ANALISIS PENEGAKAN HUKUM OLEH KEMENTERIAN KOMUNIKASI DAN INFORMATIKA TERHADAP TINDAK PIDANA PHISHING BERDASARKAN UNDANGUNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK DAN UNDANG-UNDANG PERLINDUNGAN DATA PRIBADI.

Nur Aulia Apriliani[1], Ananda Dwi Indriyani[2], Fitriana Dianty[3], Adinda Nofitria[4], Beril Fahrezi Ihsan[5], Dhimas Saputra[6], Maulana[7], Sunariyo[8]
2311102432187@umkt.ac.id[1], 2311102432171@umkt.ac.id[2], 2311102432057@umkt.ac.id[3], 2311102432061@umkt.ac.id[4], 2311102432056@umkt.ac.id[5], 231110243206@umkt.ac.id[6], 2311102432124@umkt.ac.id[7], sun487@umkt.ac.id[8]
Universitas Muhammadiyah Kalimantan Timur

ABSTRAK

Penelitian ini membahas Analisis Penegakan Hukum oleh Kementerian Komunikasi dan Informatika terhadap Tindak Pidana Phishing berdasarkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Perlindungan Data Pribadi (UU PDP). Latar belakang penelitian didasarkan pada meningkatnya kasus phishing yang terkonfirmasi melalui data Pusiknas Bareskrim Polri serta laporan IDADX yang menunjukkan lonjakan signifikan pada tahun 2025. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan, konseptual, dan komparatif, menggunakan bahan hukum primer berupa Undang-Undang Informasi Transaksi dan Elektronik (UU ITE), Undang-Undang Perlindungan Data Pribadi (UU PDP), Peraturan Kementerian Komunikasi dan Informatika terbaru, serta Kitab Undang-Undang Hukum Acara Pidana (KUHAP), dan didukung bahan hukum sekunder dari literatur dan laporan lembaga terkait. Hasil penelitian menunjukkan bahwa meskipun kerangka hukum Indonesia telah cukup memadai, implementasi penegakan hukum terhadap phishing masih menghadapi hambatan berupa keterbatasan koordinasi antar-lembaga, kendala teknis pemblokiran, rendahnya literasi digital masyarakat, serta tantangan yurisdiksi lintas negara. Penelitian ini menyimpulkan bahwa penanggulangan phishing membutuhkan sinergi antara regulasi yang kuat, pelaksanaan hukum yang konsisten, optimalisasi peran Kominfo, serta partisipasi masyarakat dalam menjaga keamanan data pribadi.

Kata Kunci: Phishing, Penegakan Hukum, Undang-Undang Informasi Dan Transaksi Elektronik (UU ITE), Undang-Undang Perlindungan Data Pribadi (UU PDP), Kominfo, Cybercrime.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan besar dalam kehidupan masyarakat, baik dalam aspek sosial, ekonomi, maupun pemerintahan. Kemudahan akses internet dan layanan digital tidak hanya memberikan manfaat, tetapi juga memunculkan ancaman baru berupa kejahatan siber *(cybercrime)*. Salah satu bentuk *cybercrime* yang paling banyak terjadi adalah *phishing*, yaitu tindak pidana yang dilakukan dengan cara mengelabui korban untuk memperoleh data pribadi atau informasi sensitif yang kemudian disalahgunakan untuk kepentingan tertentu.

Di Indonesia, tindak pidana *phishing* semakin marak seiring meningkatnya aktivitass digital masyarakat. Data Pusat Informasi Kriminal Nasional (Pusiknas) Bareskrim Polri menunjukkan terjadi peningkatan jumlah kejahatan manipulasi data secara ITE. Pada 2023, Polri menindak 11.286 kasus dengan jumlah rata-rata tiap bulan yaitu 940 kasus kejahatan manipulasi data secara ITE. Pada 2024, jumlah kasus meningkat 23,35% dibanding jumlah

pada 2023. Di sepanjang 2024, Polri menindak 13.922 kasus dengan jumlah rata-rata tiap bulan yaitu 1.160 kasus kejahatan manipulasi data secara ITE. Lalu pada 5 (lima) bulan pertama di 2025, Polri menindak 7,423 kasus dengan jumlah rata-rata 1.484 kasus kejahatan manipulasi data secara ITE. Jumlah tersebut mencapai 53,31% dari jumlah penindakan kasus kejahatan manipulasi secara ITE dalam setahun penuh di 2024 dan angka rata-rata tiap bulan meningkat 27,93% dibanding angka rata-rata per bulan kasus kejahatan tersebut di 2024[1]. Fakta ini menggambarkan bahwa phishing menjadi ancaman serius dalam perkembangan kejahatan siber di Indonesia.

Data serupa juga tercermin dari laporan IDADX (Indonesia Anti-Domain Abuse Center). Pada Kuartal I tahun 2025, tercatat 2.470 laporan phishing yang menggunakan domain berekstensi .id[2]. Laporan ini menegaskan bahwa phishing bukan hanya merugikan individu dan lembaga, tetapi juga mengancam ekosistem digital nasional karena memanfaatkan infrastruktur domain Indonesia sebagai sarana kejahatan.

Pemerintah Melalui Kementerian Komunikasi dan Informatika (Kominfo), memiliki peran sentral dalam menanggulangi kejahatan phishing. Upaya yang dilakukan meliputi regulasi, pemblokiran konten berbahaya, edukasi literasi digital, hingga koordinasi dengan aparat penegak hukum dan lembaga terkait. Penegakan hukum atas phishing juga didukung oleh instrumen hukum seperti Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) memuat ketentuan mengenai larangan akses ilegal, penyalahgunaan data elektronik, dan manipulasi informasi. Selain itu, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) memberikan perlindungan hukum bagi hak-hak subjek data sekaligus mengatur kewajiban pengendali data. Di sisi lain, Kitab UndangUndang Hukum Acara Pidana (KUHAP) tetap menjadi dasar umum prosedur penegakan hukum pidana. Sedangkan, Kementerian Komunikasi dan Informatika (Kominfo) berperan melalui berbagai Peraturan Menteri Kominfo yang memberikan pedoman teknis pencegahan, pengawasan, dan penindakan tindak pidana phishing.

Berdasarkan uraian tersebut, penelitian ini penting dilakukan untuk menganalisis penegakan hukum oleh Kementerian Kominfo terhadap tindak pidana phishing berdasarkan Undang-Undang ITE dan Undang-Undang Perlindungan Data Pribadi. Penelitian ini juga menyoroti sejauh mana efektivitas regulasi dan kebijakan pemerintah mampu menjawab tantangan kejahatan phishing yang semakin kompleks, sekaligus menggali upaya-upaya yang dapat memperkuat perlindungan hukum dan efektivitas penindakan kejahatan siber di Indonesia.

METODOLOGI PENELITIAN

Penelitian ini merupakan penelitian hukum normatif (yuridis normatif). Pendekatan yang digunakan dalam penelitian yaitu pendekatan perundang-undangan (Statute approach) dan pendekatan konseptual (conceptual approach). Pendekatan perundang-undangan berfokus pada analisis terhadap norma-norma hukum yang berlaku, sementara pendekatan

[1] https://pusiknas.polri.go.id/detail_artikel/kasus_kejahatan_manipulasi_data_secara_ite_meningkat
[2] https://api.idadx.id/documents/uploads/1745306450_Laporan%20Q1%202025%20English.pdf.pdf?utm_source=

konseptual lebih menitikberatkan pada konsep-konsep hukum yang mendasari perundang-undangan tersebut. Kombinasi kedua pendekatan ini memungkinkan penelitian untuk menggali pemahaman mendalam terkait aspek normatif dan konseptual dalam ranah hukum.

Sumber bahan hukum yang digunakan terdiri atas bahan hukum primer dan bahan hukum sekunder. Bahan hukum primer merupakan bahan hukum yang bersifat autoratif, artinya, mempunyai otoritas. Bahan hukum primer yang digunakan dalam penelitian ini antara lain: Undang-Undang Dasar 1945, Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi, Kitab Undang-Undang Hukum Acara Pidana (KUHAP) dan Peraturan Menteri Komunikasi dan Informatika. Bahan hukum sekunder adalah dokumen atau bahan hukum yang memberikan penjelasan terhadapr bahan hukum primer seperti buku-buku, artikel, jurnal, hasil penelitian, makalah dan lain sebagainya. Bahan hukum sekunder yang digunakan oleh penelitian ini antara lain: Buku, jurnal, artikel hukum siber, serta berita resmi mengenai *phishing*. Pengumpulan bahan hukum dilakukan melalui studi kepustakaan (library research) dengan menelusuri dan menginventarisasi bahan hukum yang relevan kemudian dianalisis secara kualitatif-deskriptif, yaitu dengan menguraikan ketentuan yang berlaku, membandingkan dengan praktik penegakan hukum dan menarik kesimpulan untuk menjawab rumusan masalah penelitian.

HASIL DAN PEMBAHASAN

1. Pengaturan Tindak Pidana Phishing dalam Hukum Positif Indonesia, khususnya berdasarkan Undang-Undang ITE dan Undang-Undang Perlindungan Data Pribadi

Tindak pidana phishing merupakan salah satu bentuk kejahatan siber (cybercrime) yang modus operasinya dilakukan dengan cara menipu korban melalui sarana elektronik agar menyerahkan data pribadi, informasi autentikasi, maupun akses terhadap akun digital. Dalam perspektif hukum pidana Indonesia, phishing dapat dikategorikan sebagai tindak pidana penipuan berbasis elektronik sekaligus pelanggaran terhadap hak atas data pribadi yang telah dijamin oleh hukum. Oleh karena itu, pengaturan mengenai phishing tidak hanya merujuk pada ketentuan dalam Kitab Undang-Undang Hukum Pidana (KUHP) mengenai penipuan secara umum, tetapi juga secara khusus pada peraturan perundang-undangan di bidang hukum siber, yaitu Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana diubah terakhir dengan UU Nomor 1 Tahun 2024, serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP).

Pengaturan tindak pidana phishing dalam hukum positif Indonesia tidak hanya bersumber dari peraturan perundang-undangan nasional, tetapi juga memiliki landasan nilai yang kuat dalam hukum Islam. Islam menekankan keadilan dan kejujuran serta melarang segala bentuk penipuan dan pengambilan hak orang lain secara tidak sah. Hal ini ditegaskan dalam firman Allah SWT:

ضُ عَنۡ تِجَارَةٌ تَكُونَ أَنۡ إِلَّآ بِٱلۡبَٰطِلِ بَيۡنَكُمۡ أَمۡوَٰلَكُمۡ تَأۡكُلُواْ لَا ءَامَنُواْ ٱلَّذِينَ أَيُّهَا وَلَا مِنكُمۡ تَرَا
يَا رَحِي ما بِكُمۡ كَانَ ٱللَّهَ إِنَّ أَنفُسَكُمۡ تَقۡتُلُواْ

Dalam kerangka Undang-Undang ITE, perbuatan phishing dapat dijerat melalui beberapa ketentuan, antara lain:

- Pasal 28 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik: paites“ǒǒgnaro ǒǒdengan sengaja mendistribusikan dan/atau mentransmisikan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi pemberitahuan bohong atau informasi menyesatkan yang mengakibatkan kerugian materiel bagi konsumen dalam Transaksi Elektronik.”[3]

- Pasal 30 ayat (1), (2), (3) Undang-Undang Informasi dan Transaksi Elektronik, yang melarang akses tanpa hak ke dalam sistem elektronik orang lain, termasuk dengan maksud memperoleh data pribadi.
- Pasal 32 ayat (1) dan (2) Undang-Undang Informasi dan Transaksi Elektronik, yang melarang perbuatan mengubah, menambah, mengurangi, mentransmisikan, merusak, menghilangkan, atau membuat tidak dapat digunakan suatu informasi elektronik atau dokumen elektronik milik orang lain tanpa hak.[4]
- Pasal 35 Undang-Undang Informasi dan Transaksi Elektronik: paites“ǒǒgnaroǒǒnagned ǒǒsengaja dan tanpa hak atau melawan hukum melakukan menipulasi, penciptaan, perubahan, penghilangan, pengerusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektrik tersebut dianggap seolah-olah data yang otentik.”

Pasal-pasal tersebut pada prinsipnya memberikan dasar pemidanaan terhadap pelaku phishing karena modusnya selalu terkait dengan manipulasi, penyesatan, atau penguasaan data pribadi orang lain secara melawan hukum.

Sementara itu, Undang-Undang Perlindungan Data Pribadi memberikan dimensi perlindungan hukum yang lebih spesifik terhadap aspek hak subjek data pribadi. Menurut Pasal 1 angka 1 Undang-Undang Perlindungan Data Pribadi, data pribadi adalah setiap data tentang seseorang yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasikan dengan informasi lainnya. Undang-Undang Perlindungan Data Pribadi menegaskan hak-hak subjek data, seperti hak atas privasi, hak untuk memperoleh informasi mengenai penggunaan data pribadinya, hingga hak untuk meminta penghapusan data. Dalam konteks phishing, pelaku secara nyata melakukan pelanggaran terhadap hak subjek data, sehingga dapat dikenakan ketentuan pidana sebagaimana diatur dalam Pasal 65 hingga Pasal 69 Undang-Undang Perlindungan Data Pribadi, yang mengatur sanksi pidana atas perolehan, pengumpulan, pengungkapan, dan penggunaan data pribadi secara melawan hukum.[5]

Dengan demikian, dalam hukum positif Indonesia, tindak pidana phishing ditempatkan sebagai kejahatan siber yang memiliki dimensi ganda: pertama, sebagai perbuatan melawan hukum dalam konteks sistem elektronik menurut Undang-Undang Informasi dan Transaksi Elektronik (UU ITE); dan kedua, sebagai pelanggaran terhadap hak-hak dasar subjek data pribadi sebagaimana dilindungi Undang-Undang Perlindungan Data Pribadi (UU PDP). Penempatan ini menunjukkan bahwa hukum positif Indonesia telah memiliki instrumen normatif yang cukup komprehensif untuk mengkriminalisasi phishing. Namun demikian, keberhasilan penegakan hukum tidak hanya bergantung pada keberadaan norma, melainkan juga pada efektivitas implementasi, koordinasi antar lembaga, serta kesadaran hukum masyarakat dalam melindungi data pribadinya.

2. Penegakan Hukum oleh Kementerian Komunikasi dan Informatika (Kominfo) Terhadap Tindak Pidana Phishing di Indonesia

Penegakan hukum terhadap tindak pidana phishing pada dasarnya merupakan bagian

[3] https://peraturan.bpk.go.id/Details/274494/uu-no-1-tahun-2024

[4] https://peraturan.bpk.go.id/Details/37589/uu-no-11-tahun-2008

[5] *https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022*

dari rezim hukum siber (cyber law) di Indonesia. Posisi Kementerian Komunikasi dan Informatika (Kominfo) dalam kerangka penanggulangan tindak pidana ini dapat dipahami sebagai organ eksekutif yang diberi kewenangan normatif oleh peraturan perundang-undangan untuk menjalankan fungsi administratif, regulatif, dan pengawasan, bukan sebagai aparat penegak hukum dalam arti yudisial. Kominfo tidak melakukan penyidikan atau penuntutan, melainkan menjalankan fungsi cyber patrol, pemblokiran akses, penghapusan konten, serta fasilitasi

koordinasi dengan aparat penegak hukum, khususnya Kepolisian dan Kejaksaan.[6] Dasar hukum kewenangan tersebut tertuang dalam:

- Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), sebagaimana diubah dengan Undang-Undang Nomor 1 Tahun 2024. Pasal 40 ayat (2a) dan (2b) memberikan kewenangan kepada Pemerintah untuk melakukan pemutusan akses terhadap informasi elektronik yang memiliki muatan terlarang, termasuk konten phishing yang bermuatan penipuan.
- Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) yang menegaskan peran Pemerintah sebagai pengawas perlindungan data pribadi (Pasal 58–Pasal 61). Dalam konteks phishing, UU PDP memberikan dasar untuk menindak pihak-pihak yang mengumpulkan, memproses, dan menyebarkan data pribadi tanpa persetujuan sah.
- Peraturan Menteri Kominfo Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Privat, yang mengatur tata cara pemutusan akses terhadap konten yang dilarang, termasuk situs atau tautan yang digunakan untuk phishing.

Dalam praktiknya, penegakan hukum terhadap phishing melalui Kominfo dilaksanakan dengan pola hibrid, yaitu antara pendekatan administratif dan pendekatan penal. Pada sisi administratif, Kominfo memiliki kewenangan langsung untuk melakukan pemblokiran situs dan aplikasi yang terindikasi melakukan phishing, berdasarkan laporan masyarakat atau temuan internal dari tim patroli siber. Pemblokiran ini bersifat preventif dan represif sekaligus, karena ditujukan untuk menghentikan berlanjutnya tindak pidana serta mencegah meluasnya korban.[7]

Sedangkan pada sisi penal, Kominfo berperan sebagai gatekeeper informasi untuk diteruskan kepada aparat penegak hukum. Berdasarkan Pasal 43 UU ITE, kewenangan penyidikan tetap berada pada Kepolisian, sementara Kominfo hanya menyediakan bukti digital, koordinasi teknis, serta melakukan takedown konten. Dengan demikian, konstruksi hukum yang berlaku menempatkan Kominfo sebagai organ administratif-regulatif yang bersinergi dengan organ yudisial dalam menanggulangi phishing.

Selain itu, penegakan hukum oleh Kominfo terkait phishing juga dikaitkan dengan perlindungan data pribadi. Tindakan phishing pada umumnya bertujuan memperoleh data pribadi korban secara ilegal, sehingga di samping melanggar ketentuan penipuan dalam KUHP dan Pasal 28 ayat (1) Undang-Undang Informasi dan Transaksi E, pelaku juga dapat dijerat Pasal 67 Undang-Undang Perlindungan Data Pribadi yang mengatur sanksi pidana atas pemrosesan data pribadi secara melawan hukum. Dalam hal ini, Kominfo berperan mengawasi Penyelenggara Sistem Elektronik (PSE) agar mematuhi prinsip-prinsip pengelolaan data pribadi sebagaimana diatur dalam Pasal 15–Pasal 21 Undang-Undang Perlindungan Data Pribadi.

Namun, dalam tataran implementasi, terdapat hambatan yang cukup signifikan. Pertama, keterbatasan infrastruktur teknologi di Kominfo untuk mendeteksi secara cepat

[6] https://aptika.kominfo.go.id
[7] https://kominfo.go.id

situs phishing yang terus bermetamorfosis melalui domain baru. Kedua, koordinasi lintas lembaga yang belum optimal, karena proses penyidikan tetap memerlukan alat bukti digital yang sah dan sering kali lintas yurisdiksi. Ketiga, tingkat literasi digital masyarakat yang masih rendah, sehingga meskipun Kominfo melakukan pemblokiran, situs serupa dapat dengan cepat muncul kembali dan menjaring korban baru.

Dengan demikian, dapat disimpulkan bahwa penegakan hukum oleh Kementerian Kominfo terhadap tindak pidana phishing bersifat administratif-regulatif, yang mengedepankan fungsi pengawasan, pemblokiran, dan fasilitasi koordinasi dengan aparat penegak hukum, dengan landasan hukum utama UU ITE dan UU PDP. Meskipun peran Kominfo tidak sampai pada ranah penegakan hukum represif dalam arti yuridis formal, keberadaannya tetap vital sebagai pintu pertama dalam mencegah dan menanggulangi phishing di Indonesia.

3. Hambatan yang dihadapi dan Upaya yang dapat dilakukan untuk Mengoptimalkan Peran Kementerian Kominfo dalam Penegakan Hukum Tindak Pidana Phishing.

Dalam praktiknya, penegakan hukum terhadap tindak pidana phishing di Indonesia tidak terlepas dari berbagai hambatan, baik yang bersifat normatif, struktural, maupun teknis. Hambatan tersebut dapat dianalisis sebagai berikut:

1. Hambatan Normatif

Pertama, dari sisi peraturan perundang-undangan, meskipun telah ada UndangUndang Informasi dan Transaksi Elektronik (Undang-Undang No. 11 Tahun 2008 jo. Undang-Undang No. 1 Tahun 2024) dan Undang-Undang Perlindungan Data Pribadi (Undang-Undang No. 27 Tahun 2022), namun masih terdapat beberapa kekosongan norma dan tumpang tindih pengaturan.

Kekosongan norma tampak pada belum adanya definisi eksplisit mengenai ”gnihsihp“ồ̆ồ̆malađồ̆ồ̆Undang-Undang ITE maupun Undang-Undang PDP. Phishing sering kali diposisikan sebagai bentuk penipuan elektronik atau akses ilegal, sehingga aparat penegak hukum harus menafsirkan pasal-pasal yang ada.

Tumpang tindih regulasi juga muncul ketika tindak pidana phishing bersinggungan dengan rezim hukum lain, misalnya UU Perbankan, UU TPPU, atau KUHP. Hal ini berpotensi menimbulkan perbedaan tafsir mengenai delik yang paling tepat digunakan.

Peraturan Menteri Kominfo memang memberikan dasar operasional, terutama dalam aspek teknis pemblokiran situs dan perlindungan data, tetapi bersifat administratif sehingga tidak memiliki kekuatan pidana yang sama dengan UU.

2. Hambatan Struktural

Kedua, hambatan muncul dari aspek kelembagaan. Kementerian Kominfo, meskipun memiliki kewenangan administratif dalam pengawasan dan pemblokiran konten, tidak memiliki kewenangan pro justitia untuk melakukan penyidikan pidana.

Penegakan hukum yang bersifat represif sepenuhnya berada di tangan Polri dan Kejaksaan, sehingga koordinasi antarlembaga menjadi sangat krusial. Dalam praktiknya, koordinasi ini masih menghadapi kendala birokrasi dan ego sektoral.

Keterbatasan sumber daya manusia yang memiliki keahlian di bidang digital forensik juga menjadi hambatan. Tidak semua aparat memiliki kompetensi teknis dalam mengidentifikasi dan menelusuri serangan phishing yang kerap menggunakan teknologi enkripsi dan server lintas negara.

3. Hambatan Teknis dan Praktis

Ketiga, sifat kejahatan phishing yang berbasis siber menimbulkan hambatan teknis. Anonimitas pelaku: pelaku sering menggunakan fake identity, spoofing, atau jaringan tersembunyi (dark web), sehingga sulit dilacak.

Transnasionalitas: banyak kasus phishing melibatkan server atau jaringan

internasional, yang memerlukan kerja sama lintas negara. Indonesia masih terbatas dalam kapasitas mutual legal assistance (MLA) maupun ekstradisi terkait cybercrime.

Pembuktian digital: meskipun KUHAP mengatur tata cara pembuktian, namun dalam kasus phishing, alat bukti elektronik memerlukan prosedur forensik digital yang ketat agar dapat diterima di pengadilan. Perbedaan standar dalam penanganan barang bukti digital sering menimbulkan keraguan hakim.

4. Upaya Optimalisasi Peran Kementerian Kominfo

Untuk menjawab hambatan-hambatan tersebut, diperlukan sejumlah langkah optimalisasi peran Kementerian Kominfo, antara lain: Kominfo perlu mendorong penyusunan aturan turunan yang lebih komprehensif, termasuk Peraturan Pemerintah atau Peraturan Presiden yang secara spesifik mengatur tentang phishing sebagai tindak pidana siber.

Pembentukan task force terpadu antara Kominfo, Polri, OJK, BI, dan lembaga perbankan guna mempercepat deteksi dan penindakan kasus phishing. Kominfo memiliki peran preventif strategis melalui program literasi digital kepada masyarakat agar lebih waspada terhadap phishing. Upaya preventif ini krusial karena phishing sangat mengandalkan kelemahan psikologis korban (social engineering).

Kominfo bersama Kementerian Luar Negeri dan aparat penegak hukum perlu memperkuat kerja sama dengan negara lain dalam pertukaran data intelijen siber, khususnya melalui kerangka kerja ASEAN *Cybersecurity Cooperation dan Budapest Convention on Cybercrime*. Peningkatan sumber daya manusia di bidang *cyber forensic* dan pengembangan teknologi deteksi otomatis untuk mengidentifikasi situs atau aplikasi berbahaya yang mengandung phishing.

Dengan demikian, hambatan penegakan hukum terhadap phishing tidak hanya terletak pada aspek regulasi, tetapi juga pada dimensi struktural dan teknis. Optimalisasi peran Kominfo harus dilakukan secara holistik, baik melalui penguatan regulasi, peningkatan koordinasi, maupun langkah preventif dan edukatif. Tanpa sinergi yang kuat antar lembaga, penegakan hukum atas phishing berpotensi tidak efektif dan justru memperbesar kerentanan masyarakat terhadap kejahatan siber.

KESIMPULAN

Tindak pidana phishing merupakan bentuk kejahatan siber yang semakin meningkat di Indonesia dan menimbulkan ancaman serius terhadap keamanan transaksi elektronik serta perlindungan data pribadi. Landasan hukum yang tersedia melalui Undang-Undang Informasi Transaksi dan Elektronik (UU ITE) , Undang-Undang Perlindungan Data Pribadi (UU PDP), serta aturan pelaksana berupa Peraturan Kementerian Komunikasi dan Informatika terbaru, telah memberikan pijakan yuridis yang cukup untuk menanggulangi kejahatan ini. Namun, kewenangan Kementerian Kominfo cenderung bersifat administratif dan teknis, sehingga penindakan pidana tetap membutuhkan koordinasi intensif dengan kepolisian, kejaksaan, dan pengadilan.

Dalam praktiknya, hambatan yang muncul antara lain keterbatasan koordinasi antarlembaga, keterlambatan dalam proses pemblokiran situs phishing, rendahnya literasi digital masyarakat, serta permasalahan yurisdiksi lintas negara. Oleh karena itu, efektivitas penanggulangan phishing menuntut adanya sinergi regulasi, konsistensi penegakan hukum, peningkatan kapasitas aparat, serta partisipasi aktif masyarakat dalam menjaga data pribadinya.

Berdasarkan temuan tersebut, disarankan agar Kementerian Kominfo memperkuat sistem deteksi dini, mempercepat mekanisme pemblokiran situs phishing, dan menyempurnakan regulasi pelaksana; aparat penegak hukum meningkatkan kapasitas

penyidik dan penuntut dalam perkara berbasis bukti digital; pemerintah memperkuat kerja sama internasional serta integrasi antarperaturan; dan masyarakat lebih sadar hukum serta aktif menjaga keamanan data pribadi. Sinergi antara pemerintah, aparat, dan masyarakat merupakan kunci utama keberhasilan penegakan hukum dalam menghadapi ancaman phishing di era digital.

DAFTAR PUSTAKA

Peraturan Perundang-Undangan

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. https://peraturan.bpk.go.id/Details/37589/uu-no-11-tahun-2008

Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat.

https://peraturan.bpk.go.id/Details/203049/permenkominfo-no-5-tahun-2020 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

https://peraturan.bpk.go.id/Details/274494/uu-no-1-tahun-2024 Kitab Undang-Undang Hukum Acara Pidana.

https://peraturan.bpk.go.id/47041/uu-nomor-8-tahun-1981

Buku

M. Arief Amrullah (2022), Hukum dan Kebijakan Cybercrime di Indonesia, hlm. 44.

Budi Rahardjo (2022), Hukum Siber dan Tantangan Penegakan Hukum di Indonesia, hlm. 54.

Sinta Dewi Rosadi (2023), Hukum Perlindungan Data Pribadi di Indonesia, hlm. 118.

Zainal Arifin & Emi Puasa Handayani (2023), Cybercrime: Menyelisik Penegakan Hukum dan Penanggulangannya, hlm. 17.

Danrivanto Budhijanto (2024), Hukum Perlindungan Data Pribadi – Privacy, Data Protection, Cybersecurity, hlm. 56.

Jurnal, Artikel dan Web

Kementerian Komunikasi dan Informatika Republik Indonesia (2023), Langkah Kominfo dalam Penanganan Konten Phishing.

Wicaksono, Andri (2023), Tantangan Penegakan Hukum Kejahatan Siber di Indonesia. Jurnal Hukum dan Teknologi.

Kementerian Komunikasi dan Informatika Republik Indonesia (2024), Tugas dan Fungsi Direktorat Jenderal Aplikasi Informatika.

Salsabila, Rani (2024), Analisis Peran Kominfo dalam Penanganan Tindak Pidana Siber. Jurnal Hukum dan HAM Digital.

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

Ratih Mega Puspita Sari (2025), Criminal Resposibility in Cybercrime: An Analysis of Phishing Crimes in Indonesia, JHK: Jurnal Hukum dan Keadilan.

Pusat Informasi Kriminal Nasional oleh Polisi Republik Indonesia (2025), Kasus Kejahatan Manipulasi Data Secara ITE Meningkat.

Indonesia Domain Abuse Data Exchange (IDADX), Laporan Aktivitas Abuse Domain .Id Periode Q1 2025.