Journal Juridisch

Received: 2025-06-17
Accepted: 2026-02-19
Available: 2026-03-03
Volume 4 (1) March 2026 | e-ISSN: **2621-4105** |

https://journals.usm.ac.id/index.php/jj/index
DOI: https://doi.org/10.26623/jj.v4i1.12221

Perlindungan Hukum Korban Phishing: Analisis Kriminologi dan Efektivitas Regulasi di Indonesia

Legal Protection for Phishing Victims: Criminological and Regulatory Effectiveness Analysis in Indonesia

Moh. Havidz Nevoso[1]✉, Wahab Aznul Hidaya[2], Kadi Sukarna[3], Muhammad Junaidi[4], Cita Tsaabiethah Agustria Sasti[5]
[1,3,4] Magister Hukum, Universitas Semarang, Semarang, Indonesia
[2] Fakultas Hukum, Universitas Muhammadiyah Sorong, Sorong, Indonesia
[5] Fakultas Hukum, Universitas Semarang, Semarang, Indonesia
✉ havidznevoso98@gmail.com

Abstract

This study aims to analyze the criminological factors underlying phishing cybercrime and to assess the effectiveness of legal protection for victims of personal data theft in Indonesia. The core issue lies in the persistence of phishing despite existing legal instruments, indicating a gap between crime etiology and regulatory effectiveness. Academic discourse has largely focused on normative and technical aspects, while criminological analysis of offender motivation and opportunity structures remains limited. This research employs a normative juridical method with statutory and conceptual approaches. Criminological analysis applies strain theory to explain socio-economic pressures as offender motivations and routine activity theory to examine the interaction between motivated offenders, suitable targets, and weak digital guardianship. The findings reveal that phishing expands due to low-risk economic rationality, digital system vulnerabilities, and limited public literacy and supervision. Although regulated under the Electronic Information and Transactions Law and the Personal Data Protection Law, legal protection remains suboptimal due to evidentiary challenges and low enforcement probability. Integrating criminological perspectives is essential to strengthen both preventive and repressive strategies.
Keywords: *Criminology; Cybercrime; Personal Data Protection; Phishing.*

Abstrak

Penelitian ini bertujuan menganalisis faktor kriminologis penyebab *phishing cybercrime* serta menilai efektivitas perlindungan hukum bagi korban pencurian data pribadi di Indonesia. Permasalahan terletak pada masih maraknya *phishing* meskipun instrumen hukum telah tersedia, yang menunjukkan kesenjangan antara etiologi kejahatan dan efektivitas regulasi. Kajian akademik selama ini cenderung normatif dan teknis, sementara analisis mengenai motivasi pelaku dan struktur peluang kejahatan masih terbatas. Metode yang digunakan adalah yuridis normatif dengan pendekatan peraturan perundang-undangan dan konseptual. Analisis kriminologis menggunakan *strain theory* untuk menjelaskan tekanan sosial-ekonomi sebagai motif pelaku serta *routine activity theory* untuk mengkaji interaksi antara pelaku termotivasi, target rentan, dan lemahnya pengawasan digital. Hasil penelitian menunjukkan bahwa *phishing* berkembang karena rasionalitas ekonomi berisiko rendah, kerentanan sistem digital, serta rendahnya literasi dan pengawasan. Meskipun telah diatur dalam UU ITE dan UU Perlindungan Data Pribadi, efektivitas perlindungan hukum belum optimal akibat kendala pembuktian digital dan rendahnya probabilitas penindakan. Integrasi pendekatan kriminologi diperlukan guna memperkuat pencegahan dan penegakan hukum.
Kata kunci: *Cybercrime;* Kriminologi*;* Perlindungan Data Pribadi*; Phishing.*

e-ISSN: 2621-4105
https://journals.usm.ac.id/index.php/jj/index

1. PENDAHULUAN

Perkembangan teknologi informasi telah mengubah pola aktivitas sosial, ekonomi, dan administratif masyarakat, terutama melalui pemanfaatan internet yang semakin masif dan terintegrasi dengan pengelolaan data pribadi.[1] Digitalisasi ini di satu sisi memberikan efisiensi dan kemudahan akses, namun di sisi lain juga meningkatkan risiko penyalahgunaan data dan pelanggaran privasi.[2] Kerentanan sistem informasi, rendahnya literasi keamanan siber, serta ketergantungan masyarakat pada layanan digital menjadikan kejahatan siber sebagai fenomena yang semakin relevan untuk dikaji secara ilmiah, khususnya dalam konteks perlindungan hukum dan keamanan data pribadi di Indonesia.[3]

Cybercrime merupakan bentuk kejahatan yang dilakukan melalui media digital dengan berbagai modus, antara lain penipuan daring, pencurian identitas, peretasan sistem, penyebaran *malware*, hingga pencurian data pribadi. Kejahatan ini menimbulkan dampak serius tidak hanya bagi individu sebagai korban langsung, tetapi juga bagi institusi, pelaku usaha, dan stabilitas kepercayaan publik terhadap sistem elektronik. Dalam konteks Indonesia, meningkatnya kasus kejahatan siber menunjukkan bahwa ancaman *cybercrime* tidak lagi bersifat sporadis, melainkan sistemik dan membutuhkan pendekatan hukum serta kriminologis yang komprehensif.[4]

Salah satu bentuk *cybercrime* yang paling dominan adalah *phishing*, yaitu kejahatan yang dilakukan dengan cara memperoleh data pribadi atau informasi rahasia seseorang secara ilegal melalui manipulasi psikologis dan teknologi. Modus *phishing* umumnya dilakukan melalui tautan palsu, pesan elektronik, atau iklan digital yang menyerupai platform resmi, sehingga korban secara tidak sadar menyerahkan data sensitif seperti nomor identitas, rekening bank, atau kredensial akun. Karakteristik *phishing* yang bersifat lintas wilayah, anonim, dan berbasis rekayasa sosial menjadikannya sulit dideteksi serta menimbulkan tantangan serius dalam penegakan hukum.

Urgensi permasalahan *phishing cybercrime* di Indonesia tercermin dari kasus kebocoran data pribadi pada Mei 2021 yang melibatkan sekitar 279 juta data penduduk, mencakup identitas kependudukan, informasi kontak, hingga data sosial-ekonomi. Peristiwa ini menunjukkan lemahnya perlindungan data pribadi dan besarnya potensi kerugian yang dialami masyarakat, baik secara materiil maupun non-materiil. Kondisi tersebut mendorong perlunya respons negara melalui penguatan regulasi, yang diwujudkan melalui Undang-Undang Informasi dan Transaksi

[1] S Rustam, "Analisa Clustering *Phishing* Dengan K-Means Dalam Meningkatkan Keamanan Komputer," *ILKOM Jurnal Ilmiah* 10, no. 2 (2018): 175–81. https://doi.org/10.33096/ilkom.v10i2.309.175-181.

[2] K. E. A. Tampubolon, "Perbedaan Cyber Attack, *Cybercrime*, Dan Cyber Warfare.," *Jurist-Diction* 2, no. 2 (2019): 539–554. https://doi.org/10.20473/jd.v2i2.14250.

[3] H. Rumlus, M. H., & Hartadi, "Kebijakan Penanggulangan Pencurian Data Pribadi Dalam Media Elektronik.," *Jurnal Ham* 11, no. 2 (2020): 285–299. https://doi.org/10.30641/ham.2020.11.285-299.

[4] A. B. Suharto, B., & Kurniawan, "Tindak Pidana *Cybercrime* Bagi Pelaku Pemalsuan Data Pada Situs E-Commerce (*Phishing*).," *JHP* 17 (2020): 57–61. https://doi.org/10.30996/jhp17.v5i2.6109.

e-ISSN: 2621-4105
https://journals.usm.ac.id/index.php/jj/index

Elektronik serta Undang-Undang Perlindungan Data Pribadi sebagai perangkat hukum utama dalam upaya penanggulangan kejahatan siber.[5]

Urgensi kajian *phishing cybercrime* tidak hanya bersumber dari meningkatnya insiden kebocoran data, tetapi juga dari keterbatasan kerangka analisis yang digunakan dalam memahami kejahatan tersebut. Dalam literatur hukum Indonesia, *phishing* umumnya dianalisis sebagai persoalan normatif mengenai pengaturan hukum dan pertanggungjawaban pidana, atau sebagai persoalan teknis keamanan sistem informasi. Pendekatan tersebut belum sepenuhnya menjelaskan mengapa kejahatan *phishing* terus berkembang meskipun regulasi telah tersedia, sehingga diperlukan analisis yang menempatkan *phishing* sebagai fenomena kriminologis yang dipengaruhi oleh interaksi antara struktur sosial, peluang kejahatan, dan kapasitas pengawasan hukum.

Peningkatan kasus pencurian data pribadi di Indonesia menuntut pemerintah untuk mengambil langkah yang lebih tegas guna mencegah maupun meminimalkan kemungkinan terjadinya insiden serupa di masa mendatang. Upaya tersebut dapat dilakukan melalui penguatan perlindungan hukum yang mampu memberikan respons cepat dan efektif terhadap setiap pelanggaran data. Peristiwa pencurian data pribadi berpotensi menimbulkan kerugian yang signifikan bagi korban, baik secara materiil maupun non-materiil. Dampaknya tidak hanya dirasakan oleh individu pengguna situs web atau sistem elektronik, tetapi juga oleh perusahaan yang mengelola sistem digital serta lembaga keuangan, termasuk bank sebagai mitra transaksi. Dengan demikian, korban pencurian data tidak terbatas pada individu, melainkan juga mencakup institusi terkait dan masyarakat secara luas. Oleh karena itu, penerapan kebijakan preventif dan responsif yang tepat menjadi sangat penting untuk menjamin keamanan serta perlindungan privasi data pribadi masyarakat.

Berbagai kajian sebelumnya telah membahas kejahatan *phishing* dan isu perlindungan data pribadi melalui pendekatan yang beragam. Penelitian yang dilakukan oleh Adisa (2024) memfokuskan kajiannya pada perlindungan hukum bagi korban *phishing* melalui modus penyebaran file APK, namun analisis tersebut masih dominan bersifat normatif dan belum mengaitkan fenomena *phishing* dengan faktor-faktor kriminologis yang melatarbelakangi terjadinya kejahatan.[6] Penelitian lain oleh Anjheli (2024) berfokus pada efektivitas Undang-Undang Informasi dan Transaksi Elektronik serta Undang-Undang Perlindungan Data Pribadi dalam menangani kejahatan *phishing* di Indonesia, namun pembahasannya lebih menitikberatkan pada evaluasi kebijakan hukum tanpa mengkaji secara mendalam motif dan karakteristik pelaku.[7]

---

[5] R. Luthiya, A. N., Irawan, B., & Yulia, "Kebijakan Hukum Pidana Terhadap Pengaturan Pencurian Data Pribadi Sebagai Penyalahgunaan Teknologi Komunikasi Dan Informasi.," *Jurnal Hukum Pidana Dan Kriminologi* 2, no. 2 (2021): 14–29. https://doi.org/10.51370/jhpk.v2i2.43.

[6] Artanti Zahra Adisa and Andriyanto Adhi Nugroho, "Legal Protection for *Phishing* Victims Regarding the Transmission of APK Files," *JUSTISI* 10, no. 1 (2024), https://doi.org/10.33506/js.v10i1.2980.

[7] Devi Anjheli, "Privasi Digital Dan Kejahatan *Phishing* Di Indonesia: Evaluasi Kritis Terhadap Efektivitas UU ITE Dan UU PDP," *Staatsrecht Jurnal Hukum Kenegaraan Dan Politik Islam* 4, no. 1 (2024), https://doi.org/10.14421/990epf27.

e-ISSN: 2621-4105
https://journals.usm.ac.id/index.php/jj/index

Sementara itu, Sari (2025) mengkaji aspek pertanggungjawaban pidana dan kendala pembuktian dalam tindak pidana *phishing*, meskipun kajian tersebut masih terbatas pada ranah penegakan hukum pidana.[8]

Secara konseptual, penelitian-penelitian tersebut dapat dikelompokkan ke dalam tiga kecenderungan utama. Pertama, studi yang berorientasi pada perlindungan hukum korban dan evaluasi norma hukum positif. Kedua, studi yang menitikberatkan pada aspek teknis dan mekanisme kejahatan siber. Ketiga, studi yang membahas pertanggungjawaban pidana pelaku dalam perspektif hukum pidana. Meskipun memberikan kontribusi penting dalam pengembangan regulasi dan penegakan hukum, ketiga pendekatan tersebut belum secara komprehensif mengintegrasikan analisis etiologi kejahatan, struktur peluang, dan efektivitas perlindungan hukum dalam satu kerangka kriminologis yang utuh.

Kekosongan kajian tidak hanya terletak pada kurangnya penelitian mengenai *phishing cybercrime*, tetapi pada belum berkembangnya analisis kriminologis yang menjelaskan hubungan antara faktor penyebab kejahatan dengan efektivitas perlindungan hukum terhadap korban dalam konteks sistem hukum Indonesia.

Berdasarkan kajian terdahulu tersebut, dapat disimpulkan bahwa penelitian mengenai *phishing cybercrime* masih didominasi oleh pendekatan normatif dan teknis, sementara analisis yang mengaitkan faktor kriminologis penyebab kejahatan dengan efektivitas perlindungan hukum terhadap korban masih terbatas. Keterbatasan ini menunjukkan adanya celah penelitian yang perlu diisi melalui pendekatan kriminologi untuk memahami *phishing cybercrime* tidak hanya sebagai pelanggaran hukum, tetapi sebagai fenomena sosial yang dipengaruhi oleh faktor teknis dan ekonomi.

Berdasarkan pemaparan tersebut, permasalahan yang dikaji dalam penelitian ini meliputi dua aspek utama, yaitu: pertama, faktor-faktor kriminologis yang berperan dalam terjadinya *phishing cybercrime* di Indonesia; dan kedua, bentuk serta tingkat efektivitas perlindungan hukum yang diberikan kepada korban pencurian data pribadi akibat kejahatan *phishing*. Sejalan dengan perumusan masalah tersebut, penelitian ini bertujuan untuk mengkaji faktor teknis dan ekonomi sebagai penyebab terjadinya *phishing cybercrime* dari perspektif kriminologi, serta mengevaluasi efektivitas penerapan Undang-Undang Informasi dan Transaksi Elektronik dan Undang-Undang Perlindungan Data Pribadi dalam memberikan perlindungan hukum bagi korban.

2. METODE

Jenis penelitian yang digunakan dalam penelitian ini adalah penelitian hukum yuridis normatif, yaitu penelitian yang bertujuan untuk mengkaji norma hukum, asas hukum, dan doktrin

[8] Ratih Mega Puspa Sari, "Criminal Responsibility in *Cybercrime*: An Analysis of *Phishing* Crimes in Indonesia," *JHK-AUGUST* 2, no. 5 (2025), https://doi.org/10.61942/jhk.v2i5.418.

e-ISSN: 2621-4105
https://journals.usm.ac.id/index.php/jj/index

hukum yang berkaitan dengan kejahatan *phishing cybercrime* serta perlindungan hukum terhadap korban pencurian data pribadi. Pemilihan jenis penelitian ini didasarkan pada fokus penelitian yang menelaah pengaturan hukum positif dan konstruksi konseptual kriminologi dalam menilai faktor penyebab kejahatan serta efektivitas perlindungan hukum, tanpa melibatkan pengumpulan data lapangan secara langsung.[9] Pendekatan yang digunakan meliputi pendekatan peraturan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Pendekatan peraturan perundang-undangan digunakan untuk menganalisis ketentuan dalam Undang-Undang Informasi dan Transaksi Elektronik serta Undang-Undang Perlindungan Data Pribadi, sedangkan pendekatan konseptual digunakan untuk mengkaji konsep kriminologi terkait faktor teknis dan ekonomi sebagai penyebab *phishing cybercrime*. Spesifikasi penelitian bersifat deskriptif-analitis dengan menggunakan data sekunder berupa bahan hukum primer, sekunder, dan tersier yang diperoleh melalui studi kepustakaan.[10] Data dianalisis secara kualitatif dan penarikan kesimpulan dilakukan secara deduktif, yaitu dari norma hukum dan teori umum ke dalam konteks khusus kejahatan *phishing cybercrime* di Indonesia.

3. HASIL PENELITIAN DAN PEMBAHASAN

3.1 Pengaturan Perlindungan Hukum Pencurian Data Pribadi di Indonesia

Di Indonesia, perlindungan data pribadi didukung oleh beberapa instrumen hukum utama. Undang-Undang Perlindungan Data Pribadi sebagai implementasi Pasal 28G ayat (1) UUD 1945 menjamin hak atas privasi, kehormatan, dan rasa aman. Selain itu, Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia menegaskan perlindungan atas kerahasiaan korespondensi, termasuk komunikasi elektronik, yang hanya dapat dibatasi berdasarkan perintah pengadilan. Secara khusus, Undang-Undang Informasi dan Transaksi Elektronik melalui Pasal 26 mengatur penggunaan data pribadi dengan mensyaratkan persetujuan pemilik data serta hak penghapusan data yang tidak relevan.[11] Kerangka regulasi perlindungan data pribadi di Indonesia relatif komprehensif secara normatif, namun keberadaan norma hukum tidak secara otomatis menjamin efektivitas perlindungan terhadap korban. Dalam perspektif kriminologi, efektivitas hukum harus diukur dari kemampuannya mengurangi peluang kejahatan, meningkatkan pengawasan, serta mempengaruhi rasionalitas pelaku dalam mempertimbangkan risiko dan keuntungan kejahatan. Oleh karena itu, analisis terhadap UU ITE dan UU Perlindungan Data Pribadi tidak hanya perlu menilai kelengkapan norma, tetapi juga kemampuan implementatifnya

[9] Sidi Ahyar Wiraguna, "Metode Normatif Dan Empiris Dalam Penelitian Hukum : Studi Eksploratif Di Indonesia," *Jurnal Sosial Politik, Pemerintahan Dan Hukum* 3, no. 3 (2024), https://doi.org/10.59818/jps.v3i3.1390.

[10] Lalu M. Alwin Ahadi, "Efektivitas Hukum Dalam Perspektif Filsafat Hukum: Relasi Urgensi Sosialisasi Terhadap Eksistensi Produk Hukum," *Jurnal USM Law Review* 5, no. 1 (2022): 110, https://doi.org/10.26623/julr.v5i1.4965.

[11] Lalu Heru Sujamawardi, "Analisis Yuridis Pasal 27 Ayat (1) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik," *Dialogia Iuridica* 9, no. 2 (2018), https://doi.org/10.28932/di.v9i2.974.

e-ISSN: 2621-4105
https://journals.usm.ac.id/index.php/jj/index

dalam merespons dinamika kejahatan siber yang bersifat anonim, lintas yurisdiksi, dan berbasis teknologi tinggi.

Pemerintah Indonesia menetapkan Undang-Undang Perlindungan Data Pribadi sebagai instrumen hukum untuk melindungi informasi pribadi masyarakat, dengan konsekuensi bahwa setiap pelanggaran atas pengelolaan data pribadi dikenai sanksi sesuai ketentuan peraturan perundang-undangan. Menurut Pasal 1 ayat (1) UU Perlindungan Data Pribadi, data pribadi merupakan setiap informasi mengenai seseorang yang memungkinkan identitasnya dikenali, baik secara langsung maupun tidak langsung, melalui sistem elektronik maupun non-elektronik. Lebih lanjut, Pasal 4 ayat (1) UU PDP mengklasifikasikan data pribadi ke dalam dua kategori, yaitu data pribadi yang bersifat spesifik, yang pemrosesannya berpotensi menimbulkan dampak signifikan bagi subjek data, dan data pribadi yang bersifat umum, yakni informasi pribadi yang dapat diketahui secara luas.

Penegakan hukum terhadap pelanggaran data pribadi oleh penyelenggara sistem data harus disesuaikan dengan karakter dan bentuk pelanggaran yang terjadi. Ketentuan tersebut umumnya berkaitan dengan kewajiban yang harus dipenuhi dalam proses pengelolaan data pribadi, khususnya dalam sistem elektronik. Misalnya, Pasal 26 ayat (3) UU ITE mewajibkan penyelenggara sistem elektronik untuk menghapus informasi yang sudah tidak relevan atas permintaan pemilik data, sepanjang didukung oleh putusan pengadilan. Selanjutnya, ayat (4) mengatur kewajiban penyelenggara untuk menyediakan mekanisme penghapusan dokumen elektronik tersebut. Selain itu, Pasal 15 ayat (1) menegaskan bahwa penyelenggara sistem elektronik wajib mengelola sistem secara andal dan aman serta bertanggung jawab atas operasionalnya secara cermat. Ketentuan-ketentuan ini menunjukkan bahwa dalam hal terjadi pelanggaran data pribadi, tanggung jawab utama berada pada penyelenggara sistem elektronik. Dengan demikian, penyelenggara dapat dimintai pertanggungjawaban secara langsung oleh pihak yang dirugikan akibat pelanggaran tersebut, mengingat kewajiban mereka untuk menjamin keamanan dan keandalan sistem yang dikelola.

Posisi penyelenggara sistem elektronik tidak hanya sebagai subjek yang memiliki kewajiban menjaga keamanan data, tetapi juga sebagai pihak yang secara struktural memegang kontrol atas sistem pemrosesan data. Hal ini menimbulkan konsekuensi pembalikan beban pembuktian secara fungsional, di mana penyelenggara harus mampu menunjukkan bahwa sistem yang dikelolanya telah memenuhi standar keamanan dan prinsip perlindungan data pribadi. Secara kriminologis, pendekatan ini relevan karena pelaku pengendalian sistem berada pada posisi paling mampu mencegah terjadinya pelanggaran. Namun dalam praktik, pembuktian kelalaian sistem sering menghadapi kendala teknis, seperti kompleksitas forensik digital, keterbatasan akses korban terhadap bukti elektronik, serta asimetri informasi antara penyelenggara dan pengguna layanan.

Dalam hal terjadi pelanggaran, subjek data memiliki hak untuk meminta penghapusan informasi pribadi yang sudah tidak relevan. Hak ini dikenal sebagai hak untuk dihapus (*right to*

e-ISSN: 2621-4105
https://journals.usm.ac.id/index.php/jj/index

erasure) dan hak untuk tidak dicantumkan, yang merupakan perkembangan dari konsep hak untuk dilupakan. Melalui hak tersebut, individu diberikan kewenangan untuk mengendalikan informasi pribadi yang tersimpan dalam basis data digital serta menghentikan penyebaran data yang tidak lagi sesuai dengan tujuan pemrosesan. Keberadaan hak ini menegaskan posisi subjek data sebagai pihak yang berhak menjaga kerahasiaan dan pengendalian atas data pribadinya. Mengingat tingginya risiko kebocoran dan penyalahgunaan data pribadi, pengendali dan pemroses data memiliki kewajiban untuk mengelola sistem secara andal dan aman guna menjamin perlindungan data pribadi. Dengan demikian, hak penghapusan data pribadi menegaskan pentingnya perlindungan privasi dan keamanan dalam pengelolaan informasi pribadi di lingkungan digital.[12] Keberadaan hak penghapusan data dan kewajiban keamanan sistem seharusnya berfungsi sebagai mekanisme pengurangan peluang kejahatan. Namun efektivitas mekanisme tersebut sangat bergantung pada tingkat kepatuhan penyelenggara, kapasitas pengawasan regulator, serta kesadaran pengguna dalam menuntut haknya. Tanpa pengawasan yang efektif, hak normatif tersebut berpotensi menjadi instrumen deklaratif yang tidak secara signifikan menurunkan risiko penyalahgunaan data.

Undang-Undang Perlindungan Data Pribadi memberikan pengaturan yang lebih komprehensif terhadap perlindungan data pribadi. Regulasi tersebut menegaskan bahwa apabila terjadi kegagalan dalam menjaga keamanan data pribadi, penyelenggara data berkewajiban untuk memberitahukan kejadian tersebut kepada subjek data. Kegagalan perlindungan data dimaknai sebagai kondisi terganggunya kerahasiaan, integritas, maupun ketersediaan data pribadi. Gangguan tersebut dapat berupa pelanggaran keamanan yang terjadi secara sengaja maupun tidak sengaja, yang berpotensi menimbulkan kerusakan, kehilangan, perubahan, pengungkapan, atau akses tanpa kewenangan terhadap data pribadi. Sebagai ilustrasi, pelanggaran dapat terjadi ketika suatu perusahaan mengalami serangan siber yang menyebabkan terbukanya data pribadi pengguna dalam jumlah besar, baik akibat kelemahan sistem keamanan, pengawasan akses yang tidak memadai, maupun rendahnya kesadaran terhadap risiko keamanan siber. Selain itu, Pasal 47 UU PDP mewajibkan penyelenggara untuk mematuhi prinsip-prinsip perlindungan data pribadi sebagai bentuk tanggung jawab dalam pemrosesan data.

Pertanggungjawaban atas pelanggaran data pribadi juga dapat diajukan melalui mekanisme perdata berdasarkan Pasal 1365 KUHPerdata. Ketentuan tersebut menegaskan bahwa setiap perbuatan melawan hukum yang menimbulkan kerugian bagi pihak lain mewajibkan pelakunya memberikan ganti rugi. Tanggung jawab tersebut tidak hanya berlaku bagi tindakan yang dilakukan secara sengaja, tetapi juga mencakup perbuatan yang timbul karena kelalaian, sebagaimana diatur dalam Pasal 1366 KUHPerdata. Dengan demikian, kedua pasal tersebut

[12] Karen Eklesia Gabriella Kaendo and Ade Adhari, "Comparison of The Right to Be Forgotten Regulations in Indonesia and European Union Countries," *Rechtidee* 20, no. 1 (2025), https://doi.org/10.21107/ri.v20i1.30287.

e-ISSN: 2621-4105
https://journals.usm.ac.id/index.php/jj/index

memberikan dasar hukum bagi korban untuk menuntut kompensasi atas pelanggaran data pribadi, baik yang disengaja maupun akibat kelalaian.

Tujuan gugatan atas pelanggaran data pribadi adalah memperoleh pemulihan kerugian yang dialami korban. Namun, keberhasilan gugatan mensyaratkan pembuktian beberapa unsur, yaitu adanya kewajiban penyelenggara dalam melindungi data pribadi, terjadinya pelanggaran, timbulnya kerugian nyata pada korban, serta hubungan kausal antara kerugian tersebut dan kelalaian penyelenggara. Apabila seluruh unsur tersebut dapat dibuktikan, korban berhak memperoleh ganti rugi atas pelanggaran data pribadi yang dialaminya. Secara praktis, mekanisme gugatan perdata menghadapi hambatan pembuktian yang tidak sederhana. Korban harus membuktikan hubungan kausal antara kegagalan sistem perlindungan data dengan kerugian yang dialami, sementara bukti teknis umumnya berada dalam penguasaan penyelenggara sistem elektronik. Ketimpangan akses terhadap bukti ini menimbulkan hambatan struktural dalam penegakan tanggung jawab hukum. Dalam perspektif kriminologi sistem peradilan, kondisi tersebut dapat menurunkan probabilitas penegakan hukum dan pada akhirnya melemahkan efek pencegahan terhadap pelanggaran data pribadi.

Dalam sengketa pelanggaran data pribadi berdasarkan UU PDP, pengendali dan/atau prosesor data memikul beban pembuktian atas ada atau tidaknya pelanggaran. Pasal 24 UU PDP mewajibkan pengendali data menunjukkan bukti persetujuan subjek data sebagai dasar sah pemrosesan data pribadi. Selanjutnya, Pasal 47 menegaskan tanggung jawab pengendali data untuk membuktikan bahwa seluruh kegiatan pemrosesan telah sesuai dengan prinsip perlindungan data pribadi. Oleh karena itu, apabila timbul gugatan akibat kerugian yang dialami subjek data, penyelenggara data wajib membuktikan kepatuhan mereka terhadap ketentuan perlindungan data, mengingat merekalah pihak yang memiliki kontrol dan pengetahuan atas proses pemrosesan data.

Permasalahan utama dalam perlindungan data pribadi tidak semata terletak pada kekosongan norma hukum, tetapi pada kesenjangan antara desain regulasi dan kapasitas implementasinya. Penegakan hukum terhadap pelanggaran data pribadi memerlukan kemampuan teknis forensik digital, koordinasi lintas lembaga, serta mekanisme pelaporan dan pengawasan yang responsif. Keterbatasan dalam aspek-aspek tersebut menyebabkan probabilitas penindakan terhadap pelanggaran relatif rendah, sehingga secara kriminologis tidak menghasilkan efek pencegahan yang optimal. Meskipun pengaturan perlindungan data pribadi dalam UU ITE dan UU PDP telah memberikan landasan normatif yang relatif komprehensif, efektivitas penerapannya dalam praktik masih menghadapi berbagai kendala. Dari perspektif kriminologi, keberadaan sanksi pidana dan administratif dalam kedua undang-undang tersebut diharapkan memiliki *deterrence effect* atau efek pencegah terhadap pelaku kejahatan *phishing cybercrime*. Namun, dalam praktik penegakan hukum, efek jera tersebut belum sepenuhnya optimal karena rendahnya tingkat pengungkapan kasus, kompleksitas pembuktian digital, serta keterbatasan

e-ISSN: 2621-4105
https://journals.usm.ac.id/index.php/jj/index

kapasitas aparat penegak hukum dalam menangani kejahatan siber yang bersifat lintas wilayah dan transnasional.

Apabila dikaitkan dengan teori pencegahan kejahatan (*deterrence theory*), efektivitas hukum tidak hanya ditentukan oleh beratnya ancaman sanksi, tetapi juga oleh kepastian dan konsistensi penegakan hukum. Dalam konteks *phishing cybercrime*, meskipun UU ITE dan UU PDP telah mengatur sanksi pidana dan kewajiban pertanggungjawaban penyelenggara sistem elektronik, rendahnya probabilitas pelaku untuk tertangkap dan dihukum menyebabkan ancaman pidana tersebut belum sepenuhnya mampu menekan angka kejahatan. Hal ini sejalan dengan temuan kriminologis bahwa kejahatan berbasis teknologi cenderung berkembang ketika risiko hukum yang dirasakan pelaku lebih rendah dibandingkan potensi keuntungan ekonomi yang diperoleh.

Jika dibandingkan dengan praktik internasional, beberapa negara telah mengembangkan pendekatan perlindungan data pribadi yang lebih menekankan pada penegakan administratif yang kuat dan mekanisme pengawasan independen. Sebagai contoh, Uni Eropa melalui *General Data Protection Regulation* (GDPR) menerapkan sanksi administratif yang signifikan terhadap pelanggaran data pribadi serta mewajibkan pelaporan kebocoran data dalam jangka waktu tertentu, sehingga meningkatkan akuntabilitas pengendali dan pemroses data. Pendekatan ini menunjukkan bahwa efektivitas perlindungan data pribadi tidak hanya bergantung pada norma pidana, tetapi juga pada sistem pengawasan dan penegakan administratif yang tegas dan konsisten. Model pengawasan administratif yang kuat meningkatkan persepsi risiko pelaku terhadap kemungkinan terdeteksi dan dikenai sanksi. Tingkat kepastian penegakan hukum yang tinggi terbukti lebih berpengaruh terhadap pencegahan kejahatan dibandingkan semata-mata peningkatan berat sanksi pidana. Hal ini menunjukkan bahwa efektivitas perlindungan data pribadi bergantung pada kombinasi antara regulasi, pengawasan, dan kapasitas penegakan yang konsisten.

Dengan demikian, pengaturan perlindungan data pribadi di Indonesia melalui UU ITE dan UU PDP telah menunjukkan kemajuan normatif yang signifikan, namun masih memerlukan penguatan dalam aspek implementasi. Dari sudut pandang kriminologi, peningkatan efektivitas perlindungan hukum terhadap korban *phishing cybercrime* menuntut kombinasi antara penegakan hukum yang konsisten, peningkatan kapasitas aparat, serta penguatan mekanisme pengawasan dan kepatuhan penyelenggara sistem elektronik. Pendekatan ini penting agar perlindungan hukum tidak hanya bersifat deklaratif, tetapi juga mampu memberikan efek pencegahan dan perlindungan nyata bagi masyarakat di ruang siber.

3.2 Perlindungan Hukum bagi Korban *Phishing Cybercrime* dalam Perspektif Kriminologi

Meningkatnya jumlah pengguna internet di Indonesia berimplikasi langsung pada meningkatnya kebutuhan perlindungan terhadap data pribadi. Digitalisasi berbagai sektor kehidupan telah memperluas ruang penyimpanan dan pertukaran informasi pribadi, yang pada

e-ISSN: 2621-4105
https://journals.usm.ac.id/index.php/jj/index

saat yang sama meningkatkan risiko penyalahgunaan data. Dalam praktiknya, berbagai bentuk kejahatan siber seperti pencurian identitas, penipuan daring, perdagangan data pribadi, serta penyebaran informasi pribadi tanpa izin semakin sering terjadi dan menimbulkan kerugian baik secara finansial maupun non-finansial bagi korban.[13]

Salah satu bentuk kejahatan siber yang paling dominan adalah *phishing cybercrime*, yaitu kejahatan yang dilakukan melalui manipulasi teknologi dan psikologis untuk memperoleh data pribadi korban secara ilegal. Perkembangan *phishing cybercrime* tidak terlepas dari kemudahan akses teknologi, luasnya penggunaan sistem elektronik, serta rendahnya kesadaran keamanan digital masyarakat. Dalam konteks ini, kejahatan tidak lagi terbatas pada ruang fisik, melainkan berkembang dalam ruang siber yang bersifat anonim, lintas batas, dan sulit diawasi secara konvensional.[14] Untuk memahami *phishing cybercrime* secara komprehensif, analisis perlu terlebih dahulu ditempatkan dalam kerangka teori kriminologi yang menjelaskan etiologi kejahatan, motif pelaku, serta karakteristik tipologi kriminal berbasis keahlian. Kerangka ini penting agar *phishing* tidak hanya dipahami sebagai pelanggaran hukum, tetapi sebagai fenomena kriminal yang memiliki pola sebab-akibat dan rasionalitas tindakan pelaku.

Dari perspektif kriminologi, *phishing cybercrime* tidak dapat dipahami semata-mata sebagai pelanggaran norma hukum, melainkan sebagai hasil interaksi antara tekanan struktural dan peluang kejahatan. Teori motivasi kejahatan, khususnya *strain theory,* menjelaskan bahwa tekanan sosial dan ekonomi, seperti kesenjangan pendapatan dan tuntutan pencapaian kesejahteraan dapat mendorong individu memilih cara ilegal sebagai bentuk adaptasi. Dalam konteks *phishing*, motif ekonomi menjadi faktor dominan karena kejahatan ini memungkinkan pelaku memperoleh keuntungan finansial dengan risiko relatif rendah serta tingkat anonimitas yang tinggi.[15]

Selain itu, *routine activity theory* menjelaskan bahwa terjadinya *phishing cybercrime* dipengaruhi oleh terpenuhinya tiga unsur utama, yaitu adanya pelaku yang termotivasi, target yang rentan, dan lemahnya pengawasan.[16] Rendahnya literasi hukum dan literasi digital masyarakat menjadikan pengguna internet sebagai target yang mudah dieksploitasi, sementara lemahnya sistem keamanan serta keterbatasan pengawasan di ruang siber membuka peluang terjadinya kejahatan secara berulang. Dengan demikian, *phishing cybercrime* tidak hanya disebabkan oleh kemampuan teknis pelaku, tetapi juga oleh kondisi sosial dan sistem pengawasan yang belum optimal.

---

[13] Tanti Kirana Utami et al., "Personal Data Breach Cases in Indonesia : Perspective Of Personal Data Protection Law," *Customary Law Journal* 2, no. 2 (2025): 1–21, https://doi.org/10.47134/jcl.v2i2.3742.

[14] Afifah Sahfitri and Rosmalinda Rosmalinda, "Penipuan Digital Melalui Tautan *Phishing*," *Jurnal Dialektika Hukum* 6, no. 2 (2024), https://doi.org/10.36859/jdh.v6i2.2881.

[15] Katalin Parti and Thomas Dearden, "*Cybercrime* and *Strain theory*: An Examination of Online Crime and Gender," *International Journal of Criminology and Sociology* 13 (2024), https://doi.org/10.6000/1929-4409.2024.13.19.

[16] Ai Suzuki, "Routine Activities and Consumer Fraud Victimization: Findings from a Social Survey in Chiba Prefecture, Japan," *Crime Prevention and Community Safety* 26 (2024): 373–84, https://doi.org/10.1057/s41300-024-00219-2.

e-ISSN: 2621-4105
https://journals.usm.ac.id/index.php/jj/index

Dalam perspektif kriminologi, terjadinya *phishing cybercrime* dipengaruhi oleh berbagai faktor yang berkaitan dengan motif dan tujuan pelaku kejahatan. Secara umum, motif kejahatan ini dapat diklasifikasikan ke dalam dua kelompok utama. Pertama, motif intelektual, yaitu dorongan untuk melakukan kejahatan yang didasari oleh kepuasan pribadi dan keinginan menunjukkan kemampuan teknis dalam menguasai serta mengaplikasikan teknologi informasi; motif ini umumnya dilakukan oleh individu secara mandiri. Kedua, motif ekonomi dan kriminalitas terorganisir, yaitu kejahatan yang dilakukan dengan tujuan memperoleh keuntungan finansial atau kepentingan kelompok tertentu yang berdampak merugikan pihak lain, baik secara ekonomi maupun politis, dan sering kali dilakukan secara sistematis serta melibatkan organisasi atau korporasi.

Tipologi pelaku *phishing cybercrime* menunjukkan variasi motif dan tingkat kompleksitas kejahatan. Sebagian pelaku bertindak secara individual dengan motif intelektual untuk menunjukkan kemampuan teknis, sementara pelaku lainnya beroperasi secara terorganisir dengan orientasi ekonomi dan kriminalitas yang lebih sistematis. Karakteristik ini menempatkan *phishing cybercrime* sebagai bentuk *white crime* yang berbasis keahlian sekaligus *transnational crime*, mengingat kejahatan tersebut kerap melampaui batas yurisdiksi negara. Jika dikaitkan dengan kerangka etiologi kriminal tersebut, *phishing cybercrime* berkembang bukan semata-mata karena kemajuan teknologi, tetapi karena terbentuknya rasionalitas kriminal yang memandang ruang siber sebagai lingkungan berisiko rendah dengan potensi keuntungan tinggi. Kombinasi antara tekanan ekonomi, peluang struktural, dan lemahnya pengawasan menciptakan kondisi yang secara sistematis mereproduksi kejahatan *phishing*. Dengan demikian, keberlanjutan *phishing cybercrime* mencerminkan kegagalan pengendalian sosial digital dalam mengurangi peluang kejahatan dan meningkatkan kapasitas pengawasan.

Dari segi perlindungan hukum, negara telah merespons perkembangan *phishing cybercrime* melalui pengaturan dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Pelaku pencurian data pribadi melalui *phishing* dapat dijerat, antara lain, dengan Pasal 32 ayat (2) jo. Pasal 48 ayat (2) UU ITE dan Pasal 67 ayat (1) UU PDP. Ketentuan ini menunjukkan adanya perlindungan hukum normatif bagi korban kejahatan *phishing cybercrime*. Jika dianalisis dalam kerangka kriminologi, keberadaan norma pidana tersebut belum secara langsung mengurangi faktor etiologis kejahatan, seperti peluang struktural dan lemahnya pengawasan digital. Regulasi yang berfokus pada pemidanaan pelaku lebih berorientasi pada respons represif setelah kejahatan terjadi, sementara faktor kriminogenik yang memungkinkan *phishing* berkembang—seperti kerentanan sistem elektronik dan rendahnya literasi keamanan—belum sepenuhnya diatasi secara sistemik.

Namun, dari sudut pandang kriminologi, efektivitas perlindungan hukum tidak hanya ditentukan oleh keberadaan norma hukum, tetapi juga oleh kemampuan sistem hukum dalam

e-ISSN: 2621-4105
https://journals.usm.ac.id/index.php/jj/index

merespons faktor penyebab kejahatan. Kendala pembuktian digital, rendahnya kesadaran hukum masyarakat, serta keterbatasan kapasitas aparat penegak hukum menyebabkan perlindungan hukum terhadap korban *phishing cybercrime* belum berjalan optimal. Kondisi tersebut menunjukkan bahwa perlindungan hukum terhadap *phishing cybercrime* masih bersifat normatif-deklaratif dan belum sepenuhnya berfungsi sebagai mekanisme pengendalian kejahatan yang efektif. Dalam perspektif kriminologi, hukum seharusnya tidak hanya memberikan sanksi, tetapi juga mampu menurunkan peluang kejahatan, meningkatkan pengawasan, dan mengubah rasionalitas pelaku. Oleh karena itu, perlindungan hukum terhadap korban *phishing cybercrime* harus dipahami sebagai bagian dari kebijakan penanggulangan kejahatan yang komprehensif, yang mengintegrasikan pendekatan represif melalui pemidanaan pelaku dan pendekatan preventif melalui peningkatan literasi hukum dan digital, penguatan sistem keamanan elektronik, serta perbaikan mekanisme pengawasan siber.

4. PENUTUP

Berdasarkan hasil penelitian, dapat disimpulkan bahwa *phishing cybercrime* di Indonesia dipengaruhi oleh interaksi antara kerentanan teknis sistem digital dan struktur peluang kejahatan yang memungkinkan pelaku memperoleh keuntungan ekonomi dengan risiko hukum yang relatif rendah. Dalam perspektif kriminologi, *phishing* tidak hanya merupakan pelanggaran hukum individual, tetapi fenomena kriminal struktural yang terbentuk dari kombinasi motivasi ekonomi, ketersediaan target yang rentan, serta lemahnya pengawasan dan kapasitas penegakan hukum di ruang siber. Dari sisi perlindungan hukum, Undang-Undang Informasi dan Transaksi Elektronik serta Undang-Undang Perlindungan Data Pribadi telah menyediakan kerangka normatif yang memadai, namun efektivitasnya masih terbatas oleh kendala implementasi, terutama kompleksitas pembuktian digital, rendahnya probabilitas penindakan, serta keterbatasan pengawasan dan literasi masyarakat. Kondisi ini menunjukkan adanya kesenjangan antara desain regulasi dan efektivitas pengendalian kejahatan dalam praktik. Secara ilmiah, penelitian ini berkontribusi dengan mengintegrasikan analisis etiologi kejahatan dan efektivitas perlindungan hukum dalam satu kerangka kriminologis, sehingga *phishing* dipahami sebagai fenomena sosial-struktural yang memerlukan kebijakan penanggulangan komprehensif. Oleh karena itu, penguatan kebijakan perlu diarahkan pada peningkatan kapasitas forensik digital dan konsistensi penegakan hukum, penguatan standar keamanan serta pengawasan penyelenggara sistem elektronik, dan pendekatan preventif berbasis kriminologi melalui peningkatan literasi digital serta pengurangan peluang kejahatan dalam sistem elektronik.

DAFTAR PUSTAKA

Adisa, Artanti Zahra, and Andriyanto Adhi Nugroho. “Legal Protection for *Phishing* Victims Regarding the Transmission of APK Files.” *JUSTISI* 10, no. 1 (2024).

e-ISSN: 2621-4105
https://journals.usm.ac.id/index.php/jj/index

https://doi.org/10.33506/js.v10i1.2980.

Ahadi, Lalu M. Alwin. "Efektivitas Hukum Dalam Perspektif Filsafat Hukum: Relasi Urgensi Sosialisasi Terhadap Eksistensi Produk Hukum." *Jurnal USM Law Review* 5, no. 1 (2022): 110. https://doi.org/10.26623/julr.v5i1.4965.

Anjheli, Devi. "Privasi Digital Dan Kejahatan *Phishing* Di Indonesia: Evaluasi Kritis Terhadap Efektivitas UU ITE Dan UU PDP." *Staatsrecht Jurnal Hukum Kenegaraan Dan Politik Islam* 4, no. 1 (2024). https://doi.org/10.14421/990epf27.

Budhijanto, D. *Revolusi Cyberlaw Indonesia: Pembaruan Dan Revisi Undang-Undang Informasi Dan Transaksi Elektronik 2016*. Jakarta: PT Refika Aditama, 2018.

Kaendo, Karen Eklesia Gabriella, and Ade Adhari. "Comparison of The Right to Be Forgotten Regulations in Indonesia and European Union Countries." *Rechtidee* 20, no. 1 (2025). https://doi.org/10.21107/ri.v20i1.30287.

Luthiya, A. N., Irawan, B., & Yulia, R. "Kebijakan Hukum Pidana Terhadap Pengaturan Pencurian Data Pribadi Sebagai Penyalahgunaan Teknologi Komunikasi Dan Informasi." *Jurnal Hukum Pidana Dan Kriminologi* 2, no. 2 (2021): 14–29.

Parti, Katalin, and Thomas Dearden. "*Cybercrime* and *Strain theory*: An Examination of Online Crime and Gender." *International Journal of Criminology and Sociology* 13 (2024). https://doi.org/10.6000/1929-4409.2024.13.19.

Rumlus, M. H., & Hartadi, H. "Kebijakan Penanggulangan Pencurian Data Pribadi Dalam Media Elektronik." *Jurnal Ham* 11, no. 2 (2020): 285–299.

Rustam, S. "Analisa Clustering *Phishing* Dengan K-Means Dalam Meningkatkan Keamanan Komputer." *ILKOM Jurnal Ilmiah* 10, no. 2 (2018): 175–81.

Sahfitri, Afifah, and Rosmalinda Rosmalinda. "Penipuan Digital Melalui Tautan *Phishing*." *Jurnal Dialektika Hukum* 6, no. 2 (2024). https://doi.org/10.36859/jdh.v6i2.2881.

Sari, Ratih Mega Puspa. "Criminal Responsibility in *Cybercrime*: An Analysis of *Phishing* Crimes in Indonesia." *JHK-AUGUST* 2, no. 5 (2025). https://doi.org/10.61942/jhk.v2i5.418.

Suharto, B., & Kurniawan, A. B. "Tindak Pidana *Cybercrime* Bagi Pelaku Pemalsuan Data Pada Situs E-Commerce (*Phishing*)." *JHP* 17 (2020): 57–61.

Sujamawardi, Lalu Heru. "Analisis Yuridis Pasal 27 Ayat (1) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik." *Dialogia Iuridica* 9, no. 2 (2018). https://doi.org/10.28932/di.v9i2.974.

Suzuki, Ai. "Routine Activities and Consumer Fraud Victimization: Findings from a Social Survey in Chiba Prefecture, Japan." *Crime Prevention and Community Safety* 26 (2024): 373–84. https://doi.org/10.1057/s41300-024-00219-2.

Tampubolon, K. E. A. "Perbedaan Cyber Attack, *Cybercrime*, Dan Cyber Warfare." *Jurist-Diction* 2, no. 2 (2019): 539–554.

Utami, Tanti Kirana, Salsa Octaviani Suryanto, Kayla Andini Putri, and Fina Asriani. "Personal Data Breach Cases in Indonesia : Perspective Of Personal Data Protection Law." *Customary Law Journal* 2, no. 2 (2025): 1–21. https://doi.org/10.47134/jcl.v2i2.3742.

Wiraguna, Sidi Ahyar. "Metode Normatif Dan Empiris Dalam Penelitian Hukum : Studi Eksploratif Di Indonesia." *Jurnal Sosial Politik, Pemerintahan Dan Hukum* 3, no. 3 (2024). https://doi.org/10.59818/jps.v3i3.1390.