This Article is brought to you for open access by the Central Institute for Social and Humanities Studies. It has been accepted for inclusion in Cendekia: Jurnal Hukum, Sosial dan Humaniora by an authorized editor of Central Institute for Social and Humanities Studies.
Follow this and additional works at: https://journal.lps2h.com/cendekia/index

CENDEKIA: Jurnal Hukum, Sosial & Humaniora

Volume 4 Issue 4, 2026
E-ISSN: 2985-9174
https://doi.org/10.70193/cendekia.v4i4.345

Perlindungan Data Pribadi Terhadap Tindak Pidana *Phishing* Berdasarkan Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

Freni Ayu Syahputri[1], Asyifa Maghfirah[1], Rita Zahara[1] & Dani Durahman[2]
[1] *Fakultas Hukum, Universitas Malikussaleh, Aceh, Indonesia*
[2] *Fakultas Hukum, Universitas Langlangbuana, Bandung, Indonesia*

Citation: *A.S. Freni, M. Asyifa, Z. Rita & D. Dani. "Perlindungan Data Pribadi Terhadap Tindak Pidana Phishing Berdasarkan Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi," Cendekia: Jurnal Hukum, Sosial & Humaniora, 4, no. 4 (2026): 1521-1532.*

Article history:
Received: 24 Maret 2025
Revised: 06 Agustus 2026
Published: 25 Oktober 2026

Funding:
This study received no external funding

Competing interest:
The author(s) have declared that no competing interests exist

This is an Open Access article distributed under the terms of the Creative Commons Attribution (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0/), which permits non-commercial reuse, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstrak: Transformasi digital telah meningkatkan pemanfaatan data pribadi dalam berbagai aktivitas elektronik, namun di sisi lain juga memperbesar risiko terjadinya tindak pidana *phishing* yang memperoleh data pribadi melalui rekayasa sosial dan penyamaran identitas secara melawan hukum. Sebagai respons terhadap kondisi tersebut, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi hadir sebagai dasar hukum yang mengatur perlindungan hak subjek data pribadi. Penelitian ini bertujuan menganalisis pengaturan perlindungan data pribadi terhadap tindak pidana *phishing* berdasarkan Undang-Undang Nomor 27 Tahun 2022 serta mengkaji efektivitas penerapannya. Penelitian menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan dan pendekatan konseptual. Bahan hukum primer, sekunder, dan tersier dikumpulkan melalui studi kepustakaan, kemudian dianalisis secara kualitatif menggunakan metode deskriptif-analitis. Hasil penelitian menunjukkan bahwa Undang-Undang Nomor 27 Tahun 2022 telah mengatur hak subjek data, kewajiban Pengendali Data Pribadi dan Prosesor Data Pribadi, serta sanksi administratif dan pidana terhadap penyalahgunaan data pribadi. Namun, implementasinya masih menghadapi kendala, antara lain kesulitan mengidentifikasi pelaku, pembuktian digital, karakter *cross-border crime*, dan rendahnya literasi digital masyarakat. Kebaruan penelitian ini terletak pada analisis *phishing* sebagai pelanggaran terhadap hak atas perlindungan data pribadi, sehingga penanggulangannya tidak hanya berorientasi pada pemidanaan pelaku, tetapi juga pada penguatan perlindungan hukum, kelembagaan, dan tata kelola data pribadi.

Kata Kunci: Pelindungan data pribadi; *phishing*; kejahatan siber; Undang-Undang Nomor 27 Tahun 2022; perlindungan hukum.

Abstract: *Digital transformation has increased the use of personal data in various electronic activities; however, it has also heightened the risk of phishing crimes, in which personal data is obtained through social engineering and the unlawful impersonation of others. In response to this situation, Law No. 27 of*

*Corresponding Author : Freni Ayu Syahputri, Fakultas Hukum, Universitas Malikussaleh, Aceh, Indonesia, ORCID iD: 0009-0004-7052-9281, E-mail: freni.240510305.unimal.ac.id

2022 on Personal Data Protection serves as the legal basis governing the protection of the rights of personal data subjects. This study aims to analyze the regulations on personal data protection against phishing crimes under Law No. 27 of 2022 and to assess the effectiveness of its implementation. The study employs a normative legal research method using both a statutory and a conceptual approach. Primary, secondary, and tertiary legal sources were collected through a literature review and then qualitatively analyzed using a descriptive-analytical approach. The results of the study indicate that Law No. 27 of 2022 regulates the rights of data subjects, the obligations of Personal Data Controllers and Personal Data Processors, as well as administrative and criminal sanctions for the misuse of personal data. However, its implementation still faces obstacles, including difficulties in identifying perpetrators, digital evidence, the cross-border nature of the crime, and the public's low level of digital literacy. The novelty of this study lies in its analysis of phishing as a violation of the right to personal data protection, meaning that its mitigation should not only focus on prosecuting perpetrators but also on strengthening legal protections, institutional frameworks, and the governance of personal data.

Keywords: *Personal Data Protection; Phishing; Cybercrime; Law No. 27 Of 2022; Legal Protection.*

1. PENDAHULUAN

Transformasi digital yang dipicu oleh perkembangan teknologi informasi dan komunikasi telah mengubah pola kehidupan masyarakat di berbagai bidang, mulai dari kegiatan ekonomi, penyelenggaraan pemerintahan, sektor pendidikan, hingga pelayanan publik. Perubahan tersebut menyebabkan hampir seluruh aktivitas berbasis elektronik bergantung pada pemrosesan data pribadi sebagai bagian yang esensial dalam setiap transaksi maupun layanan digital.[1] Meskipun memberikan berbagai kemudahan, kemajuan teknologi juga membawa konsekuensi berupa meningkatnya ancaman terhadap keamanan ruang siber. Beragam bentuk kejahatan siber (*cybercrime*) terus berkembang seiring dengan kemajuan teknologi, baik dari segi metode maupun tingkat kecanggihannya.[2] Salah satu kejahatan yang paling sering terjadi adalah *phishing*, yaitu tindakan memperoleh data pribadi seseorang secara tidak sah melalui penyamaran identitas sebagai pihak yang memiliki kredibilitas atau hubungan hukum dengan korban.[3]

Pada dasarnya, *phishing* merupakan modus penipuan yang memanfaatkan media elektronik untuk mengelabui korban agar memberikan informasi yang bersifat rahasia. Informasi tersebut dapat berupa nama pengguna, kata sandi, nomor rekening, data kartu pembayaran, maupun informasi keuangan lainnya yang selanjutnya digunakan oleh pelaku untuk melakukan tindakan melawan hukum.[4] Penyalahgunaan data tersebut dapat menimbulkan berbagai akibat, seperti pencurian identitas, pengambilalihan aset keuangan, hingga penyebaran informasi yang merugikan reputasi

1 K. S Choi, C. S Lee, and E. R Louderback, *Historical Evolutions of Cybercrime* (UK: Palgrave Macmillan, 2020).

2 Maharani Chandra Dewi, "Cyber Espionage in National and Global Perspective: How Indonesia Deal with This Issue?," *International Law Discourse in Southeast Asia* 1, no. 1 (2022): 1–22, https://doi.org/https://doi.org/10.15294/ildisea.v1i1.56874.

3 Ganda Arisandi Wiranata, Yoyok Ucuk Subekti, dan Dudik Djaja Sidarta, "Pertanggungjawaban Pidana terhadap Pelaku Tindak Pidana Phishing," *Jurnal Penelitian Hukum*, Vol. 4, No. 02 (Maret 2024): 13.

4 Muhammad Ghozali et al., "Kejahatan Siber (Cyber Crime) Dan Implikasi Hukumnya: Studi Kasus Peretasan Bank Syariah Indonesia (BSI)," *Cendekia : Jurnal Hukum, Sosial Dan Humaniora* 2, no. 4 (2024): 797–809, https://doi.org/https://doi.org/10.5281/zenodo.13883603.

korban.[5] Oleh karena itu, dampak tindak pidana *phishing* tidak hanya berimplikasi pada kerugian ekonomi, tetapi juga mengancam perlindungan hak privasi serta keamanan data pribadi. Dalam menjalankan aksinya, pelaku umumnya mengatasnamakan institusi resmi, seperti perbankan, perusahaan, atau lembaga pemerintah, agar korban meyakini bahwa komunikasi yang diterimanya berasal dari pihak yang sah. Kepercayaan tersebut kemudian dimanfaatkan melalui teknik *social engineering*, manipulasi psikologis, serta rekayasa teknologi sehingga korban secara sukarela menyerahkan data pribadinya.[6] Kondisi tersebut menunjukkan bahwa *phishing* telah menjadi salah satu bentuk kejahatan siber yang memerlukan perhatian serius karena dapat merugikan individu maupun institusi yang mengelola data elektronik.[7]

Meningkatnya intensitas penyalahgunaan data pribadi di ruang digital mendorong negara membentuk kerangka hukum yang secara khusus mengatur perlindungan terhadap data pribadi.[8] Upaya tersebut diwujudkan melalui pemberlakuan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang menjadi landasan yuridis dalam penyelenggaraan pemrosesan data pribadi di Indonesia. Regulasi ini tidak hanya mengakomodasi pengakuan terhadap hak-hak subjek data, tetapi juga menetapkan tanggung jawab pengendali dan prosesor data, tata cara pemrosesan data pribadi, serta konsekuensi hukum bagi setiap pihak yang melakukan pelanggaran.[9] Keberadaan undang-undang tersebut merepresentasikan komitmen negara dalam memperkuat tata kelola perlindungan data pribadi sekaligus memberikan instrumen hukum untuk menghadapi berbagai bentuk kejahatan siber yang terus mengalami perkembangan, termasuk tindak pidana *phishing*.[10]

Berangkat dari kondisi tersebut, penelitian ini menawarkan unsur kebaruan (*novelty*) melalui kajian yang secara khusus mengulas perlindungan data pribadi dari perspektif Undang-Undang Nomor 27 Tahun 2022 dalam kaitannya dengan tindak pidana *phishing*. Fokus penelitian diarahkan pada analisis mengenai sejauh mana ketentuan dalam undang-undang tersebut mampu memberikan perlindungan hukum terhadap pemilik data pribadi yang menjadi sasaran kejahatan *phishing*. Atas dasar itu, rumusan masalah yang diajukan adalah bagaimana bentuk perlindungan data pribadi terhadap tindak pidana *phishing* berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Penelitian ini bertujuan mengkaji efektivitas pengaturan hukum yang disediakan oleh undang-undang tersebut dalam menjamin keamanan data pribadi dari ancaman *phishing*. Hasil penelitian diharapkan dapat memperkaya khazanah

---

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

6 Arctic Wolf, "A Brief History of Cybercrime," www.arcticwolf.com, 2024, https://arcticwolf.com/resources/blog/decade-of-cybercrime/.

7 Dian Rachmawati, "Phising Sebagai Salah Satu Bentuk Ancaman dalam Dunia Cyber," *Jurnal Saintkom*, 13, no. 3, (2014): 211.

8 S Nahak, "Hukum Tindak Pidana Mayantara (Cybercrime) Dalam Prespektif Akademik," *Jurnal Hukum Prasada* 4, no. 1 (2017): 1–11.

9 Raodia Raodia, "Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (Cybercrime)," *Jurisprudentie : Jurusan Ilmu Hukum Fakultas Syariah Dan Hukum* 6, no. 2 (2019): 39, https://doi.org/10.24252/jurisprudentie.v6i2.11399.

10 D. Solak and M. Topaloglu, "The Perception Analysis of Cyber Crimes in View of Computer Science Students," *Procedia - Social and Behavioral Sciences* 182 (n.d.): 590–595, https://doi.org/10.1016/j.sbspro.2015.04.787.

keilmuan di bidang hukum siber, sekaligus menjadi bahan pertimbangan dalam penyempurnaan kebijakan dan penguatan sistem perlindungan data pribadi di Indonesia.

2. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif yang menitikberatkan pada penelaahan terhadap bahan hukum sebagai sumber utama penelitian.[11] Fokus penelitian diarahkan pada kajian terhadap norma-norma hukum yang mengatur perlindungan data pribadi dalam kaitannya dengan tindak pidana *phishing* sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Untuk menjawab permasalahan penelitian, digunakan dua pendekatan, yaitu pendekatan peraturan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*).[12] Pendekatan peraturan perundang-undangan diterapkan dengan menelaah berbagai ketentuan hukum yang memiliki relevansi dengan perlindungan data pribadi dan kejahatan siber, antara lain Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, serta Kitab Undang-Undang Hukum Pidana. Adapun pendekatan konseptual dimanfaatkan untuk mengkaji berbagai konsep, teori, dan doktrin hukum yang berkaitan dengan perlindungan hukum, data pribadi, serta tindak pidana *phishing* sebagai landasan dalam menganalisis permasalahan penelitian.[13]

Sumber bahan hukum dalam penelitian ini dikelompokkan ke dalam tiga kategori, yaitu bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Bahan hukum primer mencakup berbagai peraturan perundang-undangan yang menjadi dasar pengaturan terhadap objek penelitian. Selanjutnya, bahan hukum sekunder diperoleh dari literatur ilmiah berupa buku, artikel jurnal, hasil penelitian terdahulu, serta pandangan para ahli yang memiliki keterkaitan dengan isu yang dikaji. Sementara itu, bahan hukum tersier digunakan sebagai pelengkap untuk memperjelas terminologi dan konsep hukum, antara lain melalui kamus hukum dan ensiklopedia. Keseluruhan bahan hukum tersebut dihimpun melalui penelitian kepustakaan (*library research*), kemudian dianalisis menggunakan metode kualitatif dengan pendekatan deskriptif-analitis. Analisis dilakukan melalui tahapan inventarisasi, pengelompokan, penafsiran terhadap norma hukum, serta penyusunan argumentasi hukum yang berujung pada penarikan kesimpulan secara deduktif. Tahapan tersebut dilakukan untuk memperoleh pemahaman yang komprehensif mengenai bentuk perlindungan data pribadi terhadap tindak pidana *phishing* berdasarkan ketentuan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

3. HASIL DAN PEMBAHASAN

3.1 Analisis Pengaturan Perlindungan Data Pribadi dalam Penanggulangan Tindak Pidana *Phishing* Menurut Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

Transformasi digital yang berlangsung secara masif telah menjadikan data pribadi sebagai bagian penting dalam berbagai aktivitas berbasis elektronik, seperti layanan perbankan, transaksi perdagangan digital, hingga penyelenggaraan pelayanan publik. Meningkatnya

---

[11] Suratman dan Philips Dilla, "*Metode Penelitian Hukum*," (Bandung: Alfabeta, 2015).

[12] Yun-chien Chang, "The Empirical Foundation of Normative Arguments in Legal Reasoning," *European Journal of Empirical Legal Studies* 1, no. 1 (2024): 69–88, https://doi.org/https://doi.org/10.62355/ejels.18070.

[13] Theresia Anita Christiani, "Normative and Empirical Research Methods: Their Usefulness and Relevance in the Study of Law as an Object," *Procedia-Social and Behavioral Sciences* 219 (2016): 201–7, https://doi.org/http://dx.doi.org/10.1016/j.sbspro.2016.05.006.

ketergantungan terhadap teknologi informasi turut memperluas potensi terjadinya kejahatan siber (*cybercrime*), salah satunya berupa tindak pidana *phishing*.[14] Kejahatan ini dilakukan melalui penyamaran identitas, manipulasi informasi, atau rekayasa sosial untuk memperoleh data pribadi milik korban tanpa hak dan bertentangan dengan ketentuan hukum.

Besarnya ancaman *phishing* di Indonesia tercermin dari data Badan Siber dan Sandi Negara (BSSN) yang mencatat sebanyak 164.131 insiden *email phishing* sepanjang tahun 2022. Dari keseluruhan kasus tersebut, sasaran utama pelaku adalah pengguna surat elektronik pribadi dengan jumlah 59.210 kejadian, sedangkan 52.744 kasus lainnya berasal dari berbagai kategori akun *email* yang berbeda. Apabila ditinjau berdasarkan waktu terjadinya serangan, aktivitas *phishing* lebih banyak berlangsung pada jam operasional, yaitu pukul 09.00 hingga 17.00, dengan total 93.897 kasus. Sementara itu, sebanyak 79.234 insiden terjadi di luar jam kerja, yakni pada rentang waktu pukul 17.00 sampai dengan 09.00. Data tersebut menunjukkan bahwa tindak pidana *phishing* merupakan ancaman nyata terhadap keamanan data pribadi yang memerlukan penguatan sistem perlindungan hukum dan keamanan siber.[15]

3.2 Konsep Data Pribadi dan Karakteristik Tindak Pidana *Phishing*

Dalam perkembangan masyarakat digital, data pribadi telah berkembang menjadi salah satu objek hukum yang memiliki arti penting karena berkaitan erat dengan identitas, kehidupan privat, serta hak-hak fundamental setiap orang. Pesatnya pemanfaatan teknologi informasi menyebabkan data pribadi tidak lagi sekadar informasi individu, melainkan menjadi aset yang memiliki nilai hukum, sosial, dan ekonomi.[16] Oleh sebab itu, keberadaan instrumen hukum yang mampu memberikan perlindungan terhadap data pribadi menjadi suatu kebutuhan yang tidak dapat diabaikan.[17]

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi memberikan pengertian bahwa data pribadi merupakan setiap data mengenai perseorangan yang telah teridentifikasi atau dapat diidentifikasi, baik secara langsung maupun melalui penggabungan dengan informasi lainnya, baik dengan menggunakan sistem elektronik maupun non-elektronik. Dalam undang-undang yang sama, perlindungan data pribadi dimaknai sebagai serangkaian tindakan yang bertujuan menjamin terpenuhinya hak subjek data sekaligus memberikan kepastian hukum terhadap seluruh aktivitas yang berkaitan dengan pemrosesan data pribadi. Dengan demikian, perlindungan data pribadi tidak hanya berfungsi menjaga kerahasiaan informasi, tetapi juga memastikan penghormatan terhadap hak konstitusional setiap individu atas privasi dan penguasaan terhadap data yang dimilikinya.

---

[14] Tonny Rompi and Harly Stanly Muaja, "Tindak Kejahatan Siber Di Sektor Jasa Keuangan Dan Perbankan," *Lex Privatum* 9, no. 4 (2021): 183–92.

[15] Sarnita sadya, Ada 164.131 Kasus Email Phishing di Indonesia pada 2022, https://dataindonesia.id/internet/detail/ada-164131-kasus-email-phising-di-indonesia-pada-2022.

[16] M. I Alghamdi, "A Descriptive Study on the Impact of Cybercrime and Possible Measures to Curtail Its Spread Worldwide," *International Journal of Engineering Research and Technology* 9 (2020): 731–35.

[17] Zulfan, "Cybercrime in Virtual Spaces: An Overview of the Law in Indonesia," *International Journal of Law, Social Science, and Humanities (IJLSH)* 1, no. 1 (2024): 18–26, https://doi.org/https://doi.org/10.70193/ijlsh.v1i1.140.

Ditinjau dari perspektif Undang-Undang Perlindungan Data Pribadi, *phishing* merupakan perbuatan memperoleh serta memanfaatkan data pribadi tanpa dasar hukum yang sah melalui rangkaian tindakan yang bersifat manipulatif.[18] Perolehan data dengan cara demikian bertentangan dengan prinsip-prinsip pemrosesan data pribadi yang mewajibkan setiap pengendali data untuk memproses data secara sah, transparan, sesuai dengan tujuan tertentu, didasarkan pada persetujuan atau dasar hukum yang dibenarkan, serta menjamin keamanan data selama proses pemrosesan berlangsung.[19] Oleh karena itu, penggunaan metode *phishing* untuk memperoleh data pribadi tidak hanya menunjukkan adanya penguasaan data secara melawan hukum, tetapi juga mencerminkan pelanggaran terhadap hak subjek data atas privasi, keamanan, dan pengendalian terhadap informasi pribadinya. Dalam konteks tersebut, *phishing* tidak lagi dipahami semata-mata sebagai bentuk penipuan yang memanfaatkan teknologi informasi, melainkan juga sebagai perbuatan yang melanggar rezim perlindungan data pribadi sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Sejumlah penelitian terdahulu umumnya mengkaji *phishing* sebagai bentuk kejahatan penipuan yang dilakukan melalui sarana elektronik.[20] Dalam kajian tersebut, pertanggungjawaban hukum pelaku lebih banyak dianalisis berdasarkan ketentuan dalam Kitab Undang-Undang Hukum Pidana (KUHP) dan Undang-Undang tentang Informasi dan Transaksi Elektronik (UU ITE). Salah satu di antaranya adalah penelitian yang dilakukan oleh Yazid Haikal Lokapala, Fuad Januar Nurfauzi, dan Yeni Widowaty yang menyimpulkan bahwa pelaku *phishing* dapat dimintai pertanggungjawaban pidana melalui penerapan ketentuan mengenai penipuan dalam KUHP serta ketentuan pidana yang diatur dalam UU ITE.[21]

Penelitian ini menawarkan sudut pandang yang berbeda dengan menempatkan data pribadi sebagai fokus utama analisis. *Phishing* tidak hanya dipahami sebagai tindak pidana penipuan berbasis teknologi informasi, tetapi juga sebagai perbuatan yang mengakibatkan pelanggaran terhadap hak atas perlindungan data pribadi. Oleh karena itu, kajian ini menggunakan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi sebagai landasan utama dalam menganalisis konsekuensi hukum dari perolehan dan penyalahgunaan data pribadi melalui praktik *phishing*.[22] Pendekatan tersebut memperlihatkan bahwa upaya penanggulangan *phishing* tidak cukup dilakukan melalui pemberian sanksi pidana kepada pelaku semata, melainkan juga harus diiringi dengan penguatan sistem perlindungan data pribadi, pemenuhan kewajiban pengendali data pribadi, serta optimalisasi mekanisme perlindungan hukum yang telah

---

[18] Ensalina Papilaya, Sari Murti Widiyastuti, and Husni, "Adoption of Hardship Clauses in Indonesia's Contract Law Reform System," *International Journal of Law, Social Science, and Humanities* 3, no. 2 (2026): 529–535, https://doi.org/https://doi.org/10.70193/ijlsh.v3i2.302.

[19] Simon Matome Nkgapele and Regina Mapula Mokgolobotho, "Developing Transformational Strategies to Improve the Accessibility of E-Governmental Services in the South African Local Government," *International Journal of Law, Social Science, and Humanities (IJLSH)* 1, no. 2 (2024): xxx.

[20] Afifah Sahfitri dan Rosmalinda, "Penipuan Digital melalui Tautan Phishing," *Jurnal Dialektika Hukum*, 6, no. 2 (2024): 92.

[21] Yazid Haikal Lokapada, Fuad Januar Nurfauzi, dan Yeni Widowaty, "Aspek Yuridis Kejahatan *Phishing* Dalam Ketentuan Hukum Indonesia" *Indonesian Journal Of Criminal Law And Criminology* 5, no.1 (2024): 19-24. https://doi.org/10.18196/ijclc.v5i1.19853

[22] ISTR, "Internet Security Threat Report - ISTR," *Symantec Journal* 22, no. April (2017): 77, https://doi.org/10.1016/S1353-4858(05)00194-7.

dirumuskan dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

3.3 Perlindungan Hukum Terhadap Korban Phishing Berdasarkan Undang-Undang Nomor 27 Tahun 2022

Perlindungan terhadap korban tindak pidana *phishing* merupakan bagian dari jaminan hukum atas hak perlindungan data pribadi sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Melalui pengaturan tersebut, negara memberikan pengakuan terhadap hak-hak subjek data sebagai bentuk perlindungan atas privasi dan keamanan informasi pribadi. Pengakuan tersebut diwujudkan melalui pemberian berbagai hak kepada subjek data, antara lain hak untuk mengetahui identitas pihak yang melakukan pemrosesan data, dasar hukum yang menjadi landasan pemrosesan, tujuan penggunaan data pribadi, serta hak untuk memperoleh akses terhadap data yang dimiliki.[23]

Selain itu, subjek data juga memiliki kewenangan untuk memperbaiki, memperbarui, membatasi, mengakhiri pemrosesan, menghapus, dan memusnahkan data pribadinya sesuai dengan ketentuan peraturan perundang-undangan. Undang-undang ini juga memberikan hak kepada subjek data untuk mencabut persetujuan yang telah diberikan sebelumnya serta mengajukan keberatan apabila pemrosesan data dilakukan tanpa dasar hukum yang sah atau bertentangan dengan ketentuan yang berlaku.[24]

Dalam kaitannya dengan tindak pidana *phishing*, perlindungan hukum tidak berhenti pada pengakuan terhadap hak-hak subjek data, tetapi juga diwujudkan melalui mekanisme penegakan hukum terhadap setiap bentuk penyalahgunaan data pribadi. Bab XVII Undang-Undang Nomor 27 Tahun 2022 mengatur ketentuan pidana bagi setiap orang yang secara melawan hukum memperoleh, mengakses, menggunakan, mengungkapkan, memalsukan, maupun menyebarluaskan data pribadi milik orang lain. Ketentuan tersebut menjadi dasar yuridis bagi aparat penegak hukum untuk menindak pelaku yang memanfaatkan data pribadi hasil *phishing* guna memperoleh keuntungan yang tidak sah atau menimbulkan kerugian bagi pihak lain.

Selain itu, pertanggungjawaban pidana, Undang-Undang Nomor 27 Tahun 2022 juga mengenal mekanisme penegakan hukum melalui sanksi administratif. Bentuk sanksi tersebut meliputi peringatan tertulis, penghentian sementara aktivitas pemrosesan data pribadi, penghapusan data pribadi, serta pengenaan denda administratif terhadap pengendali data pribadi maupun prosesor data pribadi yang tidak melaksanakan kewajiban hukumnya. Pengaturan tersebut mencerminkan penerapan prinsip akuntabilitas (*accountability*), yaitu prinsip yang mengharuskan setiap pihak yang memproses data pribadi bertanggung jawab untuk menjamin keamanan, kerahasiaan, dan integritas data sepanjang siklus pemrosesan berlangsung.[25]

---

[23] Rosihan Luthfi, "Perlindungan Data Pribadi Sebagai Perwujudan Perlindungan Hak Asasi Manusia," *Jurnal Sosial Teknologi* 2, no. 5 (2022): 431–36, https://doi.org/10.59188/jurnalsostech.v2i5.336.

[24] Irma Nurrizki Rahmawati et al., "Pertanggungjawaban Pihak Bank Terhadap Kebocoran Data Diri Nasabah," *Aufklarung: Jurnal Pendidikan, Sosial Dan Humaniora* 3, no. 2 (2023): 208–15.

[25] Ahmad Fauzi M, "Perkembangan Teknologi Dan Tantangan Hukum Dalam Penanganan Kejahatan Mayantara: Perspektif Hukum Pidana Dan Perlindungan Data Pribadi Di Indonesia," *Indonesian Journal of Law* 1, no. 12 (2024): 312–20.

Meskipun Undang-Undang Nomor 27 Tahun 2022 memberikan landasan hukum yang komprehensif mengenai perlindungan data pribadi, penanggulangan tindak pidana *phishing* tidak dapat hanya mengandalkan rezim hukum tersebut. Dalam praktiknya, perbuatan *phishing* sering kali memiliki karakteristik yang memenuhi unsur tindak pidana lain, khususnya tindak pidana di bidang informasi dan transaksi elektronik.

Penegakan hukum terhadap pelaku *phishing* juga dapat didasarkan pada Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, terutama terhadap perbuatan yang dilakukan melalui penyebaran informasi elektronik yang menyesatkan, manipulasi sistem elektronik, maupun penyalahgunaan media elektronik untuk memperoleh data pribadi secara melawan hukum. Dengan demikian, penanganan tindak pidana *phishing* pada dasarnya memerlukan penerapan ketentuan hukum secara komplementer antara UU PDP dan Undang-Undang Informasi dan Transaksi Elektronik agar perlindungan hukum terhadap korban dapat terlaksana secara lebih efektif.

3.4 Analisis Efektivitas Perlindungan Data Pribadi dalam Menghadapi Tindak Pidana *Phishing*

Pemberlakuan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menandai terbentuknya rezim hukum yang secara khusus mengatur perlindungan data pribadi di Indonesia. Kehadiran undang-undang ini tidak hanya memberikan legitimasi terhadap hak-hak subjek data pribadi, tetapi juga membebankan tanggung jawab hukum kepada Pengendali Data Pribadi dan Prosesor Data Pribadi dalam setiap tahapan pemrosesan data.

Kemudian, undang-undang tersebut mengatur mekanisme penegakan hukum melalui pengenaan sanksi administratif maupun sanksi pidana terhadap setiap pelanggaran yang berkaitan dengan penyalahgunaan data pribadi. Dari perspektif normatif, pengaturan tersebut menunjukkan adanya pembaruan hukum karena menghimpun berbagai ketentuan mengenai perlindungan data pribadi yang sebelumnya tersebar dalam sejumlah peraturan perundang-undangan ke dalam satu instrumen hukum yang lebih terpadu.

Namun demikian, keberadaan norma yang komprehensif belum tentu menjamin tercapainya perlindungan hukum yang optimal apabila implementasinya belum berjalan secara efektif. Oleh sebab itu, perlu dilakukan pengkajian mengenai sejauh mana Undang-Undang Nomor 27 Tahun 2022 mampu memberikan respons hukum terhadap perkembangan tindak pidana *phishing* yang semakin kompleks akibat pesatnya kemajuan teknologi informasi.

Penelitian ini memusatkan perhatian pada efektivitas penerapan Undang-Undang Perlindungan Data Pribadi dalam proses penegakan hukum terhadap tindak pidana *phishing*. Analisis dilakukan dengan mengidentifikasi berbagai hambatan yang masih dihadapi dalam praktik, antara lain kesulitan menelusuri identitas pelaku, pembuktian yang bergantung pada bukti elektronik, karakter kejahatan siber yang melintasi yurisdiksi negara (*cross-border crime*), serta rendahnya tingkat literasi digital masyarakat yang meningkatkan kerentanan terhadap penyalahgunaan data pribadi.

Selain mengkaji aspek implementasi, penelitian ini juga membandingkan ketentuan dalam Undang-Undang Nomor 27 Tahun 2022 dengan hasil penelitian terdahulu untuk menilai

sejauh mana regulasi tersebut mampu mengatasi permasalahan yang selama ini muncul dalam penanganan *phishing*. Berdasarkan hasil analisis tersebut, penelitian ini merumuskan sejumlah rekomendasi yang diarahkan pada penguatan sistem perlindungan data pribadi melalui penyempurnaan kebijakan, peningkatan kapasitas penegak hukum, penguatan tata kelola pemrosesan data pribadi, serta peningkatan literasi digital masyarakat. Langkah-langkah tersebut diharapkan mampu menciptakan perlindungan hukum yang lebih efektif, memberikan kepastian hukum, serta meningkatkan kemampuan sistem hukum nasional dalam menghadapi perkembangan modus *phishing* di era digital.

3.4.1 Kendala Penegakan Hukum terhadap Tindak Pidana Phishing

Walaupun Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi telah menghadirkan kerangka hukum yang lebih komprehensif dalam menjamin keamanan data pribadi, penerapannya di lapangan masih menghadapi berbagai tantangan. Salah satu persoalan yang paling dominan adalah kesulitan dalam mengungkap identitas pelaku *phishing*.

Modus operandi kejahatan ini umumnya memanfaatkan anonimitas di ruang siber melalui penggunaan identitas fiktif, jaringan privat virtual (*Virtual Private Network*/ *VPN*), server yang berlokasi di luar wilayah Indonesia, maupun akun digital yang sulit ditelusuri. Kondisi tersebut menyebabkan proses identifikasi pelaku menjadi lebih kompleks, termasuk dalam menentukan lokasi terjadinya tindak pidana dan yurisdiksi yang berwenang untuk melakukan penegakan hukum.

Kompleksitas tersebut semakin meningkat karena *phishing* sering dikategorikan sebagai kejahatan siber lintas batas negara (*cross-border crime*), di mana pelaku, korban, dan infrastruktur teknologi informasi dapat berada pada negara yang berbeda. Oleh sebab itu, efektivitas penanganannya sangat bergantung pada mekanisme kerja sama internasional, baik dalam pertukaran informasi, proses penyidikan, maupun pelaksanaan penegakan hukum..

Permasalahan lain yang tidak kalah penting berkaitan dengan aspek pembuktian. Dibandingkan dengan tindak pidana konvensional, pembuktian dalam perkara *phishing* bertumpu pada keberadaan alat bukti elektronik yang harus memenuhi persyaratan mengenai keaslian, integritas, dan validitas sesuai dengan ketentuan hukum acara pidana serta peraturan perundang-undangan di bidang informasi dan transaksi elektronik.

Pengumpulan serta analisis barang bukti digital juga memerlukan dukungan teknologi forensik digital dan sumber daya manusia yang memiliki kompetensi khusus. Dalam praktiknya, efektivitas proses tersebut masih dipengaruhi oleh belum optimalnya koordinasi antarlembaga, baik antara aparat penegak hukum, penyelenggara sistem elektronik, lembaga jasa keuangan, maupun instansi lain yang memiliki kewenangan terkait. Hambatan tersebut tampak dalam proses penelusuran transaksi elektronik, pemblokiran rekening atau akun digital, serta upaya pemulihan data maupun kerugian yang dialami korban.

Selain faktor penegakan hukum, tingkat literasi digital masyarakat turut menentukan efektivitas perlindungan data pribadi. Masih banyak pengguna layanan digital yang belum memahami karakteristik *phishing* maupun pentingnya menjaga kerahasiaan informasi pribadi, sehingga mereka lebih mudah menjadi sasaran manipulasi pelaku.

Rendahnya kesadaran tersebut menunjukkan bahwa keberhasilan implementasi Undang-Undang Nomor 27 Tahun 2022 tidak hanya ditentukan oleh kualitas pengaturan normatif, tetapi juga oleh kesiapan institusi penegak hukum, ketersediaan sarana pendukung, kapasitas sumber daya manusia, serta partisipasi aktif masyarakat dalam melindungi data pribadinya. Dengan demikian, penguatan perlindungan data pribadi memerlukan pendekatan yang bersifat menyeluruh melalui sinergi antara regulasi, penegakan hukum, pengembangan teknologi, dan peningkatan edukasi publik agar mampu menjawab dinamika kejahatan *phishing* yang terus berkembang.[26]

3.4.2 Upaya Penguatan Perlindungan Data Pribadi di Indonesia

Penguatan sistem perlindungan data pribadi dari ancaman tindak pidana *phishing* memerlukan kebijakan yang terintegrasi dan tidak hanya berorientasi pada pembentukan norma hukum. Efektivitas pelindungan data pribadi harus didukung melalui pembenahan regulasi, penguatan kelembagaan, pemanfaatan teknologi, serta peningkatan kesadaran masyarakat sebagai pengguna layanan digital. Dari sisi regulasi, implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi perlu dilengkapi dengan peraturan pelaksana yang mengatur secara lebih rinci tata kelola pemrosesan data pribadi, prosedur pelaporan insiden kebocoran data, serta standar keamanan informasi yang wajib dipenuhi oleh Pengendali Data Pribadi maupun Prosesor Data Pribadi.[27]

Selanjutnya, optimalisasi fungsi lembaga yang berwenang melakukan pengawasan terhadap pelindungan data pribadi menjadi kebutuhan yang mendesak agar mekanisme pengawasan, penegakan kepatuhan, dan penyelesaian sengketa dapat terlaksana secara konsisten. Keberadaan lembaga pengawas yang independen juga berperan penting dalam meningkatkan kepastian hukum sekaligus memperkuat kepercayaan publik terhadap sistem pelindungan data pribadi di Indonesia.

Pada aspek penegakan hukum, peningkatan kualitas sumber daya manusia menjadi faktor yang tidak dapat diabaikan. Aparat penegak hukum perlu dibekali kompetensi di bidang forensik digital, investigasi kejahatan siber, serta penanganan alat bukti elektronik agar mampu menghadapi kompleksitas tindak pidana *phishing*. Selain itu, sinergi antarlembaga perlu diperkuat melalui kerja sama yang melibatkan penyelenggara sistem elektronik, lembaga jasa keuangan, dan mitra internasional, mengingat kejahatan *phishing* kerap memiliki dimensi lintas yurisdiksi. Bersamaan dengan itu, peningkatan literasi digital masyarakat harus dilakukan secara berkesinambungan melalui edukasi mengenai berbagai modus *phishing*, pentingnya menjaga kerahasiaan data pribadi, serta prosedur pelaporan apabila mengalami atau mengetahui adanya dugaan kejahatan siber.[28]

Berdasarkan hasil analisis dalam penelitian ini, perlindungan data pribadi tidak cukup diwujudkan melalui pendekatan represif berupa penjatuhan sanksi terhadap pelaku. Perlindungan yang efektif juga memerlukan langkah-langkah preventif yang melibatkan seluruh pemangku kepentingan, termasuk pemerintah, pelaku usaha, penyelenggara

---

[26] Rompi and Muaja, "Tindak Kejahatan Siber Di Sektor Jasa Keuangan Dan Perbankan."

[27] Luthfi, "Perlindungan Data Pribadi Sebagai Perwujudan Perlindungan Hak Asasi Manusia."

[28] George Anderson Tirta and Gunardi Lie, "Tinjauan Hukum Terhadap Tindak Pidana Cybercrime Dan Upaya Pencegahannya (Studi Kasus Peretasan Data Pengguna Bank BSI)," *MANTAP: Journal of Management Accounting, Tax and Production* 2, no. 1 (2024): 240–49, https://doi.org/10.57235/mantap.v2i1.1634.

sistem elektronik, lembaga penegak hukum, dan masyarakat. Kolaborasi tersebut diharapkan mampu memperkuat implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi sehingga perlindungan terhadap hak-hak subjek data dapat terlaksana secara lebih optimal. Pada saat yang sama, upaya tersebut akan meningkatkan kesiapan sistem hukum nasional dalam merespons perkembangan kejahatan siber yang semakin dinamis di era digital.

4. KESIMPULAN

Hasil penelitian ini menunjukkan bahwa Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi telah membentuk landasan yuridis yang penting bagi penyelenggaraan sistem perlindungan data pribadi di Indonesia, termasuk dalam merespons ancaman tindak pidana *phishing*. Pengaturan yang termuat dalam undang-undang tersebut tidak hanya memberikan pengakuan terhadap hak-hak subjek data pribadi, tetapi juga menetapkan tanggung jawab hukum bagi Pengendali Data Pribadi dan Prosesor Data Pribadi, disertai mekanisme penegakan hukum melalui sanksi administratif maupun sanksi pidana terhadap setiap bentuk penyalahgunaan data pribadi.

Apabila dibandingkan dengan pengaturan sebelumnya yang tersebar dalam berbagai peraturan perundang-undangan, keberadaan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menghadirkan sistem pengaturan yang lebih terpadu dan memberikan kepastian hukum yang lebih baik. Namun demikian, mengingat *phishing* merupakan bentuk kejahatan siber yang terus berkembang seiring dengan kemajuan teknologi informasi, perlindungan hukum terhadap korban tidak dapat hanya mengandalkan ketentuan dalam UU PDP. Penegakan hukum juga memerlukan penerapan secara harmonis dengan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta ketentuan dalam Kitab Undang-Undang Hukum Pidana.

Penelitian ini juga menemukan bahwa efektivitas perlindungan data pribadi tidak hanya ditentukan oleh keberadaan norma hukum, tetapi dipengaruhi oleh berbagai faktor yang berkaitan dengan implementasinya. Kemampuan aparat penegak hukum dalam melakukan investigasi dan pembuktian berbasis bukti elektronik, efektivitas koordinasi antarlembaga, karakter *cross-border crime* yang melekat pada kejahatan siber, serta tingkat literasi digital masyarakat merupakan faktor-faktor yang menentukan keberhasilan penerapan Undang-Undang Nomor 27 Tahun 2022.

Penguatan sistem perlindungan data pribadi perlu dilakukan melalui peningkatan kapasitas institusi penegak hukum, pengembangan kemampuan forensik digital, optimalisasi koordinasi antara pemerintah, penyelenggara sistem elektronik, dan lembaga terkait, serta perluasan edukasi kepada masyarakat mengenai keamanan data pribadi dan bahaya *phishing*. Upaya tersebut diharapkan mampu mendukung terwujudnya tujuan pembentukan Undang-Undang Nomor 27 Tahun 2022, yaitu memberikan kepastian

hukum, menjamin perlindungan terhadap hak-hak subjek data pribadi, serta membangun ekosistem digital nasional yang aman, terpercaya, dan bertanggung jawab.[29]

UCAPAN TERIMAKASIH

Penulis mengucapkan penghargaan dan rasa terima kasih yang sebesar-besarnya kepada dosen pembimbing atas segala arahan, masukan, serta pendampingan akademik yang diberikan selama proses penyusunan artikel ini. Apresiasi juga disampaikan kepada Fakultas Hukum Universitas Malikussaleh yang telah menyediakan lingkungan akademik yang mendukung terlaksananya penelitian ini. Selain itu, penulis menyampaikan rasa terima kasih kepada keluarga dan rekan-rekan yang senantiasa memberikan semangat, dukungan moral, serta motivasi selama seluruh tahapan penelitian hingga penyusunan artikel dapat diselesaikan. Penulis juga menegaskan bahwa penelitian ini dilaksanakan secara independen tanpa memperoleh bantuan atau dukungan pendanaan dari instansi pemerintah, sektor swasta, maupun organisasi lainnya.

DAFTAR PUSTAKA

Alghamdi, M. I. "A Descriptive Study on the Impact of Cybercrime and Possible Measures to Curtail Its Spread Worldwide." *International Journal of Engineering Research and Technology* 9 (2020): 731–35.

Anggen Suari KR, Sarjana IM. Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. JAH [Internet]. 2023Apr.25 [cited 2026Aug.5];6(1):132-4. https://doi.org/10.38043/jah.v6i1.4484

Aprilianti, A. (2024). Efektivitas dan Implementasi Undang-Undang Informasi dan Transaksi Elektronik sebagai Hukum Siber di Indonesia: Tantangan dan Solusi. *Begawan Abioso*, *15*(1), 41–50. https://doi.org/10.37893/abioso.v15i1.1002.

Arctic Wolf. "A Brief History of Cybercrime." www.arcticwolf.com, 2024. https://arcticwolf.com/resources/blog/decade-of-cybercrime/.

Chang, Yun-chien. "The Empirical Foundation of Normative Arguments in Legal Reasoning." *European Journal of Empirical Legal Studies* 1, no. 1 (2024): 69–88. https://doi.org/https://doi.org/10.62355/ejels.18070.

Choi, K. S, C. S Lee, and E. R Louderback. *Historical Evolutions of Cybercrime*. UK: Palgrave Macmillan, 2020.

Christiani, Theresia Anita. "Normative and Empirical Research Methods: Their Usefulness and Relevance in the Study of Law as an Object." *Procedia-Social and Behavioral Sciences* 219 (2016): 201–7. https://doi.org/http://dx.doi.org/10.1016/j.sbspro.2016.05.006.

D. Solak and M. Topaloglu. "The Perception Analysis of Cyber Crimes in View of Computer Science Students." *Procedia - Social and Behavioral Sciences* 182 (n.d.): 590–595. https://doi.org/10.1016/j.sbspro.2015.04.787.

[29] Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820, bagian Menimbang dan Penjelasan Umum.

Dewi, Maharani Chandra. "Cyber Espionage in National and Global Perspective: How Indonesia Deal with This Issue?" *International Law Discourse in Southeast Asia* 1, no. 1 (2022): 1–22. https://doi.org/https://doi.org/10.15294/ildisea.v1i1.56874.

Ghozali, Muhammad, Nora Liana, Cut Afra, Zulfadly Siregar, Nurfahni, Malahayati, and Muhammad Hatta. "Kejahatan Siber (Cyber Crime) Dan Implikasi Hukumnya: Studi Kasus Peretasan Bank Syariah Indonesia (BSI)." *Cendekia : Jurnal Hukum, Sosial Dan Humaniora* 2, no. 4 (2024): 797–809. https://doi.org/https://doi.org/10.5281/zenodo.13883603.

ISTR. "Internet Security Threat Report - ISTR." *Symantec Journal* 22, no. April (2017): 77. https://doi.org/10.1016/S1353-4858(05)00194-7.

Luthfi, Rosihan. "Perlindungan Data Pribadi Sebagai Perwujudan Perlindungan Hak Asasi Manusia." *Jurnal Sosial Teknologi* 2, no. 5 (2022): 431–36. https://doi.org/10.59188/jurnalsostech.v2i5.336.

M, Ahmad Fauzi. "Perkembangan Teknologi Dan Tantangan Hukum Dalam Penanganan Kejahatan Mayantara: Perspektif Hukum Pidana Dan Perlindungan Data Pribadi Di Indonesia." *Indonesian Journal of Law* 1, no. 12 (2024): 312–20.

Nahak, S. "Hukum Tindak Pidana Mayantara (Cybercrime) Dalam Prespektif Akademik." *Jurnal Hukum Prasada* 4, no. 1 (2017): 1–11.

Nkgapele, Simon Matome, and Regina Mapula Mokgolobotho. "Developing Transformational Strategies to Improve the Accessibility of E-Governmental Services in the South African Local Government." *International Journal of Law, Social Science, and Humanities (IJLSH)* 1, no. 2 (2024): xxx.

Papilaya, Ensalina, Sari Murti Widiyastuti, and Husni. "Adoption of Hardship Clauses in Indonesia's Contract Law Reform System." *International Journal of Law, Social Science, and Humanities* 3, no. 2 (2026): 529–535. https://doi.org/https://doi.org/10.70193/ijlsh.v3i2.302.

Rahmawati, Irma Nurrizki, Nova Rahmadani, Diyah Rosita Heni, and Sandro Kevin. "Pertanggungjawaban Pihak Bank Terhadap Kebocoran Data Diri Nasabah." *Aufklarung: Jurnal Pendidikan, Sosial Dan Humaniora* 3, no. 2 (2023): 208–15.

Raodia, Raodia. "Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (Cybercrime)." *Jurisprudentie : Jurusan Ilmu Hukum Fakultas Syariah Dan Hukum* 6, no. 2 (2019): 39. https://doi.org/10.24252/jurisprudentie.v6i2.11399.

Rompi, Tonny, and Harly Stanly Muaja. "Tindak Kejahatan Siber Di Sektor Jasa Keuangan Dan Perbankan." *Lex Privatum* 9, no. 4 (2021): 183–92.

Tirta, George Anderson, and Gunardi Lie. "Tinjauan Hukum Terhadap Tindak Pidana Cybercrime Dan Upaya Pencegahannya (Studi Kasus Peretasan Data Pengguna Bank BSI)." *MANTAP: Journal of Management Accounting, Tax and Production* 2, no. 1 (2024): 240–49. https://doi.org/10.57235/mantap.v2i1.1634.

Zulfan. "Cybercrime in Virtual Spaces: An Overview of the Law in Indonesia." *International Journal of Law, Social Science, and Humanities (IJLSH)* 1, no. 1 (2024): 18–26. https://doi.org/https://doi.org/10.70193/ijlsh.v1i1.140.

Abella, Inoi, Piawan Andarasi Manullang, Syahira Rahmania Putri Nurjani, Salsabila Astrid Alma, dan Shela Cahaya Putri. "Globalisasi Teknologi dan Informasi terhadap Masyarakat Hukum Indonesia: Urgensi dan Peran Undang-Undang ITE." *Milthree Law Journal*, Vol. 2, No. 2, Juli 2025, hlm. 183–217. https://doi.org/10.70565/mlj.v2i2.38.

Agustin, Selfina. "Dampak Kemajuan Teknologi Informasi Era Digital terhadap Keamanan Data Pribadi: Tantangan dan Penanggulangan terhadap Kejahatan *Cyber*." *Jurnal Penelitian Multidisiplin Bangsa*, Vol. 1, No. 6, 2024. https://doi.org/10.59837/jpnmb.v1i6.93.

Anggen Suari KR, Sarjana IM. Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. JAH [Internet]. 2023Apr.25 [cited 2026Aug.5];6(1):132-4. https://doi.org/10.38043/jah.v6i1.4484

Aprilianti, A. (2024). Efektivitas dan Implementasi Undang-Undang Informasi dan Transaksi Elektronik sebagai Hukum Siber di Indonesia: Tantangan dan Solusi. *Begawan Abioso*, *15*(1), 41–50. https://doi.org/10.37893/abioso.v15i1.1002.

Arctic Wolf. "A Brief History of Cybercrime." www.arcticwolf.com, 2024. https://arcticwolf.com/resources/blog/decade-of-cybercrime/.

Chang, Yun-chien. "The Empirical Foundation of Normative Arguments in Legal Reasoning." *European Journal of Empirical Legal Studies* 1, no. 1 (2024): 69–88. https://doi.org/https://doi.org/10.62355/ejels.18070.

Choi, K. S, C. S Lee, and E. R Louderback. *Historical Evolutions of Cybercrime*. UK: Palgrave Macmillan, 2020.

Christiani, Theresia Anita. "Normative and Empirical Research Methods: Their Usefulness and Relevance in the Study of Law as an Object." *Procedia-Social and Behavioral Sciences* 219 (2016): 201–7. https://doi.org/http://dx.doi.org/10.1016/j.sbspro.2016.05.006.

D. Solak and M. Topaloglu. "The Perception Analysis of Cyber Crimes in View of Computer Science Students." *Procedia - Social and Behavioral Sciences* 182 (n.d.): 590–595. https://doi.org/10.1016/j.sbspro.2015.04.787.

Dewi, Maharani Chandra. "Cyber Espionage in National and Global Perspective: How Indonesia Deal with This Issue?" *International Law Discourse in Southeast Asia* 1, no. 1 (2022): 1–22. https://doi.org/https://doi.org/10.15294/ildisea.v1i1.56874.

Ghozali, Muhammad, Nora Liana, Cut Afra, Zulfadly Siregar, Nurfahni, Malahayati, and Muhammad Hatta. "Kejahatan Siber (Cyber Crime) Dan Implikasi Hukumnya: Studi Kasus Peretasan Bank Syariah Indonesia (BSI)." *Cendekia : Jurnal Hukum, Sosial Dan Humaniora* 2, no. 4 (2024): 797–809. https://doi.org/https://doi.org/10.5281/zenodo.13883603.

ISTR. "Internet Security Threat Report - ISTR." *Symantec Journal* 22, no. April (2017): 77. https://doi.org/10.1016/S1353-4858(05)00194-7.

Luthfi, Rosihan. "Perlindungan Data Pribadi Sebagai Perwujudan Perlindungan Hak Asasi Manusia." *Jurnal Sosial Teknologi* 2, no. 5 (2022): 431–36. https://doi.org/10.59188/jurnalsostech.v2i5.336.

M, Ahmad Fauzi. "Perkembangan Teknologi Dan Tantangan Hukum Dalam Penanganan

Kejahatan Mayantara: Perspektif Hukum Pidana Dan Perlindungan Data Pribadi Di Indonesia." *Indonesian Journal of Law* 1, no. 12 (2024): 312–20.

Nahak, S. "Hukum Tindak Pidana Mayantara (Cybercrime) Dalam Prespektif Akademik." *Jurnal Hukum Prasada* 4, no. 1 (2017): 1–11.

Nkgapele, Simon Matome, and Regina Mapula Mokgolobotho. "Developing Transformational Strategies to Improve the Accessibility of E-Governmental Services in the South African Local Government." *International Journal of Law, Social Science, and Humanities (IJLSH)* 1, no. 2 (2024): xxx.

Papilaya, Ensalina, Sari Murti Widiyastuti, and Husni. "Adoption of Hardship Clauses in Indonesia's Contract Law Reform System." *International Journal of Law, Social Science, and Humanities* 3, no. 2 (2026): 529–535. https://doi.org/https://doi.org/10.70193/ijlsh.v3i2.302.

Rahmawati, Irma Nurrizki, Nova Rahmadani, Diyah Rosita Heni, and Sandro Kevin. "Pertanggungjawaban Pihak Bank Terhadap Kebocoran Data Diri Nasabah." *Aufklarung: Jurnal Pendidikan, Sosial Dan Humaniora* 3, no. 2 (2023): 208–15.

Raodia, Raodia. "Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (Cybercrime)." *Jurisprudentie : Jurusan Ilmu Hukum Fakultas Syariah Dan Hukum* 6, no. 2 (2019): 39. https://doi.org/10.24252/jurisprudentie.v6i2.11399.

Rompi, Tonny, and Harly Stanly Muaja. "Tindak Kejahatan Siber Di Sektor Jasa Keuangan Dan Perbankan." *Lex Privatum* 9, no. 4 (2021): 183–92.

Tirta, George Anderson, and Gunardi Lie. "Tinjauan Hukum Terhadap Tindak Pidana Cybercrime Dan Upaya Pencegahannya (Studi Kasus Peretasan Data Pengguna Bank BSI)." *MANTAP: Journal of Management Accounting, Tax and Production* 2, no. 1 (2024): 240–49. https://doi.org/10.57235/mantap.v2i1.1634.

Zulfan. "Cybercrime in Virtual Spaces: An Overview of the Law in Indonesia." *International Journal of Law, Social Science, and Humanities (IJLSH)* 1, no. 1 (2024): 18–26. https://doi.org/https://doi.org/10.70193/ijlsh.v1i1.140.

Hadiyati, Nur; Stathany, Hayllen. Analisis Undang-Undang Ite Berdasarkan Asas Pembentukan Peraturan Perundang-Undangan Di Indonesia. *Mizan: Jurnal Ilmu Hukum* 10, NO. 2, (2021). https://doi.org/10.32503/mizan.v10i2.1657.

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

Lubis, Hendarman, Dipa Teruna Awaludin, Dyan Prawita Sari, Lisa Astria Milasari, dan Sofyan. "Edukasi Keamanan Siber: Pelatihan Dasar Mengenali *Phishing* dan Proteksi Data Pribadi di Dunia Digital." *JIPITI: Jurnal Pengabdian kepada Masyarakat*, Vol. 2, No. 2, Mei 2025, hlm. 101–105. https://jipiti.technolabs.co.id/index.php/pkm/article/view/46

Mutiara, Upik, dan Romi Maulana. "Perlindungan Data Pribadi sebagai Bagian dari Hak Asasi Manusia atas Perlindungan Diri Pribadi." *Indonesian Journal of Law and Policy Studies*, Vol. 1, No. 1, Mei 2020, hlm. 42–54. https://doi.org/10.31000/ijlp.v1i1.2648.

Putra Y., Vikran Fasyadhiyaksa. "Modus Operandi Tindak Pidana Phishing Menurut UU ITE." *Jurnal Hukum*, Edisi No. 6, Vol. 4, Fakultas Hukum Universitas Airlangga, 2021. https://doi.org/10.36859/jdh.v6i2.2881

Rachmawati, Dian. "Phising Sebagai Salah Satu Bentuk Ancaman dalam Dunia Cyber." *Jurnal Saintkom* 13, no. 3 (2014): 211–218.

Rohmy, Atikah Mardhiya, Teguh Suratman, dan Arini Indah Nihayaty. "UU ITE dalam Perspektif Perkembangan Teknologi Informasi dan Komunikasi." *DAKWATUNA: Jurnal Dakwah dan Komunikasi Islam*, Vol. 7, No. 2, Agustus 2021.

Sadya, Sarnita. "Ada 164.131 Kasus Email *Phishing* di Indonesia pada 2022." *DataIndonesia.id*. Accessed July 26, 2026. https://dataindonesia.id/internet/detail/ada-164131-kasus-email-phising-di-indonesia-pada-2022.

Saputra, Dwi Fajar. "Literasi Digital untuk Perlindungan Data Pribadi." *Jurnal Ilmu Kepolisian*, Vol. 17, No. 3, Desember 2023, hlm. 509–516. https://doi.org/10.35879/jik.v17i3.454

Setiawan, Hezkiel Bram, dan Fatma Ulfatun Najicha. "Perlindungan Data Pribadi Warga Negara Indonesia Terkait dengan Kebocoran Data." *Jurnal Kewarganegaraan*, Vol. 6, No. 1, Juni 2022, hlm. 976. https://doi.org/10.31316/jk.v6i1.2657

Suratman, and Philips Dilla. *Metode Penelitian Hukum*. Bandung: Alfabeta, 2015.

Wahyuningtias, Nur Aini. "Analisis Normatif Perlindungan Hukum terhadap Korban Kejahatan Siber dalam Modus *Phishing* Rekening Bank di Indonesia." *Judge: Jurnal Hukum*, Vol. 6, No. 6, 2025, hlm. 1972. https://doi.org/10.54209/judge.v6i06.1564

Widianingrum, Afifah Rizqy. "Analisis Implementasi Kebijakan Hukum Terhadap Penanganan Kejahatan Siber Di Era Digital." Journal Iuris Scientia 2, no. 2 (2024): 90–102. https://doi.org/10.62263/jis.v2i2.40.

Wiranata, Ganda Arisandi, Yoyok Ucuk Subekti, dan Dudik Djaja Sidarta. "Pertanggungjawaban Pidana terhadap Pelaku Tindak Pidana Phishing." *Jurnal Penelitian Hukum*, Vol. 4, No. 2, Maret 2024. https://doi.org/10.36859/jdh.v6i2.2881

Yurita, Irma, M. Kevin Ramadhan, dan M. Candra. "Pengaruh Kemajuan Teknologi terhadap Perkembangan Tindak Pidana *Cybercrime* (Studi Kasus *Phising* sebagai Ancaman Keamanan Digital)." *Jurnal Hukum Legalita*, Vol. 5, No. 2, 2023, hlm. 143–155. https://doi.org/10.47637/legalita.v5i2.995.