P-ISSN : 2715-8888 (CETAK)
E-ISSN : 2716-5-27 (ONLINE
JURNAL PERSPEKTIF HUKUM
JURNAL PERSPEKTIF HUKUM

PENEGAKAN HUKUM TERHADAP KEJAHATAN TRANSAKSI ELEKTRONIK DENGAN MENGGUNAKAN METODE *PHISHING* (Studi Putusan Nomor: 764/Pid.Sus/2022/PN Pbr)

Mujahid Hamd
Prodi Hukum Fakultas Hukum Universitas Harapan Medan
Jalan Imam Bonjol Nomor 35 Medan
Mujahidhamd16@gmail.com

ABSTRACT

Phishing is a rapidly evolving crime that threatens the security of electronic transactions in Indonesia. This act involves deceptive methods aimed at illegally obtaining personal and financial information, typically by exploiting fraudulent emails or websites. From a legal perspective, phishing has the potential to undermine public trust in digital systems. Its impact is not only felt by individual victims but can also affect social stability and the integrity of the legal system as a whole. This research aims to analyze law enforcement and the legal regulations governing phishing, including provisions in the KUHP and the Electronic Information and Transactions Law (UU ITE). By examining Case Decision Number 764/Pid.Sus/2022/PN Pbr, this study identifies various challenges faced by law enforcement in implementing existing regulations. The research employs a normative legal approach with descriptive analysis, aiming to identify issues and provide recommendations to enhance the effectiveness of law enforcement. The findings are expected to contribute new insights for improving the legal system in Indonesia and strengthening oversight mechanisms to prevent the recurrence of phishing incidents in the future.

Keywords**: **Phishing, electronic transaction crimes, law enforcement

ABSTRAK

Phishing merupakan tindak pidana yang perkembangannya pesat dan mengancam keamanan transaksi elektronik di Indonesia. Tindakan ini dilakukan melalui metode penipuan yang bertujuan untuk memperoleh informasi pribadi dan finansial secara ilegal, biasanya dengan memanfaatkan *email* atau *website* yang palsu. Dari perspektif hukum, *phishing* berpotensi merusak kepercayaan publik terhadap sistem digital. Dampaknya tidak hanya dirasakan oleh individu yang menjadi korban, tetapi juga dapat mempengaruhi stabilitas sosial dan integritas sistem hukum secara keseluruhan. Penelitian ini bertujuan untuk menganalisis penegakan hukum dan peraturan hukum yang mengatur phishing, termasuk ketentuan yang terdapat dalam KUHP dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Dengan mengkaji Putusan Nomor 764/Pid.Sus/2022/PN Pbr, penelitian ini mengidentifikasi berbagai tantangan yang dihadapi oleh penegak hukum dalam melaksanakan peraturan yang ada. Metode penelitian yang digunakan adalah pendekatan yuridis normatif dengan analisis deskriptif, yang bertujuan untuk mengidentifikasi masalah dan memberikan rekomendasi guna meningkatkan efektivitas penegakan hukum. Hasil penelitian diharapkan dapat memberikan kontribusi baru untuk perbaikan sistem hukum di Indonesia serta memperkuat mekanisme pengawasan untuk mencegah terulangnya kasus phishing di masa mendatang.

Kata Kunci: ***Phishing*, kejahatan transaksi elektronik, penegakan hukum**

1. PENDAHULUAN

Kemajuan teknologi telah menjadi landasan lahirnya revolusi industri 4.0, yang membawa dampak signifikan tidak hanya dalam membuka peluang interaksi global, tetapi juga dalam mengubah berbagai aspek kehidupan manusia. Seiring dengan kemajuan pesat di bidang teknologi informasi dan komunikasi, terutama pada jaringan internet, teknologi ini telah membuat banyak pekerjaan menjadi lebih mudah dan praktis. Akibatnya, hampir semua sektor kehidupan kini mengoptimalkan penggunaan teknologi untuk mendukung aktivitasnya. Salah satu wujud nyata dari kemajuan teknologi ini adalah keberadaan gadget yang terhubung dengan jaringan internet, di mana jarak dan waktu tidak lagi menjadi kendala dalam berkomunikasi. Berbagai perangkat elektronik seperti televisi, ponsel, dan laptop kini telah menjadi bagian tak terpisahkan dari kehidupan masyarakat.

Hasil survei dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) mengumumkan jumlah pengguna internet Indonesia tahun 2024 mencapai 221.563.479 jiwa dari total populasi 278.696.200 jiwa penduduk Indonesia tahun 2023. Dari hasil survei penetrasi internet Indonesia 2024 yang dirilis APJII, maka tingkat penetrasi internet Indonesia menyentuh angka 79,5%. Dibandingkan dengan periode sebelumnya, maka ada peningkatan 1,4%.

Ini menandakan peningkatan konsisten grafik tren positif penetrasi internet Indonesia dalam lima tahun terakhir yang naik secara signifikan, ujar Ketua Umum APJII Muhammad Arif saat mengumumkan hasil survei pengguna internet di Kantor APJII, Jakarta, Rabu (31/1/2024).

Terhitung sejak 2018, penetrasi internet Indonesia mencapai 64,8%. Kemudian secara berurutan, 73,7% di 2020, 77,01% di 2022, dan 78,19% di 2023.. Penggunaan internet oleh masyarakat Indonesia meliputi berbagai aktivitas, termasuk penggunaan media sosial, akses informasi berita, kegiatan pendidikan, belanja online, dan layanan keuangan seperti *mobile banking*. (Zulfa Ajda Khoiriyah & Fadhilah Aini, 2024)

Meskipun teknologi informasi meberikan banyak kemudahan, dampak negatifnya juga signidikan, terutama dengan meningkatnya kejahatan transaksi elektronik. Para pelaku kejahatan memanfaatkan celah dalam keamanan siber serta kelalaian pengguna dalam melindungi dat pribadi dan finansial pada layanan seperti *internet banking*, *e-wallet*, dan *e-commerce*. Tingginya angka kejahatan dunia maya menunjukkan bahwa metode konvensional dalam menangani serangan transaksi elektronik sering kali kurang efektif. Beberapa bentuk umum kejahatan ini mencakup *carding*, *hakcing*, *phishing*, terosisme transaksi elektronik, dan penyebaran informasi yang mengganggu, dengan *phishing* menjadi fokus utama penelitian ini.

Phishing yang berasal dari bahasa Inggris (*fishing*) yang artinya memancing ini memang bermaksud memancing korbannya untuk memberikan data dan informasi-informasi sensitif yang sebenarnya tidak boleh dibagikan kepada siapapun misalnya, seperti data finansial, data akun, dan data pribadi seperti nomor rekening, kata sandi internet banking, kode *OTP* (*One Time Password*) *internet banking* atau *e-payment* lainnya, nomor handphone yang digunakan untuk internet banking atau sistem pembayaran elektronik lainnya, tempat tanggal lahir, usia, dan nomor kartu kredit yang mana data-data tersebut jika diberikan secara sukarela kepada orang lain maka orang lain akan dapat mengakses dan menggunakan saldo atau uang elektronik yang telah dibobol secara cuma-Cuma. (Irfan Fanasafa, 2022)

Kejahatan *phishing* ini pertama kali terjadi di Indonesia tahun 2001 dimana pelaku melihat adanya kelemahan sistem *internet banking* (*cyber security*) sehingga pelaku

memanfaatkan kesempatan ini untuk mencoba mempraktekkan keilmuannya dengan cara yang salah dimana pelaku merusak fasilitas dan sistem *internet banking* Bank Central Asia (BCA) pada domain *website* www.klik-bca.com dengan modus membuat 5 *link* plesetan yang mirip dengan domain *website* aslinya, seperti klikbac.com, kilkbca.com, wwwklikbca.com, clikbca,com (Dikdik M. Arief Mansur, 2018), sehingga jika nasabah BCA yang kurang teliti dan salah dalam memasukkan domain *website*nya yang mana kesalahan penulisannya tersebut mengarah pada lima domain *website* palsu tadi, maka data finansial seperti *UserID*, *password*, *Personal Identification Number* (*PIN*), nomor *credit card*, nomor rekening, tangga lahir nasabah serta nama ibu kandung nasabah sudah di *record* oleh *website* palsu tersebut.(Devi Anjheli, 2024)

Fenomena kejahatan transaksi elektronik, khususnya *phishing*, semakin mengkhawatirkan di Indonesia. Berdasarkan data dari laporan terbaru, Indonesia mencatat sebanyak 34.622 kasus *phishing* selama lima tahun terakhir mulai dari tahun 2017 sampai dengan 2022 . (Praditya Fauzi Rahman, 2022) dan Berdasarkan laporan IDADX, total pengaduan serangan *phishing* di Indonesia mengalami peningkatan signifikan. Tercatat, IDADX menerima sebanyak 26.675 laporan serangan *phishing* pada periode kuartal I 2023 sedangkan, pada periode kuartal 4 2022 hanya terdapat sekitar 6.106 laporan *phishing*. Hal tersebut mengalami kenaikan sebanyak 20.569 laporan *phishing*. (Bjcoid02, 2023)

Jumlah ini mencerminkan ancaman yang signifikan terhadap keamanan data pribadi dan finansial masyarakat, mengingat semakin banyaknya pengguna internet dan ketergantungan pada transaksi digital.

Berdasarkan Pasal 51 ayat (2) J.o Pasal 36 J.o Pasal 30 ayat (3) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik (UU ITE), sudah memenuhi unsur unsur yang dibutuhkan untuk diaplikasikan pada kejahatan elektronik dengan menggunakan metode *Phishing*. Peraturan perundang-undangan ini bertujuan memberikan kepastian hukum mengenai kegiatan yang diizinkan dan yang dilarang, serta untuk mencegah kerugian bagi warga negara di masa depan. Namun, seiring dengan meningkatnya transaksi elektronik di Indonesia, kejahatan seperti *phishing* juga semakin meningkat.

Berdasarkan latar belakang yang diuraikan diatas maka peneliti menyimpulkan rumusan masalah sebagai berikut :

1. Bagaimakah pengaturan hukum pada kejahatan transaksi elektronik dengan menggunakan metode phishing?
2. Bagaimanakah pelaksanaan ketentuan hukum tentang kejahatan transaksi elektronik dengan menggunakan metode phishing?
3. Bagaimana analisis yuridis terhadap pelaku kejahatan transaksi elektronik dengan menggunakan metode phishing (Studi Putusan Nomor: 764/Pid.Sus/2022/PN Pbr) ?

2. METODE PENELITIAN

Jenis penelitian yang digunakan pada penelitian ini adalah penelitian yuridis normatif yaitu metode penelitian hukum yang berfokus pada pengkajian dokumen-dokumen hukum utama. Tujuan utama dari penelitian ini adalah untuk mengidentifikasi, menganalisis, dan menjelaskan kaidah-kaidah hukum yang berlaku serta hubungan antar peraturan perundang-undangan. Penelitian ini dilakukan dengan cara mempelajari bahan pustaka yang relevan, seperti buku-buku, peraturan perundang-undangan, putusan pengadilan, perjanjian, teori hukum, dan doktrin ahli hukum. (Muhammad Syahrum, 2022)

Sumber data yang digunakan pada penelitian ini adalah :

1. Sumber data sekunder adalah sumber data yang tidak langsung memberikan data kepada pengumpul data, misalnya lewat orang lain atau lewat dokumen, pada penelitian ini yang digunakan merupakan bahan hukum primer yang memiliki otoritas atau bersifat autoritatif.(Peter Mahmud Marzuki, 2019) Sumber data primer meliputi:
    a. Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.
    b. Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik
    c. Putusan Nomor: 764/Pid.Sus/2022/PN PBr)
2. Bahan hukum sekunder, yaitu bahan yang berhubungan dengan bahan hukum primer atau utama yang bisa memberikan bantuan untuk menelaah dan mendalami suatu bahan hukum primer. (Suteki & Galang Taufani, 2018) Sumber data sekunder yang dipergunakan dalam penelitian ini, yaitu: buku, jurnal, hasil penelitian maupun karya tulis yang berhubungan dengan persoalan yang dibahas.
3. Sumber data tersier yang dipergunakan yaitu kamus hukum dan website-website internet resmi

3. HASIL DAN PEMBAHASAN

3.1. Pengaturan Hukum Pada Kejahatan Transaksi Elektronik Dengan Menggunakan Metode *Phishing*

Pengaturan Berdasarkan Kitab Undang-Undang Hukum Pidana

Kitab Undang-Undang Hukum Pidana (KUHP) sendiri tidak secara eksplisit membahas "transaksi elektronik khususnya *phishing*" sebagai istilah spesifik. Namun, beberapa pasal dapat diinterpretasikan untuk mencakup jenis-jenis kegiatan ilegal yang relevan dengan teknologi digital, meskipun bukan langsung menyebut "transaksi elektronik khususnya *phishing*". *Phishing* adalah salah satu bentuk kejahatan transaksi elektronik yang melibatkan penipuan dengan cara menyamar sebagai entitas yang sah untuk mendapatkan informasi pribadi, seperti kata sandi atau data kartu kredit. Regulasi terkait kejahatan ini dapat ditemukan dalam beberapa undang-undang dan peraturan di Indonesia.

Adapun beberapa unsur-unsur yang terdapat didalam Pasal 378 KUHP tersebut, yaitu:

1. Barang siapa
2. Dengan maksud untuk menguntungkan diri sendiri atau orang lain
3. Secara melawan hukum
4. Dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun dengan rangkaian kebohongan
5. Menggerakan orang lain
6. Untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi untang maupun menghapuskan piutang

Berdasarkan unsur-unsur dalam Pasal 378 KUHP tersebut, maka dapat disimpulkan bahwa barang siapa adalah subjek maksudnya ialah pelaku yang melakukan tindak pidana penipuan. Ada maksud untuk menguntungkan diri sendiri atau orang lain, artinya bahwa ada suatu kesengajaan yang dilakukan sebagai maksud (*oogmerk*). Selanjutnya perbuatan tersebut dilakukan secara melawan hukum, yang berarti pelaku penipuan itu tidak mempunyai hak sama sekali untuk menikmati keuntungan itu yaitu hasil penipuan tersebut.

Unsur selanjutnya memakai nama palsu yang menyerupai suatu *website* yang asli tentunya sering digunakan baik oleh orang yang ditipu yaitu si korban saat mengirimkan *email* kepada si korban. Martabat palsu seperti pelaku penipuan mengaku sebagai *website* asli, dengan tipu muslihat menyamakan *email* seperti *email* yang asli kepada yang ditipu yaitu si korban, dan rangkaian kebohongan yang dimaksud adalah segala upaya penipuan untuk mendapatkan keuntungan dengan cara mengirimkan *email Phishing* kepada korban dengan menggunakan Sender SMTP seolah-olah akun korban mengalami masalah dan perlu diverifikasi Kembali yang masuk ke notifikasi *email* di kotak masuk yang berisi "silakan masuk ke akun anda ke akun *coinbase* anda di bawah ini dari *browser website* untuk memverifikasi identitas anda. Anda tidak akan dapat memverifikasi identitas anda dari aplikasi *Coinbase*". Bahwa setelah mendapatkan *email Phishing* yang kirimkan oleh terdakwa dalam bentuk notifikasi seolah-olah akun milik korban terdapat masalah dan harus melakukan verifikasi kembali agar tidak dinonaktifkan permanen, korban menekan/meng-klik verifikasi identitas maka selanjutnya korban akan mengunjungi/ terhubung ke *website* palsu (*Scam Page*) yang seolah-olah mirip dengan *website Coinbase* asli yang telah terdakwa persiapkan sebelumnya.

Menggerakan orang lain yang dapat diartikan bahwa dengan cara-cara tersebut pelaku penipuan menghendaki orang yang ditipu tergerak untuk melakukan apa yang dikehendaki pelaku penipuan dengan menyerahkan suatu barang kepadanya yaitu identitas terdakwa agar bisa masuk ke akun *coinbase* asli. Untuk memberi utang ataupun menghapus piutang itu adalah bagian inti delik yang bermakna pada delik penipuan, objeknya bisa berupa hak yaitu membuat utang atau menghapus piutang. Menurut Nico Keijzer, delik yang paling tepat untuk orang yang mengutakatik komputer untuk mendapatkan keuntungan ialah Pasal 378 karena meliputi hak. Tetapi, tidak memenuhi unsur mengenai informasi elektronik dan/atau dokumen elektronik salah, oleh karena itu Pasal 378 sebenarnya tidak tepat untuk dikenakan terhadap *cyber* crime dalam bentuk *Phishing*.

Pengaturan Berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008

Telah disahkannya dan diberlakukannya Undang-Undang ITE yang pada awalnya dibentuk Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dan kemudian dibentuk lagi Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik yang telah berlaku sampai saat ini. Pada saat ini perbuatan *Phishing* tersebut diatur pada Pasal yang dirumuskan sebagai berikut:

1. Pasal 30
   Pasal 30 mengatur tentang akses ilegal ke sistem elektronik milik orang lain. *Phishing* biasanya melibatkan tindakan ilegal mengakses informasi pribadi korban melalui penyamaran sebagai entitas sah untuk mendapatkan akses ke akun atau sistem elektronik mereka. Dengan mengelabui korban, pelaku dapat mengakses komputer atau sistem elektronik tanpa izin. Ini masuk dalam tindakan yang diatur oleh Pasal 30, terutama ayat 2 dan 3, dimana pelaku berusaha memperoleh informasi elektronik secara ilegal.
2. Pasal 36
   Pasal 36 mengatur tindakan yang mengakibatkan kerugian bagi orang lain. Dalam konteks *phishing*, korban sering kali mengalami kerugian finansial atau kehilangan data pribadi akibat aksi *phishing*. Dengan cara ini, *phishing* melibatkan tindakan melawan hukum yang menyebabkan kerugian langsung kepada korban, sehingga pelaku dapat dijerat dengan Pasal 36 jika tindakan mereka menyebabkan kerugian pada korban.
3. Pasal 51

Pasal 51 memberikan sanksi berat bagi mereka yang melanggar Pasal 35 (manipulasi data elektronik) dan Pasal 36 (tindakan yang merugikan orang lain). Dalam konteks *phishing*, pelaku yang melakukan manipulasi informasi elektronik untuk tujuan penipuan dan mengakibatkan kerugian bagi korban dapat dikenai sanksi berat sebagaimana diatur dalam Pasal 51.

Pelaksanaan ketentuan hukum terhadap kejahatan transaksi elektronik melalui *phishing* sangat esensial dalam mengantisipasi dan menghambat perilaku ilegal tersebut. Dengan mengejar dan menghukum pelaku *phishing*, pihak berwenang dapat mengurangi frekuensi serangan dan meningkatkan kesadaran masyarakat tentang bahaya *phishing*.

Berdasarkan penjelasan mengenai pasal dan unsur-unsur yang ada, penulis dapat menganalisa kasus *phishing* yang melibatkan Anggi Saputra, Putusan Pengadilan Negeri Pekanbaru Nomor 764/Pid.Sus/2022/PN.Pbr tanggal 26 Agustus 2022. putusan kasus tersebut harus dipertahankan dan dikuatkan, karena mencerminkan kompleksitas kejahatan transaksi elektronik, khususnya dalam bentuk *phishing*, yang semakin marak terjadi di era digital saat ini. Anggi, seorang pria berusia 21 tahun asal Pekanbaru, didakwa melakukan tindakan ilegal dengan menciptakan *website* palsu yang menyerupai platform *cryptocurrency* asli. Ia menggunakan teknik *phishing* untuk menipu korban agar memberikan informasi pribadi dan data keuangan mereka. Proses kejahatan ini dimulai ketika Anggi mengirimkan *email* berisi tautan *website* palsunya kepada korban, *website* palsu yang tampak meyakinkan dan menginstruksikan calon korban untuk memperbarui informasi pribadi mereka. Banyak dari korban yang terjebak dan memasukkan data sensitif, seperti username, password, dan nomor kartu kredit, yang kemudian dimanfaatkan oleh Anggi untuk mengakses akun dan melakukan transaksi ilegal.

Dari segi ketentuan hukum, tindakan Anggi memenuhi unsur-unsur yang diatur dalam Pasal 51 ayat (2) jo Pasal 36 jo Pasal 30 ayat (3) Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang telah diubah dengan Undang-Undang Republik Indonesia Nomor 19 Tahun 2016. Dalam pasal-pasal tersebut dijelaskan bahwa pengaksesan sistem elektronik secara ilegal dan tanpa hak dapat dikenakan sanksi pidana. Penuntut umum menuntut Anggi berdasarkan pasal-pasal tersebut dengan tuduhan bahwa ia telah melakukan pengaksesan sistem elektronik dengan cara melanggar hukum, yang menyebabkan kerugian bagi orang lain.

Kasus Anggi Saputra mencerminkan perlunya pelakanaan ketentuan hukum yang tegas terhadap pelaku kejahatan transaksi elektronik serta penguatan regulasi untuk melindungi masyarakat dari risiko serupa di masa depan. Keberhasilan pelaksanaan ketentuan hukum dalam kasus ini akan menjadi langkah penting dalam membangun kepercayaan publik terhadap sistem keamanan transaksi elektronik di Indonesia dan memastikan bahwa masyarakat dapat hidup dengan aman dalam era teknologi yang terus berkembang.

Pengaturan Berdasarkan Peraturan Bank Indonesia Nomor 22/20/Pbi/2020 Tentang Perlindungan Konsumen Bank Indonesia

Dalam era digital yang semakin berkembang, kejahatan transaksi elektronik, termasuk phishing, menjadi ancaman serius bagi konsumen dan integritas sistem keuangan. Untuk mengatasi tantangan ini, Peraturan Bank Indonesia Nomor 22/20/PBI/2020 tentang Perlindungan Konsumen Bank Indonesia memainkan peranan penting dalam menciptakan lingkungan yang aman bagi nasabah. Regulasi ini tidak hanya mengatur hak dan kewajiban lembaga keuangan dalam melindungi konsumen, tetapi juga menyediakan kerangka kerja yang jelas untuk menangani pengaduan dan memastikan transparansi informasi. Dengan adanya peraturan ini, diharapkan konsumen dapat bertransaksi dengan lebih percaya diri

dan terlindungi dari kejahatan transaksi elektronik. Adapun pasal yang berhubungan dengan tindak kejahatan transaksi elektronik menggunakan metode *phishing* adalah:

Pasal 30

(1) Penyelenggara wajib menjaga kerahasiaan dan keamanan data dan/atau informasi Konsumen.
(2) Kewajiban menjaga kerahasiaan dan keamanan data dan/atau informasi Konsumen sebagaimana dimaksud pada ayat (1) sesuai dengan ketentuan peraturan perundang-undangan.
(3) Guna menjaga kerahasiaan dan keamanan data dan/atau informasi Konsumen sebagaimana dimaksud pada ayat
    (1), Penyelenggara wajib memiliki:
    a. fungsi yang bertanggung jawab terhadap perlindungan data dan/atau informasi Konsumen;
    b. sistem informasi yang andal untuk mendukung pelaksanaan perlindungan data dan/atau informasi Konsumen; dan
    c. mekanisme dan prosedur mengenai perlindungan data dan/atau informasi Konsumen.
(4) Dalam hal Penyelenggara bekerja sama dengan pihak lain untuk mengelola data dan/atau informasi Konsumen, Penyelenggara wajib memastikan pihak lain tersebut menjaga kerahasiaan dan keamanan data dan/atau informasi Konsumen sebagaimana dimaksud pada ayat (1).
(5) Penyelenggara yang tidak memenuhi kewajiban sebagaimana dimaksud pada ayat (1), ayat (3), dan ayat (4) dikenai sanksi administratif berupa:
    a. teguran tertulis;
    b. penghentian sementara sebagian atau seluruh kegiatan usaha; dan/atau
    c. pencabutan izin.

Secara keseluruhan, pengaturan yang dihasilkan dari Peraturan Bank Indonesia Nomor 22/20/PBI/2020 sangat krusial dalam menghadapi tantangan kejahatan transaksi elektronik seperti phishing. Dengan menekankan perlindungan konsumen, regulasi ini tidak hanya berfungsi sebagai payung hukum, tetapi juga sebagai upaya untuk meningkatkan kepercayaan masyarakat terhadap lembaga keuangan. Implementasi yang konsisten dan efektif dari peraturan ini akan memberikan dampak positif dalam mendorong partisipasi aktif konsumen di dalam sistem perbankan, serta memperkuat ketahanan sistem keuangan Indonesia dari ancaman kejahatan transaksi elektronik yang terus berkembang.

3.2. Pelaksanaan Ketentuan Tentang Kejahatan Transaksi Elktronik Dengan Menggunakan Metode Phishing

Faktor-Faktor Terjadinya Kejahatan Transaksi Elektronik Dengan Menggunakan Metode Phishing

Beberapa faktor kunci yang berkontribusi terhadap kejahatan transaksi elektronik di Indonesia sebagai berikut:

1. Kemajuan Teknologi:
   Perkembangan teknologi informasi dan komunikasi telah memberikan pelaku kejahatan akses yang lebih mudah untuk menciptakan *email* dan *website* palsu yang tampak sangat mirip dengan yang asli. Dengan alat dan perangkat lunak yang tersedia, pelaku dapat dengan cepat mengubah tampilan dan konten untuk menipu pengguna.
   Dr. Rudi Santoso menyatakan bahwa Perkembangan teknologi membuat metode serangan semakin canggih. Pelaku dapat memanfaatkan alat dan teknik yang tersedia untuk menipu pengguna dengan lebih efektif. (Budi Suhariyanto, 2013)
2. Kurangnya Kesadaran Masyarakat

Banyak pengguna internet yang tidak memahami risiko *phishing* dan cara melindungi diri mereka dari serangan ini. Ketidaktahuan ini sering kali disebabkan oleh kurangnya pendidikan tentang keamanan transaksi elektronik di kalangan masyarakat.

Prof. Budi Rahardjo menekankan bahwa Pendidikan tentang keamanan transaksi elektronik harus dimulai sejak dini. Masyarakat perlu dilatih untuk mengenali tanda-tanda *phishing* agar dapat melindungi diri mereka. (Desriyarini Gui et al., 2024)

3. Sistem Keamanan yang Lemah
   Banyak individu dan organisasi yang tidak menerapkan langkah-langkah keamanan yang memadai, seperti penggunaan autentikasi dua faktor atau enkripsi data. Ketidakmampuan untuk mengamankan sistem informasi membuat mereka rentan terhadap serangan.
4. *Anonymity* di Internet
   Pelaku *phishing* sering kali beroperasi secara anonim, membuat pelaku sulit untuk dilacak oleh pihak berwenang. *Anonymity* ini memberi mereka kebebasan untuk melakukan kejahatan tanpa takut tertangkap.

Hambatan Dalam Pelaksanaan Ketentuan Kejahatan Transaksi Elektronik Dengan Menggunakan Metode Phishing

1. Regulasi yang Tidak Memadai
   Meskipun ada undang-undang terkait (seperti UU ITE), penerapan hukum sering kali tidak mencakup semua aspek kejahatan transaksi elektronik, termasuk *phishing*. Regulasi yang ada mungkin tidak cukup spesifik untuk menangani metode baru yang digunakan oleh pelaku.
2. Kurangnya Sumber Daya
   Banyak lembaga penegak hukum tidak memiliki sumber daya atau pelatihan yang cukup untuk menangani kasus-kasus kejahatan transaksi elektronik secara efektif. Hal ini mengakibatkan keterbatasan dalam investigasi dan penuntutan.

   Dr. Joko Prasetyo menekankan bahwa Investasi dalam pelatihan dan teknologi adalah suatu keharusan bagi lembaga penegak hukum untuk menghadapi tantangan kejahatan transaksi elektronik.
3. Perbedaan Interpretasi Hukum
   Perbedaan interpretasi terhadap undang-undang yang ada dapat menjadi hambatan dalam penegakan hukum. Beberapa aparat penegak hukum mungkin memiliki pemahaman yang berbeda tentang bagaimana menerapkan undang-undang terkait kejahatan transaksi elektronik, termasuk pasal-pasal dalam KUHP dan UU ITE.

Antisipasi Terjadinya Kejahatan Transaksi Elektronik Dengan Mneggunakan Metode Phishing

Untuk mengantisipasi kejahatan transaksi elektronik menggunakan metode *phishing*, beberapa aturan atau ketentuan yang dapat diterapkan meliputi:

1. Penguatan Regulasi: Memperkenalkan pasal khusus dalam undang-undang yang secara rinci mengatur kejahatan *phishing*, termasuk definisi, sanksi, dan prosedur penegakan hukum yang jelas.
2. Edukasi dan Pelatihan: Mewajibkan lembaga keuangan dan perusahaan teknologi untuk melakukan program edukasi dan pelatihan rutin bagi karyawan dan pelanggan mengenai teknik *phishing* dan cara menghindarinya.
3. Mekanisme Pengaduan yang Efektif: Mengembangkan sistem pengaduan yang responsif dan mudah diakses bagi korban kejahatan *phishing*, sehingga mereka dapat melaporkan dengan cepat dan mendapatkan bantuan.

4. Peningkatan Teknologi Keamanan: Mendorong lembaga keuangan untuk mengadopsi teknologi keamanan yang lebih canggih, seperti autentikasi dua faktor (2FA) dan sistem deteksi penipuan berbasis AI, untuk melindungi akun nasabah.
5. Kolaborasi Antar Lembaga: Mendorong kolaborasi antara lembaga penegak hukum, institusi keuangan, dan penyedia teknologi untuk berbagi informasi dan strategi dalam mengidentifikasi serta mengatasi kejahatan *phishing*.
6. Sanksi yang Lebih Tegas: Menerapkan sanksi yang lebih berat bagi pelaku kejahatan phishing untuk memberikan efek jera dan menunjukkan keseriusan dalam menanggulangi kejahatan transaksi elektronik.
7. Kampanye Kesadaran Publik: Meluncurkan kampanye kesadaran untuk meningkatkan pengetahuan masyarakat tentang risiko *phishing*, teknik yang digunakan, dan langkah-langkah pencegahan yang dapat diambil.

Dengan mengimplementasikan ketentuan dan aturan ini, diharapkan dapat mengurangi risiko dan dampak dari kejahatan transaksi elektronik yang menggunakan metode *phishing*.

Solusi Dalam Pelaksanaan Ketentuan Kejahatan Transaksi Elektronik Dengan Menggunakan Metode Phishing

Upaya sinergis dari segala bidang ini diperlukan untuk menciptakan lingkungan yang lebih aman dan terjamin bagi pengguna internet di Indonesia.

1. Pendidikan dan Kesadaran Masyarakat
   Melakukan kampanye edukasi untuk meningkatkan kesadaran masyarakat tentang risiko *phishing* dan cara melindungi diri mereka dari serangan ini. Pendidikan harus mencakup informasi tentang cara mengenali *email* atau *website* palsu. Pendidikan adalah kunci untuk mengurangi kejahatan transaksi elektronik. Edukasi masyarakat dapat mengurangi jumlah korban potensial.
2. Penguatan Regulasi
   Memperbarui undang-undang untuk mencakup semua aspek kejahatan transaksi elektronik dan memastikan adanya sanksi tegas bagi pelaku *phishing*. Regulasi yang lebih ketat dapat memberikan efek jera bagi pelaku.
3. Kerjasama Internasional
   Membangun kerjasama internasional antara negara-negara dalam penegakan hukum terhadap kejahatan transaksi elektronik. Kerjasama ini dapat berupa perjanjian bilateral atau multilateral untuk memfasilitasi pertukaran informasi dan sumber daya.
4. Peningkatan Kapasitas Penegak Hukum
   Memberikan pelatihan khusus bagi aparat penegak hukum mengenai teknologi informasi dan cara menangani kasus-kasus kejahatan transaksi elektronik secara efektif. Pelatihan harus mencakup pemahaman tentang alat dan teknik terbaru yang digunakan oleh pelaku. Pelatihan adalah investasi penting untuk meningkatkan kemampuan penegak hukum. Peningkatan kapasitas akan membantu aparat lebih siap menghadapi tantangan modern.
5. Implementasi Teknologi Keamanan
   Mendorong penggunaan teknologi keamanan yang lebih baik di sektor swasta dan publik, seperti sistem autentikasi multi-faktor dan enkripsi data. Teknologi ini dapat membantu mencegah serangan *phishing* dengan meningkatkan lapisan perlindungan. Teknologi keamanan yang canggih dapat membantu mencegah serangan *phishing*. Implementasi solusi teknis adalah langkah proaktif dalam melindungi data pengguna.

Untuk mengatasi kejahatan *phishing*, diperlukan edukasi masyarakat agar kebih waspada terhadap *email* atau *website* palsu, didukung oleh regulasi hukum yang tegas serta kerja sama internasional dalam penegakan hukum dan pelatihan khusus bagi aparat. Selain itu, penerapan teknologi keamanan seperti autentikasi multi-faktor dan enkripsi data

disektor publik maupun swasta menjadi langkah proaktif dalam melindungi pengguna. Para ahli menekankan bahwa kombinasi edukasi, regulasi, kerja sama internasional, dan teknologi adalah kunci dalam mengurangi kejahatan elektronik, sehingga diperlukan sinergi dari berbagai pihak untuk menghadapi tantangan dunia digital yang terus berkembang.

3.3. Analisis Kasus Putusan Pengadilan Nomor:764/Pid.Sus/2022/Pn.Pbr

Kronologi Kasus

Terdakwa Anggi Saputra bin Suliandi, lahir di Pekanbaru pada tanggal 12 Maret 1994, adalah seorang pria yang tidak memiliki pekerjaan tetap dan tinggal di Jl. Garuda No. 10, Kecamatan Tampan, Kota Pekanbaru, Provinsi Riau. Dalam kasus yang berlangsung antara bulan Agustus hingga Oktober 2021, terdakwa diduga melakukan serangkaian kejahatan transaksi elektronik, dengan memanfaatkan teknik *phishing* untuk mengakses secara ilegal akun *cryptocurrency* milik beberapa korban. Aksi ini berujung pada kerugian finansial yang mencapai miliaran rupiah.

Kasus bermula pada bulan Juni 2021, ketika Anggi mendaftarkan dirinya di platform Indodax, sebuah layanan jual beli mata uang kripto. Terdakwa menggunakan identitas asli dengan alamat *email* botolminum105@gmail.com, nomor telepon 085161371303, dan username anggisaputra1994. Setelah berhasil mendaftarkan akun dan mendapatkan *wallet* address 0x8de4dff073e2b9484fe110-b2c93f4e95f7798b69, terdakwa mempelajari metode *phishing* melalui berbagai video di YouTube. Dia tertarik pada metode yang menggunakan *email* palsu, yang seolah-olah berasal dari platform *cryptocurrency coinbase*, untuk menipu korban agar memberikan informasi login mereka.

Dalam memuluskan aksinya, terdakwa bergabung dengan grup *Facebook* bernama SIXTEEN MARKET, di mana dia membeli berbagai alat untuk menjalankan aksi *phishing*-nya. Beberapa alat dan layanan yang didapatkan terdakwa antara lain daftar *email* calon korban, protokol SMTP (*Simple Mail Transfer Protocol*) untuk mengirim *email* palsu, serta aplikasi sender untuk memfasilitasi pengiriman massal *email*. Dari akun *Facebook* Rafian Vibe, terdakwa membeli satu juta daftar *email* calon korban dengan harga Rp. 300.000. Kemudian, dari akun Fatah Al-Ghazi, terdakwa membeli protokol SMTP seharga Rp. 150.000. Terdakwa juga mendapatkan aplikasi *sender* secara gratis dari akun Stiker Pentol.

Setelah memiliki semua alat yang diperlukan, terdakwa mulai menyusun skema *phishing*. Pelaku mengirimkan *email* palsu kepada korban, yang mengklaim bahwa akun *Coinbase* korban sedang mengalami masalah dan memerlukan verifikasi ulang. Dalam *email* tersebut, disertakan tautan yang mengarahkan korban ke *website* palsu yang terlihat identik dengan *website* resmi *Coinbase*. Korban diminta untuk memasukkan *username* dan *password* mereka di halaman tersebut. Informasi login yang dimasukkan korban akan otomatis terekam ke database yang dikendalikan terdakwa.

Setelah mendapatkan akses ke akun *Coinbase* korban, terdakwa memanfaatkan *OTP (One-Time Password)* yang dikirimkan ke *email* korban untuk mengakses akun secara penuh. Dengan cara ini, terdakwa berhasil memindahkan aset digital berupa *Ethereum* (ETH) dari akun korban ke *wallet* pribadinya di Indodax. Secara keseluruhan, kerugian yang dialami para korban mencapai 305,206 ETH, atau setara dengan Rp. 13,8 miliar.

Setelah berhasil memindahkan aset digital tersebut, terdakwa melakukan penarikan dana dari akun Indodax ke rekening bank pribadinya, baik di Bank BTPN maupun Bank BCA. Penarikan dana ini dilakukan secara bertahap dengan nilai yang sangat besar.

Dengan total penarikan yang mencapai miliaran rupiah, terdakwa memanfaatkan hasil curian ini untuk kepentingan pribadi. Akibat tindakannya, para korban mengalami kerugian besar, dan terdakwa didakwa melanggar hukum terkait akses ilegal terhadap sistem elektronik serta pencurian aset digital.Pada tanggal 26 Agustus 2022, Majelis Hakim

Pengadilan Negeri Pekanbaru menjatuhkan putusan terhadap Anggi Saputra setelah mendengar keterangan saksi-saksi dan mempertimbangkan semua bukti yang ada dalam persidangan sebelumnya. Dalam putusannya, hakim menyatakan bahwa Anggi terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana "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 yang menyebabkan kerugian bagi orang lain." Tindakannya diatur dalam Pasal 51 ayat (2) jo Pasal 36 jo Pasal 30 ayat (3) Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Majelis Hakim menjatuhkan pidana penjara selama lima tahun dikurangi masa penahanan sementara serta denda sebesar Rp2.000.000.000,- (dua miliar rupiah) subsidiair lima bulan penjara jika denda tidak dibayar. Keputusan ini mencerminkan keseriusan tindakannya yang merugikan banyak korban melalui metode *phishing* yang canggih serta menunjukkan komitmen sistem peradilan untuk menegakkan hukum terhadap kejahatan transaksi elektronik.

Dakwaan Jaksa Penuntut Umum

Adapun dakwaan dalam kasus yang penulis teliti. Terdakwa diajukan kepersidangan oleh Penuntut Umum didakwa berdasarkan surat dakwaan alternatif sebagai berikut::

1. Dakwaan kesatu : Perbuatan terdakwa tersebut diatur dan diancam pidana dalam Pasal 51 ayat (2) Jo Pasal 36 Jo Pasal 48 ayat (1) Jo Pasal 32 ayat (1) UU ITE Nomor 11 tahun 2008 tentang ITE sebagaimana telah diubah dengan UU ITE Nomor 19 Tahun 2016 tentang perubahan atas UU Nomor 11 Tahun 2008.
2. Dakwaan kedua : Perbuatan terdakwa tersebut diatur dan diancam pidana dalam Pasal 51 ayat (2) Jo Pasal 36 Jo Pasal 46 ayat (3) Jo Pasal 30 ayat (3) UU ITE Nomor 11 tahun 2008 tentang ITE sebagaimana telah diubah dengan UU ITE Nomor 19 Tahun 2016 tentang perubahan atas UU Nomor 11 Tahun 2008.
3. Dakwaan ketiga : Perbuatan terdakwa tersebut diatur dan diancam pidana dalam Pasal 51 ayat (2) Jo Pasal 36 Jo Pasal 46 ayat (2) Jo Pasal 30 ayat (2) UU ITE Nomor 11 tahun 2008 tentang ITE sebagaimana telah diubah dengan UU ITE Nomor 19 Tahun 2016 tentang perubahan atas UU Nomor 11 Tahun 2008.
4. Dakwaan keempat : Perbuatan terdakwa tersebut diatur dan diancam pidana dalam Pasal 51 ayat (2) Jo Pasal 36 Jo Pasal 46 ayat (1) Jo Pasal 30 ayat (1) UU ITE Nomor 11 tahun 2008 tentang ITE sebagaimana telah diubah dengan UU ITE Nomor 19 Tahun 2016 tentang perubahan atas UU Nomor 11 Tahun 2008.
5. Dakwaan kelima : Perbuatan terdakwa tersebut diatur dan diancam pidana dalam Pasal 51 ayat (2) Jo. Pasal 36 Jo. Pasal 32 ayat (1) UU ITE Nomor 11 tahun 2008 tentang ITE sebagaimana telah diubah dengan UU ITE Nomor 19 Tahun 2016 tentang perubahan atas UU Nomor 11 Tahun 2008.
6. Dakwaan keenam : Perbuatan terdakwa tersebut diatur dan diancam pidana dalam Pasal 51 ayat (2) J.o Pasal 36 Jo. Pasal 30 ayat (3) UU ITE Nomor 11 tahun 2008 tentang ITE sebagaimana telah diubah dengan UU ITE Nomor 19 Tahun 2016 tentang perubahan atas UU Nomor 11 Tahun 2008;
7. Dakwaan ketujuh : Perbuatan terdakwa tersebut diatur dan diancam pidana dalam Pasal 51 ayat (2) Jo. Pasal 36 Jo. Pasal 30 ayat (2) UU ITE Nomor 11 tahun 2008 tentang ITE sebagaimana telah diubah dengan UU ITE Nomor 19 Tahun 2016 tentang perubahan atas UU Nomor 11 Tahun 2008.

8. Dakwaan kedelapan: Perbuatan terdakwa tersebut diatur dan diancam pidana dalam Pasal 51 ayat (2) J.o Pasal 36 Jo. Pasal 30 ayat (1) UU ITE Nomor 11 tahun 2008 tentang ITE sebagaimana telah diubah dengan UU ITE Nomor 19 Tahun 2016 tentang perubahan atas UU Nomor 11 Tahun 2008. (Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Transaksi Elektronik, n.d.)

Tuntutan Jaksa Penuntut Umum

Tuntutan Jaksa Penuntut Umum yang pada pokoknya menuntut supaya Majelis Hakim yang memeriksa dan mengadili perkara ini memutuskan :

1. Menyatakan terdakwa ANGGI SAPUTRA Bin SULIANDI telah terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana ”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 yang menyebabkan kerugian bagi orang lain”, sebagaimana diatur dan diancam pidana dalam dakwaan alternatif keenam kami yakni melanggar Pasal 51 ayat (2) J.o Pasal 36 Jo. Pasal 30 ayat (3) UU ITE Nomor 11 tahun 2008 tentang ITE sebagaimana telah diubah dengan UU ITE Nomor 19 Tahun 2016 tentang perubahan atas UU Nomor 11 Tahun 2008;
2. Menjatuhkan pidana terhadap terdakwa dengan pidana penjara selama 5 (lima) tahun dikurangi selama terdakwa berada dalam tahanan sementara dengan perintah agar terdakwa tetap ditahan dan menjatuhkan denda terhadap terdakwa sebesar Rp. 2.000.000.000,- (dua miliar rupiah) subsidiair 5 (lima) bulan penjara;
3. Menyatakan barang bukti dikembalikan kepada korban, dirampas untuk dilelang guna melengkapikekurangan pengembalian kerugian kepada para korban, Dan sisa dari hasil lelang barang bukti ini dirampas untuk negara.
4. Menetapkan agar terdakwa dibebani membayar biaya perkara sebesar Rp 2.000, (dua ribu rupiah);

Putusan Hakim

Majelis Hakim Pengadilan Negeri Pekanbaru, pada hari Rabu tanggal 07 Desember 2022 memberikan putusan yang amarnya sebagai berikut berdasarkan Pasal 51 ayat (2) jo. Pasal 36 jo. Pasal 30 ayat (3) Undang-undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-undang nomor 19 Tahun 2016 tentang perubahan atas Undang-undang Nomor 11 Tahun 2008:

1. Menyatakan Terdakwa ANGGI SAPUTRA Bin SULIANDI tersebut diatas, telah terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana ”Dengan sengaja secara tanpa hak dan melawan hukum Mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan menerobos sistem pengamanan yang menyebabkan kerugian bagi orang lain”, sebagaimana dalam dakwaan alternatif Keenam;
2. Menjatuhkan pidana kepada Terdakwa oleh karena itu dengan pidana penjara selama 3 (tiga) tahun dan 4 (empat) bulan dan denda sejumlah Rp. 2.000.000.000,- (dua milyar rupiah) dengan ketentuan jika denda tidak dibayar harus diganti dengan pidana kurungan selama 2 (dua) bulan;
3. Menetapkan masa penangkapan dan penahanan yang telah dijalani Terdakwa dikurangkan seluruhnya dari pidana yang dijatuhkan;
4. Menetapkan Terdakwa tetap dalam tahanan;

5. Menyatakan barang bukti dikembalikan kepada korban, dirampas untuk dilelang guna melengkapikekurangan pengembalian kerugian kepada para korban, Dan sisa dari hasil lelang barang bukti ini dirampas untuk negara.
6. Membebankan kepada Terdakwa membayar biaya perkara sejumlah Rp. 2.000,- (dua ribu rupiah);

Analisa Penegakan Hukum Kejahatan Transaksi Elektronik Menggunakan Phishing

Penegakan hukum terhadap kejahatan transaksi elektronik dengan metode *phishing*, analisa peneliti dalam Putusan Nomor 764/Pid.Sus/2022/PN Pbr, menunjukkan kompleksitas kasus kejahatan dunia maya di Indonesia. Dalam kasus ini, terdakwa, Anggi Saputra, terbukti bersalah melakukan kejahatan *phishing* dengan mencuri *cryptocurrency* milik korban menggunakan metode rekayasa sosial. Terdakwa menggunakan *email* palsu yang menyerupai notifikasi dari *platform cryptocurrency Coinbase* untuk mengelabui korban agar memberikan akses ke akun mereka. Melalui teknik *phishing* ini, terdakwa berhasil mencuri *Ethereum* dari beberapa korban dan mentransfer aset tersebut ke *e-wallet cryptocurrency* miliknya.

Unsur-unsur tindak pidana yang terkandung dalam pasal-pasal tersebut mencakup:

1. Unsur "dengan sengaja"

Terdakwa terbukti secara sengaja melakukan tindakan *phishing*. Unsur kesengajaan ini terlihat dari bagaimana terdakwa merencanakan dan melaksanakan serangkaian tindakan untuk memperoleh data login korban. Terdakwa tidak hanya menggunakan *email* palsu yang tampak sah, tetapi juga memanfaatkan alat dan perangkat lunak yang khusus dibeli untuk mendukung aksinya, seperti *Simple Mail Transfer Protocol (SMTP)* dan *Validator*.

2. Unsur "tanpa hak atau melawan hukum"

Terdakwa mengakses akun korban tanpa hak dan secara melawan hukum. *Phishing* melibatkan pelanggaran hak privasi dan akses terhadap informasi digital milik korban tanpa izin. Dalam hal ini, tindakan terdakwa masuk ke akun *Coinbase* korban tanpa izin yang sah, sehingga memenuhi unsur melawan hukum yang diatur dalam UU ITE. (Arief, 2007)

3. Unsur "mengakses sistem elektronik dengan melanggar sistem pengamanan"

Terdakwa terbukti melakukan tindakan melawan hukum dengan mengakses sistem elektronik korban menggunakan teknik *phishing*, yang melanggar sistem pengamanan akun korban. Terdakwa menggunakan informasi palsu dan manipulasi untuk mendapatkan akses ke akun korban yang dilindungi oleh sistem keamanan (*password* dan kode *OTP*). Dengan ini, terdakwa melanggar unsur yang diatur dalam Pasal 30 ayat (3) UU ITE, yang secara spesifik menyebut tindakan melanggar atau menjebol sistem pengamanan sebagai tindak pidana.

4. Unsur "mengakibatkan kerugian bagi orang lain"

Unsur ini terpenuhi karena perbuatan terdakwa secara langsung menyebabkan kerugian finansial pada korban. Beberapa korban kehilangan aset digital yang ditransfer ke *e-wallet cryptocurrency* terdakwa. Dalam putusan, salah satu korban, Pietro Polini, kehilangan aset senilai Rp. 6,5 miliar dalam bentuk *Ethereum*, yang diambil dari akun *Coinbase* miliknya.

Pembuktian bukti yang diajukan adalah digital, jaksa harus menunjukkan bagaimana terdakwa menggunakan *email* palsu dan *website* palsu yang meniru platform *Coinbase*. Log aktivitas digital yang melacak transaksi *cryptocurrency* korban menjadi bukti penting dalam persidangan. Selain itu, para ahli forensik digital diperlukan untuk memverifikasi keaslian bukti-bukti tersebut dan menunjukkan bagaimana terdakwa mengakses akun korban menggunakan teknik *phishing*.

Tantangan yang terdapat dalam penegakan hukum kejahatan *phishing* ini terletak pada sulitnya melacak jejak digital pelaku. Sebagai kejahatan dunia maya, *phishing* sering kali melibatkan penggunaan identitas palsu dan alat-alat yang mempersulit pelacakan,

seperti penggunaan *Virtual Private Network (VPN)* atau teknologi enkripsi. Dalam kasus ini, terdakwa memanfaatkan akun anonim dan perangkat lunak khusus untuk menyembunyikan identitasnya, yang memperumit investigasi. Berdasarkan teori penegakan hukum yang dikemukakan oleh Lawrence M. Friedman, struktur hukum terkait teknologi transaksi elektronik sudah ada, tetapi substansi hukum dan kemampuan teknis aparat penegak hukum masih perlu ditingkatkan agar dapat mengikuti perkembangan teknologi yang digunakan oleh pelaku kejahatan.(Friedman, 1975)

Dalam kasus ini, meskipun terdakwa dihukum dengan pidana penjara dan denda yang besar, pengadilan menghadapi tantangan dalam memulihkan kerugian korban secara penuh. Pengembalian aset digital yang telah dicuri menjadi sulit karena sifat *cryptocurrency* yang tidak mudah dilacak setelah dipindahkan ke akun atau *e-wallet* lain. Hambatan ini menunjukkan pentingnya peningkatan teknologi dalam penegakan hukum agar aparat dapat dengan lebih cepat dan akurat melacak jejak digital yang ditinggalkan oleh pelaku.

Kasus ini menunjukkan bahwa meskipun ada aturan hukum yang mengatur kejahatan transaksi elektronik di Indonesia, penegakan hukum terhadap kejahatan *phishing* masih menghadapi banyak tantangan. Unsur-unsur tindak pidana yang dikenakan kepada terdakwa mencakup kesengajaan, pelanggaran hukum, akses ilegal ke sistem elektronik, dan kerugian yang ditimbulkan pada korban. Tantangan utama dalam kasus *phishing* adalah bukti digital yang rumit dan kesulitan dalam melacak jejak pelaku yang sering kali menggunakan teknologi canggih. Oleh karena itu, diperlukan perbaikan regulasi yang lebih spesifik dan peningkatan kapasitas teknologi penegak hukum agar kejahatan *phishing* dapat ditangani dengan lebih efektif di masa mendatang.

4. KESIMPULAN

Pengaturan hukum mengenai kejahatan phishing di Indonesia tercantum dalam dalam Undang-Undang Nomor 19 Tahun 2016 perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Phishing dikategorikan sebagai tindak pidana akses ilegal terhadap sistem elektronik, sebagaimana diatur dalam Pasal 30 UU ITE. Namun, regulasi ini belum secara spesifik mengatur modus operandi phishing yang memanfaatkan rekayasa sosial dan situs web palsu untuk mencuri data pribadi. Akibatnya, masih terdapat kekosongan hukum dalam menjerat pelaku phishing secara lebih rinci dan spesifik. Dalam praktiknya, penerapan hukum terhadap phishing telah mengalami perkembangan, tetapi masih menghadapi berbagai hambatan. Salah satu contohnya adalah kasus dalam Putusan Nomor 764/Pid.Sus/2022/PN Pbr, di mana terdakwa dijerat dengan Pasal 51 ayat (2) jo. Pasal 36 jo. Pasal 30 ayat (3) UU ITE karena melakukan akses ilegal melalui phishing. Kendala utama dalam penegakan hukum kasus ini adalah pembuktian menggunakan bukti digital yang memerlukan keahlian khusus serta kesulitan dalam melacak pelaku akibat penggunaan teknologi canggih. Faktor-faktor ini memperlambat proses hukum dan mengurangi efektivitas penegakan aturan terkait phishing. Analisis terhadap kasus tersebut menunjukkan bahwa terdakwa, Anggi Saputra, terbukti bersalah melakukan *phishing* dengan mengelabui korban untuk memberikan akses ke akun *cryptocurrency* melalui email palsu. Ia kemudian mentransfer aset digital korban ke e-wallet pribadinya. Unsur-unsur tindak pidana dalam kasus ini mencakup perbuatan yang disengaja, melanggar hukum, serta akses tanpa izin yang menyebabkan kerugian pada pihak lain. Meskipun terdakwa dijatuhi hukuman penjara dan denda, kasus ini menegaskan bahwa phishing masih sulit diberantas karena belum adanya regulasi yang secara rinci dan spesifik mengatur kejahatan tersebut.

5. UCAPAN TERIMAKASIH

Terimakasih penulis ucapkan kepada Allah SWT atas rahmatnya, Orang Tua yang telah memberikan semua yang mereka punya untuk Saya sebagai anaknya, Dekan Fakultas

Hukum Universitas Harapan Medan, Kepala Program Studi S1 Hukum, Dosen Pembimbing, Dosen Penguji, yang telah memberikan bimbingan dan arahnnya sehingga penelitian ini dapat terselesaikan dengan baik.

6. DAFTAR PUSTAKA

Arief, B. Nawawi. (2007). *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*. Kencana Prenada Media Group.

Budi Suhariyanto. (2013). *Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi Pengaturan dan Celah Hukumnya*. PT Rajagrafindo Persada.

Desriyarini Gui, M., Muliani SPd, Mp., Ketut Suardika, Mp. I., Tri Yusnanto, Ms., Hj Sri Nuryati, Mk., Mardiana, Mp., Pd Hj Badelah, M., Wardah, Mp., Pd Fahrina Yustiasari Liriwati, S., PdI Muqarramah Sulaiman Kurdi, M., & Musyarrafah Sulaiman Kurdi, Mp. (2024). *Membangun Moral Peserta Didik di Zaman Digital*. PT.Literatus Digitus Indonesia.

Devi Anjheli. (2024). Privasi Digital dan Kejahatan Phishing di Indonesia: Evaluasi Kritis terhadap Efektivitas UU ITE dan UU PDP. *Lecture Notes on Language and Literature*, *4*(1). https://doi.org/10.23977/langl.2024.070223

Friedman, L. M. (1975). *The Legal System: A Social Science Perspective*. Russell Sage Foundation.

Irfan Fanasafa. (2022). *Waspada! Kehajatan Phising Mengintai Anda*.

Muhammad Syahrum. (2022). *Pengantar Metodologi Penelitian Hukum: Kajian Penelitian Normatif, Empiris, Penulisan Proposal, Laporan Skripsi dan Tesis*. CV. Dotplus Publisher.

Peter Mahmud Marzuki. (2019). *Penelitian Hukum Edisi Revis*. PT. Kencana Prenada Media.

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Transaksi Elektronik.

Zulfa Ajda Khoiriyah & Fadhilah Aini, et. al. (2024). *Sosialisasi Pemahaman Dan Pencegahan Kekerasan Berbasis Gender Online Dalam Upaya Membentuk Kesadaran Hukum Pada Generasi Z 5.0*. *2*(2). https://doi.org/10.46924/legalempowerment.v2i2.251