Journal of Innovative and Creativity
Journal Homepage: https://joecy.org/index.php/joecy
e-mail: galungwaknook@gmail.co

Faculty of Education
University of Pahlawan Tuanku Tambusai
ISSN 2775-771X (Online)
ISSN 2962-570X (Printed)
6 (1) 2026, Page: 5854-5861

ANALISIS KEBIJAKAN PRIVASI DAN TANGGUNG JAWAB PLATFORM DIGITAL DALAM MENCEGAH PHISHING

Ibnu Fahmi[1], Muhammad Azka[2], Asmak Ul Hosnah[3]
[1 2 3] ***Fakultas Hukum, Universitas Pakuan Bogor***
Email: [1]ibnufahmi2207@gmail.com , [2]azkam619@gmail.com , [3]asmak.hosnah@unpak.ac.id

Published: Januari, 2026

ABSTRACT

Phishing attacks, which result in significant losses for digital platform users, are one of the most common types of cybercrime. This study examines how privacy policies and digital platforms' responsibilities in preventing phishing in Indonesia relate to each other. A juridical-normative approach was used in the research. This included examining relevant regulations such as the Electronic Information and Transactions Law (UU ITE) and regulations concerning Personal Data Protection, as well as evaluating how privacy policies are implemented on various digital platforms. The results indicate that, despite existing laws governing the security and protection of personal data, most platforms still do not implement the best protection standards. Factors that increase the likelihood of phishing include unclear data management, inadequate user instructions, and poor threat verification and warning systems. Furthermore, threat management is often ineffective because it is unclear how platforms, users, and electronic system operators are held accountable. This study suggests that strengthened regulations, higher security standards, and cross-sectoral collaboration are crucial to reducing losses caused by phishing. These findings are expected to form the basis for developing a better data protection and cybersecurity strategy in Indonesia.

Keywords : *Phishing, Privacy Policy, Digital Platform, Cyber Security, Personal Data.*

ABSTRAK

Serangan phishing, yang mengakibatkan kerugian besar bagi pengguna platform digital, merupakan salah satu jenis kejahatan siber yang paling umum terjadi. Studi ini melihat bagaimana kebijakan privasi dan tanggung jawab platform digital dalam upaya mencegah phishing di Indonesia berhubungan satu sama lain. Metode yuridis-normatif digunakan dalam penelitian. Ini mencakup pemeriksaan peraturan terkait seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan peraturan mengenai Perlindungan Data Pribadi, serta evaluasi bagaimana kebijakan privasi diterapkan pada berbagai platform digital. Hasilnya menunjukkan bahwa, meskipun ada undang-undang yang mengatur keamanan dan perlindungan data pribadi, sebagian besar platform masih belum menerapkan standar perlindungan terbaik. Faktor-faktor yang meningkatkan kemungkinan phishing termasuk pengelolaan data yang tidak jelas, instruksi pengguna yang tidak memadai, dan sistem verifikasi dan peringatan ancaman yang buruk. Selain itu, penanganan ancaman seringkali tidak efektif karena tidak jelas bagaimana platform, pengguna, dan penyelenggara sistem elektronik bertanggung jawab. Studi ini menunjukkan bahwa penguatan regulasi, standar keamanan yang lebih tinggi, dan kerja sama lintas sektor sangat penting untuk mengurangi kerugian yang disebabkan oleh phishing. Hasil ini diharapkan dapat menjadi dasar untuk membangun strategi perlindungan data dan keamanan siber yang lebih baik di Indonesia.

Kata Kunci : Phishing, Kebijakan Privasi, Platform Digital, Keamanan Siber, Data Pribadi.

© The Author(s). 2021 Open Access This article is licensed under a Creative Commons Atibution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0

PENDAHULUAN

Digitalisasi telah masuk ke berbagai bagian kehidupan karena kemajuan teknologi informasi dan komunikasi. Ini termasuk sektor perbankan, pendidikan, perdagangan, dan layanan publik. Banyak keuntungan dari transformasi ini, termasuk efisiensi, kemudahan akses, dan percepatan penyebaran data. Namun, kemajuan tersebut juga diiringi oleh peningkatan kejahatan siber, salah

satunya phishing.[1] Phishing adalah jenis penipuan yang menggunakan teknik rekayasa sosial untuk mendapatkan informasi pribadi dan finansial pengguna secara ilegal.[2] Fenomena ini semakin marak seiring meningkatnya penggunaan internet dan platform digital, menimbulkan ancaman besar bagi keamanan data pribadi dan stabilitas ekosistem digital.

Untuk sebagian besar pengguna, serangan phishing sulit dideteksi karena pelaku membuat situs atau pesan terlihat seperti bank, perusahaan, atau lembaga pemerintah. Metode ini menggunakan kerentanan pengguna yang tidak memahami bahaya keamanan digital. Korban mengalami kerugian yang signifikan sebagai akibat dari pencurian identitas, pengambilalihan akun, dan kehilangan uang. Karena banyaknya kasus phishing, perlu ada peraturan pemerintah dan kebijakan internal untuk melindungi data pribadi dan keamanan digital. Untuk mencegah phishing, platform harus menyediakan sistem keamanan dan mendidik pengguna.[3]

Beberapa undang-undang di Indonesia mengatur perlindungan data pribadi dan keamanan siber, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Peraturan Pemerintah terkait penyelenggaraan sistem elektronik, dan Undang-Undang Perlindungan Data Pribadi (UU PDP). Kerangka hukum ini telah menetapkan kewajiban penyelenggara sistem elektronik untuk melindungi data pribadi, tetapi masih ada beberapa masalah yang menghalangi pelaksanaannya. Tidak semua platform memiliki protokol keamanan yang memadai, seperti autentikasi berlapis, notifikasi aktivitas mencurigakan, dan sistem pelaporan cepat atas dugaan phishing. Selain itu, perbedaan dalam standar perlindungan data antar platform dapat menimbulkan masalah keamanan.

Banyak platform menggunakan kebijakan privasi dalam bahasa yang sulit dipahami, sehingga pengguna tidak tahu bagaimana mengelola data mereka. Hal ini mengakibatkan kesadaran dan kewaspadaan yang rendah terhadap kemungkinan penyalahgunaan data. Selain itu, ada beberapa situasi di mana masih ada ambiguitas mengenai tanggung jawab platform dalam kasus kebocoran data yang disebabkan oleh serangan phishing. Karena ketidakjelasan ini, ada perdebatan tentang siapa yang bertanggung jawab atas kerugian yang dialami pengguna.

Berdasarkan uraian tersebut, analisis kebijakan privasi dan tanggung jawab platform digital menjadi penting untuk memahami sejauh mana peran platform dalam mencegah phishing.[4] Dengan melihat peraturan yang berlaku dan pelaksanaannya di lapangan, penelitian ini diharapkan dapat memberikan gambaran tentang seberapa efektif kebijakan privasi dan tanggung jawab platform terhadap keamanan data pengguna. Selain itu, penelitian ini bertujuan untuk memberikan saran praktis tentang cara pemerintah, platform digital, dan masyarakat dapat meningkatkan upaya pencegahan phishing agar lingkungan digital menjadi lebih aman dan terpercaya.[5]

METODE PENELITIAN

Metode penelitian ini menggunakan yuridis normatif, yaitu suatu pendekatan yang berpusat pada analisis aturan hukum tertulis sebagai dasar analisis. Berbagai undang-undang, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Perlindungan Data Pribadi (UU PDP), dan peraturan pelaksana terkait penyelenggaraan sistem elektronik,

---

[1] Anjheli, D. (2024). Privasi Digital dan Kejahatan Phishing di Indonesia: Evaluasi Kritis terhadap Efektivitas UU ITE dan UU PDP. *Staatsrecht: Jurnal Hukum Kenegaraan dan Politik Islam*, *4*(1), 165-189.

[2] Sahfitri, A., & Rosmalinda, R. (2024). PENIPUAN DIGITAL MELALUI TAUTAN PHISHING. *Jurnal Dialektika Hukum*, *6*(2), 92-107.

[3] Nervia, C., Wardhana, K. A., Sie, P. A., Talim, T. L., & Hizkia, W. B. (2025). ANALISIS YURIDIS TERHADAP KEJAHATAN PHISING DALAM SISTEM PERBANKAN DIGITAL MELALUI SCAM LINK BERBAHAYA. *Ikon--Jurnal Ilmiah Ilmu Komunikasi*, *29*(2), 13-30.

[4] Tabrani, S., Safitri, V., & Hosnah, A. U. (2024). KEJAHATAN PHISHING DITINJAU DARI PERSPEKTIF HUKUM DAN KEJAHATAN SIBER. *Civilia: Jurnal Kajian Hukum dan Pendidikan Kewarganegaraan*, *3*(1), 1-13.

[5] Mono, J. R. (2024). Perlindungan Hukum Terhadap Hak Privasi Subjek Data Pribadi dalam Insiden Serangan Siber Pusat Data Nasional Sementara. *Jurnal Ilmu Hukum, Humaniora dan Politik (JIHHP)*, *5*(1).

berkontribusi pada metode ini. Peraturan ini mencakup keamanan siber dan perlindungan data pribadi. Selain itu, penelitian ini melihat dokumen kebijakan privasi dari berbagai platform digital untuk melihat bagaimana aturan dan pelaksanaan berlaku. Analisis dilakukan untuk menentukan dasar hukum, prinsip perlindungan data, dan tanggung jawab platform digital untuk mencegah phishing.

Penelitian ini menggunakan bahan hukum sekunder seperti literatur akademik, jurnal ilmiah dan penelitian sebelumnya. Data dianalisis secara kualitatif dengan menafsirkan dan mengaitkan undang-undang dengan praktik nyata di lapangan, terutama mengenai kebijakan privasi dan tanggung jawab platform digital. Metode ini memungkinkan peneliti untuk menilai sejauh mana undang-undang memberikan keamanan dan perlindungan bagi pengguna serta menemukan kelemahan atau kekosongan undang-undang yang dapat digunakan untuk phishing. Penelitian ini diharapkan dapat memberikan gambaran menyeluruh tentang seberapa efektif undang-undang dalam mencegah phishing serta jalan menuju pengembangan hukum yang lebih responsif terhadap dinamika kejahatan siber.

A. Rumusan Masalah

1. Bagaimana peraturan hukum Indonesia menangani kebijakan privasi dan perlindungan data pribadi di platform digital untuk mencegah phishing?
2. Sejauh mana implementasi keamanan dan kebijakan privasi yang diterapkan oleh platform digital dapat mencegah phishing?
3. Bagaimana tanggung jawab platform digital dalam kasus phishing yang merugikan pengguna? Apa faktor yang mempengaruhinya?

HASIL DAN PEMBAHASAN

1. Regulasi Kebijakan Privasi untuk Pencegahan Phishing di Indonesia

Dengan pesatnya kemajuan digital di Indonesia, muncul tantangan baru dalam hal keamanan data dan privasi pengguna. Salah satunya adalah ancaman phishing, yang menargetkan pengguna platform digital dengan menyalahgunakan data pribadi mereka. Untuk menangani situasi ini, peraturan kebijakan privasi menjadi salah satu alat penting dalam kerangka perlindungan data pribadi dan pencegahan kejahatan siber. Dalam hal Indonesia, peraturan ini mencakup pembuatan dokumen kebijakan pengguna di platform digital serta standar yang mengatur bagaimana data pribadi dikumpulkan, diproses, disimpan, dan dilindungi. Untuk memastikan bahwa platform beroperasi dengan baik, ada peraturan yang jelas yang memastikan bahwa kewajiban mereka terhadap pengguna adalah nyata dan tidak hanya formalitas dengan tujuan utama untuk mengurangi kemungkinan phishing.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) adalah peraturan utama tentang kebijakan privasi Indonesia.[6] UU PDP definisi data pribadi sebagai "data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi. baik secara langsung maupun tidak langsung melalui sistem elektronik atau non-elektronik." UU PDP juga menetapkan bahwa semua upaya untuk melindungi data pribadi meliputi Dengan UU PDP, peraturan tentang kebijakan privasi Indonesia lebih jelas, menuntut platform digital untuk menyusun kebijakan privasi sesuai dengan peraturan nasional dan memasukkan proses keamanan data ke dalam tanggung jawab mereka.

Transparansi, kewajaran, tujuan terbatas (tujuan terbatas), akurasi, keamanan data, dan pembatasan penyimpanan adalah prinsip dasar kebijakan privasi yang diatur dalam UU PDP.[7] Menurut prinsip-prinsip ini, platform digital harus menerbitkan kebijakan privasi mereka sebagai dokumen legal dan melakukan pengumpulan dan pengolahan data dengan persetujuan

6 Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Lembaran Negara 2022 No. 196.

7 Wibowo, Y., Wulan, I. A. D. P., & Ismiyanto, I. (2025). Tinjauan Yuridis Tentang Perlindungan Data Pribadi Masyarakat Pada Era Digitalisasi. *JURNAL PENELITIAN SERAMBI HUKUM*, *18*(01), 1-6.

yang jelas, menyediakan informasi yang mudah dipahami oleh pengguna, dan menetapkan jangka waktu penyimpanan yang tidak melebihi kebutuhan.[8] Kebijakan privasi yang mencakup aturan seperti verifikasi identitas pengguna, prosedur pelaporan insiden, dan pemberitahuan aktivitas mencurigakan sangat penting untuk mencegah phishing. Oleh karena itu, peraturan kebijakan privasi harus mencakup elemen teknis yang dapat memperbaiki kesalahan yang sering digunakan pelaku phishing, seperti pengumpulan data tanpa persetujuan atau melalui situs web palsu.

Selain itu, peraturan kebijakan privasi Indonesia mewajibkan penyelenggara sistem elektronik, juga dikenal sebagai platform digital, yang berfungsi sebagai pengendali atau prosesor data pribadi, untuk menjaga keamanan data pribadi dan mencegah kebocoran atau penyalahgunaan data. Pengendali data diwajibkan oleh UU PDP untuk mengambil langkah-langkah organisasional dan teknis yang tepat untuk mengurangi risiko terhadap subjek data. Untuk mencegah phishing, tanggung jawab ini dapat berupa mekanisme autentikasi berlapis, enkripsi data, pengawasan aktivitas mencurigakan, dan pelaporan pelanggaran atau kebocoran segera. Meskipun ada standar yang kuat untuk kebijakan privasi, kinerja platform digital sangat bergantung pada bagaimana kewajiban ini diterapkan dalam operasi harian.

Meskipun UU PDP telah memperkuat kebijakan privasi Indonesia, masih ada masalah dalam pelaksanaannya yang dapat memengaruhi upaya pencegahan phishing. Sebuah penelitian menunjukkan bahwa, meskipun ada peraturan yang tersedia, banyak platform masih gagal memenuhi persyaratan tata kelola data pribadi. Hal ini dapat disebabkan oleh kekurangan sumber daya, pemahaman yang buruk tentang keamanan, dan kekurangan peraturan pelaksana yang sudah siap.[9] Di antara masalah ini adalah kurangnya pengawasan independen, belum terbentuknya lembaga pengawas yang efektif untuk operasional, dan ketidaksesuaian antara regulasi sektoral yang menyebabkan tingkat kepatuhan kebijakan privasi di platform digital berbeda. Dalam kasus ini, pelaku phishing dapat memanfaatkan kelemahan aturan atau implementasi yang buruk untuk mengeksploitasi data pengguna atau memanipulasi sistem keamanan platform.

Regulasi kebijakan privasi harus dilengkapi dengan pedoman teknis, standar minimum keamanan, dan prosedur audit dan sanksi yang jelas untuk mengimbangi aturan dan praktik. Untuk pelanggaran data pribadi, UU PDP sendiri telah menetapkan sanksi administratif dan pidana, mulai dari peringatan hingga denda dan penangguhan pemrosesan data. Namun, untuk mencegah phishing, sanksi ini harus diterapkan dengan hati-hati.[10]Misalnya, platform yang gagal mendeteksi dan melaporkan peristiwa phishing atau kehilangan data pengguna dapat dikenai konsekuensi hukum yang lebih berat. Untuk menjadi bagian dari sistem perlindungan, peraturan kebijakan privasi harus menentukan siapa yang harus melaporkan insiden, melakukan audit keamanan secara teratur, dan mendidik pengguna.

Akhirnya, kebijakan privasi untuk mencegah phishing di Indonesia mencakup tidak hanya "apa yang tertulis dalam kebijakan" tetapi juga "bagaimana kebijakan itu dioperasikan". Peraturan nasional telah membentuk kerangka hukum yang kuat, tetapi keberhasilan mencegah phishing sangat bergantung pada kolaborasi kebijakan privasi, tanggung jawab teknis-organisasi platform, dan pengetahuan pengguna. Oleh karena itu, penyusunan kebijakan privasi oleh platform digital Dengan cara ini, peraturan kebijakan privasi dapat benar-benar berguna untuk melindungi pengguna di ekosistem digital Indonesia yang semakin kompleks.

2. Efektivitas Tindakan Keamanan dan Kebijakan Privasi Platform Digital terhadap Serangan Phishing

Untuk mencegah serangan phishing, yaitu upaya penipuan yang meniru institusi sah dan mengecoh pengguna untuk memberikan kredensial atau data pribadi, platform digital di

[8] Fathaniyah, L., Makbul, M., & Makhrus, M. (2023). Urgensi Perlindungan Data Pribadi pada Transaksi e-Commerce Terhadap Pembangunan Ekonomi di Indonesia. *Jurnal Hukum Ekonomi Syariah*, *6*(2), 77-88.

[9] Rinjani, M. A., & Firmansyah, R. (2025). Hambatan Implementasi UU 27/2022 dan Strategi Penguatan Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *8*(1), 70-83.

[10] Mirna, M. (2023). Analisis Pengaturan Keamanan Data Pribadi Di Indonesia. *Jurnal Ilmiah Living Law*, *15*(1), 16-30.

Indonesia telah menerapkan berbagai kebijakan privasi dan mekanisme keamanan. Kebijakan privasi umumnya mencakup persetujuan pengguna, transparansi pengolahan data, hak akses dan koreksi data, serta jaminan bahwa data disimpan dengan aman. Banyak platform menggunakan autentikasi dua faktor, enkripsi data, pemantauan aktivitas mencurigakan, dan sistem pelaporan insiden dalam hal teknologi keamanan. Namun, masih perlu dilakukan penelitian empiris untuk mengetahui apakah strategi ini berhasil mencegah phishing. Ini harus dilakukan dengan melihat kasus dan data terbaru.

Salah satu kasus yang relevan adalah tindakan Group-IB di Indonesia yang melibatkan pembajakan lebih dari 600 akun Instagram untuk menyebarkan tautan phishing yang meniru halaman login aplikasi perbankan. Dalam kasus ini, pelaku menggunakan akun sah yang tidak memiliki autentikasi multi-faktor (MFA), kemudian mengubah email pemilik asli, mengaktifkan MFA baru, dan menggunakan akun tersebut sebagai alat phishing yang kuat. Kasus ini menunjukkan bahwa, meskipun Instagram memiliki kebijakan keamanan seperti Multi-Factor Authentication (MFA) dan laporan aktivitas mencurigakan, masih ada masalah dalam pengaturan dan pengamanan akun pengguna yang memungkinkan phishing besar.[11]

Data Kaspersky juga menunjukkan bahwa sistem pendeteksian Kaspersky berhasil mencegah lebih dari 85.908 upaya phishing keuangan di Indonesia sepanjang tahun 2024.[12] Angka-angka ini menunjukkan bahwa meskipun langkah-langkah perlindungan telah dimulai, kebijakan privasi dan platform digital belum cukup untuk mengurangi risiko serangan secara signifikan. Ini menunjukkan bahwa literasi digital dan kewaspadaan pengguna tetap sangat penting untuk kebijakan dan sistem keamanan platform.

Kasus terbaru yang relevan adalah penangkapan dua warga Malaysia oleh Kepolisian Daerah Metro Jaya yang menyamar sebagai bank besar dalam SMS phishing massal ke pengguna Jakarta. Salah satu korban kehilangan sekitar Rp 100 juta. Modus ini menunjukkan bahwa platform digital tidak hanya menghadapi serangan melalui situs web atau aplikasi tetapi juga melalui kanal komunikasi eksternal (SMS) yang terkait dengan layanan digital. Ini memperluas daftar kebijakan privasi dan keamanan yang harus dipertimbangkan oleh platform digital.[13]

Dari perspektif kebijakan privasi, perlu dipertimbangkan seberapa jauh platform memberi tahu pengguna tentang risiko phishing, bagaimana mereka membuat kebijakan yang mengharuskan pengguna melakukan autentikasi yang kuat, dan bagaimana mereka menyediakan mekanisme untuk melaporkan insiden. Banyak kebijakan privasi platform masih sangat umum dan tidak mencakup phishing atau pelanggaran data yang mungkin terjadi akibat serangan tersebut. Studi menunjukkan bahwa undang-undang seperti Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) belum secara eksplisit mendefinisikan phishing sebagai tindakan kriminal yang berbeda. Akibatnya, kebijakan dan mekanisme keamanan platform sering terbatas pada pengolahan data pribadi umum.

Selain itu, kebijakan platform harus terintegrasi dengan operasi platform untuk keamanan teknis. Sebagai contoh, platform digital yang menyediakan layanan pembayaran atau e-commerce harus memantau domain palsu, melakukan penguncian otomatis (auto-lock) ketika otentikasi mencurigakan terjadi, dan memberikan pemberitahuan kepada pengguna secara real-time tentang aktivitas yang tidak biasa. Studi menunjukkan bahwa pelaku memanfaatkan peluang dari akun yang belum di-MFA dalam kampanye phishing yang besar, dan dom-situs yang baru dibuat sering lolos sebelum platform memblokirnya. Kasus Group-IB menunjukkan bahwa proses deteksi dan blokir bukanlah otomatis dan membutuhkan sikap proaktif dari platform digital, meskipun domain palsu dan tautan phishing sudah dihilangkan.

Kita dapat melihat bahwa kinerja kebijakan dan keamanan masih sangat buruk, berdasarkan data dari Otoritas Jasa Keuangan (OJK) yang menunjukkan bahwa kerugian

---

11 Alharbi, N., Alkalifah, B., Alqarawi, G., & Rassam, M. A. (2024). *Countering social media cybercrime using deep learning: Instagram fake accounts detection. Future Internet, 16*(10), 367.

12 ANTARA. (11 Maret 2025). *500 ribu phishing serang perangkat bisnis di Asia Tenggara pada 2024*. ANTARA News.

13 Polda Metro Jaya. (2025, June 24). *3 WN Malaysia tipu Warga Indonesia lewat SMS palsu, minta korban cek poin*. Kompas.com.

akibat penipuan digital, termasuk phishing, akan mencapai ratusan miliar rupiah hingga akhir 2024.[14] Serangan phishing yang cepat, skala besar, dan menggunakan berbagai kanal tidak dapat dicegah dengan kebijakan privasi yang hanya menyatakan bahwa "data akan dilindungi" tanpa rincian teknis atau mekanisme respons. Untuk mencapai hal ini, platform digital harus meninjau ulang kebijakan keamanan dan privasi mereka secara berkala dan mengikuti standar global tertinggi.

3. Tanggung Jawab Platform Digital terhadap Kerugian Pengguna Akibat Phishing

a) Tanggung Jawab Hukum (Legal Responsibility)

Platform digital diwajibkan untuk mematuhi peraturan nasional tentang keamanan siber dan perlindungan data pribadi, seperti UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) dan UU ITE. Peraturan-peraturan ini melibatkan tanggung jawab untuk mencegah data pengguna dibocorkan atau disalahgunakan. Pengguna yang tertipu oleh phishing yang terjadi karena kelalaian platform dapat dikenai sanksi administratif maupun pidana sesuai ketentuan hukum karena dianggap gagal memenuhi kewajiban normatif pemerintah.

b) Tanggung Jawab Teknis (Technical Responsibility)

Autentikasi multi-faktor (MFA), enkripsi data, pemantauan domain palsu, dan logging aktivitas mencurigakan adalah langkah-langkah yang harus dilakukan oleh platform untuk memastikan sistem teknis mereka aman dari ancaman phishing. Jika serangan phishing berhasil merugikan pengguna, tanggung jawab platform meningkat karena kelalaian dianggap sebagai bentuk kelalaian.

c) Tanggung Jawab Kebijakan Privasi (Policy Responsibility)

Setiap platform harus membuat dan menerapkan kebijakan privasi yang jelas dan mudah dipahami yang menjelaskan bagaimana data dikumpulkan, digunakan, dan dilindungi. Kebijakan ini harus jelas dan mudah dipahami oleh pengguna, termasuk bagaimana melaporkan phishing. Jika kebijakan ini tidak memadai atau ambigu, tanggung jawab platform akan meningkat karena pengguna tidak tahu bagaimana melindungi diri dari phishing.

d) Tanggung Jawab Edukasi Pengguna (User Education Responsibility)

Pengguna harus diberitahu oleh platform tentang keamanan digital dan bahaya phishing. Panduan pencegahan, kampanye kesadaran, dan petunjuk untuk perlindungan akun semuanya termasuk dalam kategori tanggung jawab ini. Kurangnya pengetahuan dapat meningkatkan kemungkinan pengguna menjadi korban phishing, jadi platform juga bertanggung jawab atas kerugian.

e) Tanggung Jawab Penanganan Insiden (Incident Response Responsibility)

Ketika terjadi serangan phishing, platform harus memiliki prosedur tanggap darurat. Prosedur ini mencakup menerima laporan pengguna, menghentikan akses akun yang disusupi, memulihkan keamanan sistem, dan berkomunikasi dengan pihak berwenang. Karena keterlambatan respons meningkatkan kerugian pengguna, ketidakmampuan menindaklanjuti insiden dengan cepat meningkatkan tanggung jawab platform.

f) Tanggung Jawab Audit dan Akuntabilitas (Audit and Accountability Responsibility)

Platform bertanggung jawab untuk menjalani audit internal dan eksternal secara berkala guna memastikan kebijakan privasi dan sistem keamanan berjalan sesuai standar. Bentuk tanggung jawab ini juga mencakup transparansi dalam melaporkan insiden, kesiapan menghadapi investigasi hukum, dan pemenuhan sanksi jika terbukti

[14] Otoritas Jasa Keuangan. (2025, May 10). *Kerugian akibat penipuan tembus Rp 2,1 triliun, OJK blokir 42.000 rekening* [Press release].

lalai.[15] Audit dan akuntabilitas menjadi mekanisme preventif sekaligus korektif agar platform dapat meminimalkan risiko phishing dan memperkuat kepercayaan pengguna.

KESIMPULAN

1. Kebjakan privasi dan sistem keamanan yang diterapkan oleh platform digital sangat penting untuk mencegah serangan phishing, tetapi keberhasilan mereka sangat bergantung pada praktik di lapangan. Kebijakan privasi yang formal tidak cukup untuk melindungi data pribadi dari phishing tanpa dukungan prosedur teknis, edukasi pengguna, dan pemantauan insiden. Namun, penerapan langkah-langkah teknis seperti autentikasi multi-faktor, enkripsi data, pemantauan domain palsu, dan prosedur tanggap insiden terbukti dapat mengurangi risiko, tetapi tetap memerlukan pengawasan terus-menerus dan pembaruan tentang pola serangan terbaru. Hal ini menunjukkan bahwa mencegah phishing memerlukan kerja sama antara hukum, teknologi, dan pengetahuan digital pengguna untuk mencapai hasil terbaik.
2. Pengguna platform digital memiliki banyak tanggung jawab, termasuk hukum, kebijakan, privasi, edukasi, tanggapan terhadap insiden, dan akuntabilitas melalui audit. Ketika terjadi kerugian yang disebabkan oleh phishing, semua tanggung jawab ini berhubungan satu sama lain dan menjadi dasar untuk evaluasi. Ketidakpatuhan atau kelalaian dalam salah satu aspek dapat meningkatkan beban pertanggungjawaban platform secara hukum dan reputasi. Oleh karena itu, platform harus menerapkan strategi pencegahan phishing yang komprehensif, seperti meningkatkan kebijakan privasi, meningkatkan keamanan teknis, dan mengedukasi pengguna secara aktif. Strategi-strategi ini akan meminimalkan risiko kerugian dan meningkatkan kepercayaan pengguna, memberikan kepastian hukum bagi seluruh ekosistem digital Indonesia.
3. Secara keseluruhan, pencegahan phishing di platform digital bergantung pada kebijakan privasi yang tertulis dan sistem keamanan yang diterapkan, serta bagaimana masing-masing komponen diintegrasikan ke dalam rutinitas operasi. Untuk mencegah celah yang sering dimanfaatkan pelaku phishing, platform harus memastikan bahwa prosedur teknis, instruksi pengguna, dan mekanisme tanggap insiden selaras. Selain itu, karena tanggung jawab platform mencakup bidang hukum, teknis, dan pendidikan, kesalahan kecil dapat menyebabkan kerugian besar bagi pengguna sekaligus meningkatkan risiko hukum bagi platform itu sendiri. Platform digital dapat meningkatkan perlindungan data pribadi, meningkatkan kepercayaan pengguna, dan mengurangi efek negatif dari serangan phishing di ekosistem digital Indonesia dengan menggunakan strategi yang terstruktur dan terpadu.

Saran

Untuk mencegah phishing, penulis menyarankan agar platform digital memperkuat kebijakan privasi dan sistem keamanan secara terpadu. Kebijakan privasi harus jelas, jelas, dan mengatur pengumpulan dan pemrosesan data pengguna, dan sistem teknis seperti autentikasi multi-faktor, enkripsi, pemantauan aktivitas mencurigakan, dan prosedur tanggap insiden harus digunakan secara konsisten. Selain itu, pengguna harus dididik lebih baik agar mereka dapat membedakan dan menghindari serangan phishing. Kompleksitas tanggung jawab platform mencakup hukum, teknis, kebijakan, pendidikan, dan akuntabilitas. Studi kasus terbaru menunjukkan bahwa kesalahan teknis dan ketidaksadaran pengguna masih menyebabkan masalah meskipun langkah-langkah ini sudah diterapkan. Oleh karena itu, untuk membuat ekosistem digital yang aman dan

[15] Abdullah, C., Durand, N., & Moonti, R. M. (2025). *Transformasi digital dan hak atas privasi: Tinjauan kritis pelaksanaan UU PDP Tahun 2022 di era big data*. Amandemen: Jurnal Ilmu Pertahanan, Politik dan Hukum Indonesia, 2(3), 233–241.

terpercaya, pendekatan yang menggabungkan regulasi, teknologi, dan literasi digital sangat penting.

DAFTAR PUSTAKA

Anjheli, D. (2024). *Privasi Digital dan Kejahatan Phishing di Indonesia: Evaluasi Kritis terhadap Efektivitas UU ITE dan UU PDP. Staatsrecht: Jurnal Hukum Kenegaraan dan Politik Islam*, *4*(1), 165-189.

Sahfitri, A., & Rosmalinda, R. (2024). *PENIPUAN DIGITAL MELALUI TAUTAN PHISHING. Jurnal Dialektika Hukum*, *6*(2), 92-107.

Nervia, C., Wardhana, K. A., Sie, P. A., Talim, T. L., & Hizkia, W. B. (2025). *ANALISIS YURIDIS TERHADAP KEJAHATAN PHISING DALAM SISTEM PERBANKAN DIGITAL MELALUI SCAM LINK BERBAHAYA. Ikon--Jurnal Ilmiah Ilmu Komunikasi*, *29*(2), 13-30.

Tabrani, S., Safitri, V., & Hosnah, A. U. (2024). *KEJAHATAN PHISHING DITINJAU DARI PERSPEKTIF HUKUM DAN KEJAHATAN SIBER. Civilia: Jurnal Kajian Hukum dan Pendidikan Kewarganegaraan*, *3*(1), 1-13.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Lembaran Negara 2022 No. 196.

Wibowo, Y., Wulan, I. A. D. P., & Ismiyanto, I. (2025). *Tinjauan Yuridis Tentang Perlindungan Data Pribadi Masyarakat Pada Era Digitalisasi. JURNAL PENELITIAN SERAMBI HUKUM, 18(01), 1-6.*

Fathaniyah, L., Makbul, M., & Makhrus, M. (2023). *Urgensi Perlindungan Data Pribadi pada Transaksi e-Commerce Terhadap Pembangunan Ekonomi di Indonesia. Jurnal Hukum Ekonomi Syariah*, *6*(2), 77-88.

Rinjani, M. A., & Firmansyah, R. (2025). *Hambatan Implementasi UU 27/2022 dan Strategi Penguatan Perlindungan Data Pribadi di Indonesia. Jurnal Analisis Hukum, 8(1), 70-83.*

Mirna, M. (2023). *Analisis Pengaturan Keamanan Data Pribadi Di Indonesia. Jurnal Ilmiah Living Law*, *15*(1), 16-30.

Alharbi, N., Alkalifah, B., Alqarawi, G., & Rassam, M. A. (2024). *Countering social media cybercrime using deep learning: Instagram fake accounts detection. Future Internet, 16*(10), 367.

ANTARA. (11 Maret 2025). *500 ribu phishing serang perangkat bisnis di Asia Tenggara pada 2024*. ANTARA News.

Polda Metro Jaya. (2025, June 24). *3 WN Malaysia tipu Warga Indonesia lewat SMS palsu, minta korban cek poin*. Kompas.com.

Otoritas Jasa Keuangan. (2025, May 10). *Kerugian akibat penipuan tembus Rp 2,1 triliun, OJK blokir 42.000 rekening* [Press release].

bdullah, C., Durand, N., & Moonti, R. M. (2025). *Transformasi digital dan hak atas privasi: Tinjauan kritis pelaksanaan UU PDP Tahun 2022 di era big data.* Amandemen: Jurnal Ilmu Pertahanan, Politik dan Hukum Indonesia, 2(3), 233–241.