p-ISSN: 2963-7856| e-ISSN: 2961-9890
Available online at jerkin.org/index.php/jerkin
Jurnal Pengabdian Masyarakat dan Riset Pendidikan
Volume 4 No. 3, Januari-Maret 2026, pp 17990-18002

Analisis Kepastian Hukum Terkait Pencegahan Tindak Pidana Penipuan Online Berdasarkan Undang-Undang ITE

Elshavira Suryaning Tyas[1]*, Adhining Prabawati Rahmahani[2]

[1,2] Fakultas Hukum, Universitas Esa Unggul, Jl. Arjuna Utara No.9, Duri Kepa, Kec. Kb. Jeruk, Kota Jakarta Barat, Daerah Khusus Ibukota Jakarta
E-mail: elshaviras@studenmetoft.esaunggul.ac.id
* Corresponding Author

https://doi.org/10.31004/jerkin.v4i3.4937

ARTICLE INFO

Article history:
Received: 07 Jan 2026
Revised: 13 Jan 2026
Accepted: 19 Jan 2026

Kata Kunci:
Penipuan Online, Undang-Undang ITE, Kepastian Hukum, Pencegahan, Penyelenggara Sistem Elektronik.

Keywords:
Online Fraud, ITE Law, Legal Certainty, Prevention, Electronic System Providers.

ABSTRACT

Revolusi digital memicu peningkatan kejahatan siber, khususnya penipuan daring dengan modus phishing yang sangat merugikan nasabah perbankan. Rumusan masalah dalam jurnal ini ialah pengaturan dan penerapan ketentuan pencegahan tindak pidana penipuan online berdasarkan Undang-Undang ITE dan analisis kepastian hukum terkait pencegahan tindak pidana penipuan online berdasarkan Undang-Undang ITE. Metode penelitian yang digunakan adalah hukum normatif dengan pendekatan perundang-undangan, serta pengumpulan data melalui studi kepustakaan. Hasil penelitian menunjukkan bahwa regulasi pencegahan telah diatur dalam Pasal 28 ayat (1) serta Pasal 40 ayat (2a) dan (2b) UU ITE, namun penerapannya di lapangan masih bersifat reaktif dan tidak efektif. Analisis kepastian hukum mengungkapkan adanya ketidakselarasan antara das sollen dan das sein yang disebabkan oleh respons lambat Penyelenggara Sistem Elektronik (PSE), ketiadaan Standar Waktu Maksimum Respons Cepat (SWMRC), serta pelanggaran terhadap asas profesionalitas bank dalam menangani aduan darurat nasabah. Kesimpulannya ialah kepastian hukum dapat terwujud dengan cara men-sinkronisasi antara kepastian norma, respons cepat perbankan yang profesional, serta adanya mekanisme pertanggungjawaban ganti rugi yang jelas bagi nasabah atas kelalaian operasional Penyelenggara Sistem Elektronik (PSE).

The digital revolution has triggered a surge in cybercrime, particularly online fraud through phishing schemes that significantly detriment banking customers. The primary objective of this study is to examine the regulation and implementation of online fraud prevention provisions under the ITE Law, as well as to analyze the legal certainty regarding these preventive measures. The research methodology employed is normative legal research with a statute approach, utilizing data collected through literature studies. The results indicate that while preventive regulations are established under Article 28 paragraph (1) and Article 40 paragraphs (2a) and (2b) of the ITE Law, their practical implementation remains reactive and ineffective. The analysis of legal certainty reveals a discrepancy between das sollen and das sein, caused by the delayed response of Electronic System Providers (PSE), the absence of a Rapid Response Time Standard (RRTS), and violations of the bank's principle of professionalism in handling emergency customer complaints. In conclusion, legal certainty can be achieved by synchronizing normative clarity, professional and rapid banking responses, and the establishment of a clear liability mechanism for damages resulting from the operational negligence of Electronic System Providers (PSE).

This is an open access article under the CC–BY-SA license.

How to Cite: Elshavira Suryaning Tyas, et al. (2026). Analisis Kepastian Hukum Terkait Pencegahan Tindak Pidana Penipuan Online Berdasarkan Undang-Undang ITE, 4(3). https://doi.org/10.31004/jerkin.v4i3.4937

PENDAHULUAN

Transformasi besar yang dipicu oleh revolusi teknologi informasi telah menggeser tatanan sosial dan ekonomi masyarakat Indonesia secara menyeluruh. Dalam konteks ini, teknologi berfungsi sebagai media pendukung yang berkontribusi penting dalam memperlancar beragam bentuk kegiatan manusia

di berbagai sektor. Melalui pemanfaatan internet, masyarakat dapat melakukan beragam kegiatan, seperti membangun relasi sosial, menjalankan pekerjaan, mengembangkan bisnis berbasis digital, serta melaksanakan transaksi secara elektronik. Perkembangan kebutuhan masyarakat yang terus mengalami peningkatan menjadikan teknologi informasi sebagai elemen penting yang memiliki peran berkelanjutan di masa kini dan masa depan. Keberadaan teknologi memberikan kemudahan bagi manusia dalam melaksanakan transaksi secara efektif dan tepat waktu, yang pada akhirnya berkontribusi terhadap optimalisasi interaksi ekonomi dan berbagai kegiatan pendukung dalam kehidupan masyarakat modern. Seiring dengan meningkatnya perkembangan teknologi, internet hadir sebagai elemen kunci yang memicu munculnya berbagai terobosan inovatif dalam kehidupan manusia, terutama yang berkaitan dengan dinamika dan pengembangan sektor bisnis. Internet yang terus berkembang memberikan kontribusi besar dalam meningkatkan efektivitas dan efisiensi pemenuhan kebutuhan serta pekerjaan masyarakat. Peningkatan jumlah pengguna internet secara berkelanjutan menjadi faktor pendorong bagi perusahaan dan pelaku pengembangan teknologi untuk menginisiasi berbagai inovasi baru yang diminati oleh masyarakat luas. Pesatnya kemajuan teknologi dari waktu ke waktu telah berdampak secara gradual terhadap transformasi perilaku sosial masyarakat, sekaligus memengaruhi arah perkembangan peradaban manusia dalam skala global. Perkembangan teknologi informasi turut menghilangkan berbagai sekat geografis antarmasyarakat, sehingga dunia semakin bersifat tanpa batas (borderless), sekaligus mempercepat berlangsungnya perubahan sosial yang berskala signifikan (Dr. Maskun & Wiwik Meilarati Saloko, 2017). Dengan demikian, teknologi informasi memiliki posisi yang krusial dalam menunjang perkembangan dan daya saing suatu negara. Di sisi lain, pemanfaatannya yang semakin luas turut membuka peluang terjadinya kejahatan siber (cybercrime). Selain berkontribusi positif dalam berbagai aspek kehidupan, teknologi informasi dan komunikasi juga menimbulkan potensi dampak negatif. Kejahatan yang memanfaatkan teknologi informasi termasuk dalam kategori white crime, sebab pelaku kriminal di dunia maya umumnya adalah individu yang memiliki keahlian dan pengetahuan mendalam mengenai penggunaan teknologi internet. Tindak pidana di ranah siber kerap dilakukan secara transnasional dengan melampaui batas-batas yurisdiksi negara, sehingga kejahatan tersebut dapat diklasifikasikan ke dalam dua kriteria kriminal, yakni white crime dan transnational crime. Di Indonesia, masyarakat dihadapkan pada beragam kasus kejahatan di dunia maya (cyber crime) yang cukup sering terjadi, seperti penipuan, perjudian daring, penyebaran informasi palsu (hoax), tindakan cracking, serta pencurian data pribadi berbasis internet (Anugerah, 2022).

Perkembangan teknologi melahirkan inovasi di sektor perbankan melalui penerapan e-banking (electronic banking), yakni sistem layanan perbankan yang berbasis internet dan dirancang untuk memfasilitasi berbagai kebutuhan transaksi serta layanan nasabah. Seiring dengan berkembangnya internet banking, sektor perbankan dituntut untuk meningkatkan kualitas kinerja dan fasilitas layanan secara menyeluruh. Peningkatan tersebut mencakup aspek keamanan transaksi berbasis internet, mutu pelayanan nasabah, serta inovasi produk perbankan agar selaras dengan kebutuhan nasabah yang semakin kompleks, namun tetap sesuai dengan ketentuan peraturan perbankan. Perbankan yang berfungsi sebagai sektor vital dalam tatanan masyarakat menghadapi risiko terjadinya penyalahgunaan kewenangan dan tindakan kriminal dalam berbagai bentuk transaksi. Risiko tersebut dapat berasal dari pihak internal maupun eksternal yang mencoba mengeksploitasi sistem perbankan untuk memperoleh keuntungan pribadi atau mendukung kegiatan yang melanggar hukum. Tindakan kriminal dalam aktivitas perbankan seringkali melibatkan pelanggaran terhadap ketentuan resmi, salah satunya adalah modus operandi yang meminta nasabah mengisi suatu link atau memberikan kode OTP kepada pihak yang mengaku sebagai pihak bank.

Modus operandi kejahatan ini terus berkembang seiring berjalannya waktu, mulai dari phising, toko online fiktif, hingga investasi bodong berbasis digital hingga pemberian link scam terhadap beberapa nasabah bank yang menjadi target penipuan. Salah satu penipuan yang sering terjadi ialah phising, phising adalah pencurian data online yang dilakukan dengan cara mengelabui korban untuk memberikan informasi pribadinya. Phising berasal dari istilah dalam bahasa inggris, yaitu fishing yang artinya “memancing”. Informasi yang dicuri sering kali dimanfaatkan untuk melakukan tindakan ekonomi yang ilegal seperti membeli barang menggunakan identitas curian dan transaksi Serangan online. Dengan menggunakan website tiruan ini, pelaku mengelabui para nasabah karena mengira website tiruan tersebut merupakan website bank (Faizah Nurfahda dkk., 2024). Phising mengeksploitasi banyak hal saat korban mengklik tautan atau membuka lampiran, pelaku kejahatan mulai mengambil

data atau menginfeksi perangkat korban. Beberapa kemungkinan skenario yaitu korban mengisi username dan password di situs palsu, file yang dibuka ternyata malware dan memberikan pelaku akses ke komputer korban, kemudian korban diperintahkan untuk mengisi informasi penting seperti nomor kartu kredit, OTP, atau file internal yang mana setelah diisi data akan berhasil dicuri. Data ini bisa langsung dimanfaatkan oleh pelaku kejahatan. Pada hal ini, penting untuk memahami bahwa keberhasilan phishing sangat bergantung pada faktor manusia, bukan pada kelemahan teknis sistem. Pelaku memanfaatkan kepercayaan, ketidaktahuan, dan tekanan situasional untuk mengelabui korban (Widya s, 2025).

Adanya perbankan elektronik muncul sebagai inovasi baru dalam sektor perbankan, dengan adanya inovasi baru tersebut tidak menutup kemungkinan bahwa penipuan online terjadi pada sektor perbankan elektronik online. Serangan phishing melalui media sosial semakin populer dengan memanfaatkan ketidakwaspadaan pengguna terhadap risiko keamanan siber. Fenomena ini dapat menimbulkan konsekuensi yang serius bagi individu maupun organisasi, termasuk pencurian identitas, kebocoran informasi sensitif, serta kerugian finansial yang signifikan. Dampak berupa terungkapnya data pribadi dan terjadinya kerugian keuangan akibat serangan ini dapat melemahkan kepercayaan publik serta mengancam stabilitas aktivitas di ruang digital (Syah, 2023). Kasus lain yang dapat dijadikan contoh adalah insiden pengurasan rekening nasabah Bank BRI hingga mencapai ratusan juta rupiah akibat korban mengklik tautan yang diterima melalui pesan WhatsApp. Pelaku kejahatan, yang berperan sebagai pihak ketiga dengan mengatasnamakan bank, memberikan informasi palsu kepada korban terkait perubahan tarif biaya transfer dari Rp6.500 per transaksi menjadi Rp150.000 per bulan. Dikarenakan besarnya biasa transaksi perbulan, tentu saja nasabah tersebut lebih berkeinginan untuk tetap dikenakan biaya Rp 6.500 per transaksi. Lalu pelaku kejahatan seolah memastikan dan mengonfirmasi jika korban yaitu nasabah BRI tetap memilih biaya Rp 6.500 per transaksi, dan meminta nasabah untuk menyalin (copy) link yang dikirimkan lewat pesan WhatsApp. Dalam upaya melancarkan aksinya, pelaku secara persuasif mengarahkan korban untuk mengisi tautan yang dibagikan, sembari memuji korban sebagai nasabah yang aktif melakukan transfer dan berpotensi memperoleh hadiah tertentu. Situasi tersebut mendorong korban untuk mengakses tautan dimaksud dan memasukkan data yang selanjutnya digunakan oleh pelaku kejahatan, yang mana data tersebut tentunya adalah data yang dibutuhkan oleh pelaku untuk melakukan aksinya yakni mencuri saldo dari rekening korban. Korban tersadar bahwa korban telah ditipu oleh pelaku kejahatan yang berhasil menyadap saldo di rekeningnya. Tentu saja rasa bersalah dan merasa dirugikan telah dirasakan oleh korban. Dengan segera korban menghubungi Call Center BRI untuk memblokir rekeningnya. Korban mengungkapkan bahwa penanganan dari petugas Call Center dinilai kurang responsif, khususnya karena korban diwajibkan untuk memblokir empat rekening dalam waktu bersamaan. Dalam rentang proses pemblokiran tersebut, aktivitas transaksi tetap berlangsung hingga saldo rekening korban terkuras mencapai Rp274.756.500. Selanjutnya, korban telah melaporkan peristiwa ini kepada pihak Bank BRI dan aparat kepolisian, serta mengharapkan adanya pengembalian atas dana yang telah hilang (nextren.grid.id, 09 Juni 2022).

Sebagai bentuk respons atas perkembangan dan kebutuhan di bidang teknologi informasi, Pemerintah Indonesia menetapkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-undang ini kemudian direvisi melalui Undang-Undang Nomor 19 Tahun 2016, yang selanjutnya disebut sebagai UU ITE (Kurnia, 2024). Secara yuridis normatif, UU ITE memberikan pengaturan mengenai larangan perbuatan menyebarkan berita bohong dan menyesatkan yang dilakukan dengan sengaja dan tanpa hak, yang berdampak pada kerugian konsumen, sebagaimana tercantum dalam Pasal 28 ayat (1). Meskipun instrumen hukum telah tersedia, realitas di lapangan menunjukkan bahwa angka penipuan online masih sangat tinggi. Hal ini memunculkan pertanyaan mendasar mengenai efektivitas hukum, bukan hanya dari sisi penindakan (represif), melainkan juga dari sisi pencegahan (preventif). Kepastian hukum idealnya tidak hanya berbicara tentang bagaimana menghukum pelaku setelah kejahatan terjadi, tetapi juga bagaimana regulasi tersebut mampu menciptakan sistem pencegahan yang efektif.

Pada dasarnya pelaku kejahatan tidak memiliki cara atau tidak mampu melakukan pembobolan terhadap rekening bank seseorang, pelaku kejahatan selalu menggunakan titik lemah dari korban yaitu kelalaian dari nasabah bank itu sendiri. Kebijakan hukum pidana siber harus bersifat integral, yang mencakup upaya penal (hukum pidana) dan non-penal (pencegahan). Tanpa adanya aturan pencegahan

Copyright © 2026, Jurnal Pengabdian Masyarakat dan Riset Pendidikan
ISSN 2963-7856 (print), ISSN 2961-9890 (online)

yang tegas dan memiliki kepastian hukum seperti mekanisme pemblokiran rekening yang cepat, verifikasi identitas penyelenggara sistem elektronik, dan literasi digital yang terstruktur maka masyarakat akan terus berada dalam posisi rentan. Berdasarkan latar belakang yang telah diuraikan sebelumnya, muncul rumusan masalah, yaitu (1) Bagaimana pengaturan dan penerapan ketentuan pencegahan tindak pidana penipuan online berdasarkan Undang-Undang ITE? dan (2) Bagaimana analisis kepastian hukum terkait pencegahan tindak pidana penipuan online berdasarkan Undang-Undang ITE?

Dengan demikian, penelitian ini akan mempelajari bagaimana pengaturan dan penerapan ketentuan pencegahan tindak pidana penipuan online berdasarkan Undang-Undang ITE, regulasi yang mengatur mengenai upaya penal (hukum pidana) juga akan dibahas dalam pembahasan, serta analisis kepastian hukum terkait pencegahan tindak pidana penipuan online berdasarkan Undang-Undang ITE. Adapun tujuan penulis mengangkat kedua permasalahan tersebut adalah untuk mengkaji serta memahami secara mendalam upaya pencegahan terjadinya tindak pidana penipuan online, sekaligus memperluas analisis mengenai kepastian hukum terhadap tindak pidana penipuan online berdasarkan ketentuan Undang-Undang ITE. Penelitian ini juga diarahkan untuk mengkaji dan mengusulkan langkah-langkah pencegahan yang tepat guna memberikan perlindungan terhadap data nasabah dari ancaman kejahatan siber, mengingat tindak pidana penipuan online semakin bergantung pada perkembangan teknologi.

METODE

Penelitian ini menggunakan pendekatan yuridis-normatif, yang menitikberatkan pada telaah mendalam terhadap ketentuan hukum positif beserta asas asas hukum yang menjadi landasan pembentukan dan penerapan sistem hukum nasional, guna mengkaji secara mendalam permasalahan hukum yang menjadi fokus penelitian (Peter Mahmud Marzuki). Dengan menitikberatkan pada peraturan tertulis, penelitian ini tergolong sebagai penelitian kepustakaan yang mengandalkan data sekunder. Seluruh proses penelitian dilakukan dengan berpedoman pada peraturan perundang-undangan yang berlaku. Penelitian ini menerapkan Pendekatan Perundang-Undangan (statute approach) dengan memanfaatkan peraturan perundang-undangan yang memiliki keterkaitan dengan objek kajian. Spesifikasi penelitian dilakukan secara deskriptif analitis, yang bertujuan untuk menggambarkan dan menganalisis hukum positif beserta implementasinya dalam praktik saat ini. Penelitian ini melibatkan proses penggalian informasi melalui pembacaan dan analisis dokumen hukum yang tersedia, Mencakup ketentuan peraturan perundang-undangan beserta berbagai karya ilmiah di bidang hukum yang berfungsi sebagai pijakan teoretis untuk menafsirkan dan menganalisis permasalahan hukum yang diangkat dalam penelitian ini (Soerjono Soekanto, 2003).

HASIL DAN PEMBAHASAN

Pengaturan dan Penerapan ketentuan pencegahan tindak pidana penipuan online berdasarkan Undang-Undang ITE

Seiring dengan kemajuan teknologi yang semakin mutakhir, sektor hukum pun dituntut untuk melakukan adaptasi serupa. Hal ini didasari pada prinsip bahwa hukum harus tumbuh beriringan dengan perkembangan masyarakat agar fungsinya sebagai pengatur tetap relevan. Di sisi lain, kemajuan peradaban digital ini mengubah wajah kriminalitas dengan munculnya kejahatan di ruang virtual. Masifnya penetrasi internet di Indonesia telah berdampak langsung pada meningkatnya intensitas tindak pidana berbasis daring. Dalam konteks ini, teknologi informasi tidak hanya berperan sebagai sarana kemajuan, tetapi juga bertransformasi menjadi alat kejahatan, yang mencerminkan residu negatif dari cepatnya arus inovasi saat ini.

Dalam ranah digital, tindak pidana penipuan sering kali terjadi melalui skema penyerahan barang atau hak kepada pihak korban yang telah dipretargetkan. Aksi ilegal ini umumnya terintegrasi langsung dalam proses distribusi atau pertukaran tersebut. Karakteristik utama dari pelaku penipuan berbasis internet adalah penggunaan atribusi identitas palsu atau akun samaran yang memanipulasi nama besar perusahaan tertentu. Penggunaan identitas fiktif ini merupakan taktik krusial bagi pelaku untuk membangun kredibilitas palsu di mata korban, sembari menciptakan proteksi terhadap profil asli mereka agar sulit diidentifikasi setelah tindakan kriminal tersebut berhasil dilakukan (Sahlepi, 2023).

Secara yuridis, pengaturan terkait upaya pencegahan dan penegakan hukum terhadap tindak pidana penipuan online di Indonesia diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang selanjutnya mengalami perubahan melalui Undang-Undang Nomor 19 Tahun 2016 serta Undang-Undang Nomor 1 Tahun 2024. Ketentuan mengenai tindak pidana penipuan online diatur dalam Pasal 28 ayat (1) UU ITE, yang berbunyi: "Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik". Kerangka hukum UU ITE secara garis besar mengatensi dua pilar utama, yakni pengaturan informasi dan transaksi elektronik serta kodifikasi terhadap tindak pidana siber atau cybercrime (Sulubara, 2025). Secara spesifik, perlindungan terhadap konsumen dalam ekosistem digital termaktub dalam Pasal 45A ayat (1), yang mengancam pelaku penyebar diseminasi informasi palsu dengan pidana penjara maksimal enam tahun atau denda mencapai Rp1 miliar. Norma ini bertujuan menjaga integritas ruang digital dengan menjadikan aspek "penyesatan" dan "kerugian konsumen" sebagai indikator determinan dalam kualifikasi tindak pidana. Kendati demikian, karakteristik anonimitas dalam ruang siber memberikan celah bagi para pihak untuk melakukan manipulasi identitas, yang pada akhirnya menyulitkan upaya penegakan hukum maupun eksekusi yuridis apabila terjadi sengketa atau penipuan dalam transaksi tersebut (Tamo Ama & Kadir, 2024).

Berdasarkan revisi terbaru UU ITE (UU No. 1 Tahun 2024), peran pemerintah dalam pencegahan penipuan online mengalami pergeseran signifikan. Jika sebelumnya pemerintah hanya berperan sebagai regulator, kini melalui Pasal 40 ayat (2a) yang berbunyi "Pemerintah wajib melakukan pencegahan penyebarluasan dan penggunaan Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang dilarang sesuai dengan ketentuan peraturan perundang-undangan", pemerintah memiliki kewajiban atributif untuk melakukan pencegahan penyebarluasan informasi yang melanggar hukum. Dalam upaya memperkuat aspek pencegahan tindak pidana penipuan online dalam UU ITE secara normatif tidak hanya terkonsentrasi pada pasal pidana Pasal 28 ayat (1) melainkan ada aturan lain yang mengatur lebih spesifik terkait pencegahan tindak pidana penipuan online yang lebih sistematis yaitu Pasal 40 UU ITE, di mana Pemerintah memiliki kewenangan sekaligus kewajiban untuk melakukan pengawasan terhadap konten internet. Pemerintah berhak melakukan pemutusan akses atau take down terhadap informasi elektronik yang dianggap melanggar hukum, termasuk akun media sosial, situs web palsu, atau aplikasi bodong yang digunakan untuk menjaring korban penipuan. Pemerintah memikul kewajiban hukum untuk melindungi kepentingan masyarakat luas dari gangguan yang disebabkan oleh penyalahgunaan Informasi Elektronik dan Transaksi Elektronik yang dapat mengancam ketertiban umum. Hal ini mencakup tindakan preventif berupa pemblokiran situs web, akun media sosial, atau aplikasi yang terindikasi melakukan aktivitas penipuan, sehingga potensi kerugian masyarakat yang lebih luas dapat segera dimitigasi sebelum jatuh lebih banyak korban. Langkah preventif ini krusial untuk menghentikan penyebaran kerugian secara massal sebelum aparat penegak hukum melakukan tindakan projustisia terhadap oknum di balik layar.

Penegakan hukum terhadap tindak pidana siber dalam kerangka Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik menganut asas jangkauan yang luas. Regulasi ini tidak hanya membatasi ruang lingkupnya pada tindakan yang terjadi di dalam negeri atau oleh subjek hukum domestik semata. Secara ekstrateritorial, undang-undang ini juga menjangkau perbuatan hukum di luar yurisdiksi nasional, baik yang dilakukan oleh individu maupun korporasi lintas negara, selama tindakan tersebut menimbulkan implikasi hukum di wilayah Indonesia. Hal ini didasarkan pada karakteristik pemanfaatan teknologi informasi yang bersifat universal dan melampaui batas-batas teritorial negara (borderless). Hal ini diatur didalam Pasal 2 Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik yang berbunyi "Undang-Undang ini berlaku untuk setiap Orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-Undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indoensia dan/ atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia".

Selain aspek pemblokiran konten, penegakan hukum terhadap tindak pidana penipuan online juga didukung oleh ancaman pidana yang cukup berat sebagai efek jera (deterrent effect). Berdasarkan Pasal 45A ayat (1) UU ITE terbaru yang berbunyi "Setiap Orang yang dengan sengaja dan tanpa hak menyiarkan, mempertunjukkan, mendistribusikan, mentransmisikan, dan/atau membuat dapat

Copyright © 2026, Jurnal Pengabdian Masyarakat dan Riset Pendidikan
ISSN 2963-7856 (print), ISSN 2961-9890 (online)

diaksesnya Informasi Elektronik dan/ atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan untuk diketahui umum sebagaimana dimaksud dalam Pasal 27 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp l.000.000.000,00 (satu miliar rupiah).", setiap orang yang memenuhi unsur pidana dalam Pasal 28 ayat (1) dapat dipidana dengan pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp1 miliar. Penjatuhan sanksi ini tidak hanya menyasar pelaku utama, tetapi juga dapat dikembangkan untuk menjerat pihak-pihak yang turut serta atau memfasilitasi terjadinya transaksi elektronik yang bersifat menipu tersebut, sesuai dengan ketentuan hukum acara pidana yang berlaku. Dalam Pasal 28 ayat (1) tersebut, unsur-unsur penipuan menurut Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik ialah:

1. Setiap Orang
2. Dengan sengaja dan tanpa hak.
3. Menyebarkan berita bohong dan menyesatkan.
4. Yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.

Secara teoritis, norma yang tertuang dalam Pasal 28 ayat (1) UU ITE berfungsi sebagai jangkar hukum yang memberikan kejelasan mengenai delik penyebaran berita bohong yang mengakibatkan kerugian konsumen. Namun, efektivitas sebuah undang-undang tidak hanya bergantung pada beratnya sanksi pidana, melainkan juga pada mandat atributif yang diberikan kepada negara untuk melakukan upaya preventif. Hal ini tercermin dalam Pasal 40 ayat (2a) dan (2b) UU ITE terbaru, di mana Pemerintah memiliki kewajiban hukum untuk melakukan pencegahan dan pemutusan akses terhadap informasi elektronik yang melanggar hukum guna melindungi kepentingan umum. Meskipun landasan yuridis telah tersedia, realitas di lapangan menunjukkan adanya hambatan teknis yang menghalangi tercapainya tujuan hukum tersebut secara maksimal.

Penegakan hukum terhadap kejahatan siber menghadapi tantangan kompleks, terutama yang berkaitan dengan integrasi kerja sama antara aparat dan pengelola ekosistem digital. Proses penyelidikan sering kali mengalami stagnasi akibat birokrasi laporan yang lamban serta kebijakan perlindungan data pribadi yang menjadi dilema dalam pengungkapan identitas pelaku. Di sisi lain, evolusi taktik manipulasi yang dilakukan oleh aktor penipuan memungkinkan mereka tetap beroperasi di bawah radar deteksi keamanan platform. Fenomena ini menunjukkan bahwa penanganan kasus tidak dapat dilakukan secara parsial; diperlukan sinkronisasi yang lebih intensif antara kebijakan platform digital dan tindakan represif aparat hukum demi menciptakan ruang siber yang lebih aman dan responsif (Yaqin dkk., 2025). Berdasarkan teori perundang-undangan, sebuah regulasi membutuhkan aturan pelaksana (implementing regulations) yang lebih spesifik untuk mengisi kekosongan operasional. Dalam konteks ini, ketiadaan standar waktu respons cepat (SWMRC) bagi Penyelenggara Sistem Elektronik (PSE) menyebabkan norma pencegahan dalam UU ITE seringkali kehilangan daya tindaknya di saat krusial, mengingat transaksi ilegal di ekosistem digital terjadi dalam hitungan detik.

Sebagai instrumen hukum pertama yang mengodifikasi kejahatan siber di tanah air, UU ITE (hasil amandemen dari UU No. 11/2008 ke UU No. 19/2016) memiliki rekam jejak penyusunan yang unik dalam dinamika hukum Indonesia. Secara sosiologi hukum, keberhasilan regulasi ini dalam menertibkan masyarakat digital sangat ditentukan oleh integrasi antara kaidah hukum dengan nilai-nilai yang hidup dan pola perilaku sosial. Ketidakmampuan untuk menyelaraskan ketiga elemen ini dapat memicu anomali dalam penegakan hukum. Oleh karena itu, keserasian antara aturan formal dengan realitas perilaku masyarakat menjadi syarat mutlak agar tujuan hukum siber dapat tercapai secara optimal. Fenomena penegakan hukum di Indonesia sering kali dimaknai sebatas legalitas formal, di mana titik tekannya terletak pada operasionalisasi undang-undang dan keputusan yudisial. Perlu dipahami bahwa interpretasi yang terbatas ini menyimpan risiko yang signifikan. Penegakan hukum yang kaku dan semata-mata bersifat administratif berpotensi merusak tatanan sosial jika hasil akhirnya justru menciptakan konflik atau ketidaknyamanan dalam masyarakat. Oleh karena itu, hukum seharusnya dipandang lebih luas daripada sekadar prosedur teknis, agar kehadirannya tetap mampu menjaga kedamaian kolektif di atas segalanya (Assegaf, 2024).

UU ITE menempatkan Penyelenggara Sistem Elektronik (PSE) sebagai garda terdepan dalam menjaga integritas transaksi digital melalui pengamanan infrastruktur elektronik mereka. Secara regulasi, PSE diamanatkan untuk menjamin bahwa sistem yang mereka operasikan berfungsi secara andal guna mencegah terjadinya eksploitasi ilegal. Ketidakmampuan dalam menutup celah keamanan

atau kegagalan dalam menjaga kerahasiaan data pengguna bukan sekadar masalah teknis, melainkan pelanggaran kepatuhan yang serius. Sebagai konsekuensinya, pemerintah memiliki kewenangan untuk menjatuhkan sanksi administratif secara berjenjang, termasuk penghentian hak operasional bagi penyelenggara yang dinilai lalai. Dengan demikian, regulasi ini menciptakan ekosistem pertanggungjawaban kolektif antara pemerintah sebagai regulator, aparat penegak hukum, pelaku usaha digital, dan masyarakat sebagai pengguna jasa layanan elektronik.

Dalam konteks penipuan phishing yang menyasar pada nasabah bank BRI, Pasal 15 ayat (1) UU ITE yang berbunyi "Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya" membebankan tanggung jawab besar kepada Penyelenggara Sistem Elektronik (PSE) untuk mengoperasikan sistem secara andal dan aman. Hal ini berarti bank harus memiliki sistem deteksi dini (fraud detection system) yang mampu mengenali pola transaksi tidak wajar secara otomatis. Bank juga wajib menyediakan mekanisme pelaporan darurat yang responsif. Meskipun Pasal 40 ayat (2b) memberikan wewenang pemutusan akses, dalam praktiknya terdapat hambatan birokrasi yang memperlemah upaya pencegahan. Proses pelaporan dari nasabah ke bank, kemudian bank ke Kominfo, seringkali memakan waktu berjam-jam bahkan hari. Sementara itu, kerugian finansial akibat penipuan phishing terjadi dalam hitungan menit atau detik.

Pencegahan penipuan online dalam kerangka UU ITE juga diintegrasikan dengan upaya peningkatan literasi digital dan perlindungan data pribadi. Pemerintah mendorong masyarakat untuk lebih teliti dalam melakukan transaksi elektronik dengan menyediakan kanal pengaduan resmi, seperti portal CekRekening.id atau Lapor.go.id, yang berfungsi sebagai pusat verifikasi dan pelaporan akun-akun mencurigakan. Melalui sinergi antara regulasi yang ketat, penegakan hukum yang konsisten, dan pengawasan sistematis terhadap transaksi elektronik, UU ITE diposisikan sebagai instrumen hukum utama untuk menjamin kepastian hukum dan rasa aman bagi seluruh warga negara dalam beraktivitas di ruang digital. Penerapan ketentuan pencegahan ini di lapangan masih menunjukkan berbagai tantangan, terutama dalam kasus penipuan phishing yang terjadi secara cepat, seperti yang dialami korban Nasabah bank BRI.

Tujuan utama dari penegakan pertanggungjawaban pidana adalah untuk mengayomi masyarakat sekaligus mencegah repetisi kejahatan dengan menjunjung tinggi supremasi hukum. Melalui sistem ini, konflik yang lahir akibat delik pidana dapat diselesaikan guna memulihkan keseimbangan hidup yang damai bagi warga negara. Secara simultan, aspek pembinaan dalam sistem peradilan pidana memegang peran krusial untuk merehabilitasi terpidana agar kembali diterima di masyarakat dengan mentalitas yang lebih baik dan bebas dari rasa bersalah. Agar selaras dengan visi masyarakat yang adil dan makmur secara lahiriah serta batiniah, unsur kesalahan harus menjadi landasan fundamental dalam setiap vonis. Hal ini menegaskan bahwa fungsi hukum pidana bukan sekadar menghukum, melainkan sebagai upaya preventif dalam meniadakan perbuatan-perbuatan yang bertentangan dengan norma kolektif.

Upaya pencegahan non-penal seharusnya mencakup pemblokiran rekening yang cepat, verifikasi identitas Penyelenggara Sistem Elektronik (PSE), dan literasi digital yang terstruktur yang diterapkan sebagai nasabah bank, namun tanpa hal tersebut masyarakat akan terus berada dalam posisi rentan. Pengaturan pencegahan dalam UU ITE tidak hanya mencakup aspek teknis, tetapi juga edukasi. Pasal 40 menekankan pentingnya peran serta masyarakat. Namun, realitas menunjukkan bahwa literasi digital masih menjadi titik lemah utama. Banyak nasabah yang masih mudah terjebak oleh manipulasi psikologis (social engineering) karena kurangnya sosialisasi mengenai modus operandi terbaru. Edukasi yang diberikan oleh perbankan seringkali bersifat umum dan tidak menyentuh prosedur teknis darurat yang harus dilakukan nasabah saat menyadari akunnya diretas. Tanpa literasi yang mumpuni, secanggih apa pun regulasi pencegahan yang dibuat, masyarakat akan tetap menjadi mata rantai terlemah dalam keamanan siber. Selain itu, ketidakjelasan batasan tanggung jawab antara pemerintah (Kementerian Kominfo) dalam pemutusan akses dan peran bank (sebagai PSE) dalam respons cepat terhadap laporan nasabah (yang dalam kasus nasabah BRI mengeluhkan respon lambat dari petugas Call Center) menjadi hambatan utama dalam implementasi pencegahan yang efektif. Ketidakjelasan ini berpotensi menciptakan celah hukum yang dimanfaatkan oleh pelaku kejahatan.

Penerapan ketentuan pencegahan tindak pidana penipuan online berlandaskan pada Pasal 40 ayat (2a) yang berbunyi "Pemerintah wajib melakukan pencegahan penyebarluasan dan penggunaan

Copyright © 2026, Jurnal Pengabdian Masyarakat dan Riset Pendidikan
ISSN 2963-7856 (print), ISSN 2961-9890 (online)

Informasi Elektronik dan/ atau Dokumen Elektronik yang memiliki muatan yang dilarang sesuai dengan ketentuan peraturan perundang-undangan" dan ayat (2b) yakni "Dalam melakukan pencegahan sebagaimana dimaksud pada ayat (2a), Pemerintah berwenang melakukan pemutusan Akses dan/atau memerintahkan kepada Penyelenggara Sistem Elektronik untuk melakukan pemutusan Akses terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar hukum". Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas UU ITE, yang memberikan kewajiban dan kewenangan kepada Pemerintah (dalam hal ini Kementerian Komunikasi dan Informatika/Kominfo) untuk melakukan tindakan preventif. Penerapan ini diwujudkan melalui dua mekanisme utama: pertama, pencegahan proaktif berupa literasi digital massal kepada masyarakat, dan kedua, pencegahan teknis reaktif berupa pemutusan akses atau blocking terhadap link atau konten yang terbukti melanggar hukum, seperti website phishing atau nomor telepon yang digunakan untuk menjebak korban tindak pidana penipuan online.

Insiden penipuan daring yang menimpa nasabah Bank BRI melalui metode tautan jebakan pada dasarnya mengindikasikan adanya celah pada aspek literasi digital nasabah serta urgensi penguatan edukasi dari pihak perbankan. Fenomena kejahatan berbasis phishing ini sebenarnya dapat dimitigasi melalui kewaspadaan terhadap pesan-pesan persuasif yang manipulatif. Langkah preventif yang krusial meliputi sikap skeptis terhadap identitas pengirim, mengingat aktor siber kerap menggunakan atribusi fiktif untuk membangun kepercayaan. Selain itu, nasabah sangat disarankan untuk tidak mengakses tautan mencurigakan, mengabaikan ancaman intimidatif, serta rutin melakukan pemutakhiran perangkat lunak keamanan. Jika terjadi interaksi yang tidak disengaja dengan situs berbahaya, tindakan segera berupa perubahan kredensial akun dan perlindungan data pribadi pada platform yang tidak terverifikasi menjadi langkah proteksi mandiri yang sangat mendesak (Tangkary dkk., 2018). Bank bisa saja melakukan temporary block atau blokir sementara terhadap rekening-rekening yang terkena hack atau sadap. Dengan demikian paling tidak sudah sedikit aman karena bisa memberhentikan aliran uang sehingga tidak ada lagi transaksi yang keluar namun biasanya untuk melakukan ini diperlukan surat dari kepolisian untuk dapat melakukan tahap penyelesaian yang lebih lanjut. Kemudian yang bisa dilakukan oleh pihak bank biasanya hanya memberikan edukasi lebih dalam mengenai aturan-aturan yang perlu dilakukan sebagai nasabah serta memberitahukan bahwa bank tidak pernah meminta mengisi link berupa data nasabah jika terkait dengan perubahan biaya transaksi. Bank harus terbuka dan nasabahnya juga harus mau untuk diberikan edukasi. Supaya tidak lagi terjadi hal-hal yang tidak diinginkan seperti penipuan online ini, yang mana sangat merugikan pihak nasabah karena uang yang ada di rekening bisa tersedot begitu saja dalam waktu hitungan menit bahkan detik. Namun, dalam kasus penipuan phishing perbankan, penerapan pencegahan ITE menunjukkan keterbatasan yang signifikan. Tindakan pemutusan akses oleh Kominfo seringkali membutuhkan proses pelaporan dan verifikasi yang sangat memakan waktu (bersifat reaktif), karena jika terjadi hal seperti itu satu detik saja sangatlah berharga dan krusial apalagi jika harus menunggu dalam sehari dan sekian hari. Hal ini bertabrakan dengan kecepatan pelaku siber dalam menguras rekening terjadi dalam hitungan beberapa menit saja seperti yang dialami korban nasabah BRI yang saldonya sangat cepat terkuras selama proses pemblokiran rekening sedang dilakukan. Kondisi ini menunjukkan adanya kesenjangan waktu respons antara kecepatan kejahatan yang dilakukan melalui online dan mekanisme pencegahan yang diatur dalam UU ITE serta regulasi turunannya.

Analisis Kepastian Hukum Terkait Pencegahan Tindak Pidana Penipuan Online berdasarkan Undang-Undang ITE

Analisis kepastian hukum terkait pencegahan penipuan online menunjukkan adanya ketidakselarasan antara das sollen (apa yang seharusnya diatur oleh hukum) dan das sein (kenyataan di lapangan). Kepastian hukum idealnya menjamin bahwa regulasi mampu menciptakan sistem pencegahan yang efektif. Namun, dalam konteks pencegahan kejahatan siber, ketidakpastian hukum sering kali timbul dalam penerapan pasal-pasal UU ITE terkait kewajiban preventif. Dalam kasus penipuan phishing, meskipun UU ITE mengatur sanksi bagi pelaku, tidak adanya Kepastian Hukum yang tegas mengenai standar waktu respons Call Center atau mekanisme penggantian kerugian oleh PSE yang terbukti memiliki kelemahan sistem (seperti yang dialami korban BRI yang rekeningnya dikuras saat proses permintaan blokir), menyebabkan korban merasa dirugikan dan tidak mendapat perlindungan hukum yang pasti. Hal ini sejalan dengan pandangan (Situmeang, 2021) bahwa lemahnya sistem keamanan dan pengawasan dalam transaksi elektronik sering kali menjadi faktor kriminogen (penyebab

kejahatan) , sehingga menghilangkan kepastian bagi masyarakat bahwa mereka terlindungi secara hukum saat bertransaksi elektronik. Proses pemutusan akses oleh Kementerian Kominfo seringkali memerlukan verifikasi yang lama, sementara dana nasabah bisa hilang dalam hitungan detik. Hal ini menunjukkan bahwa struktur hukum saat ini belum mampu memberikan kepastian hukum yang bersifat real-time. Kepastian hukum yang pincang ini menguntungkan pelaku kejahatan yang memanfaatkan anonimitas dan kecepatan transaksi digital untuk menghilangkan jejak sebelum sistem pencegahan formal sempat beroperasi.

Kepastian hukum dalam konteks pencegahan tindak pidana siber seharusnya berfungsi sebagai jaminan perlindungan dan prediktabilitas bahwa peraturan yang ada akan dilaksanakan secara efektif dan konsisten. Dalam konteks UU ITE, kepastian hukum ini disandarkan pada kewenangan pencegahan yang diatur dalam Pasal 40 ayat (2a) dan (2b), yang mewajibkan pemerintah dan memberikan kewenangan pemutusan akses untuk melindungi kepentingan umum dari gangguan penyalahgunaan informasi elektronik. Ketiadaan peraturan turunan yang bersifat Lex Specialis dan detail operasional yang mengikat bagi Penyelenggara Sistem Elektronik (PSE), khususnya di sektor jasa keuangan, menciptakan zona abu-abu. UU ITE hanya memberikan dasar hukum pencegahan secara umum, tetapi gagal memberikan kepastian bahwa mekanisme tersebut memiliki daya paksa dan kecepatan yang memadai untuk menangkal serangan siber yang bergerak secara instan.

Ketidakpastian hukum paling nyata dirasakan oleh korban ketika berhadapan dengan kelambatan respons sistem pada PSE. Dalam kasus penipuan phishing berkedok tarif bank, korban mengeluhkan respon lambat dari Call Center bank BRI saat mencoba memblokir rekening, yang berakibat pada terus terkurasnya dana hingga mencapai ratusan juta rupiah. Situasi ini membuktikan bahwa tidak adanya norma yang mengatur secara tegas Standar Waktu Maksimum Respons Cepat (SWMRC) bagi bank telah menghilangkan jaminan kepastian hukum. Hukum menjadi tidak pasti karena tidak mampu memberikan solusi pencegahan yang real-time dan andal pada momen kritis. Kegagalan sistemik ini menunjukkan bahwa meskipun UU ITE mengatur sanksi bagi pelaku (Penal), pencegahan (Non-Penal) yang seharusnya menjadi benteng perlindungan pertama justru tidak berfungsi akibat absennya ketegasan regulasi operasional. Dalam teori kepastian hukum, kepastian hukum bukan sekadar keberadaan norma tertulis, melainkan mencakup keterdugaan (predictability) atas tindakan hukum yang akan diambil ketika terjadi suatu pelanggaran. Dalam konteks pencegahan penipuan daring, kepastian hukum diuji melalui sejauh mana prosedur teknis dapat dijalankan secara konsisten dan segera untuk memitigasi kerugian. Namun, realitas pada kasus nasabah bank BRI menunjukkan adanya kegagalan pada pilar kepastian prosedur, di mana korban tidak mendapatkan jaminan waktu mengenai kapan pemblokiran rekening akan efektif dilakukan setelah laporan diterima. Oleh karena itu, kepastian hukum dalam ekosistem digital hanya dapat terwujud apabila terdapat sinkronisasi antara kepastian norma (regulasi yang jelas), kepastian aparat (respons cepat perbankan dan aparat), dan kepastian sarana (teknologi deteksi dini yang terintegrasi). Penyelenggaraan sistem elektronik oleh penyelenggara sistem elektronik (PSE) harus berlandaskan pada nilai-nilai keadilan bermartabat (Koswara W, 2022).

Dalam ranah pelayanan publik penyelenggaraan harus menerapkan prinsip-prinsip AUPB (Asas-asas umum Pemerintahan yang Baik). Kinerja staff call center Bank BRI atau disebut juga dengan PSE (Penyelenggara Sistem Elektronik) yang dinilai lambat merespon keluhan nasabah terkait telatnya pemblokiran rekening menyebabkan ketidakpuasan nasabah. Selain menciptakan rasa ketidakpuasan bagi nasabah, hal ini juga merupakan bentuk pelanggaran serius terhadap Asas Profesionalitas dan Asas Kehati-hatian bank. Dalam dunia perbankan, waktu adalah faktor krusial, terutama dalam penanganan kejahatan siber (cybercrime). Prinsip profesionalitas, yang menuntut kecakapan teknis dan kepatuhan terhadap standar etika perundang-undangan, tampak belum terimplementasi secara optimal dalam konteks ini. Penting untuk diingat bahwa posisi bank tidak sekadar sebagai lembaga jasa, tetapi juga sebagai agen pembangunan yang memfasilitasi kelancaran arus ekonomi dari hulu ke hilir. Peran sebagai agent of development menempatkan bank sebagai motor penggerak sektor produksi dan distribusi. Namun, pilar utama yang menopang seluruh arsitektur perbankan adalah posisinya sebagai agent of trust. Kepercayaan adalah komoditas utama dalam dunia perbankan; tanpanya, mekanisme penghimpunan dan pendistribusian dana masyarakat tidak akan dapat berjalan secara berkelanjutan (Tarantang dkk., 2023). Bank BRI dianggap tidak profesional jika gagal merespons situasi darurat nasabah dengan cepat. Kerugian materiil nasabah yang terus bertambah setiap menit seharusnya bisa

Copyright © 2026, Jurnal Pengabdian Masyarakat dan Riset Pendidikan
ISSN 2963-7856 (print), ISSN 2961-9890 (online)

dihentikan jika bank menjalankan fungsinya dengan cakap. Profesionalitas menuntut adanya SOP (Standard Operating Procedure) yang efektif untuk keadaan darurat. Bank BRI merupakan bentuk perusahaan persero tentu harus dapat menerapkan Good Corporate Governance (tata kelola perusahaan yang baik). Berdasarkan prinsip Good Corporate Governance, bank sebagai PSE seharusnya memikul beban pembuktian bahwa sistem keamanannya telah bekerja maksimal. Jika bank gagal memenuhi SWMRC (misalnya gagal memblokir dalam 15 menit setelah laporan), maka secara hukum harus ada kepastian bahwa bank wajib memberikan restitusi atau ganti rugi atas kerugian yang timbul sejak laporan diterima. Sinergi antara regulasi (UU ITE), pengawasan (OJK/BI), dan pelaksanaan teknis (PSE) adalah kunci. Tanpa adanya integrasi sistem pemblokiran yang otomatis antara bank pelapor dan bank penampung, kepastian hukum bagi korban untuk mendapatkan kembali haknya (uang yang dicuri) akan sangat sulit dicapai. Oleh karena itu, kepastian hukum dalam pencegahan penipuan daring harus diwujudkan melalui aturan teknis yang memaksa PSE untuk bertindak proaktif, bukan sekadar menunggu instruksi birokratis yang lambat.

Mengingat sifat ruang siber yang sangat luas dan tidak memiliki lintas batas (borderless), dan dinamis. Dalam perspektif hukum, kepastian hukum mensyaratkan adanya kejelasan norma, keterdugaan tindakan hukum, dan konsistensi dalam penegakan. Berdasarkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah terakhir dengan UU Nomor 1 Tahun 2024, analisis kepastian hukum ini dapat ditelaah melalui beberapa pilar utama: legalitas norma, wewenang eksekutif dalam mitigasi, dan tanggung jawab penyelenggara sistem.

Secara normatif, kepastian hukum bermula dari Pasal 28 ayat (1) UU ITE. Pasal ini menjadi jangkar hukum yang mendefinisikan perbuatan terlarang terkait penipuan online. Namun, analisis kepastian hukum sering kali berbenturan dengan interpretasi frasa "berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen". Dalam perkembangannya, revisi UU ITE berupaya memperjelas batasan ini agar tidak terjadi "pasal karet". Kepastian hukum dalam permasalahan tindak pidana penipuan online dicapai ketika unsur-unsur pidana tersebut dapat dibuktikan secara digital melalui alat bukti elektronik yang sah sesuai Pasal 5 UU ITE, sehingga pelaku tidak dapat mengelak atas dasar ketiadaan bukti fisik. Tanpa adanya kejelasan mengenai apa yang dikategorikan sebagai "menyesatkan", penegakan hukum akan kehilangan arah, namun UU ITE telah memitigasi ini dengan menghubungkan kerugian tersebut secara spesifik pada transaksi elektronik.

Salah satu aspek terpenting dari kepastian hukum adalah adanya aturan yang jelas mengenai tindakan pencegahan sebelum kerugian meluas. Dalam hal ini, Pasal 40 ayat (2a) dan (2b) UU ITE memberikan landasan hukum bagi Pemerintah untuk melakukan pemutusan akses. Kepastian hukum di sini diuji melalui mekanisme yang transparan: pemerintah tidak hanya memiliki hak, tetapi kewajiban untuk melindungi kepentingan umum dari gangguan penyalahgunaan informasi elektronik. Tindakan take down atau pemblokiran situs penipuan merupakan bentuk kepastian bahwa negara hadir untuk mencegah eskalasi kejahatan. Namun, kepastian hukum juga menuntut adanya prosedur operasi standar (SOP) yang jelas agar wewenang pemblokiran ini tidak dilakukan secara sewenang-wenang tanpa dasar bukti yang kuat.

Selanjutnya, kepastian hukum terkait pencegahan melibatkan peran Penyelenggara Sistem Elektronik (PSE). Berdasarkan Pasal 15 UU ITE, PSE wajib menyelenggarakan sistem elektronik secara andal dan aman. Analisis kepastian hukum menunjukkan bahwa kewajiban ini bukan sekadar imbauan moral, melainkan kewajiban hukum yang memiliki implikasi sanksi. Ketika sebuah platform digital gagal menerapkan sistem verifikasi yang mampu mendeteksi akun penipu, maka kepastian hukum bagi konsumen menjadi terancam. Oleh karena itu, regulasi turunannya (seperti Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik) hadir untuk mengisi kekosongan teknis, memastikan bahwa setiap pengelola aplikasi memiliki standar keamanan yang seragam demi melindungi pengguna.

Dari sudut pandang sanksi, kepastian hukum diwujudkan melalui Pasal 45A ayat (1) yang menetapkan ancaman pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp1 miliar. Kepastian sanksi ini berfungsi sebagai general deterrence (pencegahan umum). Analisis hukum melihat bahwa sanksi yang berat saja tidak cukup tanpa adanya kepastian penuntutan (certainty of punishment). Di sinilah peran penyidik Polri (Cyber Crime) dan PPNS (Penyidik Pegawai Negeri Sipil) menjadi vital. UU ITE memberikan legitimasi bagi penyidik untuk melakukan penyitaan aset digital dan akses data komunikasi, yang jika dilakukan sesuai prosedur hukum acara (KUHAP), akan memperkuat kepastian bahwa pelaku penipuan online tidak dapat berlindung di balik anonimitas internet. Dalam menjalankan

fungsinya, PPNS dibekali kewenangan khusus oleh UU ITE melalui Pasal 43 ayat (5) untuk mengintervensi ruang digital demi kepentingan hukum. Kewenangan ini mencakup tindakan teknis berupa pemblokiran atau pemutusan akses terhadap konten yang terindikasi melanggar hukum siber. Lebih lanjut, undang-undang ini memperkuat posisi penyidik dengan hak untuk mengakses informasi dari pihak Penyelenggara Sistem Elektronik. Sinergi informasi antara PSE dan PPNS ini merupakan instrumen krusial dalam mengungkap modus operandi kejahatan berbasis teknologi informasi yang semakin kompleks (Fitri S, 2022).

Namun, tantangan dalam mencapai kepastian hukum yang paripurna adalah sifat kejahatan siber yang sering kali bersifat transnasional. Meskipun Pasal 2 UU ITE menganut asas ekstrateritorial (berlaku bagi siapa pun yang merugikan kepentingan Indonesia meski berada di luar negeri), efektivitasnya sangat bergantung pada kerja sama internasional (Mutual Legal Assistance). Tanpa adanya eksekusi yang nyata terhadap pelaku di luar negeri, kepastian hukum bagi korban di dalam negeri akan terasa pincang. Oleh karena itu, analisis hukum menyimpulkan bahwa pencegahan tidak bisa hanya mengandalkan teks undang-undang, tetapi juga harus mencakup kekuatan diplomasi hukum internasional.

Dalam konteks keterlambatan pemblokiran rekening oleh Bank (PSE), terjadi ketidakpastian hukum karena meskipun UU ITE Pasal 15 mewajibkan PSE menyelenggarakan sistem yang andal dan aman , tidak ada parameter kuantitatif yang jelas mengenai apa yang dimaksud dengan "andal" dalam situasi darurat. Ketiadaan standar waktu seperti Standar Waktu Maksimum Respons Cepat (SWMRC) menyebabkan interpretasi terhadap "pelayanan yang profesional" menjadi subjektif. Ketika nasabah melaporkan adanya serangan phishing yang menyedot saldo dalam hitungan menit, namun bank merespons dengan lambat, maka perlindungan hukum yang dijanjikan oleh Pasal 40 UU ITE menjadi bersifat ilusi (illusory protection). Kepastian hukum bagi nasabah hilang karena mereka tidak dapat memprediksi kapan tindakan penyelamatan dana akan dilakukan oleh pihak bank. Penipuan online juga bisa dilakukan oleh pelaku yang berada di luar yurisdiksi Indonesia. UU ITE Pasal 2 menganut asas ekstrateritorial, yang memungkinkan hukum Indonesia menjangkau perbuatan hukum yang dilakukan di luar wilayah Indonesia jika merugikan kepentingan nasional. Namun, dalam hal pencegahan, penerapan asas ini sangat bergantung pada kerjasama internasional (Mutual Legal Assistance). Tanpa adanya sinergi antarnegara untuk memutus akses server di luar negeri secara cepat, upaya pencegahan domestik akan selalu menghadapi tembok pembatas yang sulit ditembus.

PENUTUP

Pengaturan pencegahan tindak pidana penipuan online secara normatif telah memiliki landasan kuat melalui Pasal 28 ayat (1) UU ITE yang mendefinisikan delik penipuan, serta Pasal 40 ayat (2a) dan (2b) yang memberikan mandat atributif kepada Pemerintah untuk melakukan pencegahan dan pemutusan akses terhadap informasi elektronik yang melanggar hukum. Namun, dalam implementasinya, ditemukan bahwa penerapan ketentuan tersebut masih bersifat reaktif dan seringkali terhambat oleh kendala birokrasi serta teknis. Penyelenggara Sistem Elektronik (PSE), khususnya perbankan, memiliki tanggung jawab hukum berdasarkan Pasal 15 UU ITE untuk menyelenggarakan sistem yang andal dan aman, namun dalam realitanya, mekanisme mitigasi seperti respons terhadap laporan phishing masih sangat lamban. Selain itu, efektivitas pencegahan sangat bergantung pada literasi digital masyarakat yang saat ini masih menjadi titik lemah, sehingga edukasi berkelanjutan menjadi instrumen non-penal yang krusial namun belum terintegrasi secara maksimal dalam ekosistem perbankan digital.

Terdapat kesenjangan signifikan (discrepancy) antara das sollen (hukum yang dicita-citakan) dan das sein (kenyataan di lapangan) dalam mewujudkan kepastian hukum. Ketiadaan regulasi pelaksana yang bersifat lex specialis, seperti Standar Waktu Maksimum Respons Cepat (SWMRC), menyebabkan perlindungan hukum bagi nasabah menjadi bersifat semu (illusory protection) karena tidak adanya jaminan durasi waktu bagi bank (PSE) untuk melakukan tindakan darurat seperti pemblokiran rekening setelah laporan diterima. Kepastian hukum hanya dapat terwujud apabila terdapat sinkronisasi antara kepastian norma, respons cepat perbankan yang profesional, serta adanya mekanisme pertanggungjawaban ganti rugi yang jelas bagi nasabah atas kelalaian operasional PSE.

Copyright © 2026, Jurnal Pengabdian Masyarakat dan Riset Pendidikan
ISSN 2963-7856 (print), ISSN 2961-9890 (online)

Penguatan ekosistem perlindungan hukum bagi nasabah perbankan digital di Indonesia memerlukan sinergi kebijakan yang dimulai dengan perumusan regulasi turunan UU ITE oleh Pemerintah dan OJK yang mengatur tentang Standar Waktu Maksimum Respons Cepat (SWMRC) agar terdapat kepastian durasi waktu bagi bank dalam melakukan tindakan preventif seperti pemblokiran akun segera setelah laporan diterima. Hal ini harus diimbangi dengan peningkatan profesionalitas Penyelenggara Sistem Elektronik (PSE) perbankan melalui investasi pada teknologi kecerdasan buatan untuk deteksi dini transaksi anomali serta penyediaan mekanisme pelaporan darurat yang tidak hanya bersifat administratif, tetapi memiliki kewenangan teknis langsung untuk merespons aduan dalam hitungan menit guna memitigasi kerugian materiil nasabah secara nyata. Pada akhirnya, upaya teknis dan regulasi tersebut akan mencapai efektivitas maksimal apabila didukung oleh kesadaran nasabah dalam meningkatkan literasi digital serta kewaspadaan terhadap manipulasi psikologis, sehingga tercipta kolaborasi pertahanan yang solid antara ketaatan hukum masyarakat, keandalan sistem perbankan, dan ketegasan pengawasan pemerintah di ruang siber.

UCAPAN TERIMA KASIH

Puji syukur penulis panjatkan kepada Tuhan Yang Maha Esa atas kelancaran proses penyusunan artikel ini. Penulis mengucapkan terima kasih yang sebesar-besarnya kepada Bu Adhining Prabawati Rahmahani selaku dosen pembimbing dan rekan penulis (co-author) yang telah memberikan arahan, koreksi, dan pandangan hukum yang tajam selama penyusunan naskah ini. Terima kasih juga penulis sampaikan kepada Civitas Akademika Universitas Esa Unggul dan rekan-rekan mahasiswa yang telah memberikan dukungan moril dan diskusi yang bermanfaat terkait isu reformasi birokrasi dan perizinan digital.

REFERENSI

Anugerah, F. (2022). Pencurian data pribadi di internet dalam perspektif kriminologi. *Jurnal Komunikasi Hukum, 8*(1). https://ejournal.undiksha.ac.id/index.php/jkh

Assegaf, V. N. (2024). Upaya pencegahan tindak pidana penipuan arisan online Indonesia. *Jurnal Ilmu Pengetahuan Naratif, 5*(4). https://ijurnal.com/1/index.php/jipn

Faizah Nurfahda, A., Putri, A. J., Yardi, N. A., & Deni, F. (2024). Analisis penipuan online dalam bentuk phishing menurut perspektif hukum Indonesia. *Sahid Banking Journal, 4*(1). https://jurnal.febi-inais.ac.id/index.php/SahidBankingJ

Fitri, S. (2022). Politik hukum pembentukan cyber law Undang-Undang Informasi dan Transaksi Elektronik di Indonesia. *Jurnal Ilmu Hukum, Perundang-Undangan dan Pranata Sosial, 7*(1).

Hukum Acara Pidana Indonesia. (n.d.). *Kitab Undang-Undang Hukum Acara Pidana (KUHAP)*.

Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.

Indonesia. (2016). *Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.

Indonesia. (2024). *Undang-Undang Nomor 1 Tahun 2024 tentang perubahan kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.

Koswara, W. (2022). Implementasi peraturan perlindungan data pribadi. *Paradigma Hukum Pembangunan, 7*(2). https://www.suara.com/tekno/2022/01/01/015822/daftar-kasus-kebocoran-data-di-indonesia-selama-

Kurnia, I. (2024). *Hukum pidana siber: Aspek teoretis dan praktis dalam era digital di Indonesia*. CV Eureka Media Aksara.

Maskun, M., & Saloko, W. M. (2017). *Aspek hukum penipuan berbasis internet*. Keni Media.

Sahlepi, M. A. (2023). Tinjauan yuridis terhadap tindak pidana penipuan secara online ditinjau dari Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. *Innovative: Journal of Social Science Research, 3*(6), 1402–1412.

Situmeang, S. M. T. (2021). Penyalahgunaan data pribadi sebagai bentuk kejahatan sempurna dalam perspektif hukum siber. *SASI, 27*(1), 38. https://doi.org/10.47268/sasi.v27i1.394

Sulubara, S. M. (2025). *Perlindungan hukum tindak pidana cybercrime dalam cyberlaw di Indonesia: Perkembangan teknologi dan tantangan hukum dalam mewujudkan cybersecurity*. CV Tahta Media Group.

Syah, R. (2023). Strategi kepolisian dalam pencegahan kejahatan phishing melalui media sosial di ruang siber. *Jurnal Impresi Indonesia, 2*(9), 864–870. https://doi.org/10.58344/jii.v2i9.3594

Tamo Ama, J., & Kadir, S. A. (2024). Tinjauan yuridis terhadap tindak pidana penipuan online. *Media Hukum Indonesia (MHI), 2*(2), 241. https://doi.org/10.5281/zenodo.11318026

Tangkary, S., Hartono, H., Ameliah, R., Ahmad, D., Ningrum, D. W., Styawan, H., Harinanda, I. R. L. I., Magdalena, M., & Butar Butar, R. (2018). *Keamanan siber untuk e-commerce* (D. B. U. & I. Banyumurt, Eds.). Kementerian Komunikasi dan Informatika Republik Indonesia. https://www.literasidigital.id

Tarantang, J., Pelu, I. E. A. S., Akbar, W., Kurniawan, R., & Wahyuni, A. S. (2023). Perlindungan hukum terhadap nasabah bank dalam transaksi digital. *Morality: Jurnal Ilmu Hukum, 9*(1), 15. https://doi.org/10.52947/morality.v9i1.321

Widya, S. (2025). *Mengenal phishing: Ancaman nyata di era digital*. Widya Security Team.

Yaqin, H., Heriyanto, H., & Dairani, D. (2025). Analisis yuridis perlindungan hukum terhadap korban tindak pidana penipuan dalam transaksi e-commerce. *Maras: Jurnal Penelitian Multidisiplin, 3*(1), 411–418. https://doi.org/10.60126/maras.v3i1.790

Subyanto, W. (2022, June 9). *Ngeri, cuma klik link dari pesan WhatsApp rekening nasabah BRI terkuras hingga Rp11 miliar*. Nextren. https://nextren.grid.id/read/013320306/ngeri-cuma-klik-link-dari-pesan-wa-rekening-nasabah-bri-terkuras-hingga-rp-11-miliar?page=all

Copyright © 2026, Jurnal Pengabdian Masyarakat dan Riset Pendidikan
ISSN 2963-7856 (print), ISSN 2961-9890 (online)