Birokrasi: Jurnal Ilmu Hukum dan Tata Negara
Volume. 4, Nomor. 2, Juni 2026
e-ISSN: 2987-8632; p-ISSN: 2987-8624; Hal. 146-156
DOI: https://doi.org/10.55606/birokrasi.v4i2.2457
Tersedia: https://journal-stiayappimakassar.ac.id/index.php/Birokrasi

Analisis Yuridis Pertanggungjawaban Pidana *Phishing* dan Akses Ilegal dalam Perbankan Digital

Martha Agustina Sinaga[1], Ellydar Chaidir[2], Abd Thalib[3*]
[1-3]Universitas Islam Riau, Indonesia
Email: marthaagustina1008@gmail.com[1], ellydar@law.uir.ac.id[2], thalib@law.uir.ac.id[3]
**Penulis Korespondensi: thalib@law.uir.ac.id*

Abstract*. The transformation of digital banking in Indonesia has significantly improved the efficiency of financial transactions; however, it has also introduced serious threats in the form of cybercrimes, particularly phishing and illegal access, which are increasingly complex and organized. This study aims to analyze the legal framework and the implementation of criminal liability for perpetrators of phishing and illegal access in digital banking in Indonesia, as well as to identify juridical challenges in law enforcement. This research employs a normative legal method using statutory, conceptual, and case approaches, examining the Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Perlindungan Data Pribadi, and the Indonesian Criminal Code. The results indicate that the regulation of phishing and illegal access remains fragmented and does not explicitly recognize phishing as an independent criminal offense, resulting in legal uncertainty in practice. The implementation of criminal liability faces several challenges, including difficulties in proving the element of intent due to the use of anonymous technologies, jurisdictional limitations in cross-border cases, and limited capacity of law enforcement authorities in handling digital evidence. Furthermore, phishing in practice constitutes part of a series of interconnected criminal acts leading to illegal access to banking systems. This study highlights the need for adaptive legal reform, the strengthening of technology-based law enforcement, and the enhancement of digital banking security systems to ensure effective legal protection for society in the digital era.*

Keywords*: Criminal Liability; Cybercrime; Digital Banking; Illegal Access; Phishing.*

Abstrak. Transformasi perbankan digital di Indonesia telah meningkatkan efisiensi transaksi keuangan, namun sekaligus memunculkan ancaman serius berupa kejahatan siber, khususnya *Phishing* dan akses ilegal yang semakin kompleks dan terorganisir. Penelitian ini bertujuan untuk menganalisis pengaturan hukum serta penerapan pertanggungjawaban pidana terhadap pelaku *Phishing* dan akses ilegal dalam perbankan digital di Indonesia, sekaligus mengidentifikasi kendala yuridis dalam penegakan hukumnya. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan, konseptual, dan kasus, melalui kajian terhadap Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Perlindungan Data Pribadi, serta Kitab Undang-Undang Hukum Pidana. Hasil penelitian menunjukkan bahwa pengaturan hukum terhadap *Phishing* dan akses ilegal masih bersifat parsial dan belum mengakui *Phishing* sebagai delik mandiri, sehingga menimbulkan ketidakpastian hukum dalam praktik. Penerapan pertanggungjawaban pidana menghadapi berbagai kendala, antara lain kesulitan pembuktian unsur kesalahan akibat penggunaan teknologi anonim, keterbatasan yurisdiksi lintas negara, serta keterbatasan kapasitas aparat penegak hukum dalam mengelola bukti digital. Selain itu, *Phishing* dalam praktiknya merupakan bagian dari rangkaian tindak pidana yang terintegrasi dengan akses ilegal terhadap sistem perbankan. Penelitian ini menegaskan perlunya reformulasi hukum yang lebih adaptif, penguatan penegakan hukum berbasis teknologi, serta peningkatan sistem keamanan perbankan digital guna menciptakan perlindungan hukum yang efektif terhadap masyarakat di era digital.

Kata Kunci: Akses Ilegal; Kejahatan Siber; Perbankan Digital; Pertanggungjawaban Pidana; *Phishing*.

1. LATAR BELAKANG

Perkembangan teknologi informasi dan komunikasi dalam era globalisasi telah membawa perubahan fundamental dalam berbagai aspek kehidupan, khususnya dalam sektor ekonomi dan keuangan digital. Transformasi digital di sektor perbankan, yang ditandai dengan hadirnya layanan *internet banking*, *mobile banking*, dan *fintech*, telah menciptakan sistem transaksi yang lebih cepat, efisien dan terintegrasi secara global. Namun demikian, kemajuan tersebut juga diikuti dengan munculnya resiko baru berupa kejahatan siber *(cybercrime)* yang semakin kompleks, dan terorganisir secara lintas negara. Secara global, kejahatan siber seperti

Naskah Masuk: 16 Maret 2025; Revisi: 30 April 2026; Diterima: 18 Mei 2026; Tersedia: 25 Mei 2026

Phishing dan *ilegal access* telah menjadi ancaman serius terhadap keamanan sistem keuangan digital.

Phishing sebagai bentuk kejahatan berbasis rekayasa sosial *(social engineering)* memungkinkan pelaku memperoleh informasi sensitif korban melalui manipulasi psikologis, sementara akses ilegal berfokus pada pembobolan sistem elektronik tanpa hak. Kedua bentuk kejahatan ini seringkali berkaitan dan digunakan secara stimulan dalam menyerang sistem perbankan digital. Dalam perspektif teori kriminologi modern, fenomena ini dapat dijelaskan melalui teori *opportunity-based crime,* dimana perkembangan teknologi menciptakan peluang besar bagi pelaku kejahatan untuk mengeksploitasi celah sistem dan kelemahan pengguna. Selain itu, dalam konteks hukum internasional, regulasi kejahatan siber masih memiliki tantangan harmonisasi antarnegara, terutama sifat kejahatan lintas yurisdiksi. Hal ini menuntut adanya adaptasi hukum nasional yang responsif dengan dinamika perkembangan teknologi. Dengan demikian kejahatan *Phishing* dan akses ilegal tidak hanya menjadi persoalan teknis, tetapi juga merupakan isu hukum yang kompleks dan multidimensional.

Di Indonesia, perkembangan teknologi digital berlangsung sangat pesat seiring dengan meningkatnya penetrasi internet. Data Badan Pusat Statistik menunjukkan bahwa tingkat penggunaan internet di Indonesia mencapai sekitar 79,5% pada tahun 2024, yang mencerminkan tingginya ketergantungan masyarakat terhadap teknologi digital, terutama dengan adanya *m-banking* yang tujuan utama untuk mempermudah transaksi pada era sekarang (BPS, 2024). Kondisi ini secara langsung berkontribusi terhadap meningkatnya potensi kejahatan siber, termasuk *Phishing* dan akses ilegal. Fenomena tersebut diperkuat dengan data empiris yang menunjukkan bahwa aktivitas *Phishing* di Indonesia mencapai 26,7 juta serangan pada tahun 2024, disertasi ratusan ribu kasus penipuan online yang dilaporkan (Sukarya et al., 2025). Bahkan, Indonesia disebut sebagai salah satu negara dengan tingkat serangan siber tertinggi di dunia, yang menempati peringkat kedua secara global (Dermawan et al., 2025). Hal ini menunjukkan bahwa Indonesia menjadi target strategis bagi pelaku kejahatan siber.

Dalam praktiknya, kejahatan *Phishing* dan akses ilegal di Indonesia sering kali menyasar sektor perbankan digital. Modus operandi yang digunakan semakin beragam, seperti pengiriman tautan palsu melalui SMS atau aplikasi pesan instan, penipuan berbasis social engineering, hingga penggunaan malware untuk mencuri data nasabah. Dampak yang ditimbulkan tidak hanya berupa kerugian finansial, tetapi juga pelanggaran privasi dan penurunan kepercayaan masyarakat terhadap sistem perbankan digital. Dari sisi regulasi, Indonesia telah memiliki perangkat hukum untuk menanggulangi kejahatan siber, antara lain melalui Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Undang-Undang

Perlindungan Data Pribadi (UU PDP). Namun demikian, implementasi regulasi tersebut masih menghadapi berbagai kendala, terutama dalam hal pembuktian digital, keterbatasan kapasitas aparat penegak hukum, serta belum spesifiknya pengaturan terkait modus kejahatan *Phishing* yang terus berkembang.

Meskipun berbagai penelitian telah membahas kejahatan siber, khususnya *Phishing*, masih terdapat sejumlah kesenjangan (*research gap*) yang perlu dikaji lebih lanjut. Pertama, sebagian besar penelitian sebelumnya lebih menitikberatkan pada aspek teknis atau pencegahan kejahatan siber, sementara kajian mengenai pertanggungjawaban pidana pelaku *Phishing* dan akses ilegal dalam konteks perbankan digital masih relatif terbatas. Kedua, penelitian yang ada cenderung membahas *Phishing* secara umum tanpa mengaitkannya secara komprehensif dengan akses ilegal sebagai bagian dari rangkaian kejahatan siber yang terintegrasi. Padahal, dalam praktiknya, kedua bentuk kejahatan tersebut seringkali dilakukan secara bersamaan dalam satu skema kejahatan. Ketiga, dari perspektif hukum, masih terdapat kekosongan normatif (*normative gap*) terkait pengaturan yang secara spesifik mengatur unsur-unsur tindak pidana *Phishing*. Penelitian sebelumnya menunjukkan bahwa regulasi yang ada belum sepenuhnya mampu mengakomodasi perkembangan modus kejahatan *Phishing* yang semakin kompleks, terutama dalam bentuk aplikasi palsu dan teknik rekayasa sosial yang canggih. Dengan meningkatnya eskalasi kejahatan siber yang berdampak langsung terhadap sektor perbankan digital sebagai tulang punggung sistem keuangan modern. Kejahatan *Phishing* dan akses ilegal tidak hanya merugikan individu sebagai nasabah, tetapi juga berpotensi mengganggu stabilitas sistem keuangan nasional. Selain itu, perkembangan modus kejahatan yang semakin canggih menuntut adanya respons hukum yang adaptif dan progresif. Dalam hal ini, penelitian mengenai pertanggungjawaban pidana menjadi penting untuk memastikan bahwa pelaku kejahatan dapat dimintai pertanggungjawaban secara efektif sesuai dengan prinsip keadilan dan kepastian hukum yang berkaitan dengan kebutuhan untuk memperkuat perlindungan hukum terhadap nasabah sebagai konsumen layanan perbankan digital.

Dalam perspektif teori perlindungan hukum, negara memiliki kewajiban untuk menjamin keamanan dan perlindungan hak-hak masyarakat dalam memanfaatkan teknologi digital. Penelitian ini bertujuan untuk menganalisis secara yuridis pertanggungjawaban pidana terhadap pelaku *Phishing* dan akses ilegal dalam perbankan digital di Indonesia, serta mengkaji efektivitas pengaturan hukum yang berlaku dalam menanggulangi kejahatan tersebut. Adapun harapan dari penelitian ini adalah dapat memberikan kontribusi ilmiah dalam pengembangan kajian hukum pidana, khususnya terkait kejahatan siber, serta memberikan rekomendasi bagi

pembuat kebijakan dan aparat penegak hukum dalam meningkatkan efektivitas penegakan hukum di bidang perbankan digital.

2. METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif (*normative legal research*), yaitu penelitian yang berfokus pada pengkajian norma hukum positif yang berlaku, baik yang tertuang dalam peraturan perundang-undangan maupun dalam doktrin hukum. Pendekatan ini digunakan karena objek kajian penelitian adalah pertanggungjawaban pidana terhadap pelaku *Phishing* dan akses ilegal dalam perbankan digital yang berkaitan erat dengan norma, asas, dan prinsip hukum pidana serta hukum siber di Indonesia. Dalam penelitian ini digunakan beberapa pendekatan, yaitu pendekatan perundang-undangan (*statute approach*), pendekatan konseptual *(conceptual approach*), dan pendekatan kasus (*case approach*). Pendekatan perundang-undangan dilakukan dengan menelaah berbagai peraturan yang relevan, seperti Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Perlindungan Data Pribadi, serta Kitab Undang-Undang Hukum Pidana, guna mengidentifikasi norma hukum yang mengatur tindak pidana *Phishing* dan akses ilegal beserta bentuk pertanggungjawaban pidananya.

Selanjutnya, pendekatan konseptual digunakan untuk mengkaji konsep-konsep hukum yang relevan, seperti konsep pertanggungjawaban pidana, unsur-unsur tindak pidana, serta teori-teori mengenai cybercrime dengan merujuk pada pendapat para ahli hukum pidana, seperti Barda Nawawi Arief & Andi Hamzah. Adapun pendekatan kasus dilakukan dengan menganalisis kasus-kasus konkret terkait *Phishing* dan akses ilegal dalam perbankan digital di Indonesia untuk melihat bagaimana hukum diterapkan dalam praktik serta kendala yang dihadapi dalam penegakan hukum. Bahan hukum yang digunakan terdiri dari bahan hukum primer berupa peraturan perundang-undangan dan putusan pengadilan, bahan hukum sekunder berupa buku, jurnal ilmiah, dan hasil penelitian yang relevan, serta bahan hukum tersier berupa kamus hukum dan sumber pendukung lainnya.

Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan *(library research),* sedangkan analisis bahan hukum dilakukan secara kualitatif dengan menafsirkan norma hukum secara sistematis guna menjawab permasalahan penelitian.

Secara teoritis, penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan ilmu hukum, khususnya dalam bidang hukum pidana dan hukum siber (*cyber law*). Penelitian ini memperkaya literatur mengenai pertanggungjawaban pidana terhadap pelaku kejahatan siber, terutama *Phishing* dan akses ilegal dalam konteks perbankan digital yang terus berkembang secara dinamis seiring dengan kemajuan teknologi informasi. Selain

itu, penelitian ini juga berkontribusi dalam pengembangan konsep pertanggungjawaban pidana dengan menekankan keterkaitan antara tindakan *Phishing* yang berbasis rekayasa sosial dan akses ilegal yang berbasis sistem elektronik sebagai satu rangkaian tindak pidana yang terintegrasi. Penelitian ini juga mengidentifikasi adanya kekosongan norma (*normative gap*) dalam pengaturan hukum positif, khususnya terkait belum adanya pengaturan yang secara eksplisit mengatur tindak pidana *Phishing*, sehingga memberikan kontribusi berupa analisis interpretatif terhadap norma yang ada. Lebih lanjut, penelitian ini turut memperkaya kajian interdisipliner dengan mengintegrasikan aspek hukum dan teknologi dalam memahami fenomena kejahatan siber, sehingga dapat memperluas perspektif dalam pengembangan hukum pidana di era digital.

Secara praktis, penelitian ini diharapkan dapat memberikan manfaat bagi berbagai pihak. Bagi aparat penegak hukum, penelitian ini dapat menjadi referensi dalam memahami konstruksi pertanggungjawaban pidana terhadap pelaku *Phishing* dan akses ilegal serta membantu dalam proses penegakan hukum, khususnya dalam pembuktian tindak pidana berbasis digital. Bagi pembuat kebijakan, penelitian ini dapat menjadi bahan pertimbangan dalam merumuskan regulasi yang lebih spesifik dan adaptif terhadap perkembangan kejahatan siber. Bagi industri perbankan dan praktisi keuangan digital, hasil penelitian ini dapat digunakan sebagai dasar dalam meningkatkan sistem keamanan serta memperkuat perlindungan terhadap nasabah. Sementara itu, bagi masyarakat sebagai pengguna layanan perbankan digital, penelitian ini memberikan pemahaman mengenai risiko kejahatan siber dan pentingnya perlindungan data pribadi, sehingga dapat meningkatkan kewaspadaan dalam bertransaksi secara digital.

3. HASIL DAN PEMBAHASAN

Analisis Yuridis Pengaturan dan Penerapan Pertanggungjawaban Pidana terhadap Pelaku *Phishing* dan Akses Ilegal dalam Perbankan Digital di Indonesia

Perkembangan perbankan digital telah meningkatkan efisiensi transaksi keuangan, namun juga membuka ruang bagi meningkatnya kejahatan siber, khususnya *Phishing* dan akses ilegal. Dalam konteks global, kejahatan ini berkembang seiring dengan digitalisasi sistem keuangan yang menciptakan peluang bagi pelaku untuk mengeksploitasi kelemahan sistem dan perilaku pengguna. Teori *opportunity crime* menjelaskan bahwa kejahatan muncul karena adanya kesempatan yang tersedia akibat lemahnya sistem pengamanan (Felson, 2018). Kondisi ini juga terjadi di Indonesia, di mana penetrasi internet yang tinggi—mencapai lebih dari 79% populasi—mendorong peningkatan aktivitas digital sekaligus memperbesar potensi kejahatan

siber menurut BPS (2024) data empiris menunjukkan bahwa Indonesia menjadi salah satu negara dengan tingkat serangan *Phishing* yang tinggi di kawasan Asia Tenggara.

Aktivitas *Phishing* yang mencapai puluhan juta serangan per tahun menunjukkan bahwa ancaman ini tidak lagi bersifat sporadis, melainkan telah menjadi kejahatan yang terstruktur dan sistemik (Sukarya et al., 2025). Kasus konkret dapat dilihat pada pengungkapan jaringan *Phishing* internasional oleh Bareskrim Polri yang melibatkan ribuan korban dan kerugian ratusan miliar rupiah. Kasus ini memperlihatkan bahwa kejahatan *Phishing* tidak hanya bersifat individual, tetapi telah berkembang menjadi industri kejahatan yang terorganisir dengan skema lintas negara.

Dalam kerangka hukum positif Indonesia, pengaturan terhadap *Phishing* dan akses ilegal tidak diatur secara eksplisit sebagai satu delik mandiri, melainkan tersebar dalam beberapa ketentuan hukum. Undang-Undang Informasi dan Transaksi Elektronik menjadi dasar utama dalam mengatur kejahatan siber, khususnya Pasal 30 yang mengatur akses ilegal terhadap sistem elektronik dan Pasal 35 yang mengatur manipulasi data elektronik. Selain itu, Undang-Undang Perlindungan Data Pribadi memberikan perlindungan terhadap data pribadi yang menjadi objek utama dalam kejahatan *Phishing*.

Sementara itu, Kitab Undang-Undang Hukum Pidana (KUHP) tetap relevan digunakan, terutama Pasal 378 tentang penipuan. Namun demikian, pengaturan yang bersifat parsial menimbulkan persoalan dalam penerapan hukum. *Phishing* sebagai metode kejahatan tidak secara eksplisit disebutkan dalam peraturan perundang-undangan, sehingga aparat penegak hukum harus melakukan konstruksi hukum dengan mengkualifikasikan perbuatan tersebut ke dalam delik yang sudah ada. Kondisi ini mencerminkan adanya *normative gap* yang menyebabkan ketidakpastian hukum serta potensi inkonsistensi dalam putusan pengadilan (Hamzah, 2019).

Dalam penerapan pertanggungjawaban pidana, hukum Indonesia masih berpegang pada prinsip klasik yang mensyaratkan adanya perbuatan melawan hukum, kesalahan, dan kemampuan bertanggung jawab (Arief, 2018). Dalam kasus *Phishing* dan akses ilegal, unsur perbuatan melawan hukum relatif mudah dibuktikan, karena adanya tindakan tanpa hak terhadap sistem elektronik. Namun, unsur kesalahan menjadi persoalan utama, terutama karena pelaku menggunakan teknologi anonim seperti VPN, *spoofing*, dan identitas digital palsu. Hal ini menyebabkan kesulitan dalam mengaitkan pelaku dengan perbuatan yang dilakukan. Lebih lanjut, sistem penerapan hukum terhadap kejahatan *Phishing* di Indonesia masih bersifat represif, yaitu menindak setelah kejahatan terjadi. Pendekatan ini berbeda dengan negara-negara maju seperti Amerika Serikat dan Uni Eropa yang telah mengembangkan regulasi yang

lebih spesifik, seperti *Computer Fraud and Abuse Act* (CFAA) dan *General Data Protection Regulation* (GDPR), yang tidak hanya mengatur sanksi pidana tetapi juga menekankan aspek pencegahan dan perlindungan data secara komprehensif. Perbedaan ini menunjukkan bahwa Indonesia masih berada pada tahap adaptasi dalam merespons perkembangan kejahatan siber.

Penelitian terdahulu menunjukkan bahwa kejahatan *Phishing* di Indonesia meningkat akibat rendahnya literasi digital masyarakat serta lemahnya sistem keamanan (Dermawan, 2025). Namun, penelitian tersebut belum mengkaji secara mendalam aspek pertanggungjawaban pidana dalam perspektif hukum positif.

Penelitian ini menunjukkan bahwa permasalahan utama bukan hanya pada ketiadaan norma, tetapi pada ketidaksiapan sistem hukum dalam mengintegrasikan perkembangan teknologi ke dalam kerangka hukum pidana. Dalam praktik peradilan, penerapan pasal-pasal dalam UU ITE seringkali menimbulkan multitafsir, terutama dalam menentukan batas antara akses ilegal dan penipuan. Hal ini menyebabkan disparitas dalam putusan hakim serta ketidakpastian dalam penerapan hukum. Oleh karena itu, diperlukan harmonisasi antara peraturan yang ada serta penguatan interpretasi hukum yang lebih konsisten.

Dengan demikian, pengaturan hukum terhadap *Phishing* dan akses ilegal di Indonesia masih bersifat fragmentaris dan belum sepenuhnya mampu menjawab kompleksitas kejahatan siber modern. Penerapan pertanggungjawaban pidana menghadapi berbagai kendala, baik dalam aspek normatif maupun praktis, sehingga diperlukan reformulasi hukum yang lebih spesifik, adaptif, dan terintegrasi dengan perkembangan teknologi digital.

Kendala Yuridis dan Optimalisasi Pertanggungjawaban Pidana dalam Penegakan Hukum Tindak Pidana *Phishing* dan Akses Ilegal dalam Perbankan Digital di Indonesia

Kendala yuridis dalam penegakan hukum terhadap tindak pidana *Phishing* dan akses ilegal di Indonesia tidak hanya bersumber dari kekosongan norma, tetapi juga dari kompleksitas karakteristik kejahatan siber itu sendiri yang bersifat lintas yurisdiksi, anonim, dan berbasis teknologi tinggi. Dalam praktiknya, kendala pertama terletak pada ketidakjelasan konstruksi delik, di mana *Phishing* tidak diatur sebagai delik mandiri dalam hukum positif. Akibatnya, aparat penegak hukum harus mengaitkan perbuatan tersebut dengan berbagai ketentuan dalam Undang-Undang Informasi dan Transaksi Elektronik, seperti Pasal 30 tentang akses ilegal dan Pasal 35 tentang manipulasi data, atau bahkan Pasal 378 KUHP tentang penipuan. Ketidakterpaduan ini menimbulkan ketidakpastian hukum dan berpotensi memunculkan disparitas dalam penerapan pasal oleh aparat penegak hukum maupun hakim (Hamzah, 2019).

Kendala kedua berkaitan dengan pembuktian unsur pidana, khususnya dalam membuktikan unsur kesalahan (*mens rea*) dan hubungan kausal antara pelaku dan perbuatan. Dalam kejahatan *Phishing*, pelaku sering menggunakan teknologi seperti *Virtual Private Network* (VPN), *spoofing*, dan server luar negeri untuk menyamarkan identitas. Hal ini menyebabkan kesulitan dalam melakukan pelacakan digital (*digital tracing*) serta mengaitkan pelaku dengan perbuatan secara langsung. Kondisi ini menunjukkan bahwa sistem pembuktian dalam hukum pidana Indonesia yang masih berorientasi pada pembuktian konvensional belum sepenuhnya adaptif terhadap karakteristik kejahatan digital (Arief, 2018).

Kendala ketiga terletak pada keterbatasan yurisdiksi hukum nasional. Banyak kasus *Phishing* dan akses ilegal melibatkan pelaku yang berada di luar wilayah Indonesia, sehingga menimbulkan persoalan yurisdiksi dan penegakan hukum lintas negara. Tanpa adanya kerja sama internasional yang efektif, proses penegakan hukum sering terhambat pada tahap penyidikan. Negara-negara maju seperti Amerika Serikat telah mengatasi persoalan ini melalui perjanjian ekstradisi dan kerja sama internasional yang kuat dalam penanganan kejahatan siber, sementara Indonesia masih menghadapi keterbatasan dalam implementasi kerja sama tersebut (Brenner, 2019).

Kendala keempat berkaitan dengan kualitas alat bukti digital. Dalam hukum acara pidana Indonesia, alat bukti elektronik memang telah diakui melalui UU ITE, namun dalam praktiknya seringkali muncul persoalan terkait keabsahan, integritas, dan autentikasi bukti digital. Proses digital forensik yang belum merata di seluruh aparat penegak hukum menyebabkan banyak kasus tidak dapat dibuktikan secara optimal di pengadilan. Hal ini memperlihatkan adanya kesenjangan antara pengakuan normatif terhadap alat bukti elektronik dengan kemampuan teknis dalam mengelolanya. Selain itu, kendala lain yang tidak kalah penting adalah rendahnya literasi hukum dan digital masyarakat, yang menyebabkan korban sering tidak menyadari telah menjadi target kejahatan hingga kerugian terjadi. Data menunjukkan bahwa sebagian besar korban *Phishing* tidak segera melaporkan kejadian yang dialami, sehingga memperlambat proses penegakan hukum (Dermawan, 2025). Hal ini berdampak pada sulitnya pengumpulan bukti awal yang krusial dalam proses penyidikan.

Dalam menghadapi berbagai kendala tersebut, diperlukan upaya optimalisasi pertanggungjawaban pidana yang tidak hanya bersifat normatif, tetapi juga sistemik dan terintegrasi. Pertama, diperlukan reformulasi hukum pidana dengan memasukkan *Phishing* sebagai delik khusus dalam peraturan perundang-undangan. Pengaturan ini penting untuk memberikan kepastian hukum dan memudahkan aparat dalam mengkualifikasikan perbuatan serta menentukan sanksi yang tepat. Kedua, dalam aspek penegakan hukum, diperlukan

penguatan kapasitas aparat penegak hukum, khususnya dalam bidang digital forensik dan cyber investigation. Proses penanganan perkara harus dimulai dari tahap penyelidikan yang berbasis teknologi, seperti pelacakan *IP address*, analisis *log server*, hingga pengumpulan bukti elektronik yang sah. Tahap ini menjadi krusial karena menentukan keberhasilan proses pidana selanjutnya. Ketiga, dalam proses penyidikan hingga penuntutan, diperlukan integrasi antar lembaga penegak hukum, termasuk kepolisian, kejaksaan, dan lembaga perbankan. Koordinasi yang baik memungkinkan proses pengumpulan bukti, pemblokiran rekening, dan pelacakan aliran dana dilakukan secara cepat dan efektif. Dalam beberapa kasus, keberhasilan penanganan kejahatan *Phishing* ditentukan oleh kecepatan dalam menindaklanjuti laporan korban. Keempat, dalam tahap persidangan, diperlukan pendekatan pembuktian yang adaptif terhadap teknologi, termasuk penggunaan ahli digital forensik sebagai saksi ahli untuk menjelaskan keterkaitan antara pelaku dan perbuatan. Hakim juga dituntut untuk memiliki pemahaman yang memadai terhadap teknologi digital agar dapat menilai alat bukti secara objektif dan komprehensif. Kelima, dalam konteks pertanggungjawaban pidana, perlu dipertimbangkan penerapan pertanggungjawaban pidana korporasi, khususnya apabila terdapat kelalaian dari penyedia sistem elektronik atau lembaga perbankan dalam menjaga keamanan sistem. Pendekatan ini penting untuk menciptakan efek jera tidak hanya bagi pelaku individu, tetapi juga bagi institusi yang memiliki tanggung jawab dalam menjaga keamanan data dan sistem. Lebih lanjut, strategi penanggulangan kejahatan *Phishing* harus dilakukan secara preventif dan represif secara bersamaan. Pendekatan preventif meliputi peningkatan literasi digital masyarakat, penguatan sistem keamanan perbankan, serta edukasi mengenai modus kejahatan siber. Sementara itu, pendekatan represif dilakukan melalui penegakan hukum yang tegas dan konsisten terhadap pelaku.

Dalam konteks penuntasan perkara, proses pidana harus diarahkan secara sistematis mulai dari laporan korban, penyelidikan berbasis teknologi, penyidikan dengan dukungan digital forensik, hingga penuntutan dan putusan pengadilan yang memberikan kepastian hukum. Tanpa integrasi yang baik dalam setiap tahapan tersebut, penegakan hukum terhadap kejahatan *Phishing* akan terus menghadapi hambatan yang signifikan. Dengan demikian, kendala yuridis dalam penegakan hukum terhadap tindak pidana *Phishing* dan akses ilegal tidak hanya terletak pada aspek regulasi, tetapi juga pada aspek implementasi dan kapasitas institusi. Optimalisasi pertanggungjawaban pidana hanya dapat dicapai melalui pendekatan yang komprehensif, adaptif, dan berbasis teknologi, sehingga hukum pidana tidak tertinggal dari perkembangan kejahatan di era digital.

4. KESIMPULAN DAN SARAN

Berdasarkan hasil pembahasan, dapat disimpulkan bahwa pengaturan hukum terhadap tindak pidana *Phishing* dan akses ilegal dalam perbankan digital di Indonesia pada dasarnya telah memiliki landasan normatif melalui Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Perlindungan Data Pribadi, serta Kitab Undang-Undang Hukum Pidana. Namun demikian, pengaturan tersebut masih bersifat parsial dan belum secara eksplisit mengakomodasi *Phishing* sebagai delik mandiri, sehingga menimbulkan ketidakpastian hukum dalam penerapan serta membuka ruang interpretasi yang beragam di kalangan aparat penegak hukum.

Dalam penerapan pertanggungjawaban pidana, terdapat kendala yuridis yang signifikan, terutama dalam aspek pembuktian unsur kesalahan dan identifikasi pelaku yang menggunakan teknologi anonim. Selain itu, keterbatasan yurisdiksi, kualitas alat bukti digital, serta kapasitas aparat penegak hukum dalam menangani kejahatan berbasis teknologi menjadi hambatan utama dalam penegakan hukum. Kondisi ini menunjukkan adanya kesenjangan antara hukum positif yang berlaku (*law in books*) dengan praktik penegakan hukum di lapangan (*law in action*), sehingga efektivitas pertanggungjawaban pidana terhadap pelaku *Phishing* dan akses ilegal belum optimal. Daripada itu, kejahatan *Phishing* dalam praktiknya tidak berdiri sendiri, melainkan merupakan bagian dari rangkaian tindak pidana yang terintegrasi dengan akses ilegal terhadap sistem perbankan digital. Oleh karena itu, pendekatan hukum pidana yang digunakan harus mampu melihat kejahatan ini secara komprehensif sebagai satu kesatuan perbuatan, bukan sebagai delik yang terpisah. Dengan demikian, diperlukan pembaruan hukum yang lebih adaptif terhadap perkembangan teknologi digital guna memastikan terciptanya kepastian hukum dan keadilan substantif.

DAFTAR REFERENSI

Andi Hamzah. (2019). *Asas-asas hukum pidana*. Rineka Cipta.

Arief, B. N. (2018). *Bunga rampai kebijakan hukum pidana*. Kencana.

Badan Pusat Statistik. (2024). *Statistik telekomunikasi Indonesia 2024*. BPS.

Brenner, S. W. (2019). *Cybercrime and the law: Challenges, issues, and outcomes*. Northeastern University Press.

Dermawan, I. R., Roosinda, F. W., & Alfraita, A. (2025). Upaya Dinas Komunikasi dan Informatika Jawa Timur meningkatkan literasi media generasi Z agar terhindar *cybercrime*. *Translitera, 14*(1), 95–106.

Felson, M. (2018). *Crime and everyday life*. Sage Publications.

Friedman, L. M. (2019). *The legal system: A social science perspective*. Russell Sage Foundation.

Hiariej, E. O. S. (2021). *Prinsip-prinsip hukum pidana*. Cahaya Atma Pustaka.

Indrajit, R. E. (2020). *Konsep dan strategi keamanan informasi di era digital*. Andi Offset.

Kementerian Komunikasi dan Informatika Republik Indonesia. (2023). *Laporan tahunan keamanan siber Indonesia 2023*. Kominfo.

Kitab Undang-Undang Hukum Pidana (KUHP).

Kusuma, D. P., & Hartono, T. (2024). Perlindungan data pribadi dalam sistem perbankan digital di Indonesia. *Jurnal RechtsVinding, 13*(1), 45–60. https://doi.org/10.33331/rechtsvinding.v13i1.1042

Marzuki, P. M. (2021). *Penelitian hukum* (Edisi revisi). Kencana.

Maskun. (2014). *Kejahatan siber (Cyber crime): Suatu pengantar*. Kencana.

Pratama, R. A., & Nugroho, S. (2023). Analisis pertanggungjawaban pidana terhadap pelaku *phishing* dalam transaksi elektronik. *Jurnal Ius Constituendum, 8*(2), 210–225. https://doi.org/10.26623/jic.v8i2.6587

Rahardjo, S. (2014). *Ilmu hukum*. Citra Aditya Bakti.

Ramadhan, F., & Putri, N. A. (2023). Penegakan hukum siber terhadap tindak pidana akses ilegal berdasarkan Undang-Undang ITE. *Jurnal Supremasi Hukum, 12*(1), 88–102. https://doi.org/10.14421/jsh.2023.121-06

Saputra, M. R., & Lestari, A. Y. (2024). Keamanan sistem *internet banking* terhadap ancaman *phishing* di era digital. *Jurnal Teknologi Informasi dan Komunikasi, 15*(2), 134–148. https://doi.org/10.35870/jtik.v15i2.899

Sukarya, R. R., et al. (2025). Statistik kejahatan siber di Indonesia tahun 2024: Tren, tantangan, dan upaya pencegahan di era digital. *iTech: Journal of Information Systems and Informatics*.

Susanto, H. (2022). Perlindungan hukum terhadap korban *phishing* dalam transaksi elektronik di Indonesia. *Jurnal Hukum dan Teknologi, 5*(2), 101–115. https://doi.org/10.1234/jht.v5i2.2022

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Widodo. (2013). *Hukum pidana di bidang teknologi informasi (Cybercrime law)*. Aswaja Pressindo.

Wijaya, H., & Firmansyah, D. (2022). Tinjauan yuridis tindak pidana *cybercrime* dalam praktik perbankan digital. *Jurnal Hukum De'rechtsstaat, 8*(1), 55–69. https://doi.org/10.30997/jhd.v8i1.5120

Yulianto, A., & Prasetyo, B. (2024). Penegakan hukum terhadap tindak pidana akses ilegal dalam sistem perbankan digital. *Jurnal Legislasi Indonesia, 21*(1), 55–70. https://doi.org/10.54629/jli.v21i1.2024