PERLINDUNGAN HUKUM NASABAH BANK TERHADAP TINDAK PIDANA PENIPUAN DAN PENCURIAN DATA NASABAH PERBANKAN MELALUI MODUS SIBER DAN ELEKTRONIK[1]

Oleh:
Maria Tesalonika Bawintil[2]
tesalonikabawintil@gmail.com
Flora P. Kalalo[3]
Fonnyke Pongkorung[4]

ABSTRAK

Di era serba digital, kejahatan yang terjadi pada dunia perbankan hadir dalam berbagai bentuk. Bentuk kejahatan tersebut umumnya dilakukan dengan ragam cara dan modus. Pada awalnya pembobolan kartu kredit (*carding*), sudah sering terdengar, namun kemudian bentuk kejahatannya makin canggih yaitu pencurian data kartu (*card skimming*) hingga menggunakan saluran internet banking untuk mendapatkan data kartu kredit korban (*phising*). Hal tersebut terjadi karena kemajuan teknologi yang memberikan peluang baru bagi pelaku kejahatan.

Pelaku kejahatan perbankan mencuri data pribadi, mengakses rekening hingga melakukan transaksi illegal tanpa sepengetahuan nasabah. Untuk itu, masyarakat perlu selalu waspada akan segala kemungkinan kejahatan perbankan yang terjadi dengan mengedukasi diri meningkatkan literasi keuangan dengan mengikuti seminar-seminar perbankan. Terpenting menjaga dan melindungi data informasi seperti mengganti secara teratur sandi atau PIN, tidak memberikan data pribadi kepada phishing (tautan yang tidak dikenal) dan menghindari mengakses transaksi perbankan via wifi publik. Menyoal sindikat kejahatan perbankan yang turut melibatkan orang dalam, hal tersebut terjadi karena adanya *accessibility* yang memungkinkan dapat mencuri data nasabah dan memanipulasi transaksi atau mengungkapkan informasi rahasia kepada pihak ketiga; adanya penyalahgunaan posisi atau wewenang untuk tujuan pribadi dan keuntungan finansial semata; dan adanya kesempatan atau kelemahan sistem internal Perusahaan.

Dalam era digital yang serba terhubung, kejahatan tidak hanya terbatas pada dunia nyata, tetapi juga merambah ke dunia maya. Salah satu isu yang menjadi perhatian besar adalah tindak pidana siber yang semakin canggih dan memanfaatkan teknologi digital. Tindak Pidana di era digital dapat terjadi melalui berbagai modus operandi yang melibatkan teknologi informasi, ini menunjukkan bagaimana teknologi dapat menjadi pedang bermata dua yang artinya dapat memberikan kemudahan, tetapi juga sekaligus membuka peluang untuk kejahatan baru. Kejahatan digital kini menjadi bagian dari spektrum kejahatan siber (cyber crime) yang semakin kompleks.

Kata Kunci : Nasabah Bank, Tindak Pidana Perbankan, Siber dan Elektronik.

ABSTRACT

In the digital era, banking crimes take various forms. These crimes are generally committed using a variety of methods and methods. Initially, credit card fraud (carding) was commonplace, but now the forms of crime are becoming more sophisticated, including card skimming and using internet banking channels to obtain victims' credit card data (phishing). This is due to technological advances that provide new opportunities for criminals.

Banking criminals steal personal data, access accounts, and conduct illegal transactions without customers' knowledge. Therefore, the public needs to remain vigilant against all possible banking crimes by educating themselves and improving their financial literacy through attending banking seminars. Most importantly, safeguard and protect personal information, such as regularly changing passwords or PINs, not providing personal data to phishing (unknown links), and avoiding accessing banking transactions via public Wi-Fi. Regarding banking crime syndicates that involve insiders, this occurs due to accessibility that allows them to steal customer data and manipulate transactions or disclose confidential information to third parties; abuse of position or authority for personal gain or financial gain; and opportunities or weaknesses in the company's internal systems.

In this digital, interconnected era, crime is no longer confined to the physical world but has also spread to cyberspace. One issue of significant concern is the increasingly sophisticated nature of cybercrime, which utilizes digital technology. Crime in the digital era can occur through various methods involving information technology. This demonstrates how technology can be a double-edged sword: it can provide convenience but also open up opportunities for new crimes. Digital crime is now part of the increasingly complex spectrum of cybercrime.

Keywords: Bank Customers, Banking Crimes, Cyber and Electronics.

---

[1] Artikel Skripsi
[2] Mahasiswa Fakultas Hukum Unsrat, Nim.220711011125
[3] Fakultas Hukum, Doktor Ilmu Hukum
[4] Fakultas Hukum, Magister Ilmu Hukum

PENDAHULUAN

A. Latar Belakang Masalah

Perkembangan teknologi ikut mempengaruhi perkembangan masyarakat termasuk kejahatan yang ada disekitar masyarakat ikut berkembang pula, begitu juga dibidang perbankan saat ini semakin marak modus operandi tindak pidana dibidang perbankan. Tindak pidana terhadap bank bisa terjadi karena kegiatan yang dilakukan oleh bank berhubungan langsung dengan uang yang telah disetujui sebagai alat tukar-menukar yang sah dan seiring dengan perkembangan zaman, uang kemudian tidak hanya dikenal sebagai alat tukar-menukar saja, tetapi juga sebagai alat untuk menyimpan dan mempertahankan nilai suatu barang, menjadi satuan hitung dari jasa yang telah dikerjakan, dan ukuran pembayaran yang tertunda sehingga dapat disebut pula sebagai "Alat Pembayaran".

Tindak pidana terhadap bank kemudian dapat digolongkan kembali ke dalam kejahatan bisnis, yaitu tindakan pidana yang timbul akibat praktik-praktik bisnis yang sering kali berhubungan dengan ekonomi dan uang. Kejahatan bisnis sendiri dianggap sebagai sebuah "kejahatan" karena sifatnya yang sangat terikat dengan hak seseorang untuk mempertahankan harta bendanya dari segala tindakan yang menghilangkan haknya tersebut. Oleh karena perbankan merupakan suatu ekosistem industri, maka di dalamnya berisi sebuah pekerjaan, profesi, menghasilkan penghasilan, mendapatkan keuntungan dan lain sebagainya. Terlebih lagi industri ini memanfaatkan kepercayaan konsumennya untuk tetap dapat berjalan, oleh karenanya apabila terdapat kejahatan terhadap ekosistem ini maka dampaknya bukan hanya kepada pihak bank saja, melainkan kepada para subjek hukum yang menggantungkan dirinya kepada industri ini. Oleh sebab itu, muncul-*lah* konsep baru yang berhubungan dengan tindak pidana yang terjadi di dalam ekosistem ini, yaitu "Tindak Pidana Perbankan" dan "Tindak Pidana di Bidang Perbankan".[5]

Memasuki era digital yang serba cepat ini, modus kejahatan keuangan semakin berkembang dan canggih. Pelaku kejahatan memanfaatkan sistem keuangan dan kelengahan masyarakat untuk menjalankan berbagai aksi penipuan. Mulai dari phishing, skimming, hingga investasi bodong, semua dilakukan dengan tujuan mengambil keuntungan secara ilegal.

Tindak Pidana di bidang perbankan yang sebelumnya dilakukan secara konvensional tanpa menggunakan komputer saat ini siber dan elektronik menjadi tantangan yang cukup besar khusunya dalam pencurian data pribadi nasabah. Mudahnya akses internet membuat kreativitas masyarakat dalam melakukan kejahatan juga berkembang pesat. Terkait dengan hal tersebut, yang terfokus pada kajian hukum pidana terhadap modus kejahatan siber dan elektronik yang marak terjadi di sektor perbankan yang menyebabkan kerugian besar bagi nasabah maupun institusi, antara lain dengan modus kejahatan Phishing, Carding, Skimming, dan Pharming, Penipuan Transaksi Belanja Online, Penipuan Investasi Penipuan Mengaku Pihak Lain (Fake Call), dan Penipuan Social Engineering.

Otoritas Jasa Keuangan (OJK) mengungkapkan sedikitnya ada 10 jenis modus penipuan atau scam keuangan yang paling banyak terjadi di Indonesia, yaitu: Penipuan Transaksi Belanja Online, Penipuan Mengaku Pihak Lain (Fake Call), Penipuan Investasi, Penipuan Penawaran Kerja, Penipuan Mendapatkan Hadiah, Penipuan Melalui Media Sosial, Phishing, Social Engineering, Penipuan Online Fiktif dan Penipuan Berkedok Kiriman File APK via WhatsApp. Temuan ini berdasarkan data laporan yang dihimpun Indonesia Anti-Scam Centre (IASC) sejak November 2024 hingga 15 Oktober 2025. Selama periode tersebut, IASC mencatat sebanyak 299.237 laporan kasus penipuan dengan total 487.378 rekening yang terlibat. Angka ini menunjukkan betapa masifnya praktik penipuan digital di Indonesia, terutama di tengah meningkatnya penggunaan layanan keuangan dan transaksi elektronik daring. [6]

Di era serba digital, kejahatan yang terjadi pada dunia perbankan hadir dalam berbagai bentuk. Bentuk kejahatan tersebut umumnya dilakukan dengan ragam cara dan modus. Pada awalnya pembobolan kartu kredit (*carding*), sudah sering terdengar, namun kemudian bentuk kejahatannya makin canggih yaitu pencurian data kartu (*card skimming*) hingga menggunakan saluran internet banking untuk mendapatkan data kartu kredit korban (*phising*). Hal tersebut terjadi karena kemajuan teknologi yang memberikan peluang baru bagi pelaku kejahatan.[7]

Pelaku kejahatan perbankan mencuri data pribadi, mengakses rekening hingga melakukan transaksi illegal tanpa sepengetahuan nasabah. Untuk itu, masyarakat perlu selalu waspada akan segala kemungkinan kejahatan perbankan yang terjadi dengan mengedukasi diri meningkatkan literasi keuangan

[5] Dr. Hassanain Haykal, S.H., M.Hum. https://www.hukumonline.com/berita/a/tindak-pidana-perbankan-lt61d7e36d85d74?page=3

[6] https://www.kompas.tv/info-publik/624563/10-modus-penipuan-paling-marak-di-indonesia-menurut-ojk

[7] Etikah Karyani Suwondo Peneliti Senior Core Indonesia https://infobanknews.com/waspada-kejahatan-perbankan-seperti-ini-modus-operasinya/

dengan mengikuti seminar-seminar perbankan. Terpenting menjaga dan melindungi data informasi seperti mengganti secara teratur sandi atau PIN, tidak memberikan data pribadi kepada phishing (tautan yang tidak dikenal) dan menghindari mengakses transaksi perbankan via wifi publik. Menyoal sindikat kejahatan perbankan yang turut melibatkan orang dalam, hal tersebut terjadi karena adanya *accessibility* yang memungkinkan dapat mencuri data nasabah dan memanipulasi transaksi atau mengungkapkan informasi rahasia kepada pihak ketiga; adanya penyalahgunaan posisi atau wewenang untuk tujuan pribadi dan keuntungan finansial semata; dan adanya kesempatan atau kelemahan sistem internal Perusahaan.

Pengamat Perbankan Paul Sutaryono menjelaskan kasus kejahatan perbankan yang melibatkan orang dalam masih bisa ditemui saat ini. Untuk mengantisipasi hal tersebut, penting untuk meningkatkan penerapan manajemen risiko (risk management) oleh bank itu sendiri. Manajemen risiko yang harus diterapkan bank mencakup risiko kredit, risiko pasar, risiko likuiditas, dan risiko operasional. Dalam risiko operasional itu terdapat risiko orang (*people risk*)[8]

Ciri khas dari "Tindak Pidana Perbankan" yang kemudian membedakannya pula dari konsep "Tindak Pidana di Bidang Perbankan" adalah subjek pelaku yang melakukan kejahatannya. Dalam "Tindak Pidana di Bidang Perbankan" subjek pelaku kejahatannya dapat siapa saja, asalkan perbuatan kejahatannya itu menggunakan bank sebagai sarana kejahatannya, sedangkan "Tindak Pidana Perbankan" subjek kejahatannya itu hanya terbatas kepada organ-organ yang terdapat di dalam bank itu sendiri, seperti Pegawai Bank, Pemegang Saham, Direksi, Komisaris, Pihak Terafiliasi, dan Pemegang Saham.

Di era revolusi industri 4.0, sektor perbankan telah bertransformasi sepenuhnya ke arah digitalisasi. Layanan *mobile banking*, *internet banking*, dan transaksi *e-commerce* memberikan kemudahan luar biasa bagi masyarakat. Namun, ketergantungan pada teknologi ini ibarat pedang bermata dua; di satu sisi mempercepat transaksi, namun di sisi lain membuka celah keamanan baru yang dieksploitasi oleh pelaku kejahatan siber.

Belakangan ini, semakin marak modus kejahatan siber (cyber crime) dan modus operandi penipuan dan pencurian data nasabah semakin canggih dan variatif. Beberapa metode yang sering merugikan nasabah meliputi: Phishing dengan modus pengelabuan melalui link palsu untuk mencuri kredensial. Social Engineering dengan modus manipulasi psikologis untuk mendapatkan kode OTP atau PIN. Skimming dan Malware dengan modus penggunaan perangkat lunak jahat untuk menyadap data transaksi. Sniffing dengan modus Peretasan data melalui jaringan Wi-Fi publik. Dalam era digital yang serba terhubung, kejahatan tidak hanya terbatas pada dunia nyata, tetapi juga merambah ke dunia maya. Salah satu isu yang menjadi perhatian besar adalah tindak pidana siber yang semakin canggih dan memanfaatkan teknologi digital.

Dalam hubungan hukum antara bank dan nasabah, terdapat ketimpangan posisi tawar. Bank sebagai penyedia sistem memiliki kendali penuh atas teknologi keamanan, sementara nasabah seringkali hanya menjadi objek yang kurang memahami risiko teknis (literasi digital rendah). Ketika terjadi kehilangan dana akibat kejahatan siber, nasabah sering kali berada di pihak yang lemah saat harus membuktikan bahwa kesalahan bukan berada di pihak mereka. Selain itu terdapat Permasalahan Penegakan Hukum dan Pertanggungjawaban sekalipun secara regulasi, Indonesia telah memiliki UU ITE (Informasi dan Transaksi Elektronik), UU Perlindungan Data Pribadi (UU PDP), serta peraturan turunan dari Otoritas Jasa Keuangan (OJK) dan Bank Indonesia. Namun, dalam praktiknya, implementasi perlindungan hukum masih menemui kendala, seperti: Kesulitan dalam pelacakan pelaku yang bersifat anonim dan lintas negara, Debat mengenai siapa yang harus bertanggung jawab (Bank atau Nasabah) jika dana hilang akibat kelalaian sistem vs kesalahan pengguna dan Proses ganti rugi yang seringkali memakan waktu lama dan birokrasi yang rumit. Terkati dengan permasalahan diatas, betapa pentingnya Kepastian Hukum, karena tanpa perlindungan hukum yang kuat dan responsif, kepercayaan masyarakat terhadap sistem perbankan nasional dapat tergerus. Oleh karena itu, diperlukan kajian mendalam mengenai sejauh mana instrumen hukum saat ini mampu memberikan perlindungan preventif maupun represif bagi nasabah yang menjadi korban kejahatan siber.

Dalam penggunaan teknologi informasi dalam transaksi elektronik ini masih rawan akan penipuan. Melihat kondisi ini diharapkan suatu perangkat aturan yang khusus mengatur tentang kejahatan komputer dan perlindungan hukum terhadap pemanfaatan teknologi informasi, media dan komunikasi agar dapat berkembang secara optimal. Untuk mengatasi berbagai permasalahan tersebut pemerintah telah membuat aturan yang dituangkan dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disingkat UU ITE). Secara umum UU ITE dapat dibagi dua bagian besar ialah mengatur mengenai transaksi elektronik dan mengatur perbuatan yang dilarang (cyber crimes).

[8] https://infobanknews.com/waspada-kejahatan-perbankan-seperti-ini-modus-operasinya/

Memperhatikan berbagai resiko dan permasalahan hukum dapatlah disebut sebagai kejahatan perbankan. Untuk itu perlu dijelaskan tentang kejahatan dalam KUHPidana membedakan antara kejahatan (delik hukum) dan pelanggaran (delik undang-undang). Adapun pengertian dari tindakan kejahatan adalah suatu perilaku yang dilakukan dengan melanggar suatu aturan. Dalam pendefinisian kejahatan, ada beberapa pendapat tentang perilaku apa yang bisa dikatakan sebagai suatu kejahatan. Dalam yuridis kejahatan adalah suatu perilaku yang melanggar peraturan perundangundangan atau ketentuan yang sudah berlaku serta telah diakui secara legal. Secara kriminilogis berbasis sosiologis mendefisikan kejahatan sebagai suatu pola tingkah laku yang dapat mengakibatkan kerugian terhadap masyarakat serta suatu pola tingkah laku yang dapat reaksi social.[9]

Perkembangan teknologi informasi membawa sebuah perubahan dalam masyarakat. Lahirnya media sosial menjadikan pola perilaku masyarakat mengalami pergeseran baik budaya, etika dan norma yang ada. Media sosial adalah sebuah media online yang mendukung segala interaksi social yang menggunakan teknologi berbasis web dapat mengubah komunikasi menjadi suatu dialog interkatif. Ada beberapa situs media sosial yang saat ini populer seperti Blog, Twitter, Facebook, Instagram, Path, dan Wikipedia. Van Dijk memberikan definisi dari media sosial adalah platform media yang terfokus pada eksistensi pengguna yang menyediakan fasilitas dalam melakukan kegiatan, maka dari itu media sosial dapat dikatakan sebagai fasiliator online penguat hubungan antar pengguna sekaligus sebuah ikatan sosial.[10]

Internet merupakan sistem teknologi informasi yang mempunyai potensi untuk menggeserkan paradigma pakar ahli hukum terhadap definsi kejahatan komputer. Umumnya, pakar ahli hukum hanya fokus pada alat atau perangkat keras yakni komputer. Tetapi, dengan munculnya kemajuan teknologi informasi yaitu jaringan internet, membuat pusat dari identifikasi dari pengertian cyber crime menjadi diperluas, menjadi suatu kegiatan yang dilakukan di dunia cyber melalui sistem informasi yang digunakan. Dengan begini, cyber crime bukan hanya berfokus pada komponen hard-ware saja untuk melakukan kejahatan, tetapi telah diperluas dalam lingkup dunia yang sudah dijelajahi oleh sistem teknologi informasi yang bersangkutan. Maka dari itu, cyber crime di maknakan sebagai kejahatan teknologi informasi serta juga sebagai kejahatan dunia maya.[11]

Perkembangan teknologi digital yang pesat, di satu sisi, memberikan kemudahan bagi banyak orang dalam beraktivitas, termasuk dalam bertransaksi dan berbelanja. Namun, di sisi lain, hal ini juga membuka peluang bagi para pelaku *cyber crime* untuk melancarkan aksi kejahatan mereka dengan lebih mudah dan beragam. Tindak Pidana di era digital dapat terjadi melalui berbagai modus operandi yang melibatkan teknologi informasi, ini menunjukkan bagaimana teknologi dapat menjadi pedang bermata dua yang artinya dapat memberikan kemudahan, tetapi juga sekaligus membuka peluang untuk kejahatan baru.

B. Rumusan Masalah

1. Bagaimana Penerapan Hukum Tindak Pidana Penipuan dan Pencurian Data Nasabah Perbankan melalui modus Siber dan Elektronik?
2. Bagaimana Perlindungan Hukum Terhadap Nasabah Bank akibat tindak Pidana Perbankan?

C. Metode Penelitian

Penelitian Skripsi ini menggunakan Metode Penelitian yuridis normatif, yaitu jenis penelitian hukum yang mengkaji berbagai sumber hukum yang berlaku. Sumber-sumber tersebut meliputi peraturan perundang-undangan, putusan pengadilan, literatur hukum, hingga praktik hukum yang telah berkembang melalui studi pustaka.

PEMBAHASAN

A. Penerapan Hukum Tindak Pidana Penipuan dan Pencurian Data Nasabah Perbankan melalui modus Siber dan Elektronik.

Penerapan hukum terhadap tindak pidana penipuan dan pencurian data nasabah perbankan di Indonesia melibatkan "payung hukum berlapis" (*multi-layered legal framework*), karena modus operandi siber bersifat kompleks (seperti *phishing*, *skimming*, atau *social engineering*), aparat penegak hukum biasanya menggunakan kombinasi beberapa undang-undang sekaligus. Berikut adalah analisis mendalam mengenai penerapan hukumnya:

1. Instrumen Hukum Utama

Penerapan sanksi bergantung pada peran pelaku dan cara kejahatan dilakukan:

a) Undang-Undang ITE No. 11 Tahun 2008 jo. Undang-Undang Nomor 1 Tahun 2024, Fokus pada aspek teknis siber.
   1) Pasal 30 dan 46: Larangan mengakses sistem elektronik orang lain (misal: *hacking* atau *account takeover*).

[9] Muhammad Mustafa, 2007. Kriminologi, Fisip Ui Press, Depok, hlm. 16

[10] Rulli Nasrullah, 2017. Media Sosial : Perspektif Komunikasi, Budaya, Dan Sosioteknologi, Remaja Rosdakarya, Bandung, hlm.11

[11] Aswan, 2019. Tindak Pidana Penipuan Berbasis Transaksi Elektronik, Guepedia, Bogor, hlm. 44

2) Pasal 32 dan 48: Larangan mengubah, merusak, atau memindahkan data elektronik milik orang lain secara tanpa hak.
3) Pasal 35 dan 51: Pemalsuan dokumen elektronik seolah-olah asli (sering digunakan untuk kasus *phishing* atau situs bank palsu, kasus ini lagi marak-maraknya bersamaan dengan kemajuan teknologi).

b) Undang-Undang Pelindungan Data Pribadi (Undang-Undang Nomor 27 Tahun 2022), Fokus pada data spesifik nasabah. Pasal 65 dan 67: Mengatur sanksi pidana bagi siapa saja yang secara melawan hukum memperoleh atau mengungkapkan data pribadi (termasuk data keuangan) milik orang lain untuk menguntungkan diri sendiri.
c) Undang-Undang Perbankan (Undang-Undang No. 10 Tahun 1998):
Pasal 47 dan 49: Mengatur sanksi bagi pihak (terutama oknum bank) yang dengan sengaja tidak merahasiakan data nasabah atau memanipulasi catatan bank.
d) KUHP (Kitab Undang-Undang Hukum Pidana):
1) Pasal 378 (Penipuan): Digunakan jika ada unsur tipu muslihat untuk menggerakkan orang lain menyerahkan barang/uang.
2) Pasal 362 (Pencurian): Digunakan dalam kasus pengambilan dana di rekening sebagai bentuk "barang" milik orang lain.

2. Tanggung Jawab Perbankan & Hak Nasabah

Dalam perspektif hukum perdata dan administrasi, bank memiliki kewajiban menjaga keamanan sistem sesuai POJK No. 22 Tahun 2023 tentang Pelindungan Konsumen:

1. Strict Liability: Jika kerugian nasabah disebabkan oleh kegagalan sistem keamanan bank (bukan kelalaian nasabah), bank wajib bertanggung jawab mengganti rugi.
2. Sanksi Administratif: OJK dapat menjatuhkan denda hingga Rp15.000.000.000 kepada bank yang lalai melindungi data nasabah.
3. Gugatan Perdata: Nasabah dapat menggugat berdasarkan Pasal 1365 KUHPerdata (Perbuatan Melawan Hukum) jika bank terbukti lalai dalam menjaga rahasia bank.

3. Kendala Penegakan Hukum

Meskipun aturannya sudah cukup lengkap, penegakan hukum siber perbankan sering terkendala oleh:

a) Anonimitas & Lokasi Pelaku: Pelaku sering berada di luar yurisdiksi atau menggunakan identitas palsu yang sulit dilacak.
b) Pembuktian Digital: Membutuhkan audit forensik digital yang memakan waktu dan biaya besar.
c) Kurangnya Literasi: Banyak kasus dianggap sebagai kelalaian nasabah (*social engineering*), sehingga sulit untuk menuntut ganti rugi ke pihak bank.

Kitab Undang-Undang Hukum Pidana memuat ketentuan umum mengenai hukum siber. Dalam peraturan perundang-undangan di Indonesia berlaku asas Lex Specialis derogat legi Generalis yang berarti peraturan perundang-undangan yang bersifat khusus menggantikan peraturan perundang undangan yang bersifat umum. Secara khusus, Indonesia telah memiliki peraturan perundang undangan yang mengatur hukum siber di bidang perbankan, yaitu Undang-Undang Informasi dan Transaksi Elektronik Nomor 11 Tahun 2008 yang diubah dengan Undang-Undang Nomor 19 Tahun 2016, Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan, serta Undang-Undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (PDP). Adanya perlindungan hukum bagi nasabah memberikan rasa aman kepada nasabah terkait dengan eksploitasi data pribadinya.[12] Selain itu ada juga, Peraturan Otoritas Jasa Keuangan, dan berbagai aturan lain yang dibutuhkan untuk mencegah cybercrime.

Kegagalan dan kesalahan dalam teknologi informasi dan sistem elektronik terkadang berasal dari langkah-langkah keamanan yang tidak memadai yang dirancang untuk melindungi data pribadi pelanggan yang telah mendaftar di platform daring. perangkat lunak komputer, jaringan telekomunikasi, dan sistem komunikasi elektronik.[13] Dalam sistem implementasinya, teknologi informasi dan komunikasi berfungsi sebagai pedang bermata dua. Teknologi informasi menawarkan berbagai keuntungan untuk meningkatkan kebahagiaan dan peradaban manusia, serta memajukan layanan publik dan internal dalam industri jasa. Sebaliknya, teknologi informasi dimanfaatkan oleh oknum yang tidak bertanggung

[12] Triputri, D. H., Mofea, S., Yulviani, D., & Pratama, R. (2023). Analisis Yuridis Terhadap Penerapan Sanksi Pidana Bagi Pelaku Penipuan Dalam Transaksi Elektronik Berdasarkan Asas Lex Specialis Derogat Legi Generali Ditinjau Dari Kuhp Dan UU ITE.Lex Veritatis,2(01), 42-51.

[13] Kusuma, A. C., & Rahmani, A. D. (2022). Analisis Yuridis Kebocoran Data Pada Sistem Perbankan Di Indonesia (Studi Kasus Kebocoran Data Pada Bank Indonesia). SUPREMASI: Jurnal Hukum, 5(1), 46-63.

jawab untuk melakukan tindakan ilegal yang melanggar kepentingan hukum individu, masyarakat, dan negara.[14]

Permasalahan penyalahgunaan data pribadi misalnya, telah menjadi fenomena global, termasuk di Indonesia. Kasus-kasus yang telah tercatat merupakan representasi dari ribuan kasus pelanggaran privasi yang terjadi. Permasalahan pencurian data pribadi menuntut adanya perlindungan hukum yang lebih komprehensif. Regulasi yang berlaku saat ini, meskipun telah ada, dinilai belum cukup memadai untuk melindungi hak privasi individu.

Saat ini undang-undang yang digunakan untuk melindungi data pribadi yaitu Undang-Undang pada Pasal 7914 ayat (1) Undang-Undang Nomor 24 Tahun 2013 Tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan (UU Administrasi Kependudukan), Pasal 5815 Peraturan Pemerintah Nomor 37 Tahun 2007 tentang Pelaksanaan Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (PP Administrasi Kependudukan), dan pada Pasal 26 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.[15]

B. Perlindungan Hukum Terhadap Nasabah Bank akibat tindak Pidana Perbankan.

Hukum berfungsi untuk melindungi kepentingan manusia. Untuk melindungi kepentingan manusia, hukum harus ditegakkan. Perlindungan hukum mengacu pada perlindungan yang diberikan oleh hukum atau peraturan perundang-undangan untuk menegakkan kepentingan manusia, sehingga memfasilitasi perkembangan kehidupan manusia yang normal dan damai.

Hukum adalah suatu sistem yang terdiri dari sub sistem hukum yang saling berkaitan satu sama lainnya dan saling bekerja sama untuk mencapai pada tujuan hukum yakni keadilan (gerechtigkeit), kemanfaatan (zweckmassighkeit), dan kepastian hukum (rechtssichherheit). Setiap sistem hukum terdiri dari sub sistem hukum secara seterusnya sehingga sub-sub sistem tersebut berangkaian dan bersama-sama berencana mencapai suatu tujuan.[16]

Perlindungan hukum sangat krusial karena adanya ketimpangan posisi antara pihak yang kuat (bank/institusi) dengan pihak yang lebih lemah (nasabah). Tanpa perlindungan hukum yang jelas, hak-hak individu mudah terabaikan.

Berikut adalah alasan utama mengapa perlindungan hukum itu penting, khususnya dalam konteks perbankan dan kehidupan bermasyarakat:

1. Menjamin Kepastian Hukum (*Legal Certainty*)

Masyarakat perlu tahu bahwa hak-hak mereka diakui secara tertulis. Dalam perbankan, kepastian ini menjamin bahwa uang yang disimpan tidak bisa hilang begitu saja tanpa ada pertanggungjawaban yang jelas. Jika terjadi sengketa, sudah ada aturan main yang menentukan siapa yang salah dan siapa yang benar.

2. Menjaga Keseimbangan Posisi Tawar

Bank memiliki sumber daya finansial, teknologi, dan tim hukum yang besar, sedangkan nasabah umumnya hanya individu. Perlindungan hukum (seperti Undang-Undang Perlindungan Konsumen) hadir untuk:

a) Mencegah adanya klausula baku yang sepihak (aturan yang hanya menguntungkan bank).
b) Memberikan ruang bagi nasabah untuk menggugat jika terjadi kelalaian sistem.

3. Menumbuhkan Kepercayaan Publik (*Public Trust*)

Ekonomi sebuah negara sangat bergantung pada kepercayaan. Jika nasabah merasa uangnya tidak aman di bank karena lemahnya hukum, mereka akan menarik dana secara massal (*rush money*). Perlindungan hukum memastikan sistem keuangan tetap stabil karena masyarakat merasa aman untuk bertransaksi.

4. Memberikan Rasa Aman dan Keadilan

Secara psikologis, hukum berfungsi sebagai "jaring pengaman". Perlindungan ini memastikan bahwa:

a) Setiap pelanggaran atau tindak pidana akan mendapatkan sanksi (fungsi pencegahan).
b) Korban yang dirugikan mendapatkan kompensasi atau ganti rugi yang setimpal (fungsi pemulihan).

5. Mencegah Tindakan Sewenang-wenang

Tanpa hukum yang melindungi, pihak yang memiliki kekuatan (baik itu penguasa maupun korporasi) bisa bertindak subyektif. Hukum menetapkan batasan-batasan apa yang boleh dan tidak boleh dilakukan oleh bank dalam mengelola dana masyarakat.

Berdasarkan pemahaman tersebut diatas, maka Perlindungan hukum terhadap nasabah merupakan pilar utama dalam menjaga kepercayaan masyarakat terhadap sistem perbankan. Di Indonesia, perlindungan ini dibagi menjadi dua mekanisme utama: perlindungan preventif (pencegahan) dan perlindungan represif

[14] Adam Chazawi. 2015. Tindak Pidana Informasi Dan Transaksi Elektronik. Penerbit Media Nusa Crative, Jakarta, hlm. 107.

[15] Rumlus, M. H., & Hartadi, H. (2020). Kebijakan penanggulangan pencurian data pribadi dalam media elektronik. Jurnal HAM, 11(2), hlm. 285 299.

[16] Umar Said Sugiharto, (2017), Pengantar Hukum Indonesia, cet. I, Jakarta: Sinar Grafika. h. 30

(penanganan setelah kejadian). Berikut adalah poin-poin penting mengenai perlindungan hukum nasabah akibat tindak pidana perbankan:

1. Dasar Hukum Utama

Beberapa regulasi yang menjadi payung hukum perlindungan nasabah antara lain:

a) Undang-Undang No. 10 Tahun 1998 tentang Perubahan atas Undang-Undang No. 7 Tahun 1992 tentang Perbankan.
b) Undang-Undang No. 8 Tahun 1999 tentang Perlindungan Konsumen.
c) Undang-Undang No. 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan (UU PPSK).
d) Peraturan Otoritas Jasa Keuangan (POJK) terkait perlindungan konsumen di sektor jasa keuangan.
e) POJK No. 22 Tahun 2023 mengatur perlindungan konsumen dan masyarakat di sektor jasa keuangan secara menyeluruh, termasuk kewajiban iktikad baik oleh bank.

2. Tanggung Jawab Bank dalam Tindak Pidana

Jika terjadi tindak pidana yang dilakukan oleh oknum internal bank (seperti penggelapan dana nasabah atau *fraud*), bank secara korporasi tetap memiliki tanggung jawab:

a) Strict Liability**:** Bank wajib bertanggung jawab atas kerugian nasabah jika terbukti ada kelemahan dalam sistem keamanan atau pengawasan internal bank.
b) Pengembalian Dana**:** Nasabah berhak menuntut pengembalian dana beserta bunga jika kerugian timbul bukan karena kelalaian nasabah (misalnya korban *skimming* atau pembobolan sistem).
c) Tindakan hukum : Bank wajib melakukan tindakan terhadap para pelaku yang melakukan penggelapan pada proses hukum yang berlaku

3. Peran Lembaga Penjamin Simpanan (LPS)

LPS berfungsi sebagai jaring pengaman jika sebuah bank dicabut izin usahanya akibat tindak pidana yang menyebabkan bank gagal.

a) LPS menjamin simpanan nasabah hingga Rp 2 Miliar per nasabah per bank.
b) Syarat Layak Bayar: Tercatat dalam pembukuan bank, Tingkat bunga tidak melebihi bunga penjaminan, dan Tidak melakukan tindakan yang merugikan bank (misal: kredit macet).

Dalam hukum perbankan, tanggung jawab bank terhadap tindak pidana tidak hanya bersifat individu (oknum pelaku), tetapi juga bersifat korporasi. Bank memiliki kewajiban untuk menjaga dana masyarakat berdasarkan Prinsip Kepercayaan (*Fiduciary Relation Principle*) dan Prinsip Kehati-hatian (*Prudential Principle*). Meskipun pelaku kejahatan adalah oknum karyawan atau pihak ketiga, bank tetap memiliki tanggung jawab perdata kepada nasabah.

Globalisasi yang menjadikan pendorong sebagai lahirnya era perkembangan teknologi informasi, sehingga kebutuhan akan teknologi jaringan komputer semakin meningkat. Seiring perkembangan zaman dan semakin canggihnya suatu teknologi, pelaku kejahatan siber (cyber crime) berevolusi menjadi berbagai jenis kejahatan baru dengan modus operandi yang baru juga. Berbagai bentuk kejahatan siber (cyber crime) terus berkembang dengan pesat seperti hacking, cracking, carding hingga yang lebih spesifik lagi yaitu: probe (usaha untuk memperoleh akses ke dalam suatu sistem), scan (probe dalam jumlah besar), account compromise (penggunaan account secara ilegal), root compromise (account compromise dengan privilege bagi si penyusup), denial of service atau dos (membuat jaringan tidak berfungsi karena kebanjiran traffic), dan penyalahgunaan domain name.[17]

Cyber crime di Indonesia terjadi sejak tahun 1983, terutama di bidang perbankan. Dalam setiap tahun sampai saat ini di Indonesia banyak terjadi cybercrime, misalnya pembajakan program komputer, cracking, penipuan penggunaan kartu kredit pihak lain secara tidak sah(carding), pembobolan bank (banking fround), pornografi, menduplikasi dan merekam data kartu ATM (skimming ATM), termasuk kejahatan terhadap nama domain (domain name).[18] Pelanggaran terhadap hak privasi melalui penyalahgunaan data pribadi juga makin marak, khususnya di sektor perbankan. Praktik pertukaran data nasabah secara bebas antar pusat kartu kredit, pengungkapan informasi transaksi kepada pihak yang tidak berwenang, serta perdagangan data nasabah baik di antara lembaga perbankan maupun melalui pihak ketiga yang tidak bertanggung jawab, merupakan contoh nyata dari pelanggaran tersebut.[19]

Dalam kasus tindak pidana perbankan, adalah skimming di Indonesia yang paling sering terjadi, namun pada peneliti keamanan siber dari CISSREC Ibnu Dwi Cahyo menyatakan bahwa dunia perbankan di Indonesia memang cukup rawan menjadi sasaran aksi skimming (pencurian data). Berdasarkan data yang diperoleh dari Kepolisian Uni Eropa, Indonesia menjadi

[17] Dian Ekawati, (2018), Perlindungan Hukum Terhadap Nasabah Bank Yang Dirugikan Akibat Kejahatan Skimming Ditinjau Dari Perspeketif Teknologi Informasi Dan Perbankan, UNES Law Review, Vol 1., Issue 2. hlm. 158.

[18] Widodo, (2009), Sistem Pemidanaan Dalam Cyber Crime, Yogyakarta: Laksbang Mediatama. hlm. 29

[19] Siti Yuniarti, "Perlindungan Hukum Data Pribadi Di Indonesia," Jurnal Becoss Vol.1, No. (2019): hlm.148.

peringkat ketujuh lokasi favorit para pelaku skimming. Kejahatan skimming pada tahun 2015 ada 5.500 kasus skimming ATM di dunia, sebanyak 1.549 kasus diantaranya terjadi di Indonesia. Bank yang sering terjadi kejahatan tersebut adalah Bank Mandiri dan Bank BRI itu yang terbesar di tanah air dan resikonya jauh lebih besar jaringannya sampai daerah. Menurut Europol (Kepolisan Uni Eropa) daerah Bali menjadi lokasi ketiga terfavorit untuk para pelaku skimming ATM.[20]

Pentingnya perlindungan hukum terhadap data pribadi semakin mendapat perhatian seiring dengan peningkatan jumlah pengguna telepon seluler dan internet. Berbagai kasus yang mencuat, terutama yang berkaitan dengan kebocoran data pribadi yang berujung pada penipuan atau tindak kriminal seperti pornografi, semakin memperkuat urgensi penyusunan regulasi hukum untuk melindungi data pribadi. Perlindungan data pribadi berhubungan erat dengan konsep privasi, yang pada dasarnya merupakan upaya menjaga martabat dan integritas individu secara pribadi.[21] Konsep privasi, yang sering diasosiasikan dengan negara-negara maju, merujuk pada hak fundamental individu untuk menjaga kehidupan pribadi dari campur tangan yang tidak sah.[22]

Pasal 1 Angka 1 Undang-Undang Nomor 10 Tahun 1998 mendefinisikan perbankan sebagai segala sesuatu yang berhubungan atau menyangkut tentang bank baik dilihat secara kelembagaan, kegiatan usaha serta cara dan proses dalam menjalankan kegiatan usahanya. Ketentuan hukum yang dapat digunakan untuk menetapkan dan memberikan perlindungan hukum dalam penyelenggaraan layanan internet banking dapat dicermati pada Pasal 29 ayat (4) Undang-Undang Nomor 10 Tahun 1998 yang menyatakan bahwa bank berkewajiban untuk menyediakan dan menyampaikan informasi mengenai kemungkinan adanya risiko kerugian terkait dengan transaksi nasabah yang dilakukan oleh bank demi tercapainya kepentingan nasabahnya. Pada permasalahan perlindungan hukum terhadap kerugian nasabah akibat error system, penerapan peraturan ini wajib untuk dilakukan oleh bank secara pro aktif dalam memberikan informasi-informasi sehubungan dengan risiko kerugian atas pemanfaatan layanan bank oleh nasabah.[23]

Dalam upaya mencegah tindak pidana pencurian data pribadi, OJK mengembangkan berbagai pedoman dan regulasi yang harus diikuti oleh lembaga perbankan. Salah satu peraturan yang sangat relevan adalah kewajiban bank untuk menerapkan sistem keamanan yang memadai dalam transaksi elektronik dan pengelolaan data pribadi nasabah. OJK memastikan bahwa setiap bank melakukan evaluasi terhadap sistem keamanan secara berkala untuk mengidentifikasi dan mengatasi potensi yang dapat dimanfaatkan pelaku kejahatan siber. OJK berperan memberikan pelatihan dan sosialisasi kepada lembaga perbankan mengenai pentingnya perlindungan data pribadi. Melalui berbagai program edukasi, OJK membantu bank memahami bagaimana cara mengelola dan melindungi data nasabah dengan baik, serta bagaimana menghindari tindakan yang dapat membuka celah bagi pencurian data, untuk itu butuh kesadaran dari semua pihak terutama nasabah, pentingnya kehati-hatian dan kepedulian untuk melindungi data pribadi.

Berdasarkan Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan, Otoritas Jasa Keuangan (OJK) merupakan organisasi independen yang mempunyai kewenangan mengawasi dan mengatur seluruh kegiatan sektor jasa keuangan Indonesia secara komprehensif. Hal ini mencakup pasar modal, perbankan, dan sektor jasa keuangan non-bank lainnya seperti asuransi, dana pensiun, lembaga pembiayaan, dan lembaga jasa keuangan lainnya.[24] Di era digital, penyebaran data yang tidak disetujui tentu menimbulkan risiko yang signifikan dan dapat mengikis kepercayaan konsumen terhadap organisasi jasa keuangan. Bank sendiri diakui mempunyai kewajiban untuk menjaga informasi pribadi nasabahnya, termasuk transaksi keuangan dan identifikasi. Dalam hal ini, OJK tentu berperan sebagai pengawas dan regulator yang bertugas mencegah bank-bank yang lalai membocorkan dan menyalahgunakan data konsumen.[25]

Kejahatan perbankan tidak dapat lagi digolongkan sebagai kejahatan konvensional yang dapat dilakukan oleh sembarang orang, tapi lebih tepatnya sudah tergolong sebagai kejahatan non

[20] Jpnn.com. (19 Maret 2018). Ketahuilah, Indonesia Memang Lokasi Favorit Skimming, https://m.jpnn.com/news/ketahuilah-indonesia-memang-lokasi-favorit-skimming?page=2,

[21] Wahyudi Djafar dan Asep Komarudin, 2014. Perlindungan Hak Atas Privasi Di Internet-Beberapa Penjelasan Kunci. Penerbit Elsam, Jakarta, hlm. 2.

[22] Rosalinda Elsina Latumahina, 2014. "Aspek Hukum Perlindungan Data Pribadi Di Dunia Maya," Jurnal Gema Aktualita 3, no. 2 , hlm. 17.

[23] Alamudi, I. A. A. I. A. (2023). Analisis Perundang-undangan: Kajian Kritis Undang-Undang Perbankan Syariah. Qonun Iqtishad EL Madani Journal, 2(2), hlm. 30-38.

[24] Muhammad Tazil Ramadhan and Diana Wiyanti, "Peran Otoritas Jasa Keuangan Dalam Mengawasi Kegiatan Lembaga Bank Berdasarkan Undang-Undang Otoritas Jasa Keuangan Nomor 21 Tahun 2011 Dan Undang-Undang Perbankan Nomor 10 Tahun 1998 Terkait," Bandung Conference Series: Law Studies4, No. 1 (2024): hlm.766 Https://Doi.Org/10.29313/Bcsls.V4i1.12484.

[25] Ruth Devisa Br Sukatendel, 2021. "Peran Otoritas Jasa Keuangan Terhadap Tindak Pidana Penyebaran Data Pribadi Oleh Perusahaan Financial Technology," hlm. 38.

konvensional atau apa yang oleh Edwin H Sutherland disebut sebagai white collar crime, yaitu kejahatan yang dilakukan oleh orang-orang yang memiliki kedudukan sosial yang tinggi dan terhormat dalam pekerjaannya. Dengan posisi strategi seperti itu sudah tentu para penjahat bank tidak akan pasrah, tapi dengan kekuatan posisi tawar yang mereka miliki akan menghindar dari jeratan hukum. Oleh karena itu dalam Kongres PBB ke 6 Tahun 1980, dikatakan bahwa bentuk-bentuk pelanggaran dibidang ekonomi termasuk bentuk-bentuk pelanggaran yang sulit dijangkau oleh hukum.[26]

Kemajuan teknologi informasi dan komunikasi telah membawa manfaat besar bagi kehidupan manusia, khususnya dalam sektor perbankan. Namun, kemajuan ini juga memunculkan tantangan serius berupa tindak pidana Cyber Crime. Berbagai regulasi, seperti Undang-Undang ITE, Undang-Undang Perbankan, Undang-Undang Perlindungan Data Pribadi, serta peraturan Otoritas Jasa Keuangan (OJK), telah dirancang untuk melindungi nasabah dari ancaman ini. Perlindungan hukum mencakup hak atas privasi data, kewajiban bank menjaga kerahasiaan nasabah, serta sanksi bagi pelanggar. OJK, sebagai lembaga pengawas sektor jasa keuangan, memainkan peran kunci dalam memastikan kepatuhan lembaga perbankan terhadap standar perlindungan terhadap Pidana Penipuan Dan Pencurian Data Nasabah Perbankan Melalui Modus Siber dan Elektronik Hal ini termasuk memastikan adanya sistem keamanan yang memadai dan memberikan efek jera kepada pelanggar. Meski demikian, implementasi aturan masih menghadapi berbagai tantangan, seperti kurangnya kesadaran di kalangan masyarakat dan kelalaian lembaga perbankan.

Sumber daya manusia dalam penegakan hukum pidana adalah mereka yang selama ini kita kenal sebagai penegak hukum, yang tergabung dalam istitusi sistem peradilan pidana, mulai dari Kepolisian,Kejaksaan, Pengadilan dan Lembaga Pemasyarakatan. Mereka adalah para aktor yang sangat menentukan dalam penegakan hukum. Oleh karena itu meskipun sebaik dan sesempurna apapun aturan yang dibuat akhirnya akan ditentukan oleh orang-orang yang menegakkan aturan tersebut. Menyangkut hal ini maka prasyarat yangharus dipenuhi adalah pertama, menyangkut kuantitas SDM dan kedua adalah kualitas SDM, baik kualitas intelektual maupun moral. Prasyarat tersebut penting, apalagi dikaitkan dengan karakteristik kejahatan perbankan dan peningkatan jumlah kejahatan perbankan akhir-akhir ini, maka disamping jumlah yang memadai juga sudah tentu membutuhkan skill yang tinggi dan moralitas yang tangguh.

Kualitas dari SDM yang biasa-biasa saja tentu tidak akan dapat bersaing dengan kecerdikan para pelaku kejahatan perbankan yang terpelajar, terpandang, dan memiliki banyak uang. Oleh karena itu jika selama ini penegakan hukum terhadap kejahatan perbankan belum optimal, maka memang perlu dipertanyakan kuantitas dan kualitas SDM penegak hukum. Untuk itu di sini perlunya penyidik, penuntut umum dan hakim memiliki wawasan yang memadai dibidang perbankan melalui training secara terpadu dan berkelanjutan sebagaimana di lakukan di Jepang[27]

Disisi lain, dalam penegakan hukum pidana terhadap kejahatan perbankan sulit dihindari intervensi dari kelompok-kelompok kepentingan dalam masyarakat, terutama adalah kepentingan politik dan kepentingan ekonomi. Menyangkut kepentingan ekonomi, sebenarnya merupakan hal yang wajar dalam usaha perbankan, karena itulah tujuannya namun akan menjadi kriminal ketika cara mengaktualisasikan kepentingan itu telah melanggar kaidah-kaidah hukum dan sosial yang sangat merugikan. Justru banyaknya kejahatan perbankan muncul bersumber dari persoalan ini. Persoalannya kemudian mereka merasa sebagai orang-orang yang tidak berdosa dan berusaha sekuat tenaga untuk mempengaruhi bahkan menafikan bekerjanya hukum pidana terhadap mereka. Hal ini memang menyangkut persoalan yang kompleks, mulai dari etika bisnis yang rapuh, para pejabat yang mudah diajak berkolusi, sampai masih rendahnya pemahaman masyarakat di bidang perbankan. Kemampuan dan keunggulan dalam posisi tawar yang dapat mempengaruhi jalannya penegakkan hukum.

Pengaruh yang tidak kalah pentinnya dalam penegakan hukum pidana terhadap kejahatan perbankan adalah intervensi kekuasaan atau politik. Sebenarnya kekuasaan merupakan hal penting dalam konteks ini, karena tanpa dukungan kekuasaan tidak mungkin hukum pidana dapat ditegakkan, namun disisi lain kekuasaan juga dapat memandulkan tegak dan berfungsinya hukum itu sendiri.

Dalam kasus kejahatan perbankan, kasus bebasnya para "pembobol Bank" adalah contoh betapa kekuasaan politik telah membuat hukum pidana tidak mandul. Agar kasus-kasus semacam ini tidak terus bermunculan perlu keterlibatan dan peran aktif dari lembaga peradilan Kepolisian, Kejaksaan, Pengadilan, Lembaga Pemasyarakatan menjadi kunci utama Perlindungan Hukum Nasabah Bank Terhadap Tindak Pidana Penipuan Dan Pencurian Data Nasabah Perbankan Melalui Modus Siber Dan Elektronik, namun dalam pelaksanaannya Perlindungan hukum bagi nasabah bank di era siber bukan hanya bergantung pada satu aspek, melainkan kombinasi antara regulasi pemerintah, tanggung jawab bank, dan kesadaran nasabah itu sendiri.

[26] Muladi dan Barda Nawawi Arif, 1992. Bunga Rampai Hukum Pidana. Alumni, Bandung., hlm 157

[27] Muladi dan Barda Nawawi Arif, 1992. Bunga Rampai Hukum Pidana. Alumni, Bandung, hlm.9

PENUTUP

A. Kesimpulan

1. Pengaturan Hukum Tindak Pidana Penipuan dan Pencurian Data Nasabah Perbankan melalui modus Siber dan Elektronik bersifat simbiotik. Hukum melindungi nasabah melalui regulasi yang ketat terhadap bank, namun nasabah juga dituntut untuk menjaga kerahasiaan data pribadi. Pengaturan hukum saat ini mulai bergeser dari sekadar menghukum pelaku (kriminal) menjadi fokus pada tanggung jawab bank sebagai penyelenggara system, namun meskipun regulasi sudah kuat, penegakan hukum di lapangan menghadapi tantangan pada modus Social Engineering (manipulasi psikologis). Secara hukum, jika nasabah secara sadar memberikan data rahasia (OTP/PIN) kepada penipu, bank seringkali terbebas dari tanggung jawab ganti rugi. Oleh karena itu, regulasi kini lebih menekankan pada kewajiban bank untuk menyediakan fitur keamanan berlapis (*Multi-Factor Authentication*).
2. Perlindungan hukum bagi terhadap tindak pidana perbankan di Indonesia berpijak pada dua jalur Preventif (pencegahan melalui pengawasan ketat OJK, prinsip kehati-hatian, dan sistem keamanan IT) serta Represif (penyelesaian sengketa melalui LAPS SJK, ganti rugi perdata berdasarkan Pasal 1367 KUHPerdata, dan penuntutan pidana bagi pelaku). Bank memiliki tanggung jawab yang luas tidak hanya secara personal (oknum), tetapi juga secara korporasi serta penguatan regulasi modern, memperkuat perlindungan terhadap nasabah.

B. Saran

1. Bagi Nasabah (Tindakan Preventif & Represif)
   a) Aktivasi Fitur Keamanan Berlapis: Selalu gunakan *Two-Factor Authentication* (2FA) dan hindari menggunakan jaringan Wi-Fi publik saat melakukan transaksi perbankan.
   b) Prinsip "Zero Trust": Jangan pernah memberikan OTP, PIN, atau data kartu (CVV) kepada siapa pun, termasuk pihak yang mengaku sebagai pegawai bank. Secara hukum, kelalaian ini dapat menggugurkan hak ganti rugi nasabah.
   c) Dokumentasi Cepat: Jika terjadi transaksi mencurigakan, segera ambil tangkapan layar (*screenshot*) dan buat Laporan Sanggahan tertulis ke bank dalam waktu maksimal 24 jam untuk memperkuat posisi tawar nasabah secara hukum.
   d) Gunakan Jalur OJK & LAPS SJK: Jika pengaduan di bank (jalur internal) buntu, jangan ragu untuk melapor ke OJK melalui Aplikasi Portal Perlindungan Konsumen (APPK) karena mediasi di sini lebih efektif dan berbiaya rendah dibandingkan jalur pengadilan.
2. Bagi Institusi Perbankan (Kepatuhan Regulasi)
   a) Audit Keamanan Berkala: Sesuai amanat UU PDP, bank harus melakukan audit sistem keamanan secara rutin untuk memastikan tidak ada celah akses ilegal (hacking).
   b) Transparansi Informasi: Pastikan setiap produk perbankan dijelaskan risiko dan biayanya secara jujur kepada nasabah untuk menghindari sengketa akibat "klausula baku" yang dianggap menjebak.
   c) Peningkatan Kualitas Customer Service: Petugas bank harus dibekali pemahaman hukum perlindungan konsumen agar penanganan pengaduan tidak bersifat defensif, melainkan solutif.

DAFTAR PUSTAKA

BUKU

Adam Chazawi. 2015. Tindak Pidana Informasi Dan Transaksi Elektronik. Penerbit Media Nusa Crative, Jakarta.

Aswan, 2019. Tindak Pidana Penipuan Berbasis Transaksi Elektronik, Guepedia, Bogor.

Hermansyah, 2010. Hukum Perbankan Nasional Indonesia, Ed.2. Penerbit Kencana Prenada Media Group, Jakarta.

Muhammad Mustafa, 2007. Kriminologi, Fisip Ui Press, Depok.

Peter Mahmud, 2011., *Penelitian Hukum*, Penerbit Prenada, Media, Jakarta.

Ruth Devisa Br Sukatendel, 2021. “Peran Otoritas Jasa Keuangan Terhadap Tindak Pidana Penyebaran Data Pribadi Oleh Perusahaan Financial Technology.

Wahyudi Djafar dan Asep Komarudin, 2014. Perlindungan Hak Atas Privasi Di Internet-Beberapa Penjelasan Kunci. Penerbit Elsam, Jakarta

Widodo, (2009), Sistem Pemidanaan Dalam Cyber Crime, Laksbang Mediatama. Yogyakarta.

PERUNDANG-UNDANGAN

Undang-Undang Dasar 1945

KUHPerdata dan KUHPidana

Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan

Undang-Undang Nomor 23 Tahun 1999 tentang Bank Indonesia

Undang-Undang Nomor 6 Tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta Kerja menjadi Undang-Undang yang mengatur tentang Bank Sentral

Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan (PPSK)

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

Undang-Undang No. 11 Tahun 2008 jo. Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik

Undang-Undang No. 8 Tahun 1999 tentang Perlindungan Konsumen
Undang-Undang No. 21 Tahun 2011 tentang OJK

JURNAL

Alamudi, I. A. A. I. A. (2023). Analisis Perundang-undangan: Kajian Kritis Undang-Undang Perbankan Syariah. Qonun Iqtishad EL Madani Journal.

Dian Ekawati, (2018), Perlindungan Hukum Terhadap Nasabah Bank Yang Dirugikan Akibat Kejahatan Skimming Ditinjau Dari Perspeketif Teknologi Informasi Dan Perbankan, UNES Law Review, Vol 1., Issue 2.

Muhammad Prima Ersya, Permasalahan Hukum dalam Menanggulangi Cyber Crime di Indonesia, Jurnal of Moral and Civic Education, Vol. I No. 1, 2017

Rosalinda Elsina Latumahina, 2014. “Aspek Hukum Perlindungan Data Pribadi Di Dunia Maya,” Jurnal Gema Aktualita 3, no. 2

Siti Yuniarti, “Perlindungan Hukum Data Pribadi Di Indonesia,” Jurnal Becoss Vol.1, No. (2019)

INTERNET / WEB

Dr. Hassanain Haykal, S.H., M.Hum. https://www.hukumonline.com/berita/a/tindak-pidana-perbankan-lt61d7e36d85d74?page=3

https://www.kompas.tv/info-publik/624563/10-modus-penipuan-paling-marak-di-indonesia-menurut-ojk?page=2

Etikah Karyani Suwondo Peneliti Senior Core Indonesia https://infobanknews.com/waspada-kejahatan-perbankan-seperti-ini-modus-operasinya/

https://infobanknews.com/waspada-kejahatan-perbankan-seperti-ini-modus-operasinya/

https://infobanknews.com/waspada-kejahatan-perbankan-seperti-ini-modus-operasinya/