Jurnal Hukum, Administrasi Publik dan Negara
Volume. 2, Nomor. 4 Juli 2025
e-ISSN: 3063-7864; p-ISSN : 3063-7872, Hal. 01-14
DOI: https://doi.org/10.62383/hukum.v2i4.290
Available online at: https://ejournal.appisi.or.id/index.php/hukum

Perlindungan Keamanan Data Pribadi di Era Digital Menghadapi Serangan *Phishing* Ditinjau dari Undang-Undang Pelindungan Data Pribadi Nomor 27 Tahun 2022

Bella Fistya Asherli[1*], Sidi Ahyar Wiraguna[2]
[1,2]Fakultas Hukum, Hukum, Universitas Esa Unggul Jakarta

Alamat: Jl. Arjuna Utara No. 9, Duri Kepa, Kec. Kb. Jeruk, Kota Jakarta Barat 11510
Korespondensi penulis: bellafistyaa@gmail.com

Abstract. *The rapid development of information technology has had a significant impact on the pattern of collecting, processing, and storing personal data in the digital era. However, this progress is also accompanied by an increasing threat of cybercrime, one of which is phishing attacks. Phishing is a digital fraud mode that aims to obtain personal data illegally through social engineering and manipulation of electronic systems. This study aims to analyze the form of legal protection for phishing victims in the perspective of Law Number 27 of 2022 concerning Personal Data Protection (UU PDP). Using normative legal methods and conceptual approaches, this study examines the role of state authorities such as the National Cyber and Crypto Agency (BSSN) and the Directorate of Cyber Crime (Dittipidsiber) of the National Police Criminal Investigation Unit in the procedures for handling and prosecuting phishing. The results of the study show that although the PDP Law has provided a clear legal framework, its implementation still faces challenges in technical aspects, institutional coordination, and public digital literacy. Therefore, strong synergy is needed between regulation, supervision, and public education to realize effective and sustainable personal data protection in the digital era.*

Keywords: *phishing, personal data, PDP Law, cyber security, BSSN, Dittipidsiber.*

Abstrak. Pesatnya perkembangan teknologi informasi telah membawa dampak signifikan terhadap pola pengumpulan, pengolahan, dan penyimpanan data pribadi di era digital. Namun, kemajuan ini juga dibarengi dengan meningkatnya ancaman kejahatan siber, salah satunya adalah serangan *phishing*. Phishing merupakan modus penipuan digital yang bertujuan memperoleh data pribadi secara ilegal melalui rekayasa sosial dan manipulasi sistem elektronik. Penelitian ini bertujuan untuk menganalisis bentuk perlindungan hukum terhadap korban phishing dalam perspektif Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Dengan menggunakan metode yuridis normatif dan pendekatan konseptual, penelitian ini mengkaji peran otoritas negara seperti Badan Siber dan Sandi Negara (BSSN) serta Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri dalam prosedur penanganan dan penindakan phishing. Hasil kajian menunjukkan bahwa meskipun Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi telah memberikan kerangka hukum yang jelas, implementasinya masih menghadapi tantangan pada aspek teknis, koordinasi kelembagaan, dan literasi digital masyarakat. Oleh karena itu, diperlukan sinergi yang kuat antara regulasi, pengawasan, dan edukasi publik untuk mewujudkan perlindungan data pribadi yang efektif dan berkelanjutan di era digital.

Kata kunci: phishing, data pribadi, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, keamanan siber, BSSN, Dittipidsiber.

1. LATAR BELAKANG

Perkembangan teknologi informasi dan komunikasi yang masif telah membawa masyarakat global memasuki era digital, di mana berbagai aktivitas sehari-hari baik individu maupun institusional bergantung pada sistem digital dan pertukaran data secara daring. Di Indonesia, digitalisasi telah menyentuh hampir semua sektor kehidupan, mulai dari layanan keuangan, pendidikan, pemerintahan, hingga sektor kesehatan. Bersamaan dengan itu, data pribadi menjadi komoditas penting yang tidak hanya menyimpan identitas seseorang, tetapi

Received: April 04, 2025; Revised: April 19, 2025; Accepted: Mei 03, 2025; Published: Mei 31, 2025

juga memiliki nilai ekonomi dan strategis. (Maulana, 2022) Oleh karena itu, isu pelindungan data pribadi menjadi sangat penting dan sensitif dalam tata kelola informasi digital dewasa ini. Apalagi dengan tingginya ketergantungan terhadap platform digital, maka potensi penyalahgunaan data pribadi pun semakin tinggi. Dalam konteks ini, ancaman seperti *phishing* yakni praktik memperoleh informasi pribadi melalui penyamaran digital menjadi salah satu modus serangan yang marak terjadi dan berdampak luas bagi masyarakat. (Yusuf, 2022)

Phishing bukanlah isu baru dalam dunia kejahatan siber, namun kompleksitas dan skalanya terus meningkat seiring dengan kemajuan teknologi. Menurut laporan Badan Siber dan Sandi Negara (BSSN), sepanjang tahun 2023 terjadi lebih dari 400 juta insiden siber, di mana *phishing* menduduki peringkat teratas sebagai jenis serangan yang paling sering dilaporkan oleh masyarakat pengguna internet di Indonesia. (Negara, 2023) Modus operandi *phishing* semakin bervariasi, mulai dari email palsu yang menyerupai institusi resmi, tautan berbahaya dalam media sosial, hingga website tiruan yang dibuat sedemikian rupa menyerupai situs asli. Fenomena ini diperparah dengan masih rendahnya literasi digital masyarakat Indonesia, terutama dalam hal mengenali dan mencegah ancaman *phishing*. (Nasution, 2021) Di sisi lain, perusahaan dan institusi pengelola data juga belum semuanya memiliki standar keamanan informasi yang memadai. Dalam banyak kasus, korban tidak mengetahui hak-haknya dan pelaku seringkali tidak terjerat secara hukum. Kondisi ini menimbulkan pertanyaan besar tentang seberapa efektif sistem hukum yang berlaku dalam memberikan pelindungan nyata terhadap data pribadi masyarakat, khususnya dari kejahatan *phishing*. (Wijaya, 2021)

Meski telah banyak literatur dan regulasi yang membahas keamanan siber, kajian spesifik mengenai phishing dalam kaitannya dengan efektivitas pelindungan hukum berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi masih sangat terbatas. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi sebagai payung hukum utama dalam pelindungan data pribadi di Indonesia membawa harapan besar dalam menanggulangi penyalahgunaan data, termasuk dalam bentuk serangan phishing. Namun dalam implementasinya, sering terjadi kesenjangan antara *sollen* dengan *sein*. Misalnya, meskipun Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi telah mengatur hak-hak subjek data dan kewajiban pengendali data, namun dalam praktiknya, korban serangan *phishing* seringkali kesulitan untuk memperoleh ganti rugi atau bahkan mengidentifikasi siapa yang harus bertanggung jawab. (Budiarto, 2020) Selain itu, penegakan hukum terhadap pelaku phishing yang menggunakan data pribadi secara ilegal belum optimal karena keterbatasan aparat, kurangnya mekanisme pelaporan, dan lambatnya proses hukum.

Penelitian ini menjadi penting karena memberikan kajian yuridis-kritis terhadap bagaimana pelindungan hukum yang dijanjikan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi diimplementasikan dalam kasus serangan phishing. (Mulyani, 2023) Dalam era digital saat ini, pelindungan data pribadi tidak bisa lagi dianggap sebagai isu teknis semata, melainkan telah menjadi bagian dari hak asasi manusia yang harus dijamin oleh negara. (Sihombing, 2021) Penelitian ini juga merespons kondisi nyata di masyarakat di mana kasus-kasus kebocoran data dan phishing tidak hanya menimbulkan kerugian ekonomi, tetapi juga berimplikasi pada kepercayaan publik terhadap sistem digital nasional. Dengan demikian, penting untuk menggali secara mendalam mekanisme pelindungan, bentuk tanggung jawab pengendali data, serta bagaimana sistem hukum dapat memastikan keadilan bagi korban serangan phishing. (Fadillah, 2022) Di tengah dinamika global dan regional yang semakin kompleks, penelitian ini juga relevan untuk memberikan kontribusi terhadap penyempurnaan kebijakan nasional di bidang keamanan siber dan pelindungan data pribadi. (Hadi, 2023)

Penelitian ini memiliki kebaruan dalam pendekatannya yang tidak hanya bersifat normatif, tetapi juga menggabungkan perspektif kritis berbasis fakta empirik dan studi kasus aktual. (Pratama, 2023) Sebagian besar kajian terdahulu lebih berfokus pada aspek teknis pelindungan data atau pada norma hukum yang ada, namun belum secara spesifik mengkaji bagaimana Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dapat digunakan secara konkret untuk menanggulangi serangan phishing sebagai bentuk kejahatan siber. (Sari, 2023) Dengan pendekatan yuridis-analitis, penelitian ini mengidentifikasi kelemahan struktural maupun fungsional dalam penerapan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, serta memberikan rekomendasi perbaikan berdasarkan prinsip pelindungan data berbasis HAM dan praktik baik dari negara lain. (Kurniawan R. , 2023) Oleh karena itu, hasil penelitian ini diharapkan tidak hanya memperkaya khazanah keilmuan hukum siber di Indonesia, tetapi juga memberikan masukan nyata bagi pembuat kebijakan, aparat penegak hukum, serta institusi pengendali data pribadi.

Rumusan Masalah

1. Bagaimana efektivitas penerapan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dalam memberikan perlindungan hukum terhadap korban serangan phishing?

2. Bagaimana peran Badan Siber dan Sandi Negara (BSSN) serta Direktorat Tindak Pidana Siber (Dittipidsiber) dalam upaya pencegahan dan penindakan terhadap kejahatan phishing?

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan yuridis normatif yang berfokus pada studi pustaka dan analisis terhadap norma hukum yang mengatur pelindungan data pribadi, khususnya dalam konteks serangan *phishing*. (Soekanto, 2007) Pendekatan ini dipilih karena penelitian menitikberatkan pada kajian terhadap peraturan perundang-undangan yang berlaku serta doktrin hukum yang relevan. Pendekatan yuridis-normatif dianggap paling tepat untuk menganalisis keefektifan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dalam memberikan jaminan pelindungan hukum bagi subjek data yang menjadi korban kejahatan phishing (Sidi, 2025). (Marzuki, 2005) Penelitian ini juga mempertimbangkan relevansi Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, beserta peraturan pelaksananya, guna melihat keselarasan dan tumpang tindih norma dalam sistem hukum nasional. (Salim, 2013)

Dalam penelitian ini digunakan tiga jenis bahan hukum, yaitu bahan hukum primer, sekunder, dan tersier. Bahan hukum primer mencakup peraturan perundang-undangan seperti Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dan ketentuan lainnya yang mengatur hak atas data pribadi dan penanggulangan kejahatan siber. (Zainuddin, 2021) Sementara itu, bahan hukum sekunder meliputi literatur hukum, jurnal ilmiah, artikel ilmiah, serta pendapat ahli yang membahas isu-isu terkait keamanan siber dan pelindungan data. (Wiraguna, 2024) Adapun bahan hukum tersier digunakan untuk mendukung pemahaman terhadap konsep-konsep dasar melalui kamus hukum, ensiklopedia, dan sumber penunjang lainnya. (Mertokusumo, 2003) Teknik pengumpulan data dilakukan melalui studi kepustakaan (*library research*), dengan menelaah dokumen hukum dan kajian akademik yang relevan, baik dalam konteks nasional maupun internasional. (Rachmadi, 2020)

Analisis data dalam penelitian ini dilakukan secara kualitatif dengan metode deskriptif analitis. Analisis deskriptif digunakan untuk menggambarkan dan menjelaskan ketentuan hukum yang berlaku secara sistematis, (Rahman, 2023) sedangkan analisis analitis digunakan untuk mengevaluasi efektivitas dan implementasi norma hukum tersebut dalam praktik. (Suteki & Taufani, 2018) Penelitian ini bertujuan tidak hanya untuk menggambarkan kondisi normatif,

tetapi juga untuk mengidentifikasi kesenjangan antara ketentuan hukum dan implementasinya di lapangan, terutama dalam konteks penanggulangan *phishing*. (Notoatmodjo, 2010) Penelitian ini dilaksanakan di Jakarta sebagai pusat regulasi dan aktivitas digital nasional, dengan waktu pelaksanaan selama enam bulan, yakni dari Januari hingga Juni 2025.

3. HASIL DAN PEMBAHASAN

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi hadir sebagai respons atas meningkatnya kebutuhan pelindungan terhadap informasi pribadi di era digital. Dalam konteks ini, data pribadi tidak lagi bersifat statis, melainkan menjadi komoditas yang sangat bernilai di ruang siber, sehingga rentan terhadap penyalahgunaan. (Kurniawan R. D., 2023) Salah satu bentuk penyalahgunaan tersebut adalah serangan phishing, yaitu teknik manipulatif yang digunakan untuk mendapatkan akses ilegal terhadap informasi pribadi seseorang melalui tipu daya digital. Dalam kaitannya dengan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, phishing merupakan bentuk pemrosesan data pribadi yang dilakukan tanpa dasar hukum yang sah, yang pada dasarnya bertentangan dengan prinsip pelindungan data sebagaimana diatur dalam (Situmorang, 2023)Pasal 20 ayat (1), yaitu pemrosesan data pribadi harus berdasarkan persetujuan subjek data dan prinsip keabsahan hukum lainnya.

Pada Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, terdapat prinsip-prinsip dasar pemrosesan data pribadi seperti prinsip transparansi, pembatasan tujuan, minimalisasi data, akurasi, integritas, dan kerahasiaan. Akan tetapi, dalam praktiknya, prinsip-prinsip tersebut belum diimplementasikan secara konsisten oleh seluruh pengendali dan prosesor data. Pengendali data pribadi, seperti lembaga keuangan, institusi pendidikan, maupun penyedia layanan digital, masih belum optimal dalam menerapkan perlindungan berlapis terhadap data yang dikumpulkan dari individu. Hal ini menyebabkan banyaknya celah yang dapat dimanfaatkan oleh pelaku phishing. Ketika terjadi pencurian data akibat phishing, proses pemulihan hak subjek data juga belum efektif karena belum tersedianya sistem pengaduan yang terintegrasi dan kejelasan lembaga yang bertanggung jawab penuh untuk menyelesaikan persoalan tersebut.

Kondisi tersebut mencerminkan adanya kesenjangan antara peraturan yang bersifat *lex scripta* (tertulis) dengan implementasinya dalam realitas digital masyarakat *(lex lata).* Meskipun ketentuan pidana telah ditegaskan dalam Pasal 67 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi bahwa setiap orang yang memproses data pribadi secara melawan hukum dapat dikenakan sanksi pidana, namun penegakan hukum terhadap

pelaku serangan phishing masih sangat terbatas. (Anggraeni, 2023) Hal ini diperburuk oleh keterbatasan aparat penegak hukum dalam menindaklanjuti kejahatan digital yang bersifat kompleks dan lintas batas negara. Akibatnya, korban serangan phishing seringkali mengalami kerugian material dan imaterial tanpa ada pemulihan hukum yang memadai. (Sulaiman, 2021) Dalam perspektif perlindungan hukum, hal ini menunjukkan bahwa keberadaan norma belum menjamin terwujudnya keadilan substantif bagi subjek data.

Berdasarkan ketentuan Pasal 3 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menjelaskan beberapa asas yang menjadi dasar perlindungan data pribadi. Ada delapan asas yang menjadi landasan, yaitu:

1. Asas Pelindungan
2. Asas Kepastian Hukum
3. Asas Kepentingan Umum
4. Asas Kemanfaatan
5. Asas Kehati-Hatian
6. Asas Keseimbangan
7. Asas Pertanggungjawaban
8. Asas Kerahasiaan.

Kasus-kasus yang berkaitan dengan pelindungan data pribadi kini semakin sering terjadi, tidak hanya dalam interaksi langsung secara fisik, tetapi juga melalui berbagai aktivitas di platform digital. Ranah digital menjadi salah satu titik rawan terjadinya kebocoran data, baik dalam konteks transaksi daring maupun pengelolaan akun media sosial, yang kerap disalahgunakan oleh pihak-pihak tidak bertanggung jawab. (Haris, 2023) Menyikapi kondisi tersebut, pemerintah menetapkan Undang-Undang Nomor 27 Tahun 2022 sebagai upaya untuk memberikan perlindungan hukum yang lebih kuat terhadap data pribadi dalam menghadapi tantangan di era digital ini.

Kepatuhan terhadap Undang-Undang Pelindungan Data Pribadi juga telah menjadi fokus utama di lembaga keuangan sejak disahkannya undang-undang tersebut. (Simanjuntak, 2022) Lembaga keuangan, terutama perbankan merupakan salah satu yang paling rentan terhadap pencurian data pribadi. Informasi sensitif yang dikelola oleh bank dan lembaga keuangan, seperti informasi identitas, transaksi, dan data keuangan pribadi menjadikannya sasaran utama bagi pelaku kejahatan siber untuk mendapatkan data pribadi. Kepatuhan terhadap Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi membantu dalam melindungi data dari penyalahgunaan yang dapat mengancam privasi serta keamanan finansial pelanggan. (Kominfo, 2023)

Penerapan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) dalam sektor perbankan bertujuan untuk memperkuat sistem keamanan data serta meningkatkan kepercayaan masyarakat terhadap institusi keuangan. Kepercayaan nasabah merupakan elemen krusial dalam keberlangsungan industri perbankan. Kepatuhan lembaga perbankan terhadap ketentuan dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi mencerminkan komitmen tinggi mereka dalam menjaga informasi pribadi nasabah, yang secara langsung berkontribusi pada pembentukan dan pemeliharaan kepercayaan publik. Pentingnya aspek ini tidak dapat diabaikan, mengingat pelanggaran data dapat mengakibatkan kerugian finansial yang signifikan, baik secara langsung melalui kebocoran informasi maupun secara tidak langsung melalui penurunan reputasi dan hilangnya kepercayaan nasabah (Anesya Fritiana, 2025).

Pelindungan terhadap data pribadi telah menjadi komponen vital dalam aktivitas perbankan serta kehidupan masyarakat di era digital saat ini (Shafa Salsabila, 2025). Dengan diberlakukannya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, perbankan dituntut untuk menjalankan tanggung jawab dalam menjaga kerahasiaan dan integritas data nasabah. Untuk mewujudkan hal tersebut, diperlukan langkah-langkah strategis seperti edukasi, sosialisasi, serta kolaborasi yang erat antara pihak perbankan dan otoritas pengawas. Upaya kolektif ini diharapkan mampu membentuk budaya perlindungan privasi yang kuat, meningkatkan kepercayaan masyarakat terhadap institusi perbankan, serta menegaskan bahwa keamanan data merupakan prioritas utama seluruh pemangku kepentingan (Elvina Putri Maheswari, 2025).

Di sisi lain, pelaksanaan prinsip akuntabilitas dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi juga belum berjalan optimal. Prinsip ini mengharuskan pengendali data untuk bertanggung jawab atas keamanan data yang dikelolanya, termasuk ketika terjadi pelanggaran akibat serangan eksternal. Namun dalam praktik, tidak semua pengendali data melaporkan adanya pelanggaran atau kebocoran data kepada subjek data sebagaimana diamanatkan dalam Pasal 46. Akibatnya, subjek data kehilangan kesempatan untuk mengambil langkah preventif dan pemulihan. Minimnya pelaporan pelanggaran data ini memperburuk dampak serangan phishing karena memungkinkan penyalahgunaan data dalam jangka panjang tanpa diketahui oleh pemiliknya. Hal ini menjadi bukti bahwa norma kewajiban pemberitahuan masih belum diinternalisasi sebagai tanggung jawab hukum oleh pelaku usaha digital di Indonesia (Khetrina Maria Angnesia, 2025).

Selanjutnya, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi telah mengamanatkan pembentukan lembaga otoritas pelindungan data pribadi sebagai badan

independen yang berfungsi mengawasi pemrosesan data dan menangani sengketa pelanggaran data pribadi. Keberadaan lembaga ini seharusnya menjadi instrumen penting dalam mengatasi tantangan hukum seperti phishing. Namun hingga saat ini, lembaga tersebut belum terbentuk secara fungsional (Berto Purnomo Sidik, 2025). Ketiadaan lembaga pengawas menyebabkan ketidakjelasan dalam mekanisme pengaduan, pemantauan pelanggaran, dan penjatuhan sanksi administratif kepada pelaku usaha yang lalai dalam melindungi data pribadi konsumen. Dalam konteks ini, negara masih belum hadir secara penuh dalam menjamin hak konstitusional atas rasa aman dan perlindungan data di ruang digital, sebagaimana tercantum dalam Pasal 28G ayat (1) UUD NRI Tahun 1945.

Lebih lanjut, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi memang mengatur kewajiban perlindungan teknologi secara preventif seperti enkripsi, autentikasi ganda, dan sistem keamanan informasi. Namun hal tersebut tidak akan efektif tanpa didukung oleh literasi digital masyarakat. Dalam kondisi saat ini, masyarakat masih minim pengetahuan tentang modus phishing, bagaimana cara mengenalinya, dan tindakan hukum yang dapat diambil apabila menjadi korban. Padahal, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi telah memberikan hak kepada subjek data untuk menarik persetujuan, menghapus data, dan meminta pertanggungjawaban dari pengendali data. Ketidaktahuan terhadap hak-hak ini menyebabkan masyarakat tidak mampu memperjuangkan hak hukumnya, yang pada akhirnya membuat keberadaan norma hukum menjadi tidak berarti secara praktis (Wyanda Kinanti Syauqi Ramadhani, 2025).

Dalam upaya menghadapi serangan phishing yang semakin kompleks dan merugikan, pelindungan data pribadi tidak hanya menjadi tanggung jawab pengendali data, tetapi juga memerlukan peran aktif dari lembaga negara yang berwenang di bidang keamanan siber. Salah satu lembaga yang memiliki otoritas dan mandat khusus dalam menjaga keamanan informasi digital nasional adalah Badan Siber dan Sandi Negara (BSSN)**.** Lembaga ini berperan penting dalam mencegah, mendeteksi, dan merespons berbagai bentuk ancaman siber, termasuk *phishing*, melalui pendekatan teknis, strategis, dan edukatif yang terintegrasi.

Badan Siber dan Sandi Negara (BSSN) Prosedur Penanganan Phishing

Badan Siber dan Sandi Negara (BSSN) merupakan lembaga pemerintah non-kementerian yang memiliki peran strategis dalam menjaga keamanan ruang siber nasional. Dibentuk melalui Peraturan Presiden Nomor 53 Tahun 2017 jo. Peraturan Presiden Nomor 133 Tahun 2017, BSSN berfungsi sebagai otoritas nasional dalam perlindungan dan pengamanan data serta informasi yang bersifat strategis, termasuk pelindungan dari ancaman serangan siber seperti

phishing. Phishing, sebagai bentuk kejahatan siber yang menargetkan data pribadi pengguna, menjadi salah satu fokus utama dalam agenda keamanan siber BSSN, mengingat dampaknya yang sistemik terhadap individu, institusi, dan infrastruktur digital nasional. (BSSN, 2022)

Dalam menjalankan fungsinya, BSSN memiliki beberapa tugas pokok terkait pencegahan dan penanganan phishing. Pertama, BSSN menyelenggarakan *Computer Security Incident Response Team* (CSIRT) baik di tingkat nasional (Indonesia CSIRT) maupun sektor-sektor strategis. CSIRT bertugas menerima laporan insiden, mengoordinasikan respons teknis, dan memberikan panduan kepada pihak yang terdampak phishing. Prosedur standar yang diterapkan oleh CSIRT BSSN dimulai dari tahap identifikasi insiden, verifikasi sumber dan dampak, analisis teknis terhadap vektor serangan, hingga pelaksanaan mitigasi dan pemulihan sistem. Dalam proses ini, pelaporan dari masyarakat maupun institusi menjadi unsur penting, sehingga BSSN menyediakan kanal pelaporan terbuka melalui situs resmi dan layanan darurat siber.

Kedua, BSSN melakukan pengawasan dan pemantauan aktif terhadap lalu lintas siber nasional melalui sistem deteksi dini. Sistem ini memungkinkan identifikasi aktivitas mencurigakan seperti pengalihan domain palsu, penyebaran tautan berbahaya, atau pemalsuan kredensial *(credential harvesting)* yang lazim digunakan dalam serangan phishing. Ketika ancaman terdeteksi, BSSN berwenang memberikan peringatan dini dan rekomendasi tindakan mitigatif kepada entitas terkait, termasuk pemerintah daerah, sektor swasta, dan penyelenggara sistem elektronik. Dalam kasus phishing berskala besar, BSSN juga dapat bekerja sama dengan Kominfo dan aparat penegak hukum untuk melakukan takedown situs atau pemblokiran akses terhadap infrastruktur digital yang digunakan oleh pelaku.

Ketiga, BSSN menjalankan fungsi edukatif dan preventif melalui kampanye literasi keamanan siber kepada masyarakat umum. Dalam konteks phishing, BSSN secara rutin menerbitkan buletin, panduan, dan simulasi digital guna meningkatkan kesadaran publik mengenai cara mengenali modus penipuan digital, menjaga keamanan kredensial, serta langkah pelaporan jika menjadi korban. Melalui pendekatan ini, BSSN tidak hanya bertindak sebagai reaktif terhadap insiden, tetapi juga proaktif dalam menciptakan ketahanan siber masyarakat Indonesia secara menyeluruh.

Secara normatif, peran BSSN dalam menangani phishing sejalan dengan amanat Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, khususnya terkait prinsip keamanan dan pencegahan penyalahgunaan data. Walaupun BSSN tidak memiliki kewenangan pemidanaan, lembaga ini menjadi pilar utama dalam arsitektur teknis pelindungan data pribadi, bekerja berdampingan dengan otoritas pengawas data dan aparat penegak hukum.

Oleh karena itu, penguatan kapasitas kelembagaan BSSN, baik dari sisi anggaran, sumber daya manusia, maupun kerangka koordinasi antar instansi, menjadi hal yang mendesak untuk memperkuat efektivitas nasional dalam menghadapi ancaman phishing yang semakin canggih dan terorganisasi.

Menghadapi fenomena phishing yang semakin meresahkan di era digital, pelindungan data pribadi tidak hanya menjadi isu teknis, melainkan juga menyangkut aspek hukum dan penegakan aturan. Oleh karena itu, kolaborasi antar lembaga menjadi krusial dalam merespons ancaman ini secara komprehensif. Badan Siber dan Sandi Negara (BSSN) sebagai otoritas di bidang keamanan siber berperan dalam pencegahan dan deteksi teknis insiden phishing, sementara Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri memegang peran penting dalam aspek penegakan hukum terhadap pelaku kejahatan siber. Kedua institusi ini menjalankan prosedur penanganan phishing berdasarkan fungsi masing-masing, yang mencerminkan pendekatan integratif antara teknis dan yuridis dalam perlindungan data pribadi di Indonesia.

Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri Prosedur Penanganan Phishing.

Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri merupakan unit khusus dalam kepolisian yang bertugas menangani kejahatan siber, termasuk phishing. Dalam praktiknya, Dittipidsiber menerima laporan masyarakat terkait tindak pidana phishing melalui kanal resmi pengaduan, baik secara langsung maupun daring. Setelah menerima laporan, unit ini melakukan analisis forensik digital guna mengidentifikasi pelaku dan alat bukti, seperti email palsu, situs tiruan, atau transaksi elektronik yang mencurigakan. Prosedur ini melibatkan pelacakan digital, identifikasi IP, serta koordinasi dengan pihak bank, penyedia layanan internet, dan lembaga terkait. (Polri, 2021)

Jika ditemukan unsur pidana, Dittipidsiber akan melanjutkan proses penyidikan dan menetapkan tersangka berdasarkan ketentuan dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Undang - Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Penanganan ini juga diperkuat dengan kegiatan preventif berupa edukasi publik, sosialisasi literasi digital, dan publikasi modus *phishing* terbaru (A Sulaiman, 2024). Meski menghadapi tantangan berupa kerahasiaan digital dan pelaku lintas negara, Dittipidsiber terus berupaya meningkatkan efektivitas penindakan melalui kerja sama nasional dan internasional. Peran strategis ini menjadi kunci dalam memperkuat perlindungan hukum atas data pribadi di era digital. Oleh karena itu, Dittipidsiber juga menjalin

kerja sama internasional melalui INTERPOL, ASEANAPOL, dan perjanjian bilateral dalam hal ekstradisi atau pertukaran data digital untuk mempermudah proses investigasi lintas yurisdiksi.

Dari hasil kajian di atas, dapat disimpulkan bahwa pelindungan terhadap data pribadi dalam konteks serangan phishing masih menghadapi hambatan struktural dan fungsional. Hambatan struktural berkaitan dengan belum lengkapnya infrastruktur hukum seperti lembaga pengawas dan peraturan pelaksana, sedangkan hambatan fungsional meliputi lemahnya penegakan hukum, rendahnya kesadaran hukum masyarakat, dan kurangnya akuntabilitas pelaku usaha digital. Oleh karena itu, untuk menjawab permasalahan hukum secara menyeluruh, perlu dilakukan penguatan pada tataran kelembagaan, peningkatan koordinasi antar instansi terkait, serta edukasi publik secara masif mengenai pelindungan data pribadi dan pencegahan kejahatan *phishing*.

4. KESIMPULAN DAN SARAN

Serangan *phishing* merupakan salah satu bentuk ancaman nyata dalam era digital yang secara langsung mengancam keamanan data pribadi masyarakat. Modus penipuan ini semakin berkembang, tidak hanya dari sisi teknis, tetapi juga dari sisi psikologis, dengan memanfaatkan kelengahan pengguna terhadap komunikasi digital palsu yang tampak sah. Dalam konteks hukum di Indonesia, pelindungan data pribadi dari serangan semacam ini telah mendapatkan dasar hukum yang lebih kuat melalui disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP)**.** Undang-Undang ini menegaskan bahwa setiap individu memiliki hak atas data pribadinya, dan setiap pengendali data wajib menjamin keamanannya dari akses ilegal, termasuk melalui phishing.

Seiring dengan pesatnya perkembangan era digital, berbagai aktivitas daring telah menjadi bagian tak terpisahkan dari kehidupan sehari-hari. Namun demikian, kemajuan teknologi internet juga membuka celah bagi tindak kejahatan siber, seperti *phishing*, yang semakin marak terjadi. Untuk mengatasi permasalahan ini, pemerintah Indonesia telah membentuk sejumlah lembaga yang memiliki wewenang untuk menangani kasus *phishing* melalui penerapan strategi dan prosedur yang telah ditetapkan masing-masing institusi, penanganan *phishing* melibatkan koordinasi dua otoritas utama: Badan Siber dan Sandi Negara (BSSN) dan Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri**.** BSSN menjalankan fungsi pencegahan dan deteksi teknis melalui sistem pemantauan insiden siber, serta memberikan edukasi kepada publik mengenai ancaman digital. Di sisi lain, Dittipidsiber

bertugas menindak secara hukum pelaku phishing, melalui pelacakan digital, investigasi forensik, dan penegakan sanksi pidana berdasarkan UU ITE dan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Secara keseluruhan, pelindungan data pribadi dalam menghadapi phishing membutuhkan pendekatan yang tidak hanya legalistik, tetapi juga teknologis dan edukatif. Implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi harus diiringi dengan peningkatan kesadaran publik, penguatan institusi keamanan siber, serta pembaruan regulasi yang adaptif terhadap dinamika kejahatan digital. Dengan sinergi antara perangkat hukum, kelembagaan, dan literasi digital masyarakat, maka ketahanan siber nasional dapat diperkuat guna melindungi hak privasi warga negara di tengah perkembangan teknologi informasi yang pesat.

DAFTAR REFERENSI

A Sulaiman, M. B. (2024). Implementation of Consumer Personal Data Protection in Ecommerce from the Perspective of Law No. 27 of 2022. *jurnal Word of Science (JWS)*, 410-418.

Anesya Fritiana, S. A. (2025). Penyalahgunaan Data Pribadi Pada Layanan Pinjaman Online: Analisis Perlindungan dan Sanksi Hukum. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, 523-529.

Anggraeni, D. (2023). elindungan Data Pribadi: Antara Regulasi dan Realita. *Jurnal Kebijakan Digital Nasional*, 55–66.

Berto Purnomo Sidik, S. A. (2025). Tinjauan Hukum terhadap Aplikasi Digital sebagai Upaya Meningkatkan Kesadaran Perlindungan Hak Privasi Data Pribadi. *Hukum Inovatif: Jurnal Ilmu Hukum Sosial dan Humaniora*, 219-232.

BSSN. (2022). *Pedoman Perlindungan Infrastruktur Informasi Vital Nasional*. Jakarta: BSSN.

Budiarto, A. (2020). Phishing sebagai Kejahatan Siber: Analisis Hukum Pidana. *Jurnal Hukum dan HAM*, 20–35.

Elvina Putri Maheswari, S. A. (2025). Urgensi persetujuan pemilik data dalam pengelolaan data pribadi oleh platform digital. *Jurnal Ilmu Komunikasi Dan Sosial Politik*, 08-914.

Fadillah, N. (2022). Tinjauan Kriminologis terhadap Kejahatan Phishing. *Jurnal Kriminologi Indonesia*, 45–58.

Hadi, F. &. (2023). Cybercrime dan Pelindungan Privasi Digital di Indonesia. *Jurnal Arsitekta*, 15–27.

Haris, A. (2023). Literasi Digital sebagai Upaya Preventif Terhadap Ancaman Phishing. *Jurnal Literasi Siber*, 41–53.

Khetrina Maria Angnesia, S. A. (2025). Analisis Pertanggungjawaban Hukum Pemerintah dalam Menegakkan Pelindungan Data Pribadi di Era Digital. *Perspektif Administrasi Publik dan hukum*, 176-187.

Kominfo. (2023). *Modul Perlindungan Data Pribadi untuk Publik.* Jakarta: Kemenkominfo.

Kurniawan, R. (2023). Analisis Yuridis terhadap Perlindungan Data Pribadi di Indonesia. *Indonesian Social Science Review*, 40–51.

Kurniawan, R. D. (2023). Pengaruh Literasi Keuangan terhadap Perilaku Konsumtif Mahasiswa di Kota Bandung. *urnal Wawasan Sosial*, 215-225.

Marzuki, P. M. (2005). *Penelitian Hukum.* Jakarta: Kencana Prenada Media Group.

Maulana, I. (2022). UU PDP dan Tantangan Implementasinya dalam Konteks Digital. *Jurnal Legislasi Indonesia*, 150–162.

Mertokusumo, S. (2003). *Penemuan Hukum: Sebuah Pengantar.* Yogyakarta: Liberty.

Mulyani, D. (2023). Perlindungan Data Pribadi dalam Transaksi Elektronik. *urnal Ekonomi Digital*, 12-24.

Nasution, A. (2021). Penanggulangan Phishing oleh Aparat Penegak Hukum. *Jurnal Hukum dan Teknologi*, 110–122.

Negara, B. S. (2023). *Laporan Tahunan Keamanan Siber Nasional.* Jakarta: BSSN.

Notoatmodjo, S. (2010). *Metodologi Penelitian Kesehatan.* Jakarta: Rineka Cipta.

Polri, D. B. (2021). *Prosedur Penanganan Kejahatan Siber.* Jakarta: Mabes Polri.

Pratama, A. (2023). Pelindungan Data Pribadi dalam Era Digital: Tinjauan UU PDP. *Jurnal Penelitian Sosial*, 22-35.

Rachmadi, U. (2020). *Metode Penelitian Ilmu Hukum.* Jakarta: Sinar Grafika.

Rahman, A. &. (2023). Efektivitas Media Sosial sebagai Sarana Komunikasi Politik di Era Digital. *Jurnal Politik Sosialisme*, 111-128.

Salim, H. S. (2013). *Penerapan Teori Hukum pada Penelitian Tesis dan Disertasi.* Jakarta: Raja Grafindo Persada.

Sari, I. (2023). Ancaman Phishing terhadap Keamanan Informasi dan Peran Masyarakat. *Jurnal Wawasan Sosial*, 55–67.

Shafa Salsabila, S. A. (2025). Pertanggungjawaban hukum atas pelanggaran data pribadi dalam perspektif Undang-Undang Pelindungan Data Pribadi Indonesia. *Konsensus: Jurnal Ilmu Pertahanan, Hukum dan Ilmu Komunikasi*, 145-157.

Sidi, A. w. (2025). EKSPLORASI METODE PENELITIAN DENGAN PENDEKATAN NORMATIF DAN EMPIRIS DALAM PENELITIAN HUKUM DI INDONESIA. *Lex Jurnalica*, 66-72.

Sihombing, T. (2021). Kolaborasi Pemerintah dalam Menangani Ancaman Siber. *Jurnal Kebijakan Publik*, 66–77.

Simanjuntak, J. (2022). Sanksi terhadap Pengendali Data dalam UU PDP. *Jurnal Etika Digital*, 33-44.

Situmorang, B. &. (2023). Analisis Pelaksanaan Perlindungan Data Pribadi di Instansi Pemerintah Berdasarkan UU No. 27 Tahun 2022. *Indonesian Social Science*, 345-359.

Soekanto, S. (2007). *Pengantar Penelitian Hukum.* Jakarta: UI Press.

Sulaiman, B. (2021). Tinjauan Hukum terhadap Serangan Phishing dan Peran Negara. *Jurnal Hukum & HAM Digital*, 12–25.

Suteki & Taufani, A. (2018). *Metodologi Penelitian Hukum: Filsafat, Teori, dan Praktik.* Depok: Rajawali Pers.

Wijaya, R. (2021). iterasi Digital sebagai Upaya Pencegahan Kejahatan Siber. *urnal Komunikasi Digital*, 78–89.

Wiraguna, S. P. (2024). Metode Penelitian Kualitatif di Era Transformasi Digital. *Arsitekta: Jurnal Arsitektur dan Kota Berkelanjutan*, 59-60.

Wyanda Kinanti Syauqi Ramadhani, S. A. (2025). Implementasi Pelindungan Data Pribadi dalam Sistem Informasi pada Perusahaan Jasa Keuangan. *Perspektif Administrasi Publik dan hukum*, 158-175.

Yusuf, R. (2022). Strategi Nasional Keamanan Siber Indonesia: Tantangan dan Solusi. *Jurnal Keamanan Nasional*, 30-44.

Zainuddin, A. (2021). Pendekatan Yuridis dalam Kajian Perlindungan Data Pribadi. *Jurnal Hukum dan Regulasi Digital*, 100–111.