CAUSA
ISSN 3031-0369

Jurnal Hukum dan Kewarganegaraan
Vol 13 No 2 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

Pelindungan Hukum bagi Nasabah Bank Digital terhadap Ancaman Pencurian Data melalui BTS Palsu *(Fake BTS)*

Yoan Shevila Kristiyenda[1], Tasya Safiranita Ramli[2]
Ilmu Hukum, Fakultas Hukum, Universitas Padjadjaran
Email : Yoan21001@mail.unpad.ac.id

ABSTRAK

Perkembangan teknologi perbankan digital telah mempermudah transaksi, namun memunculkan ancaman kejahatan siber, khususnya pencurian data melalui teknologi *Base Transceiver Station* (BTS) palsu. Penelitian ini menganalisis pelindungan hukum bagi nasabah bank online dari ancaman tersebut berdasarkan UU No.1/2024 tentang Informasi dan Transaksi Elektronik dan UU No.36/1999 tentang Telekomunikasi. Menggunakan pendekatan yuridis normatif dengan elemen empiris, penelitian ini meneliti kasus kejahatan siber yang diungkap Bareskrim Polri pada Maret 2025, di mana pelaku memanfaatkan BTS palsu untuk menyebarkan SMS *phishing*, menyebabkan kerugian Rp473 juta. UU ITE mengatur kejahatan seperti manipulasi data elektronik dan akses ilegal, sementara UU Telekomunikasi melarang penyadapan jaringan. Namun, implementasi hukum terhambat oleh ketiadaan regulasi spesifik, penegakan hukum yang reaktif, dan rendahnya literasi digital. Penelitian ini merekomendasikan penyempurnaan regulasi, penguatan keamanan bank, dan edukasi masyarakat untuk meningkatkan pelindungan nasabah. Hasil penelitian diharapkan mendukung kebijakan yang responsif terhadap kejahatan siber, memperkuat kepercayaan publik terhadap perbankan digital di Indonesia.

Kata Kunci: BTS Palsu, Nasabah Bank Online, Pelindungan Hukum

ABSTRACT

The development of digital banking technology has simplified transactions but also introduced the threat of cybercrime, particularly data theft through fake Base Transceiver Station (BTS) technology. This study analyzes the legal protection available to online banking customers against such threats based on ITE Law and Telecommunications Law. Using a normative juridical approach with empirical elements, this research examines a cybercrime case disclosed by the Indonesian National Police's Criminal Investigation Department (Bareskrim Polri) in March 2025, in which perpetrators used fake BTS to distribute phishing SMS, resulting in losses amounting to IDR 473 million. The ITE Law regulates crimes such

Article History
Received: Mei 2025
Reviewed: Mei 2025
Published: Mei 2025

Plagirism Checker No 234
Prefix DOI : Prefix DOI : 10.8734/CAUSA.v1i2.365

Publish by : CAUSA

CAUSA
ISSN 3031-0369
Jurnal Hukum dan Kewarganegaraan
Vol 13 No 2 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

as electronic data manipulation and illegal access, while the Telecommunications Law prohibits network interception. However, legal implementation faces obstacles due to the lack of specific regulations, reactive law enforcement, and low levels of digital literacy. This study recommends regulatory improvements, enhanced banking security, and public education to strengthen customer protection. The findings are expected to support policies that are responsive to cybercrime and reinforce public trust in Indonesia's digital banking sector.

Keywords: *Fake BTS, Online Banking Customers, Legal Protection*

PENDAHULUAN

Inovasi yang berkembang cepat di ranah teknologi informasi dan komunikasi turut mendorong perubahan yang berarti dalam berbagai sektor, khususnya dalam bidang perbankan. (Awaludin, Yasin, & Risyda, 2024). Saat ini, transaksi perbankan tidak lagi terbatas pada layanan tatap muka di kantor cabang, melainkan banyak dilakukan secara online melalui aplikasi dan internet banking. Kemudahan ini tentunya memberikan banyak manfaat bagi nasabah, seperti kemudahan akses, kecepatan transaksi, dan efisiensi waktu.

Namun, di balik kemudahan tersebut, nasabah bank online juga menghadapi berbagai ancaman keamanan yang semakin kompleks, salah satunya adalah pencurian data dan dana melalui teknologi *Base Transceiver Station* (BTS) palsu. BTS merupakan komponen utama dalam jaringan telekomunikasi seluler yang biasanya berupa menara dengan tinggi tertentu, dilengkapi antena pemancar dan penerima, serta perangkat telekomunikasi yang ditempatkan di dalam shelter khusus. Keberadaan BTS memiliki peran krusial dalam sistem telekomunikasi karena berfungsi sebagai penghubung antara jaringan milik operator seluler dengan perangkat milik pengguna. (Yogi Yunefri, 2015). Dengan fungsi vital tersebut, BTS menjadi salah satu elemen kunci dalam menjaga konektivitas data dan komunikasi antara perangkat pengguna dan sistem jaringan operator.

Ancaman ini menjadi semakin nyata ketika pelaku kejahatan memanfaatkan kelemahan infrastruktur telekomunikasi, khususnya dengan menyalahgunakan fungsi dan keberadaan BTS yang seharusnya mendukung konektivitas menjadi sarana untuk melakukan tindakan kriminal. BTS palsu adalah perangkat yang beroperasi secara ilegal dengan meniru identitas menara BTS milik operator resmi, sehingga mampu menjalankan fungsi komunikasi seperti pengiriman SMS massal ke ponsel di sekitarnya tanpa terdeteksi oleh infrastruktur pengawasan operator seluler. (BCA, 2025). Modus ini sangat berbahaya karena sulit terdeteksi dan dapat menimbulkan kerugian finansial yang besar bagi nasabah. (Dewi et al., 2023)

Modus semacam ini tidak lagi bersifat teoritis, melainkan telah terbukti terjadi secara nyata di lapangan melalui pengungkapan kasus kejahatan siber oleh aparat penegak hukum. Dalam konferensi pers yang digelar pada tanggal 24 Maret 2025, Kepala Bareskrim Polri, Komisaris Jenderal Polisi Wahyu Widada, menjelaskan bahwa dalam kasus ini, dua orang warga negara asing (WNA) asal Tiongkok berinisial XC dan YXC ditangkap di kawasan pusat bisnis SCBD, Jakarta Selatan. Penangkapan ini dilakukan setelah salah satu bank swasta

CAUSA
ISSN 3031-0369
Jurnal Hukum dan Kewarganegaraan
Vol 13 No 2 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

melaporkan adanya 259 keluhan nasabah yang menerima pesan singkat mencurigakan. Dari laporan tersebut, tercatat sebanyak 12 nasabah mengalami kerugian dengan total mencapai Rp473 juta setelah mengakses tautan *phishing* yang terdapat dalam SMS tersebut. Pelaku menggunakan kendaraan bermodifikasi dengan BTS palsu untuk menjangkau area publik, mengeksploitasi kelemahan infrastruktur telekomunikasi dan rendahnya literasi keamanan digital masyarakat (Abdi, 2025).

Meskipun Indonesia memiliki regulasi seperti Undang-Undang No. 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik serta Undang-Undang No. 36 Tahun 1999 tentang Telekomunikasi, implementasi pelindungan hukum terhadap nasabah bank online masih menghadapi tantangan. Permasalahan ini mendorong perlunya pengkajian lebih lanjut mengenai bentuk ancaman yang ditimbulkan oleh penyalahgunaan teknologi BTS palsu serta efektivitas pelindungan hukum yang tersedia bagi nasabah. Dengan mempertimbangkan latar belakang yang telah dipaparkan, penelitian ini dirancang untuk menjawab permasalahan berikut:

1. Bagaimana ancaman pencurian terhadap nasabah bank online melalui teknologi BTS palsu?
2. Bagaimana bentuk pelindungan hukum yang berlaku bagi nasabah bank online terhadap ancaman pencurian data dan dana melalui teknologi BTS palsu?

Penelitian ini diharapkan memberikan sumbangsih terhadap perumusan kebijakan yang lebih tanggap terhadap tindak kejahatan siber, memperkuat sistem perlindungan nasabah, dan menumbuhkan kepercayaan publik terhadap perkembangan ekosistem perbankan digital nasional.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan yuridis normatif, yaitu metode kajian hukum yang berfokus pada analisis terhadap peraturan perundang-undangan, dokumen resmi, serta sumber-sumber hukum yang relevan sebagai landasan teori. Pendekatan ini dipilih untuk menganalisis kerangka hukum yang mengatur pelindungan nasabah bank online dari ancaman pencurian melalui teknologi *Base Transceiver Station* (BTS) palsu, dengan meneliti konsistensi, relevansi, dan efektivitas regulasi yang ada. Untuk memperkaya analisis, pendekatan ini dikombinasikan dengan elemen yuridis empiris guna memeriksa implementasi hukum dalam praktik, khususnya melalui kasus kejahatan siber yang diungkap oleh Dittipidsiber pada Maret 2025.

HASIL DAN PEMBAHASAN

Ancaman Pencurian Terhadap Nasabah Bank Online Melalui Teknologi BTS Palsu

Bank merupakan lembaga keuangan yang menjalankan fungsi sebagai perantara dalam menghimpun dan menyalurkan dana masyarakat, di mana keberlangsungan operasionalnya sangat ditentukan oleh kepercayaan publik terhadap kemampuannya dalam menjaga keamanan, integritas, dan pelayanan jasa keuangan (Zaki et al., 2024). Namun, kepercayaan tersebut kini menghadapi tantangan serius akibat maraknya kejahatan siber, salah satunya adalah *phishing*.

Phishing merupakan salah satu bentuk kejahatan siber yang dilakukan dengan cara menipu dan mengecoh korban. Umumnya, modus ini dijalankan melalui media digital seperti

CAUSA
ISSN 3031-0369
Jurnal Hukum dan Kewarganegaraan
Vol 13 No 2 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

email maupun platform media sosial, dengan mengirimkan tautan palsu, menciptakan situs web tiruan, dan teknik manipulasi digital lainnya. Sasaran utama dari aktivitas ini adalah mengumpulkan data pribadi yang sensitif milik korban, seperti informasi identitas, *password*, PIN, dan kode OTP, yang berkaitan dengan berbagai layanan keuangan digital seperti internet banking, mobile banking, dompet digital, kartu kredit, serta sistem pembayaran *paylater*. (Budiono,Fachri, Novayandra, 2025).

Salah satu bentuk turunan dari *phishing* yang kini semakin marak terjadi adalah *smishing,* yaitu penipuan dengan pendekatan serupa namun dilakukan melalui pesan singkat atau SMS. *Smishing* adalah salah satu bentuk tindak kejahatan digital yang dilakukan dengan mengirimkan pesan atau panggilan yang menipu, seolah-olah berasal dari institusi keuangan, kepada pengguna layanan *mobile banking*. Serangan ini semakin berbahaya apabila perangkat pengguna yang digunakan untuk transaksi hilang atau dicuri, karena fitur keamanannya dapat disusupi. (Indra, Indrayeni, 2024)

Modus penipuan terkait pembobolan rekening dapat menyasar siapa pun, tanpa memandang latar belakang. Penipuan ini biasanya diawali dengan pesan dari nomor tidak dikenal, di mana pelaku menyamar sebagai pihak tertentu dan mengirimkan file berformat APK melalui aplikasi WhatsApp. File tersebut didesain menyerupai tampilan gambar dari kurir pengiriman barang belanja daring, surat tilang elektronik, hingga undangan pernikahan. Rendahnya literasi digital di kalangan masyarakat menyebabkan banyak pengguna mobile banking menjadi korban, karena secara tidak sadar mengakses file tersebut. Setelah file dibuka, pelaku dapat memperoleh informasi sensitif seperti kode OTP, yang kemudian digunakan untuk mengakses dan mengosongkan saldo rekening korban secara ilegal.

Base Transceiver Station (BTS) adalah merupakan komponen utama dalam sistem komunikasi seluler yang biasanya berbentuk menara tinggi, dilengkapi dengan antena untuk mengirim dan menerima sinyal, serta dilengkapi perangkat pendukung yang ditempatkan dalam bangunan pelindung (shelter). Keberadaan BTS sangat penting karena berfungsi sebagai perantara antara penyedia layanan seluler dengan para penggunanya (Tasya, Rico, Dudi, 2020). Namun, seiring dengan kemajuan teknologi, keberadaan BTS justru dimanfaatkan secara tidak sah oleh pelaku kejahatan untuk menciptakan versi tiruannya yang dikenal sebagai BTS palsu.

Teknologi BTS palsu merupakan salah satu modus kejahatan siber yang semakin marak terjadi dalam dunia perbankan digital. BTS palsu ini berfungsi sebagai alat penyadap yang meniru sinyal jaringan seluler resmi untuk mengelabui perangkat komunikasi nasabah, seperti ponsel atau smartphone. Dengan terkoneksi pada BTS palsu, para pelaku kejahatan dapat memantau dan mengintersep komunikasi data nasabah secara diam-diam tanpa diketahui oleh korban maupun penyedia layanan resmi.

Kejahatan siber berbasis BTS palsu mengancam keamanan nasabah bank online di Indonesia. Pada 24 Maret 2025, Dittipidsiber mengungkap sindikat penipuan daring yang menyebabkan kerugian Rp473 juta melalui *smishing* berbasis BTS palsu. untuk mengintersepsi sinyal 4G, kemudian menurunkannya ke jaringan 2G, dan menyebarkan SMS *phishing* yang mengatasnamakan bank swasta tertentu.. Tautan palsu dalam SMS mengelabui nasabah untuk memasukkan kredensial perbankan. Dari 259 keluhan nasabah, 12 korban kehilangan dana setelah mengakses tautan tersebut. Dua warga negara Tiongkok, XC dan YXC, ditangkap di SCBD, Jakarta Selatan, saat mengoperasikan kendaraan dengan perangkat BTS palsu. Mereka

berperan sebagai operator lapangan, dikendalikan dari pusat, dengan YXC terafiliasi grup Telegram "Stasiun Pangkalan Indonesia."

Barang bukti yang disita meliputi dua kendaraan dengan BTS palsu, tujuh ponsel, tiga kartu SIM, dua kartu ATM, dan dokumen identitas. Tersangka dijerat dengan UU No. 1 Tahun 2024 tentang ITE, UU No. 36 Tahun 1999 tentang Telekomunikasi, UU No. 8 Tahun 2010 tentang TPPU, dan Pasal 55 KUHP, dengan ancaman 12 tahun penjara dan denda Rp12 miliar. Bareskrim Polri akan melanjutkan penyidikan dengan melibatkan Kementerian Komunikasi dan Informatika, Imigrasi, dan Interpol untuk menelusuri jaringan internasional (Abdi, 2025).

Kasus ini menunjukkan kerentanan infrastruktur telekomunikasi dan rendahnya literasi digital, yang memperparah risiko *phishing*. Ancaman ini mengguncang kepercayaan publik terhadap perbankan digital. Respons yang diperlukan mencakup penguatan teknologi, edukasi masyarakat, dan regulasi spesifik untuk kejahatan siber berbasis BTS palsu.

Pelindungan Hukum Yang Berlaku Bagi Nasabah Bank Online Dari Ancaman Tersebut

Ancaman kejahatan siber berbasis teknologi BTS palsu, yang memungkinkan pelaku menyebarkan SMS *phishing* untuk mencuri data nasabah bank online, menuntut pelindungan hukum yang efektif di Indonesia. Kerangka hukum yang berlaku mencakup UU No. 1 Tahun 2024 tentang Perubahan Kedua atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang mengatur kejahatan siber seperti penipuan daring, serta UU No. 36 Tahun 1999 tentang Telekomunikasi, yang melarang penyalahgunaan infrastruktur jaringan. Selain itu, UU No. 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (TPPU) dan Pasal 55 Kitab UU Hukum Pidana (KUHP) digunakan untuk menjerat pelaku yang terlibat dalam sindikat, seperti operator lapangan yang menjalankan BTS palsu. Kasus yang diungkap Bareskrim Polri pada 24 Maret 2025, di mana dua warga negara Tiongkok ditangkap dengan ancaman hukuman hingga 12 tahun penjara dan denda Rp12 miliar, menunjukkan penerapan regulasi ini untuk menangani kejahatan yang merugikan 12 nasabah sebesar Rp473 juta.

UU ITE menjadi dasar hukum yang kokoh dalam menangani berbagai bentuk kejahatan berbasis teknologi informasi, termasuk kejahatan *phishing* melalui BTS palsu. Dalam konteks ini, tindakan pelaku yang mengirimkan pesan singkat (SMS) palsu seolah-olah berasal dari institusi resmi, dengan tujuan menipu nasabah dan memperoleh akses terhadap data pribadi maupun akun keuangan, merupakan bentuk penipuan berbasis elektronik yang secara tegas dilarang dalam peraturan perundang-undangan tersebut.

Secara khusus, Pasal 35 jo. Pasal 51 UU ITE mengatur mengenai perbuatan manipulasi informasi elektronik. Pasal 35 berbunyi: *"Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik."*

Pasal 51 berbunyi: *"(1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah). (2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 36 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah)."*

CAUSA
ISSN 3031-0369
Jurnal Hukum dan Kewarganegaraan
Vol 13 No 2 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

Lebih lanjut, apabila pelaku melakukan akses ilegal terhadap sistem elektronik dengan menggunakan identitas dan kata sandi milik korban, maka perbuatan tersebut dapat dikualifikasikan sebagai pelanggaran terhadap Pasal 30 ayat (3) jo. Pasal 46 ayat (3) UU ITE, Pasal 30 ayat (3) berbunyi: *"Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan."*

Pasal 46 ayat (3) berbunyi: *"Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah)."*

Tidak hanya itu, apabila pelaku kemudian memindahkan atau mentransfer informasi atau dokumen elektronik yang diperoleh secara melawan hukum, seperti data isi rekening bank atau informasi finansial lainnya, maka tindakan tersebut dapat dijerat melalui Pasal 32 ayat (2) jo. Pasal 48 ayat (2) UU ITE. Pasal 32 ayat (2) berbunyi: *"Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak."*

Pasal 48 ayat (2) berbunyi: *"Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp3.000.000.000,00 (tiga miliar rupiah)."*

Di sisi lain, penggunaan BTS palsu sebagai alat utama dalam melancarkan serangan *phishing* juga bertentangan dengan ketentuan dalam UU No. 36 Tahun 1999 tentang Telekomunikasi. UU ini secara tegas melarang penyalahgunaan infrastruktur jaringan dan aktivitas yang dapat mengganggu sistem telekomunikasi nasional. Misalnya, Pasal 40 yang berbunyi *"Setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun."*. BTS palsu yang berfungsi untuk menyadap komunikasi dan meniru sinyal operator resmi jelas bertentangan dengan ketentuan ini.

Kasus konkret yang diungkap oleh Bareskrim Polri pada tanggal 24 Maret 2025 menjadi contoh aktual penerapan ketentuan hukum tersebut. Dalam kasus tersebut, dua warga negara asing asal Tiongkok berhasil diamankan karena mengoperasikan BTS palsu dan menyebarkan SMS blast yang menipu nasabah bank digital. Kerugian yang ditimbulkan mencapai Rp473 juta dari 12 nasabah yang menjadi korban, dan para pelaku terancam pidana hingga 12 tahun penjara dan denda Rp12 miliar. Kasus ini menunjukkan bahwa penegakan hukum terhadap pelaku kejahatan siber melalui skema BTS palsu dapat dilakukan dengan kombinasi antara ketentuan dalam UU ITE, UU Telekomunikasi, serta ketentuan pidana umum lainnya seperti Pasal 55 KUHP dan UU No. 8 Tahun 2010 tentang Tindak Pidana Pencucian Uang (TPPU) jika terbukti terdapat aliran dana hasil kejahatan.

Untuk meningkatkan pelindungan hukum terhadap nasabah bank online dari ancaman pencurian yang memanfaatkan teknologi BTS palsu, diperlukan beberapa upaya strategis yang melibatkan berbagai pihak, baik pemerintah, lembaga perbankan, maupun masyarakat. Pertama, pemerintah memiliki tanggung jawab untuk memperketat aturan serta meningkatkan mekanisme pengawasan dalam pemanfaatan teknologi telekomunikasi. khususnya yang berkaitan dengan jaringan BTS (Dovie, 2020). Hal ini mencakup pengaturan yang lebih ketat terkait lisensi dan pengoperasian BTSguna mencegah potensi eksploitasi oleh pihak-pihak yang tidak berwenang. Selain itu, penegakan hukum terhadap pelaku kejahatan siber harus dilakukan secara tegas dan transparan untuk memberikan efek jera.

CAUSA
ISSN 3031-0369
Jurnal Hukum dan Kewarganegaraan
Vol 13 No 2 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

Kedua, lembaga perbankan harus meningkatkan sistem keamanan teknologi informasi mereka dengan mengadopsi teknologi enkripsi yang lebih canggih dan sistem deteksi dini terhadap aktivitas mencurigakan. Bank juga perlu mengedukasi nasabah mengenai risiko keamanan digital serta cara-cara menjaga kerahasiaan data pribadi, seperti pentingnya verifikasi ganda *(two-factor authentication)* dan kewaspadaan terhadap komunikasi yang mencurigakan. Peningkatan kerja sama antara bank dengan penyedia layanan telekomunikasi dan aparat penegak hukum juga sangat penting untuk saling bertukar informasi dan cepat merespons ancaman yang muncul (Amiliya, 2023).

Selain itu, masyarakat juga harus diberikan pemahaman yang cukup tentang bahaya BTS palsu dan bagaimana mengenali tanda-tanda ancaman tersebut. Melalui sosialisasi dan kampanye keamanan digital, diharapkan kesadaran kolektif akan meningkat sehingga dapat mengurangi risiko terjadinya pencurian data nasabah. Secara keseluruhan, upaya-upaya ini harus berjalan secara terpadu agar pelindungan hukum bagi nasabah bank online dapat berjalan efektif dan memberikan rasa aman dalam bertransaksi di dunia digital.

KESIMPULAN

Ancaman pencurian data nasabah bank online melalui teknologi BTS *(Base Transceiver Station)* palsu merupakan bentuk kejahatan siber yang semakin canggih. Modus ini memanfaatkan kelemahan jaringan komunikasi seluler dengan cara membuat perangkat yang menyerupai menara BTS asli, sehingga perangkat korban secara otomatis terhubung ke BTS palsu tanpa disadari. Melalui koneksi tersebut, pelaku dapat menyadap dan mencuri informasi penting seperti data login, nomor rekening, PIN, hingga OTP *(One Time Password)* secara diam-diam. Aktivitas kriminal ini menimbulkan kerugian yang luas, baik dalam aspek keuangan maupun dalam hal pengamanan informasi pribadi nasabah. Oleh karena itu, kejahatan semacam ini membutuhkan perhatian serius dari seluruh pemangku kepentingan.

Pelindungan hukum terhadap nasabah bank online dari kejahatan siber yang menggunakan teknologi BTS palsu telah diakomodasi melalui berbagai peraturan perundang-undangan, seperti UU ITE, UU Telekomunikasi, serta aturan tambahan seperti UU TPPU dan ketentuan dalam KUHP. Ketentuan-ketentuan ini memberikan dasar hukum yang kokoh guna menjerat pelaku *phishing*, manipulasi data elektronik, akses ilegal terhadap sistem elektronik, serta penyalahgunaan infrastruktur jaringan telekomunikasi. Kasus konkret yang ditangani oleh Bareskrim Polri membuktikan bahwa hukum positif Indonesia sudah mampu merespons bentuk kejahatan ini secara efektif, termasuk menjatuhkan sanksi berat bagi pelaku.

Namun, melihat semakin kompleksnya modus kejahatan digital, pelindungan hukum yang ada perlu terus diperkuat. Untuk meningkatkan efektivitas pelindungan terhadap nasabah, diperlukan upaya kolaboratif antara pemerintah, lembaga keuangan, dan masyarakat. Pemerintah perlu memperbarui dan memperketat regulasi agar mampu mengimbangi perkembangan teknologi. Pihak bank harus terus meningkatkan sistem keamanan teknologi informasi yang digunakan, termasuk enkripsi data, sistem deteksi dini, dan pengawasan ketat terhadap aktivitas mencurigakan. Sementara itu, edukasi dan literasi digital bagi masyarakat juga sangat penting agar nasabah lebih waspada dalam melakukan transaksi online, serta memahami cara mengenali dan menghindari potensi ancaman siber. Dengan sinergi yang kuat antara regulasi, teknologi, dan kesadaran masyarakat, maka kepercayaan terhadap layanan perbankan digital dapat terus terjaga dan ditingkatkan.

DAFTAR PUSTAKA

Awaludin, M., Yasin, V., & Risyda, F. (2024). The Influence of Artificial Intelligence Technology, Infrastructure and Human Resource Competence on Internet Access Networks. Inform: Jurnal Ilmiah Bidang Teknologi Informasi Dan Komunikasi, 9(2), 111–120. https://doi.org/10.25139/inform.v9i2.8109

Bank Central Asia. (2025, 21 Maret). Awas Modus Penipuan SMS dengan Metode Fake BTS. Diakses pada 15 Mei 2025, dari https://www.bca.co.id/id/informasi/awas-modus/2025/03/21/08/02/awas-modus-penipuan-sms-dengan-metode-fake-bts

Budiono, Budiono, Fachri Rizky Fadillah, and Novayandra Arinudin. "The Dangers of Phishing to Personal Data Security." Formosa Journal of Applied Sciences 4.3 (2025): 831–844.

Fatmala Putri, Dewi, and Widya Ratna Sari. "Analisis pelindungan Nasabah BSI Terhadap Kebocoran Data Dalam Menggunakan Digital Banking." Jurnal Ilmiah Ekonomi Dan Manajemen 1, no. 4 (2023): 173–181. https://doi.org/10.61722/jiem.v1i4.331.

Febrianti, Reisha Resmalah, and Otto Yudianto. "Upaya pelindungan Hukum Bagi Korban Tindak Pidana Pencurian Secara Digital." Sosialita 2, no. 1 (2023): 75–84.

Handayani, Amiliya. "pelindungan Hukum Terhadap Tindakan Pencurian Data Pribadi Pada Layanan Fintech Lending Atas Ancaman Cyber Security Di Indonesia." Jurist-Diction 6, no. 4 (2023): 605–630. https://doi.org/10.20473/jd.v6i4.51212.

Kusuma, Tasya Utami, Rico Imanta Ginting, and Dudi Rahmadiansyah. "Sistem Pendukung Keputusan Penentuan Lokasi Tower BTS (Base Transceiver Station) Pada PT. Trinity Teknologi Nusantara Menggunakan Metode MOORA." Jurnal Cyber Tech 3.5 (2020): 834–843.

Rizaldi, M. Zaki, et al. "KETIDAKPASTIAN HUKUM TERHADAP NASABAH BANK BRI YANG TERKENA PENIPUAN MELALUI MOBILE BANKING." Jurnal Penelitian Multidisiplin Terpadu 8.6 (2024).

Tribunnews.com. (2025, 24 Maret). Polri bongkar sindikat penipuan online fake BTS dan SMS blast, korban rugi ratusan juta. Diakses pada 15 Mei 2025, dari https://www.tribunnews.com/nasional/2025/03/24/polri-bongkar-sindikat-penipuan-online-fake-bts-dan-sms-blast-korban-rugi-ratusan-juta?page=all

Undang-Undang No. 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik.

Undang-Undang No. 36 Tahun 1999 tentang Telekomunikasi.

Yosefine, Yosefine, Rani Sri Agustina, and Dede Agus. "pelindungan Hukum Terhadap Nasabah BTPN Jenius Akibat Tindakan Phishing (Studi Kasus Bank Tabungan Pensiunan Nasional Jenius)." Yustisia Tirtayasa: Jurnal Tugas Akhir 3, no. 1 (2023): 57. https://doi.org/10.51825/yta.v3i1.17650.

Yuliastanti, Fika. "Pengaruh Mobile Banking, Ukuran Perusahaan, Struktur Modal dan Growth Opportunity terhadap Kinerja Keuangan Perusahaan Perbankan yang Terdaftar di Bursa Efek Indonesia periode 2018–2022." Jurnal Akuntansi Keuangan Dan Bisnis 1.4 (2024): 636.

Zhendy, Dovie Eudy. "PEMANFAATAN TEKNIK DATA CELL DUMP SATRESKRIM POLRES SALATIGA Utilization of Cell Dump Data Technique in Investigation of Theft Crimes by Weighting by the Salatiga Regional Police Jurisdictions." Indonesian Journal of Police Studies 1, no. 1 (2020): 108–172. https://journal.akademikepolisian.com/index.php/ijps/article/view/76/43