatur jenis-jenis kejahatan baru seperti phishing. Banyak kalangan menilai bahwa revisi UU ITE harus memasukkan pasal-pasal yang lebih eksplisit mengenai kejahatan manipulatif berbasis teknologi. Selain itu, KUHP yang baru juga perlu dirancang agar mampu merespons kejahatan digital dengan pendekatan progresif yang sesuai dengan prinsip negara hukum modern.

Di sisi lain, pembaruan hukum tidak hanya berarti menambah pasal, tetapi juga harus mencakup penguatan sistem penegakan hukum. Penegak hukum harus dibekali kemampuan forensik digital yang mumpuni agar dapat mengumpulkan dan menganalisis bukti elektronik secara profesional. Tanpa itu, perubahan regulasi tidak akan berdampak nyata. Pembaruan hukum pidana siber juga harus melibatkan partisipasi publik dan pemangku kepentingan agar dapat merespons kebutuhan masyarakat digital secara adil dan berimbang. (Mubarok & Syahrul, 2022)

Konsep Kejahatan Transnasional dan Yurisdiksi Hukum

Phishing merupakan bentuk kejahatan transnasional karena dapat melibatkan pelaku dan korban dari negara berbeda. Hal ini menimbulkan persoalan yurisdiksi hukum, terutama dalam penegakan dan penindakan terhadap pelaku yang berada di luar wilayah negara korban. Dalam sistem hukum pidana Indonesia, yurisdiksi teritorial menjadi batas utama, sehingga penindakan terhadap pelaku luar negeri memerlukan kerja sama internasional melalui mutual legal assistance (MLA) atau interpol.

Sayangnya, keterbatasan infrastruktur hukum dan lemahnya koordinasi antarnegara menjadi kendala dalam menangani kasus phishing lintas batas. Untuk itu, Indonesia perlu memperkuat diplomasi hukum dan menjadi bagian aktif dalam perumusan standar internasional penanganan cybercrime. Harmonisasi hukum, perjanjian ekstradisi, dan pengakuan bukti digital lintas negara menjadi agenda penting untuk menciptakan sistem hukum pidana yang tangguh menghadapi kejahatan phishing global. (Yudhistira & Malik, 2023)

Fungsi Preventif Hukum Pidana

Hukum pidana tidak hanya bertujuan menghukum, tetapi juga mencegah terjadinya kejahatan. Fungsi preventif ini dapat dicapai melalui pengaturan yang jelas, sanksi yang tegas,

serta edukasi kepada masyarakat. Dalam konteks phishing, hukum pidana harus mampu memberikan sinyal kuat bahwa perbuatan tersebut akan ditindak dengan serius. Hal ini dapat dilakukan dengan kampanye penegakan hukum dan publikasi terhadap kasus-kasus yang berhasil diadili.

Selain itu, edukasi hukum kepada masyarakat juga merupakan bagian dari fungsi preventif. Masyarakat perlu dibekali pemahaman mengenai hak-hak digital, cara melindungi data pribadi, dan mekanisme pelaporan jika menjadi korban. Upaya preventif tidak akan efektif jika tidak disertai kesadaran hukum masyarakat. Oleh karena itu, sinergi antara lembaga penegak hukum, kementerian, dan masyarakat sipil menjadi penting dalam membangun sistem hukum yang mencegah berkembangnya kejahatan phishing. (Simanjuntak & Rahmat, 2020)

Aspek Pembuktian dalam Kejahatan Siber

Salah satu tantangan utama dalam kejahatan phishing adalah pembuktian. Bukti elektronik seperti email, log server, atau transaksi digital sering kali sulit diverifikasi dan mudah dihapus. Oleh karena itu, aparat penegak hukum harus memiliki alat dan kompetensi dalam digital forensics. Di Indonesia, pembuktian kejahatan siber masih menjadi tantangan karena kurangnya keahlian, keterbatasan alat, dan belum optimalnya aturan pembuktian elektronik.

Dalam sistem pembuktian hukum pidana, alat bukti harus memenuhi syarat formil dan materiil. Bukti digital harus dapat menunjukkan siapa pelaku, apa perbuatannya, dan akibat hukumnya secara valid. Oleh sebab itu, perlu adanya penguatan regulasi mengenai otoritas penyidik siber, standar keamanan data, serta prosedur pengumpulan bukti digital yang sah secara hukum. (Utami & Nugraha, 2022)

Perbandingan Internasional: Best Practices

Beberapa negara telah mengatur phishing secara spesifik dalam regulasi nasional mereka. Misalnya, Amerika Serikat menggunakan Computer Fraud and Abuse Act (CFAA), sementara Uni Eropa menggunakan General Data Protection Regulation (GDPR) yang memberikan perlindungan ketat terhadap data pribadi. Negara-negara ini juga memiliki unit cybercrime khusus dengan wewenang luas dan teknologi canggih.

Indonesia dapat mengambil pelajaran dari praktik terbaik internasional dalam pengaturan dan penegakan hukum terhadap phishing. Harmonisasi dengan hukum internasional tidak hanya meningkatkan efektivitas penindakan, tetapi juga memperkuat posisi Indonesia dalam kerja sama lintas batas. Oleh karena itu, studi perbandingan perlu terus

dilakukan sebagai bagian dari pengembangan kebijakan hukum pidana nasional yang responsif terhadap dinamika kejahatan siber. (Rizqi & Azzahra, 2023)

3. METODE PENELITIAN

Metode penelitian ini menggunakan pendekatan kualitatif dengan jenis penelitian normatif-yuridis yang menitikberatkan pada analisis terhadap norma hukum positif yang berlaku di Indonesia. Sumber data utama dalam penelitian ini adalah bahan hukum primer berupa peraturan perundang-undangan, khususnya Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik serta Kitab Undang-Undang Hukum Pidana (KUHP). Selain itu, penelitian ini juga memanfaatkan bahan hukum sekunder berupa jurnal, buku, dan literatur hukum yang relevan untuk memperkuat argumentasi analitis. Teknik pengumpulan data dilakukan melalui studi kepustakaan (library research), sedangkan teknik analisis data dilakukan secara deskriptif kualitatif. Pendekatan ini digunakan untuk mengkaji kesesuaian antara ketentuan hukum pidana yang ada dengan karakteristik kejahatan phishing yang bersifat siber, serta mengevaluasi efektivitas sanksi pidana yang diterapkan terhadap pelaku phishing. Penelitian ini tidak menggunakan data lapangan karena fokus utamanya terletak pada kajian hukum normatif, bukan pada persepsi atau sikap masyarakat terhadap kejahatan phishing.

4. HASIL DAN PEMBAHASAN

Hasil penelitian menunjukkan bahwa meskipun kejahatan phishing belum secara eksplisit diatur dalam perundang-undangan Indonesia, perbuatan tersebut dapat dikualifikasikan sebagai tindak pidana berdasarkan unsur-unsur yang terdapat dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Kitab Undang-Undang Hukum Pidana (KUHP). Pasal 35 dan Pasal 36 UU ITE memberikan ruang untuk menjerat pelaku phishing yang melakukan manipulasi data elektronik dengan maksud untuk memperoleh keuntungan dan/atau merugikan orang lain. Selain itu, Pasal 378 KUHP tentang penipuan dan Pasal 362 KUHP tentang pencurian juga dapat digunakan jika tindakan phishing memenuhi unsur-unsur perbuatan melawan hukum, niat jahat, serta akibat berupa kerugian bagi korban. Namun dalam implementasinya, aparat penegak hukum masih menghadapi tantangan besar dalam proses pembuktian, mengingat phishing umumnya dilakukan secara anonim, melintasi yurisdiksi, serta menggunakan perangkat digital yang tidak mudah dilacak.

Pembahasan lebih lanjut menunjukkan bahwa sanksi pidana terhadap pelaku phishing belum sepenuhnya memberikan efek jera maupun perlindungan yang optimal kepada korban. Minimnya regulasi khusus membuat penegakan hukum bergantung pada penafsiran norma yang bersifat umum, yang berisiko menimbulkan multitafsir dan inkonsistensi dalam praktik peradilan. Selain itu, ketiadaan skema kompensasi bagi korban phishing memperburuk keadaan, karena proses pidana tidak menjamin pemulihan kerugian yang dialami. Situasi ini menunjukkan bahwa meskipun Indonesia telah memiliki dasar hukum untuk menindak pelaku phishing, efektivitas penerapan sanksi pidananya masih lemah. Oleh karena itu, perlu adanya pembaruan regulasi yang secara khusus mengatur phishing, serta penguatan kapasitas teknis aparat penegak hukum agar sistem hukum pidana Indonesia dapat merespons ancaman kejahatan digital secara komprehensif dan adil.

Tabel 1: Jenis-jenis Phishing Berdasarkan Media yang Digunakan

No	Media Phishing	Contoh Kasus	Bentuk Penipuan
1	Email	Surat Bank Palsu	Link login palsu bank digital
2	Website Tiruan	Situs e-commerce tiruan	Transaksi fiktif
3	SMS (Smishing)	Pesan undian hadiah	Permintaan klik tautan berbahaya
4	Media Sosial	Akun toko online palsu	Penipuan pembelian barang
5	Aplikasi Mobile Palsu	Aplikasi pinjaman online	Pencurian data kontak dan dompet digital

Penjelasan:

Tabel ini menggambarkan variasi media yang digunakan dalam kejahatan phishing. Pelaku phishing tidak terbatas hanya pada email, tetapi juga menggunakan media lain seperti SMS, media sosial, hingga aplikasi palsu. Strategi phishing terus berinovasi untuk mengecoh korban yang kurang paham teknologi digital, dan ini memperluas risiko ke berbagai kelompok masyarakat.

Kejahatan melalui aplikasi mobile dan website tiruan semakin marak karena mudah diakses dan tidak mudah dibedakan dari aplikasi asli. Ini menjadi tantangan besar bagi penegak hukum karena membutuhkan pendekatan digital forensik untuk mengungkap pelaku. Hukum pidana harus berkembang sesuai dengan pola kejahatan digital yang dinamis seperti ini.

Tabel 2: Dasar Hukum Pidana untuk Menjerat Pelaku Phishing

No	Regulasi	Pasal yang Dikenakan	Substansi Hukum
1	UU ITE 19/2016	Pasal 35 & 36	Manipulasi data dan kerugian elektronik
2	KUHP	Pasal 378	Penipuan dengan tipu muslihat
3	KUHP	Pasal 362	Pencurian data dan keuntungan melawan hukum
4	UU Perlindungan Data	Pasal 67 (Rancangan)	Penggunaan data pribadi tanpa izin
5	Peraturan Bank Indonesia	SE BI No.16/25/DKSP	Keamanan transaksi digital di perbankan

Penjelasan:

Tabel ini menunjukkan regulasi yang bisa digunakan untuk menjerat pelaku phishing dalam konteks hukum pidana Indonesia. Meski UU ITE menjadi rujukan utama, pasal-pasal dari KUHP tetap digunakan sebagai landasan hukum jika perbuatan phishing memenuhi unsur penipuan atau pencurian. Ini menunjukkan adanya tumpang tindih sekaligus peluang perluasan norma hukum.

Regulasi terkait perlindungan data pribadi yang saat ini masih berupa rancangan, memiliki potensi besar dalam memperkuat perlindungan terhadap korban phishing. Adapun surat edaran dari lembaga keuangan seperti Bank Indonesia menekankan pada penguatan sistem pengamanan perbankan sebagai bagian dari pencegahan phishing di sektor keuangan digital.

Tabel 3: Hambatan Penegakan Hukum terhadap Kejahatan Phishing

No	Aspek Kendala	Keterangan	Dampak
1	Pembuktian Digital	Bukti mudah dihapus dan tidak langsung	Sulit menjangkau pelaku
2	Kewenangan Lembaga	Tidak semua aparat paham IT forensik	Penanganan lambat
3	Lokasi Pelaku	Sering berada di luar negeri	Masalah yurisdiksi dan ekstradisi

4	Kesadaran Masyarakat	Rendahnya literasi digital	Korban mudah tertipu
5	Regulasi Belum Spesifik	Tidak ada pasal eksplisit soal phishing	Tafsir hukum multitafsir

Penjelasan:

Tabel ini mengidentifikasi berbagai hambatan yang dihadapi dalam menegakkan hukum terhadap kejahatan phishing. Hambatan paling utama adalah kesulitan dalam pembuktian karena sifat bukti digital yang mudah dimanipulasi atau dihapus. Selain itu, aparat penegak hukum masih mengalami keterbatasan dalam pemahaman teknis.

Permasalahan lintas yurisdiksi menjadi tantangan serius karena banyak pelaku yang melakukan aksinya dari luar negeri. Tanpa kerja sama internasional yang efektif, proses hukum menjadi sulit dilaksanakan. Kurangnya regulasi spesifik juga membuat proses hukum berjalan lambat dan tidak optimal.

Tabel 4: Perlindungan Terhadap Korban Phishing

No	Jenis Perlindungan	Bentuk Implementasi	Kelemahan
1	Pemidanaan pelaku	Proses hukum melalui UU ITE dan KUHP	Belum menjamin ganti rugi bagi korban
2	Edukasi dan literasi digital	Sosialisasi melalui media dan sekolah	Belum merata dan minim akses daerah
3	Pemulihan kerugian	Gugatan perdata oleh korban	Proses lambat dan biaya tinggi
4	Skema kompensasi negara	Restitusi oleh pemerintah	Belum ada dasar hukum nasional
5	Keamanan transaksi digital	Sistem otentikasi ganda (2FA)	Belum semua platform menerapkannya

Penjelasan:

Tabel ini menggambarkan bentuk perlindungan terhadap korban kejahatan phishing. Perlindungan paling umum saat ini adalah dalam bentuk pemidanaan terhadap pelaku. Namun demikian, aspek pemulihan kerugian materiil belum terakomodasi secara optimal dalam sistem hukum pidana Indonesia.

Upaya edukasi dan keamanan digital telah mulai dilakukan, tetapi masih terbatas pada wilayah perkotaan dan belum menjangkau seluruh masyarakat. Oleh karena itu, diperlukan pendekatan hukum terpadu yang tidak hanya menghukum pelaku, tetapi juga memberikan keadilan dan pemulihan yang layak kepada korban.

5. KESIMPULAN

Kesimpulan ini menunjukkan bahwa integrasi antara sektor manufaktur dan jasa dalam sistem Supply Chain Management pada industri otomotif memberikan dampak signifikan terhadap peningkatan efisiensi operasional dan ketahanan rantai pasok. Kolaborasi lintas fungsi, baik secara vertikal antar level organisasi maupun horizontal antar mitra kerja seperti pemasok dan penyedia jasa, terbukti memperkuat kemampuan perusahaan dalam merespons dinamika permintaan pasar secara lebih adaptif. Digitalisasi sistem informasi melalui platform terintegrasi juga menjadi kunci dalam meningkatkan transparansi, kecepatan komunikasi, serta pengambilan keputusan berbasis data yang akurat. Hasil studi mengindikasikan bahwa pendekatan holistik yang menggabungkan aspek teknologi, hubungan antar mitra, dan penyelarasan strategi operasional menjadi fondasi penting dalam membangun supply chain yang tangguh di era industri 4.0. Oleh karena itu, perusahaan otomotif yang ingin memperkuat daya saingnya disarankan untuk mengadopsi strategi integrasi yang mengedepankan sinergi lintas sektor secara sistematis dan berkelanjutan. Temuan ini juga memberikan kontribusi praktis bagi pengambil kebijakan dalam mendorong transformasi supply chain nasional ke arah yang lebih kolaboratif dan adaptif.

REFERENSI

Anugerah, R. A., & Suryani, D. (2021). Penegakan Hukum terhadap Kejahatan Siber dalam Era Digital: Studi Kasus Phishing di Indonesia. Jurnal Hukum dan Teknologi, 7(1), 45–60.

Fadillah, N., & Mulyani, R. (2021). Perlindungan Korban Kejahatan Siber dalam Perspektif Restorative Justice. Jurnal Ilmu Hukum Humaniora, 9(2), 122–138.

Fitriani, L., & Nugroho, T. A. (2022). Efektivitas Pasal 35 dan 36 UU ITE terhadap Tindak Pidana Phishing. Jurnal Legislasi Indonesia, 19(1), 66–79.

Handayani, A. S., & Yusuf, D. (2023). Perlindungan Hukum terhadap Korban Phishing: Tinjauan Yuridis Normatif. Jurnal Hukum Pidana dan Kriminologi, 15(1), 50–65.

Hasibuan, R. T., & Kusuma, E. (2023). Kesiapan Aparat Penegak Hukum dalam Menangani Kejahatan Siber. Jurnal Hukum Siber Nasional, 6(1), 99–114.

Hutapea, B., & Iskandar, A. (2021). Kriminologi Siber dan Dinamika Kejahatan Phishing di Indonesia. Jurnal Kriminologi Kontemporer, 5(2), 80–94.

Lestari, V. A., & Prabowo, S. H. (2020). Asas Legalitas dalam Penegakan Hukum Pidana Siber: Studi terhadap Kasus Phishing. Jurnal Hukum dan Etika Siber, 4(3), 33–47.

Mubarok, A. R., & Syahrul, M. (2022). Urgensi Pembaruan Hukum Pidana untuk Menanggulangi Cybercrime. Jurnal Reformasi Hukum Nasional, 10(2), 110–125.

Nursalim, A., & Wahyuni, R. (2020). Literasi Digital sebagai Upaya Preventif Tindak Pidana Phishing. Jurnal Pendidikan dan Hukum Teknologi, 3(4), 142–155.

Rahayu, D., & Putra, W. (2021). Teori Tujuan Pemidanaan dalam Penanggulangan Kejahatan Siber. Jurnal Teori dan Praktik Hukum Pidana, 8(2), 70–84.

Ramadhan, I., & Widodo, B. (2020). Dinamika Kejahatan Siber dan Urgensi Pembaruan Hukum Pidana Indonesia. Jurnal Hukum Nasional Indonesia, 11(3), 90–105.

Santoso, R., & Hidayat, A. (2023). Tinjauan Hukum Internasional terhadap Kejahatan Siber: Urgensi Harmonisasi Regulasi. Jurnal Hukum Internasional dan Siber, 6(2), 55–70.

Saragih, H. T., & Mulya, D. (2019). Unsur Tindak Pidana Penipuan dalam Kasus Kejahatan Siber. Jurnal Hukum dan Teknologi Informasi, 5(1), 25–39.

Wijaya, L., & Lestari, A. S. (2019). Analisis Penerapan KUHP terhadap Kejahatan Phishing di Indonesia. Jurnal Penegakan Hukum dan Kejahatan Siber, 7(2), 45–60.

Yulianto, A., & Prasetya, D. R. (2024). Kebutuhan Reformulasi Hukum Pidana terhadap Kejahatan Phishing. Jurnal Kebijakan dan Hukum Digital, 8(1), 18–33.