



## Kajian Hukum Tindak Pidana *Cyber Phising* Ditinjau dari Undang-Undang Nomor 27 Tahun 2022 Tentang Data Pribadi

Putu Ryanniva Karenina

Ilmu Hukum, Universitas Pendidikan Ganesha, Indonesia

Penulis Korespondensi: [ryanniva@student.undiksha.ac.id](mailto:ryanniva@student.undiksha.ac.id)

**Abstract:** *This study aims to evaluate the effectiveness of implementing Law Number 27 of 2022 concerning Personal Data Protection in Indonesia's efforts to prevent and combat phishing crimes. This research employs a normative legal method to analyze the implementation of the PDP Law in the context of preventing and combating phishing crimes. The findings indicate that the PDP Law has provided a comprehensive legal framework for protecting personal data, including data that is often targeted by phishing attacks. The implementation of the PDP Law is overseen by the Personal Data Protection Authority, which has the authority to impose administrative sanctions, support law enforcement processes, and evaluate cross-border data transfers. To achieve maximum effectiveness in combating phishing crimes, strong synergy is needed between the government, private sector, and the public. The PDP Law has provided a good legal framework, but the success of its implementation is highly dependent on the commitment of all parties to work together in protecting personal data.*

**Keywords:** *Administrative Sanctions; Government; Law Enforcement; Personal Data,; Phishing.*

**Abstrak:** Penelitian ini bertujuan untuk mengevaluasi efektivitas implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dalam upaya pemerintah Indonesia untuk mencegah dan menanggulangi tindak pidana phishing. Penelitian ini menerapkan metode hukum normatif untuk menganalisis implementasi UU PDP dalam konteks pencegahan dan penanggulangan tindak pidana phishing. Hasil kajian menunjukkan bahwa UU PDP telah memberikan kerangka hukum yang komprehensif dalam melindungi data pribadi, termasuk data yang sering menjadi target serangan phishing. Pelaksanaan UU PDP berada di bawah pengawasan Lembaga Otoritas Perlindungan Data Pribadi yang memiliki kewenangan untuk memberikan sanksi administratif, mendukung proses penegakan hukum, serta mengevaluasi transfer data lintas negara. Untuk mencapai efektivitas yang maksimal dalam menanggulangi kejahatan phishing, diperlukan sinergi yang kuat antara pemerintah, lembaga swasta, dan masyarakat. UU PDP telah memberikan kerangka hukum yang baik, namun keberhasilan implementasinya sangat bergantung pada komitmen semua pihak untuk bekerja sama dalam melindungi data pribadi.

**Kata kunci:** Data Pribadi; Pemerintah; Penegakan Hukum; Phising; Sanksi Administratif.

### 1. LATAR BELAKANG

Kehadiran internet telah membuka peluang baru dan memperkaya kehidupan manusia di berbagai bidang, seperti komunikasi, bisnis, dan pendidikan. Kemajuan teknologi dan akses informasi yang lebih mudah juga berkontribusi pada peningkatan peluang serta persaingan di masyarakat. Jika tidak mau tertinggal, masyarakat harus mau meninggalkan kebiasaan lama dan mengadopsi gaya hidup yang lebih modern (Marunung dkk, 2022).

Sebagai platform digital yang serba bisa, internet mendukung beragam kegiatan, mulai dari *e-commerce*, *e-learning*, hingga *e-government*. Kemampuan internet dalam mengelola data secara efisien telah memberikan manfaat yang besar bagi perusahaan dan masyarakat (Setiawan dkk, 2022). Sebagian besar penduduk Indonesia telah mengadopsi internet sebagai alat untuk berbagai aktivitas, mulai dari komunikasi hingga bisnis. Data survei APJII 2016 menunjukkan bahwa penetrasi internet di Indonesia sangat tinggi, terutama di Pulau Jawa.

Sebanyak 97,4% pengguna internet di Indonesia aktif bermain di media sosial, dan persentase yang hampir sama juga menggunakan internet untuk hiburan dan akses berita.

Pesatnya perkembangan teknologi telah melahirkan beragam bentuk kejahatan siber yang semakin kompleks dan sulit untuk dideteksi. Kejahatan siber tidak hanya terbatas pada peretasan atau penipuan kartu kredit, tetapi juga mencakup berbagai jenis pelanggaran lainnya yang memanfaatkan teknologi. Jenis kejahatan siber ini meliputi upaya untuk menembus sistem keamanan (probe), pemindaian sistem secara menyeluruh (scan), pengambilalihan akun pengguna (account compromise), pengambilalihan kendali penuh atas sistem (root compromise), serangan yang menyebabkan layanan tidak dapat diakses (denial of service), serta penyalahgunaan nama domain (Saputra dkk, 2023). Kejahatan siber seperti penyebaran spam dan penipuan seringkali diawali dengan pencurian data pribadi. Hal ini dapat menyebabkan korban mengalami kerugian uang dan nama baik. teknik phishing seringkali digunakan oleh pelaku pencurian data untuk memanfaatkan informasi yang sudah dicuri. Oleh karena itu pemerintah bertanggung jawab secara konstitusional untuk melindungi hak privasi warga negara dengan menerapkan undang-undang perlindungan data pribadi secara konsisten (Priliasari, 2023).

*Phishing* merupakan teknik penipuan siber yang bertujuan untuk merayu korban agar menyerahkan informasi pribadi secara sukarela. Informasi yang menjadi target phishing mencakup data identitas, kredensial akun, dan data finansial. Istilah ini berasal dari kata "fishing" yang mengibaratkan upaya "menangkap" korban dengan umpan palsu.

*Phishing* adalah kejahatan siber yang menggunakan teknik rekayasa sosial untuk membujuk korban agar menyerahkan informasi sensitif secara sukarela. Pelaku phishing, atau phishers, biasanya menyamar sebagai entitas yang dikenal dan dipercaya korban, seperti bank atau layanan email populer, melalui email, pesan teks, atau situs web palsu. Pelaku phishing menerapkan beragam teknik rekayasa sosial, seperti spear phishing dan website cloning, untuk memanipulasi korban agar mengungkapkan *kredensial login* dan informasi sensitif lainnya. Setelah berhasil mendapatkan informasi pribadi korban melalui *phishing*, para pelaku kejahatan siber dapat menyalahgunakan data tersebut untuk melakukan berbagai tindakan kriminal, termasuk mencuri identitas, melakukan penipuan kartu kredit, dan jenis penipuan finansial lainnya (Sutarli dkk, 2023).

Kejahatan siber berupa phishing melalui platform WhatsApp, seperti yang dilakukan oleh modus operandi Rediroff.ru, masih terus menjadi ancaman yang signifikan. Pelaku kejahatan ini menggunakan teknik rekayasa sosial yang semakin canggih untuk memperoleh data pribadi dan keuangan pengguna secara ilegal (Marunung dkk, 2022). Modus operandi

penipuan ini biasanya dimulai dengan mengirimkan tautan yang mengklaim korban telah memenangkan hadiah atau mengajak mereka untuk mengikuti survei. Namun, ketika diklik, tautan tersebut akan mengarahkan korban ke situs palsu yang dirancang untuk mencuri data pribadi seperti nama, alamat, dan informasi perbankan. Informasi pribadi yang berhasil dicuri oleh pelaku phishing dapat disalahgunakan untuk melakukan berbagai tindakan kejahatan, seperti mencuri identitas, melakukan penipuan finansial, mengirim spam, menyebarkan virus, atau bahkan mengambil alih perangkat korban secara jarak jauh. Modus penipuan ini seringkali disesuaikan dengan lokasi geografis korban untuk meningkatkan keberhasilannya. Pengguna WhatsApp disarankan untuk proaktif dalam menjaga keamanan data pribadi mereka. Jika menerima tautan mencurigakan seperti Rediroff.ru, segera hapus pesan tersebut dan laporkan. Jika tidak sengaja mengklik tautan tersebut, segera lakukan pemindaian menyeluruh pada perangkat untuk mendeteksi dan menghapus potensi malware atau aplikasi berbahaya yang mungkin telah terpasang (Marunung dkk, 2022).

Artikel ini akan mengkaji secara mendalam peran penting Undang-Undang Perlindungan Data Pribadi dalam upaya melindungi masyarakat Indonesia dari ancaman kejahatan siber, khususnya phishing. Pembahasan akan mencakup kontribusi undang-undang ini dalam menjaga privasi individu, serta strategi pencegahan yang efektif untuk menghindari penyalahgunaan data pribadi. Tujuan utama dari tulisan ini adalah untuk meningkatkan kesadaran masyarakat dan organisasi akan pentingnya perlindungan data pribadi di era digital.

## **2. KAJIAN TEORITIS**

Dalam konteks kejahatan teknologi informasi, phishing merupakan salah satu bentuk kejahatan yang semakin merajalela dan mengancam keamanan digital baik di Indonesia maupun di tingkat global. Secara teori, phishing dapat dipahami sebagai metode penipuan di dunia maya yang bertujuan memperoleh data pribadi, seperti username, password, maupun informasi keuangan korban secara ilegal (Marunung dkk, 2022). Phishing termasuk dalam kategori social engineering, yang memanfaatkan kepolosan dan ketidakwaspadaan korban untuk mengelabui mereka agar mengungkapkan data sensitif melalui email palsu, situs web palsu, atau pesan digital lainnya.

Teori komunikasi dan psikologi sosial menyatakan bahwa keberhasilan phishing sangat bergantung pada aspek psikologis korban, seperti rasa takut, kepercayaan, dan ketertarikan terhadap tawaran tertentu (Priliasari, 2023). Selain itu, perkembangan teknologi dan metode baru dalam kejahatan siber, seperti spear phishing dan whaling, menunjukkan bahwa para

pelaku semakin cerdas dalam menyesuaikan taktik mereka agar tampak lebih meyakinkan dan personal.

Dari sudut pandang hukum, keberadaan regulasi seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia menjadi landasan utama dalam penanggulangan kejahatan siber, termasuk phishing. UU ITE memberikan dasar hukum untuk menjerat pelaku kejahatan siber yang merugikan korban secara finansial dan reputasi. Namun, literatur juga menunjukkan bahwa efektivitas UU ITE dalam konteks penanganan phishing masih menghadapi tantangan, terutama terkait ketidakjelasan definisi dan potensi penyalahgunaan regulasi tersebut.

Secara umum, literatur menegaskan bahwa penanggulangan phishing tidak cukup hanya mengandalkan regulasi hukum semata, tetapi juga membutuhkan pendekatan pencegahan yang komprehensif. Upaya ini meliputi peningkatan kapasitas lembaga penegak hukum, edukasi masyarakat, dan kolaborasi lintas sektor antara pemerintah dan industri teknologi (Suari dkk, 2023). Pendekatan holistik ini penting agar ancaman phishing dapat diminimalisasi secara efektif, mengingat kejahatan ini terus berkembang dan menyesuaikan diri dengan evolusi teknologi digital.

Kajian pustaka ini menegaskan bahwa phishing merupakan fenomena kejahatan siber yang kompleks dan memerlukan penanganan yang tidak hanya bersifat hukum formal, tetapi juga melibatkan edukasi dan kerjasama strategis untuk melindungi hak-hak individu serta menjaga keamanan dunia maya secara menyeluruh.

### **3. METODE PENELITIAN**

Penelitian ini menggunakan metode penelitian hukum normatif, yaitu pendekatan yang berfokus pada analisis norma-norma hukum yang berlaku di masyarakat, baik yang tertulis dalam peraturan perundang-undangan maupun yang tidak tertulis, seperti prinsip-prinsip etika dan moral. Metode ini bertujuan untuk memahami aturan hukum yang berhubungan, mengevaluasinya, serta mengenali bagaimana praktik tersebut diimplementasikan dan menemukan hambatan yang mungkin terjadi. Dalam kajian ini, data dan informasi dikumpulkan melalui studi kepustakaan, yang meliputi pengumpulan bahan hukum primer, sekunder, dan tersier. Bahan hukum primer terdiri dari Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, peraturan pelaksana, dan dokumen resmi lainnya. Bahan hukum sekunder terdiri dari buku, artikel ilmiah, serta penelitian terdahulu yang relevan, sedangkan bahan hukum tersier berupa kamus hukum dan sumber penunjang lainnya.

#### 4. HASIL DAN PEMBAHASAN

##### **Regulasi Pencegahan Tindak Pidana *Cyber Phising* dalam Undang-Undang Nomor 27 Tahun 2022**

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menjadi dasar hukum yang krusial untuk melindungi data pribadi warga Indonesia serta mencegah kejahatan siber, seperti phishing. Phishing merupakan serangan siber yang memanfaatkan rekayasa sosial untuk menipu korban agar mengungkapkan data pribadi yang dapat mengakibatkan kerugian finansial, pelanggaran privasi, atau bahkan kerusakan reputasi. Dalam hal ini, UU PDP berfungsi sebagai langkah penting untuk melindungi hak privasi individu dan memberikan kejelasan dalam penegakan hukum terhadap para pelaku phishing.

Undang-undang Perlindungan Data Pribadi (UU PDP) menuntut perusahaan untuk bertanggung jawab atas keamanan data pribadi kita. Pasal 39 UU PDP mewajibkan mereka untuk menerapkan sistem keamanan yang memadai untuk mencegah akses tidak sah, termasuk serangan phishing. Hal ini terjadi karena para pelaku phising sering memanfaatkan celah dalam sistem untuk mengambil informasi pribadi seperti nama, nomor identitas, kata sandi, serta data sensitif lainnya.

Selain itu, UU ini mengharuskan pengendali data untuk segera memberitahukan subjek data jika terjadi pelanggaran perlindungan data, seperti kebocoran informasi akibat serangan phishing sesuai dengan Pasal 46 UU PDP. Tujuan dari ketentuan ini adalah untuk menciptakan transparansi dan memungkinkan subjek data untuk segera mengambil tindakan perbaikan, seperti mengganti kata sandi, membatasi akses tertentu, atau melaporkan insiden kepada pihak berwenang.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menempatkan hak subjek data sebagai elemen fundamental dalam upaya perlindungan privasi di era digital. Pasal 5 hingga Pasal 15 UU PDP memberikan jaminan atas berbagai hak, seperti hak akses, hak perbaikan, hak penghapusan, dan hak pembatasan pemrosesan data pribadi, yang secara langsung memperkuat posisi hukum individu dalam mengendalikan data pribadinya. Keberadaan hak-hak tersebut menjadi sangat relevan dalam konteks pencegahan kejahatan phishing, karena memungkinkan korban untuk segera mengambil langkah korektif ketika terjadi penyalahgunaan data, sehingga potensi kerugian lanjutan dapat diminimalkan (Muryani & Wiraguna, 2025; Tarumanagara University Law Review, 2025). Perlindungan ini juga menunjukkan adanya pergeseran paradigma hukum dari pendekatan reaktif menuju pendekatan preventif dalam sistem perlindungan data pribadi di Indonesia (Abdullah et al., 2025).

Selain menjamin hak subjek data, UU PDP juga memperkuat aspek penegakan hukum melalui pengaturan sanksi pidana dan administratif yang tegas. Pasal 67 dan Pasal 68 UU PDP mengatur ancaman pidana penjara dan denda yang signifikan bagi pelaku yang secara sengaja dan tanpa hak memperoleh, menggunakan, atau memalsukan data pribadi untuk keuntungan tertentu. Ketentuan sanksi ini dimaksudkan untuk menciptakan efek jera serta menekan tingkat kejahatan berbasis data, termasuk phishing yang kerap memanfaatkan kelalaian perlindungan data pribadi (Usman & Prakasa, 2024; Albaldan & Lisasih, 2025). Namun demikian, efektivitas norma pidana tersebut sangat bergantung pada konsistensi penegakan hukum dan kapasitas institusi pengawas yang dibentuk berdasarkan UU PDP (Firdaus & Wardhani, 2025). Lebih lanjut, peran pemerintah dan partisipasi masyarakat menjadi faktor penentu dalam keberhasilan implementasi UU PDP. Lembaga pengawas perlindungan data pribadi memiliki kewenangan strategis dalam melakukan pengawasan, menjatuhkan sanksi administratif, serta menyelesaikan sengketa yang timbul akibat pelanggaran hak subjek data. Di sisi lain, Pasal 63 UU PDP menekankan pentingnya peran aktif masyarakat melalui edukasi, sosialisasi, dan pengawasan terhadap praktik pengelolaan data pribadi, khususnya di sektor digital dan transaksi elektronik yang rentan terhadap serangan phishing (Sihombing et al., 2025; Asmak UI Hosnah et al., 2025). Dengan demikian, UU PDP tidak hanya berfungsi sebagai instrumen hukum perlindungan data, tetapi juga sebagai kerangka kolaboratif antara negara dan masyarakat dalam menciptakan ekosistem digital yang aman dan berkeadilan.

### **Pemerintah Melalui UU Perlindungan Data Pribadi Dalam Menanggulangi Phising Di Indonesia**

Hukum merupakan seperangkat aturan yang secara formal mengatur interaksi dan perilaku individu dalam suatu tatanan sosial. Sumber hukum dapat bervariasi dan bergantung pada faktor-faktor yang memengaruhi pembentukan dan penerapannya. Terdapat dua kategori utama sumber hukum, yakni sumber hukum materiil dan sumber hukum immateriil. Sumber hukum materiil merujuk pada keseluruhan peraturan perundang-undangan yang telah disahkan oleh lembaga legislatif. Aturan-aturan ini mencakup peraturan perundang-undangan, konstitusi, dan kebijakan hukum yang berlaku. Sumber hukum material berfokus pada isi dan substansi hukum itu sendiri yang membentuk dasar-dasar hukum di suatu wilayah. Sementara itu, sumber hukum immaterial melibatkan faktor-faktor non-tulis yang berpengaruh dalam penerapan hukum. Hal ini mencakup budaya hukum, adat istiadat, serta peran penegak hukum seperti hakim, aparat kepolisian, dan lembaga penegak hukum lainnya. Faktor-faktor ini

mempengaruhi bagaimana hukum diterapkan dan dipahami oleh masyarakat, serta bagaimana hukum dilaksanakan dalam konteks sosial yang lebih luas (Confido, 2022).

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) memiliki peran yang krusial dalam mengatasi phishing di Indonesia. Undang-undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) merupakan upaya hukum negara untuk melindungi hak-hak individu atas data pribadinya. UU ini memberikan hukuman yang keras kepada orang-orang yang melakukan kejahatan siber, seperti tindakan phishing. Pemerintah berkewajiban untuk memastikan efektivitas pelaksanaan UU PDP guna melindungi kepentingan masyarakat. Dalam upaya mencegah dan menindak pelaku phishing, pemerintah berperan aktif dalam mengimplementasikan UU PDP dengan memperkuat kolaborasi antara berbagai lembaga yang bertanggung jawab di bidang keamanan siber, seperti Kepolisian Negara Republik Indonesia, Badan Siber dan Sandi Negara (BSSN), serta Komisi Perlindungan Anak Indonesia (KPAI) (Setiawan dkk, 2022). Selain itu, pemerintah juga harus memberikan hukuman kepada orang yang melakukan penipuan phishing. Diharapkan sanksi yang diterapkan dapat memberikan efek jera serta dapat mencegah mereka dari tindakan serupa di masa yang akan datang. Sanksi tersebut diharapkan dapat memberikan efek jera bagi pelaku Sesuai Pasal 58 UU PDP, Lembaga Otoritas Perlindungan Data Pribadi (LOPDP) yang dibentuk berdasarkan Peraturan Presiden memiliki kewenangan penuh dalam mengawasi dan memastikan pelaksanaan UU PDP untuk melindungi data pribadi masyarakat. Tugas dan wewenang LOPDP sesuai UU PDP meliputi: Merancang dan mengimplementasikan kebijakan perlindungan data pribadi yang efektif untuk menjamin keamanan data individu, serta memastikan bahwa kebijakan tersebut senantiasa relevan dengan perkembangan teknologi informasi dan dinamika lingkungan bisnis; Memberikan hukuman berupa sanksi administratif kepada individu atau organisasi yang melanggar ketentuan perlindungan data pribadi, Meningkatkan kesadaran hukum melalui penerapan sanksi; Bersama-sama dengan pihak berwajib, berkomitmen untuk mencegah dan memberantas kejahatan siber yang mengancam privasi data individu dengan cara memberikan dukungan penuh dalam proses penyelidikan dan penuntutan; Bertanggung jawab untuk melakukan evaluasi terhadap pemenuhan persyaratan yang berlaku dalam proses pengalihan data pribadi ke luar negeri, serta menjamin keamanan dan kerahasiaan data selama proses pengalihan. Adapun wewenang dari LOPDP yakni: a. Memberikan sanksi tegas berupa denda dan tindakan administratif terhadap pelanggar aturan privasi data; Menjatuhkan sanksi administratif berupa penghentian sementara terhadap pengolahan data pribadi yang tidak sah; c. Melakukan investigasi independen terhadap

kasus pelanggaran data dan mempublikasikan hasilnya; d. Menjadi perwakilan dalam merumuskan standar perlindungan data internasional (Marunung dkk, 2022).

Dalam melaksanakan tugas dan fungsinya, lembaga otoritas perlindungan data pribadi perlu menjaga kemandirian, dengan sumber daya manusia yang profesional, dan menerapkan prinsip transparansi dalam setiap kegiatannya. Lembaga ini perlu memastikan bahwa ruang lingkup tugas dan wewenangnya tidak tumpang tindih dengan lembaga pemerintah lainnya, sehingga dapat menghindari konflik kewenangan dan meningkatkan efisiensi pelaksanaan tugas (Marunung dkk, 2022). LOPDP wajib menjalankan tugasnya sesuai dengan kerangka hukum yang berlaku dan batasan kewenangan yang diberikan. Di samping itu, lembaga ini perlu bekerja sama dengan lembaga perlindungan data internasional untuk melindungi data pribadi pengguna secara komprehensif, baik di dalam maupun di luar negeri.

Undang-undang perlindungan data pribadi memberikan payung hukum bagi perlindungan data pribadi masyarakat dengan menetapkan sanksi tegas bagi pelaku kejahatan siber, seperti tindakan phising. Sanksi tersebut diberikan agar orang yang melakukan kesalahan merasa takut dan tidak melakukannya lagi di masa depan. Pelaku phising yang melanggar bisa dikenai sanksi pidana sesuai Pasal 67 UU PDP, dengan hukuman penjara maksimal 5 tahun dan/atau denda hingga 5 miliar rupiah. Phising merupakan tindakan penipuan siber yang dilakukan dengan cara memalsukan identitas atau data pribadi seseorang secara tidak sah, dengan maksud mendapatkan keuntungan atau akses ke informasi pribadi milik orang lain. Apabila tindakan phising tersebut melibatkan pengumpulan data pribadi orang lain secara bertentangan dengan hukum, maka tindakan tersebut dapat dianggap sebagai pelanggaran terhadap ketentuan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Apabila suatu badan usaha melakukan tindak pidana, maka tanggung jawab pidana tidak hanya terletak pada badan usaha itu sendiri, tetapi juga bisa menimpa pengurus, pemegang kendali, orang yang memberi perintah, pemilik manfaat, atau kombinasi dari beberapa pihak tersebut. Selain hukuman pokok berupa penjara dan/atau denda, pengadilan juga bisa berwenang menjatuhkan pidana tambahan seperti penyitaan aset hasil kejahatan dan kewajiban membayar ganti rugi kepada korban. Terhadap pidana denda yang dijatuhkan, terpidana diberikan tenggang waktu satu bulan untuk melunasi. Apabila dalam jangka waktu tersebut pidana denda belum dilunasi, maka jaksa dapat melakukan penyitaan serta pelelangan terhadap harta kekayaan atau pendapatan terpidana untuk menutupi kekurangan pembayaran denda.

Adanya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dan dibentuknya Lembaga Otoritas Perlindungan Data Pribadi diharapkan dapat menjadi langkah signifikan dalam upaya pemerintah untuk mencegah dan memberantas tindak pidana siber,

hususnya kejahatan phishing. Melalui penegakan hukum yang tegas terhadap pelaku kejahatan siber serta kerja sama yang erat dengan berbagai pihak terkait.

## 5. KESIMPULAN DAN SARAN

UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) berperan penting dalam mencegah dan mengatasi kejahatan siber, termasuk phishing, di Indonesia. Phishing adalah upaya penipuan yang memanfaatkan teknik manipulasi untuk memperoleh data pribadi korban secara ilegal, yang dapat menyebabkan kerugian finansial, pelanggaran privasi, dan kerusakan reputasi. UU PDP mengatur kewajiban bagi pengendali data pribadi untuk menjaga keamanan data dari akses yang tidak sah dan menetapkan sanksi tegas, baik pidana maupun administratif. Sanksi pidana yang tercantum dalam Pasal 67 UU PDP, seperti hukuman penjara hingga lima tahun dan denda maksimal lima miliar rupiah, bertujuan untuk memberikan efek jera dan mencegah pelaku phishing dari melakukan kejahatan serupa. Selain itu, Pasal 46 mengharuskan pengendali data untuk memberikan notifikasi kepada subjek data jika terjadi pelanggaran perlindungan data, seperti kebocoran akibat serangan phishing. Efektivitas UU PDP dalam meminimalisir kejahatan phishing juga bergantung pada pelaksanaan yang konsisten. Lembaga Otoritas Perlindungan Data Pribadi (LOPDP) berperan kunci dalam pengawasan dan penegakan hukum, bekerja sama dengan pemerintah, lembaga, perusahaan swasta, dan media massa untuk meningkatkan kesadaran masyarakat. Dengan kerjasama ini, diharapkan masyarakat menjadi lebih hati-hati dan bisa melindungi data pribadi mereka, sehingga tindakan phishing dapat dikurangi dan keamanan siber di Indonesia menjadi lebih baik.

UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) memiliki peran yang sangat penting dalam menangani kejahatan siber, seperti phishing, di Indonesia. UU ini menetapkan sanksi pidana dan administratif yang tegas, termasuk hukuman penjara hingga lima tahun dan denda maksimal lima miliar rupiah bagi pelaku yang tidak taat dengan ketentuan perlindungan data pribadi. Phishing, yang melibatkan pemalsuan identitas atau data pribadi untuk mendapatkan keuntungan, dikategorikan sebagai pelanggaran berdasarkan UU PDP jika melibatkan pengumpulan data pribadi tanpa izin. Dengan adanya Lembaga Otoritas Perlindungan Data Pribadi (LOPDP), diharapkan pemerintah dapat lebih proaktif dalam mengawasi dan menegakkan hukum, serta bekerja sama dengan perusahaan swasta seperti marketplace, e-commerce, dan penyedia jasa ekspedisi untuk memperkuat perlindungan data pribadi. Selain penegakan hukum, media massa juga memiliki peran krusial dalam meningkatkan kesadaran masyarakat akan ancaman phishing. Melalui pemberitaan dan

kampanye edukasi, diharapkan UU PDP dapat efektif dalam mengurangi kasus phishing dan menciptakan ruang siber yang lebih aman.

## DAFTAR REFERENSI

- Abdullah, C., Durand, N., & Moonti, R. M. (2025). *Transformasi digital dan hak atas privasi: Tinjauan kritis pelaksanaan UU Perlindungan Data Pribadi (PDP) Tahun 2022. Amandemen: Jurnal Ilmu Pertahanan, Politik dan Hukum Indonesia*, 2(3), 233–241. <https://doi.org/10.62383/amandemen.v2i3.1073>
- Albaldan, K. A., & Lisasih, N. Y. (2025). *Personal data security violations in East Jakarta regional elections: Legal analysis through personal data protection legislation*. *Journal of Law and Economics*, 4(2). <https://doi.org/10.56347/jle.v4i2.330>
- Asmak Ul Hosnah, Latif, N., Juliandi, A., Desiana, A. R., & Ilhan Ma'ruf, R. M. (2025). *Analisis perlindungan data pribadi dalam implementasi UU Nomor 27 Tahun 2022 di era Artificial Intelligence*. *QAWIUN: Jurnal Penelitian dan Pengabdian Masyarakat*, 1(2). <https://doi.org/10.61104/qw.v1i2.649>
- Firdaus, A., & Wardhani, D. F. (2025). *Protecting privacy in the digital era: Personal data security in Indonesia*. *Inovasi Pembangunan: Jurnal Kelitbangan*, 13(1). <https://doi.org/10.35450/jip.v13i1.915>
- Manurung, E. A. P., & Thalib, E. F. (2022). Tinjauan yuridis perlindungan data pribadi berdasarkan UU nomor 27 tahun 2022. *Jurnal Hukum Saraswati*, 4(2), 139-148.
- Muryani, V. D., & Wiraguna, S. A. (2025). *Efektivitas Undang-Undang Perlindungan Data Pribadi dalam menjawab tantangan keamanan siber di Indonesia*. *Causa: Jurnal Hukum dan Kewarganegaraan*, 12(3), 81–90. <https://doi.org/10.3783/causa.v12i3.12780>
- Priliasari, E. (2023). Perlindungan data pribadi konsumen dalam transaksi e-commerce. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, 12(2).
- Saputra, D., & Marpaung, Z. A. (2023). Analisis Yuridis Penanggulangan Penyalahgunaan Data Pribadi Dalam Bentuk Phising Yang Dilakukan Oleh Paid Verified Account Di media Sosial Menurut Undang-Undang Perlindungan Data Pribadi. *UNES Law Review*, 5(4), 4764-4775.
- Setiawan, H. B., & Najicha, F. U. (2022). Perlindungan data pribadi warga negara Indonesia terkait dengan kebocoran data. *Jurnal Kewarganegaraan*, 6(1), 976-982.
- Sihombing, P., Widiarty, W. S., & Nadapdap, B. (2025). *Perlindungan hukum terhadap data pribadi konsumen dalam transaksi e-commerce di Indonesia*. *Jurnal Sosial Teknologi*, 6(1). <https://doi.org/10.59188/jurnalsostech.v6i1.32627>
- Suari, K. R. A., & Sarjana, I. M. (2023). Menjaga privasi di era digital: Perlindungan data pribadi di Indonesia. *Jurnal Analisis Hukum*, 6(1), 132-142.
- Sutarli, A. F., & Kurniawan, S. (2023). Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi dalam Menanggulangi Phising di Indonesia. *Innovative: Journal Of Social Science Research*, 3(2), 4208-4221.
- Tarumanagara University Law Review. (2025). *Personal data subject rights protection: A comparative study between Indonesian PDP Law and the UK Data Protection Act*. *Jurnal USM Law Review*, 8(2). <https://doi.org/10.26623/julr.v8i2.12076>

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

Usman, N. U., & Prakasa, S. U. W. (2024). *Perlindungan hukum data pribadi dan pertanggungjawaban otoritas terhadap keamanan siber menurut tinjauan UU PDP*. Doktrina: Journal of Law, 7(2). <https://doi.org/10.31289/doktrina.v7i2.11627>