BAB I

PENDAHULUAN

A. Latar Belakang

Kemajuan teknologi informasi dan komunikasi telah mempermudah aktivitas perbankan, termasuk dalam hal transaksi. Namun, perkembangan ini juga meningkatkan risiko kejahatan, seperti pembobolan rekening bank melalui phishing. Kejahatan siber semacam ini sulit dilacak dan memberatkan penegakan hukum karena sifatnya yang kompleks. Tindak pidana ITE adalah kejahatan yang menggunakan perangkat elektronik atau komputer yang terhubung ke internet sebagai sarana untuk melakukan pelanggaran hukum.[1]

Kasus pembobolan rekening bank biasanya dilakukan dengan menggunakan modus yang canggih dan terstruktur, Mulai dari penipuan dalam jual beli barang, pemalsuan alamat email, penipuan melalui investasi saham, pembajakan ATM nasabah, hingga rekayasa mesin ATM agar dapat dibobol.[2] Aktivitas ini termasuk dalam kategori tindak pidana pencurian atau penipuan berbasis elektronik, dan dapat dijerat dengan Pasal 30, 32, 35 dan 46 UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang telah diubah oleh UU No. 19 Tahun 2016.[3]

---

[1] Yoanda Tesalonika Lendo, Maarthen Youseph Tampanguma, dan Dicky Janeman Paseki, "Kajian Yuridis terhadap Kejahatan Pembobolan Rekening dalam Kasus Phising di Sektor Perbankan," *Lex Privatum* 15, no. 5 (2025): hlm. 1.

[2] Fajar Januarta Kuwado, *"Waspada, Rekening Nasabah di Indonesia Rentan Dibobol,"* Kompas.com, 2015, https://www.kompas.com.

[3] Undang-Undang 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 tentang Informasi dan Transaksi Elektronik, Pasal 30, Pasal 32, Pasal 35, dan Pasal 46.

Kepolisian Negara Republik Indonesia (Polri) memiliki peran sentral dalam penegakan hukum, terutama terhadap tindak pidana siber (*cybercrime*). Sebagai institusi yang bertanggung jawab atas keamanan dan ketertiban, Polri berada di garis depan dalam menangani kejahatan berbasis teknologi informasi. Sesuai Pasal 13 huruf b Undang-Undang Nomor 2 Tahun 2002, tugas pokok Polri mencakup penegakan hukum.[4] Namun, keberhasilan upaya tersebut juga memerlukan partisipasi aktif masyarakat. Kesadaran hukum publik menjadi faktor penting dalam menciptakan tatanan hukum yang tertib dan berkelanjutan.

Dalam menghadapi kejahatan siber yang terus berkembang, Polri dituntut untuk meningkatkan kapasitas teknologi, sumber daya manusia, dan kerja sama lintas lembaga. Penanganan *cybercrime* tidak hanya membutuhkan pendekatan represif, tetapi juga preventif melalui edukasi hukum dan literasi digital kepada masyarakat. Kolaborasi antara Polri, pemerintah, sektor swasta, dan masyarakat sipil menjadi kunci dalam membangun sistem perlindungan yang adaptif terhadap dinamika kejahatan di era digital.[5]

Menurut Satjipto Rahardjo, penegakan hukum merupakan suatu proses untuk merealisasikan tujuan hukum, yakni mengaktualisasikan gagasan atau kehendak pembentuk undang-undang yang telah dituangkan dalam bentuk peraturan perundang-undangan ke dalam kehidupan nyata.[6]

---

[4] Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia, Pasal 13 huruf b.

[5] Nura Damayanti Ariningsih, Normalita Destyarini, dan Aryono Aryono, "Peran Kepolisian Daerah Jawa Tengah dalam Penegakan Hukum terhadap Tindak Pidana Judi Online," *MANDUB: Jurnal Politik, Sosial, Hukum dan Humaniora*, Vol. 1, No. 3 (September 2023): hlm. 236.

[6] Satjipto Rahardjo, *Masalah Penegakan Hukum*, Sinar baru, Bandung, 1983, hal. 24.

Penegakan hukum dilakukan dengan tujuan menciptakan ketertiban serta kepastian hukum dalam kehidupan sosial masyarakat. Selain itu, penegakan hukum juga berperan sebagai sarana perlindungan terhadap hak dan kepentingan manusia, sehingga hukum harus ditegakkan demi menjamin rasa aman dan keadilan.[7] Dalam upaya memberantas tindak kejahatan, aparat penegak hukum telah mencatat sejumlah kasus pembobolan rekening bank melalui sistem elektronik yang terjadi di wilayah Daerah Istimewa Yogyakarta:[8]

Tahun	Tindak pidana pembobolan rekening bank elekrtonik
2023	13 kasus
2024	26 kasus
2025	18 kasus

Fenomena ini mengindikasikan perlunya peninjauan lebih mendalam terhadap aspek penindakan hukum, khususnya terkait modus operandi pelaku dan strategi penyidikan oleh aparat Kepolisian Daerah Istimewa Yogyakarta. Oleh sebab itu, penelitian ini bertujuan untuk menganalisis peran Kepolisian Daerah Istimewa Yogyakarta dalam menghadapi tantangan pengungkapan kasus pembobolan rekening bank elektronik, serta merumuskan langkah-langkah preventif dan represif yang dapat dioptimalkan. Berdasarkan kutipan diatas, Maka penulis bermaksud untuk melakukan penelitian dengan judul

[7] Sudikno Mertokusumo, *Mengenal Hukum*, Liberty, Yogyakarta, 1999, hal.145.

[8] Wawancara dengan Bripda Alfian Nurfauzi selaku perwakilan Siber Ditreskrimsus Kepolisian Daerah Provinsi Daerah Istimewa Yogyakarta, di Yogyakarta, tanggal 8 Agustus 2025

"**MODUS OPERANDI DAN PENEGAKAN HUKUM OLEH KEPOLISIAN DAERAH ISTIMEWA YOGYAKARTA TERHADAP KASUS PEMBOBOLAN REKENING BANK MELALUI SISTEM ELEKTRONIK"**

B. Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan, maka penelitian ini disusun dengan rumusan masalah, sebagai berikut.

1. Bagaimana modus operandi yang digunakan dalam tindak pidana pembobolan rekening bank melalui akses ilegal terhadap sistem elektronik di Kepolisian Daerah Istimewa Yogyakarta?
2. Bagaimana penegakan hukum oleh Kepolisian Daerah Istimewa Yogyakarta dalam mencegah dan memberantas kejahatan pembobolan rekening bank nasabah melalui sistem elektronik?

C. Tujuan Penelitian

Berdasarkan atas rumusan masalah, Peneliti memiliki tujuan, yaitu:

1. Menganalisis penegakan hukum pidana oleh Kepolisian Daerah Istimewa Yogyakarta dalam mencegah dan memberantas kejahatan pembobolan rekening bank nasabah melalui sistem elektronik.
2. Menganalisis modus operandi yang digunakan dalam tindak pidana pembobolan rekening bank melalui akses ilegal terhadap sistem elektronik di Kepolisian Daerah Istimewa Yogyakarta.

D. Manfaat Penelitian

Pihak terkait diharapkan mendapatkan manfaat dari hasil penelitian empiris yang dilakukan oleh peneliti yaitu:

1. Manfaat Kepolisian Daerah Istimewa Yogyakarta

   Hasil penelitian ini dapat menjadi referensi guna untuk penyumbangan gagasan atau ide-ide dalam suatu pengungkapan untuk menangani kasus modus operandi pembobolan rekening bank melalui sistem elektronik.

2. Manfaat Masyarakat di Wilayah DIY

   Hasil penelitian ini dapat menjadi referensi guna untuk penyumbangan gagasan atau ide-ide dalam pengetahuan bahaya modus operandi pembobolan rekening bank melalui sistem elektronik oleh seluruh masyarakat di wilayah DIY dengan mengetahui segala bentuk modus operandi yang digunakan pelaku pembobolan rekening bank memalui sistem elektronik. Selain itu, Penelitian ini diharapkan dapat memberi pemahaman praktis agar masyarakat lebih waspada dan berhati-hati akan bahaya tindak pidana melalui media sosial elektronik (*cybercrime*) terutama tindak pidana pembobolan rekening bank melalui sistem elektronik untuk sekitar wilayah Daerah Istimewa Yogyakarta.

3. Manfaat Penelitian

   Hasil penelitian ini diharapkan dapat menambah ilmu pengetahuan dan menambah wawasan tentang analisis peran Kepolisian Daerah Istimewa Yogyakarta dalam penegakan dan mengungkap kasus modus

operandi pembobolan rekening bank melalui sistem elektronik di wilayah Daerah Istimewa Yogyakarta.

E. Orisinalitas Penelitan

Orisinalitas penelitian ini ditunjukkan melalui perbedaan fokus kajian antara penelitian yang dilakukan oleh peneliti dengan studi-studi sebelumnya. Hal ini bertujuan untuk menghindari tumpang tindih topik kajian dan memastikan bahwa penelitian ini memiliki kontribusi baru. Untuk mempermudah pemahaman terhadap perbedaan tersebut, peneliti menyajikannya dalam bentuk tabel perbandingan, yang dinilai lebih efektif dibandingkan dengan penyajian secara naratif. Oleh karena itu, peneliti menampilkan tiga contoh penelitian terdahulu sebagai bahan perbandingan dalam bentuk tabel berikut :

No.	Nama Penliti	Judul	Perbandingan
1.	Hizkia Eliezer Malalangi	Pertanggung jawaban pidana pelaku pembobolan kartu kredit dengan modus carding menurut undang-undang informasi dan transaksi elektronik	Fokus permasalahan dalam penelitian lebih menekankan analisis normatif terhadap pertanggungjawaban pidana pelaku carding berdasarkan UU ITE. sedangkan fokus permasalahan yang diteliti penulis adalah Modus operandi dan penegakan hukum oleh Kepolisian Daerah Istimewa Yogyakarta terhadap kasus pembobolan rekening melalui sistem elektronik.

2	Gibran Mahendra Dewantara	Penegakan Hukum terhadap Pelaku Tindak Pidana Cyber Crime Metode Phising oleh Kepolisian Daerah Provinsi Daerah Istimewa Yogyakarta.	Fokus permasalahan dalam penelitian lebih menekankan analisis hukum terhadap pelaku phishing sebagai bentuk cybercrime yang diteliti penulis adalah Modus operandi dan penegakan hukum oleh Kepolisian Daerah Istimewa Yogyakarta terhadap kasus pembobolan rekening melalui sistem elektronik.
3	Dwi Aprilia Ghoniyantun	Strategi pengembangan kompetensi Subdit V Siber Polda DIY dalam pengungkapan kasus cyber crime di wilayah Daerah Istimewa Yogyakarta.	Fokus permasalahan dalam penelitian lebih menekankan pada peningkatan kompetensi personel Subdit V Siber Polda DIY yang diteliti penulis adalah Modus operandi dan penegakan hukum oleh Kepolisian Daerah Istimewa Yogyakarta terhadap kasus pembobolan rekening melalui sistem elektronik.

Berdasarkan kajian terhadap penelitian-penelitian sebelumnya, diketahui bahwa belum ditemukan studi yang secara khusus mengulas mengenai modus operandi serta upaya penegakan hukum oleh Kepolisian Daerah Istimewa Yogyakarta dalam menangani kasus pembobolan rekening bank melalui sistem elektronik. Oleh karena itu, orisinalitas penelitian ini dapat dibuktikan. Selain

itu, penelitian ini disusun tanpa unsur plagiarisme dan telah mencantumkan sumber-sumber relevan dari penelitian terdahulu sebagai landasan konseptual.

F. Tinjauan Pustaka

1. Tindak Pidana *Cyber Crime*

Tindak pidana *cyber crime* merupakan jenis kejahatan yang memiliki karakteristik berbeda dari kejahatan konvensional. Kejahatan ini muncul sebagai dampak dari kemajuan teknologi informasi. Salah satu ciri khas dari revolusi teknologi informasi adalah interaksi sosial yang tidak lagi membutuhkan kehadiran fisik secara langsung. Dalam konteks ini, bentuk penyimpangan sosial juga ikut berkembang dan menyesuaikan diri dengan pola serta karakteristik kejahatan yang baru.[9]

Dengan demikian, tindak pidana *cyber crime* dapat dipahami dalam dua perspektif, yaitu sempit dan luas. Dalam pengertian sempit, kejahatan siber merujuk pada tindakan melawan hukum yang dilakukan melalui pemanfaatan teknologi komputer. Sementara itu, dalam pengertian yang lebih luas, *cyber crime* mencakup seluruh bentuk kejahatan yang menyasar sistem komputer, jaringan, maupun penggunanya, termasuk juga kejahatan konvensional yang dilakukan dengan bantuan teknologi komputer.

Dalam kerangka peraturan perundang-undangan di Indonesia, tindak pidana *cyber crime* kerap diklasifikasikan sebagai kejahatan yang

[9] Didik M. Arief Mansur dan Elisatris Gultom, Cyber Law Aspek Hukum Teknologi Informasi, Refika Aditama, Bandung, 2005, hlm. 25.

berkaitan erat dengan pemanfaatan teknologi informasi. Salah satu definisi yang digunakan menyatakan bahwa penyalahgunaan komputer secara umum diartikan sebagai suatu peristiwa yang melibatkan teknologi komputer, di mana pihak korban mengalami atau berpotensi mengalami kerugian, sementara pelaku secara sadar dan terencana memperoleh, atau berpeluang memperoleh, keuntungan dari tindakan tersebut.[10]

2. Pembobolan Rekening Bank Elektronik

Pembobolan rekening bank merupakan suatu tindakan kejahatan dalam sektor perbankan yang dilakukan dengan cara mengakses secara ilegal, mencuri, atau memalsukan data serta identitas korban guna mengambil hak milik korban untuk memperoleh keuntungan pribadi.[11] Dalam sektor perbankan, kejahatan ini kerap dilakukan melalui berbagai teknik, seperti memanfaatkan metode manipulasi teknologi seperti *phishing, malware*, atau teknik SIM *swap*, tindakan ini diklasifikasikan sebagai kejahatan siber karena dilakukan melalui media elektronik serta berkaitan dengan pelanggaran terhadap sistem keamanan data.

Secara Istilah pembobolan menggambarkan suatu tindakan atau proses merusak atau menembus suatu sistem atau penghalang. Membobol dapat dimaknai sebagai tindakan menerobos,

[10] Andi Hamzah, Hukum Pidana yang berkaitan dengan komputer, Sinar Grafika Offset, Jakarta, 1993, hlm. 18.

[11] Barda Nawawi Arif , Sari Kuliah Hukum Pidana II. Fakultas Hukum Undip.1984, hlm: 37

menghancurkan, merusak secara paksa, atau melakukan penetrasi dengan unsur kekerasan maupun paksaan.[12]

Tindakan pembobolan rekening bank dapat dikenakan sanksi pidana berdasarkan ketentuan dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang tentang Transfer Dana, serta Kitab Undang-Undang Hukum Pidana (KUHP) yang mengatur mengenai tindak pidana pencurian dan penipuan. Di samping itu, pihak bank juga memiliki kewajiban hukum untuk memberikan perlindungan dan ganti rugi kepada nasabah apabila pembobolan tersebut terjadi akibat kelalaian di pihak bank.

Dasar hukum terkait pembobolan rekening bank meliputi beberapa peraturan perundang-undangan di Indonesia, antara lain:

a) Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) No. 11 Tahun 2008, khususnya Pasal 30 ayat (1), ayat (3), dan Pasal 32 ayat (2) yang mengatur tentang akses ilegal ke sistem elektronik, perusakan, dan pemindahan informasi elektronik tanpa hak[13], yang berbunyi :

   Pasal 30

[12] I Nyoman Putu Budiartha dan I Nyoman Gede Sugiartha, "Sanksi Pidana Terhadap Tindak Pidana Pembobolan Rekening Melalui Anjungan Tunai Mandiri (ATM)," *Analogi Hukum: Jurnal Ilmiah Ilmu Hukum Fakultas Hukum Universitas Warmadewa*, Vol. 2, No. 2 (2020): hlm. 235.

[13] *Undang-Undang Nomor 11 Tahun 2008...*, *Op.Cit.*, Pasal 30 dan Pasal 32.

Ayat (1), Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.

Ayat (3), Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Pasal 32

Ayat (2), Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.

b) Kitab Undang-Undang Hukum Pidana (KUHP), khusunya pasal Pasal 362 tentang pencurian, Pasal 263 ayat (1) dan (2) terkait pemalsuan surat yang dapat menimbulkan kerugian.[14]

c) Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan.[15]

3. Modus Operandi dalam Kejahatan Siber

Modus operandi merupakan istilah asal bahasa Latin yang secara harfiah berarti “cara bertindak” atau “cara melakukan.” Dalam konteks

[14] Kitab Undang-Undang Hukum Pidana (KUHP), Pasal 362, Staatsblad Tahun 1915 Nomor 732 sebagaimana telah diubah dan ditambah.

[15] Undang-Undang Republik Indonesia Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan, Lembaran Negara Republik Indonesia Tahun 1998 Nomor 182, Tambahan Lembaran Negara Republik Indonesia Nomor 3790.

kriminologi, istilah ini menunjukkan pola khas atau teknik tertentu yang digunakan pelaku dalam melancarkan kejahatan mulai dari perencanaan, pelaksanaan, hingga upaya menyembunyikan jejak atau melarikan diri. Pola ini tidak hanya membantu penegak hukum mengenali ciri pelaku, tetapi juga mengkaitkan sejumlah tindak kejahatan yang mungkin dilakukan oleh orang yang sama.[16]

Faktor-faktor seperti kondisi sosial, ekonomi, dan psikologis turut membentuk keputusan individu, yang pada akhirnya menentukan tindakan mereka sesuai dengan keinginan pribadi. Modus operandi merupakan teknik dan metode operasional khas yang digunakan oleh pelaku kriminal untuk menjalankan tindakan pidana, dimulai dari perencanaan hingga eksekusi kejahatan.[17] Beberapa modus umum dalam pembobolan rekening bank antara lain:

a. Phising merupakan tindakan penipuan yang dilakukan dengan cara mengecoh target untuk mencuri akun miliknya, biasanya melalui penyebaran pesan massal seperti email palsu yang berisi informasi menyesatkan dan mengarahkan korban ke situs tiruan. Situs tersebut dirancang agar korban secara tidak sadar memberikan akses akun kepada pelaku. Meski demikian, praktik phishing masih menyimpan

[16] Moeljatno, *Modus Operandi Hukum Pidana*, Bina Aksara, Jakarta, 2015, hlm. 9

[17] R. Soesilo. *Taktik dan Teknik Penyidikan Perkara Kriminil.* Bandung: PT. Karya Nusantara 1980, hlm 98

sejumlah ketidakjelasan, khususnya terkait pola atau modus operandi yang digunakan oleh pelaku.[18]

b. Malware singkatan dari *malicious software*, adalah jenis perangkat lunak berbahaya yang sengaja dirancang untuk menyerang sistem operasi. Setelah berhasil masuk ke sistem pengguna tanpa disadari, malware dapat merusak atau mengganggu fungsi dasar sistem tersebut. Selain itu, malware menggunakan sumber daya perangkat seperti CPU, memori, dan jaringan secara diam-diam, serta mengumpulkan data pribadi (seperti kredensial, riwayat aktivitas, atau informasi keuangan), lalu mengirimkannya ke pihak ketiga tanpa izin pengguna.[19]

c. SIM Swap Fraud merupakan kejahatan siber di mana pelaku mengambil alih nomor ponsel korban dengan mengalihkan kartu SIM ke perangkat milik mereka. Setelah berhasil, penipu akan menerima kode OTP yang biasanya dikirim via SMS, sehingga mereka dapat memasuki akun penting seperti perbankan, dompet digital, e-commerce, maupun media sosial milik korban secara mudah.[20]

---

[18] Vikran Fasyadhiyaksa Putra Y, "Modus Operandi Tindak Pidana Phising Menurut UU ITE," *Jurist Diction*, Vol. 4, No. 6 (November 2021): 2525.

[19] Aura Nasha Ramadhanti, Tessa Ayuning Tias, Erin Dwi Lestari, dan Asmak Ul Hosnah, "Cara Operasi Kejahatan Phising di Ranah Siber yang Diatur Oleh Hukum Positif Indonesia," *Jurnal Pendidikan Tambusai* 8, no. 1 (April 2024): 1299–1305, https://doi.org/10.31004/jptam.v8i1.12549

[20] **"**SIM Swap Fraud: Pengertian, Cara Kerja, dan Cara Menghindarinya**,"** *Vida*, diakses 4 Juli 2025, *judul halaman*, tersedia di https://vida.id/id/blog/sim-swap-fraud

d. Social engineering merupakan taktik manipulasi psikologis yang digunakan oleh penipu untuk menipu korban agar mengungkapkan informasi pribadi seperti kata sandi, data kartu kredit, atau akses ke akun penting. Teknik ini tidak selalu melibatkan kecanggihan teknologi; sebaliknya, pelaku memanfaatkan kelengahan dan rasa percaya korban. Dengan mengeksploitasi emosi seperti rasa takut, urgensi, atau simpati, penipu berhasil membuat korban secara sukarela menyerahkan data sensitif tanpa disadari.[21]

4. Penegak Hukum

Penegakan hukum adalah proses yang dilakukan untuk memastikan bahwa norma-norma hukum benar-benar dijalankan sebagai acuan perilaku dalam interaksi hukum di tengah masyarakat dan negara. Selain itu, penegakan hukum juga mencerminkan implementasi nyata dari aturan hukum, dengan tujuan mewujudkan nilai-nilai keadilan, kepastian hukum, serta manfaat sosial yang dapat dirasakan dalam kehidupan sehari-hari.[22]

Penegakan hukum pidana yang efektif sangat bergantung pada keberadaan unsur moral. Unsur ini mencerminkan nilai-nilai etis dan rasa tanggung jawab dalam hubungan antara norma hukum dan nilai

[21] **“**Waspada Jangan Mudah Tertipu, Kenali Apa Itu Social Engineering**,”** *Eraspace*, diterbitkan sekitar 3 bulan lalu, diakses 4 Juli 2025, tersedia di https://eraspace.com/artikel/post/waspada-jangan-mudah-tertipu-kenali-apa-itu-social-engineering?

[22] Satjipto Raharjo, Hukum dan Masyarakat, Angkasa, Bandung, 1980, hlm. 15.

kemanusiaan. Moralitas menjadi fondasi yang menentukan keberhasilan penegakan, karena upaya penegakan hukum tidak cukup hanya berdasarkan prosedur teknis, melainkan harus dijalankan secara adil dan objektif. Proses menemukan fakta pun harus bebas dari bias, memecahkan masalah dengan penuh integritas, serta menjunjung tinggi keadilan dan kelayakan setiap keputusan.[23]

Penegakan hukum dapat ditempuh melalui dua pendekatan, yaitu pencegahan (preventif) dan penindakan (represif). Kedua pendekatan ini dapat dilaksanakan baik melalui mekanisme hukum pidana maupun di luar sistem hukum pidana. Upaya preventif di luar jalur pidana bertujuan mencegah terjadinya tindak pidana tanpa menggunakan sanksi pidana, serta dapat dilakukan oleh masyarakat maupun aparat penegak hukum. Sementara itu, pendekatan represif dalam ranah hukum pidana dilakukan setelah tindak pidana terjadi, sebagai bentuk penindakan dan proses hukum terhadap pelaku.

G. Definisi Operasional

Untuk mempermudah dalam analisis dan pembahasan hasil penelitian yang berjudul "MODUS OPERANDI DAN PENEGAKAN HUKUM OLEH KEPOLISIAN DAERAH ISTIMEWA YOGYKARTA" terhadap kasus pembobolan rekening bank melalui sistem elektronik, Maka diperlukan definisi operasional. Adapun definisi operasional pada penelitian sebagai berikut:

1. Tindak Pidana *Cyber Crime*

[23] Muladi, Hak Asasi Manusia, Refika Aditama, Bandung, 2009, hlm. 4.

Tindak Pidana *Cyber* Crime didefinisikan secara operasional dalam dua perspektif: (1) dalam arti sempit, yaitu tindakan ilegal yang dilancarkan langsung menggunakan teknologi komputer atau jaringan, seperti akses tanpa izin, penyebaran malware, dan intersepsi data sesuai dengan pasal-pasal dalam UU ITE yang secara khusus mengatur kejahatan siber; (2) dalam arti luas, mencakup semua bentuk kejahatan, termasuk kejahatan konvensional yang dilakukan dengan memanfaatkan sistem elektronik sebagai sarana, seperti pembobolan rekening bank atau penipuan online. Selanjutnya, penyalahgunaan komputer diartikan sebagai tindakan yang sengaja dan direncanakan, menggunakan sistem elektronik untuk merugikan korban sekaligus memberikan keuntungan kepada pelaku, misalnya melalui manipulasi data atau transfer dana tanpa izin indikatornya dapat terlihat dari bukti akses ilegal dan transfer mencurigakan dalam kasus di Kepolisian Daerah Istimewa Yogyakarta.

2. Pembobolan Rekening Bank Elektronik

Pembobolan rekening bank adalah kejahatan siber di sektor perbankan di mana pelaku secara ilegal mengakses atau memalsukan data dan identitas korban untuk memperoleh asetnya, biasanya melalui teknik phishing, malware, atau SIM swap. Istilah ini merujuk pada tindakan paksa memasuki sistem yang dilindungi. Pelaku dapat dikenai sanksi berdasarkan UU ITE No. 11/2008 (Pasal 30 dan 32), KUHP (Pasal 362 dan 263), dan UU Perbankan No. 10/1998. Selain itu, bank

wajib memberikan perlindungan serta ganti rugi jika pembobolan terjadi karena kelalaian mereka.

3. Modus Operandi dalam Kejahatan Siber

Modus operandi adalah frasa Latin yang berarti “cara beroperasi”. Dalam kriminologi, istilah ini menunjuk pada pola atau metode khas yang berulang kali digunakan oleh pelaku mulai dari persiapan, eksekusi, hingga pelarian sehingga dapat membantu penegak hukum mengenali dan menghubungkan kejahatan yang dilakukan oleh orang yang sama.[24] Beberapa modus umum dalam pembobolan rekening bank antara lain :

a. Phising, metode penipuan melalui email, SMS, atau situs palsu yang meniru lembaga resmi untuk mencuri data seperti login dan kata sandi korban.
b. Malware perangkat lunak berbahaya yang diam-diam menginfeksi sistem, mencuri data, dan mengirimkannya ke penyerang.
c. SIM Swap Fraud pelaku menipu operator seluler agar nomor korban dipindahkan ke SIM miliknya, sehingga bisa menerima kode OTP dan mengakses akun digital korban.

[24] R. Soesilo. *Taktik dan Teknik Penyidikan Perkara Kriminil.* Bandung: PT. Karya Nusantara 1980, hlm 98.

d. *Social engineering* taktik psikologis yang mengeksploitasi kepercayaan atau emosi korban, tanpa memerlukan teknologi canggih, untuk mengungkapkan informasi sensitif.

4. Penegak Hukum

Penegakan hukum adalah serangkaian upaya institusional untuk menerapkan norma hukum dalam kehidupan bermasyarakat dan bernegara, bertujuan mewujudkan tiga nilai utama: keadilan, kepastian hukum, dan kemanfaatan sosial.

H. Metode Penelitian

Penelitian merupakan suatu upaya ilmiah yang sistematis dan objektif untuk mencari kebenaran atas temuan terutama yang dikemukakan oleh para ahli terpercaya. Dalam proses ini, peneliti melakukan investigasi terstruktur, mulai dari pengumpulan, analisis, hingga interpretasi data, dengan tujuan mengonfirmasi atau menolak pendapat ilmiah sebelumnya.[25] Adapun metode penelitian yang digunakan dalam menyusun skripsi ini, diuraikan lebih rinci sebagai berikut:

1. Tipologi Penelitian

Metode penelitian yang digunakan penulis adalah yuridis empiris, yaitu metode yang menggabungkan analisis terhadap norma hukum (yuridis) dengan verifikasi melalui fakta atau data empiris di lapangan. Metode ini mengkaji penerapan hukum normatif seperti undang-undang

[25] Soejono Soekanto, *Pengantar Penelitian Hukum*, Penerbit Universitas Indonesia (UI Press), Jakarta, , 2014, hlm. 9

dan kontrak dalam praktik nyata masyarakat (*in action*), dengan tujuan mengevaluasi efektivitas dan implementasi ketentuan hukum tersebut.[26]

2. Pendekatan Penelitian

   Metode penelitian yang digunakan adalah pendekatan sosiologis, yang menyelidiki objek penelitian berdasarkan interaksi sosial di lapangan dengan tujuan menggali data primer dari masyarakat secara langsung. Pendekatan ini menempatkan hukum sebagai fenomena sosial nyata dan relevan dalam konteks kehidupan masyarakat, serta memadukan observasi lapangan dan wawancara untuk memahami bagaimana norma hukum diimplementasikan dalam praktik sehari-hari.

3. Objek Penelitian

   Objek penelitian adalah fokus utama studi seperti fenomena, perilaku, dokumen, atau data yang dipilih peneliti untuk dikaji secara mendalam. Elemen ini berfungsi sebagai sumber informasi utama dalam menjawab permasalahan penelitian, Objek penelitian ini meliputi:

   a. Bagaimana modus operandi yang digunakan dalam tindak pidana pembobolan rekening bank melalui akses ilegal terhadap sistem elektronik di Kepolisian Daerah Istimewa Yogyakarta.
   b. penegakan hukum pidana oleh Kepolisian Daerah Istimewa Yogyakarta dalam mencegah dan

[26] Abdul Kadir Muhammad, *Hukum dan Penelitian Hukum*, Citra Aditya Bakti, Bandung, 2004, hlm. 134.

memberantas kejahatan pembobolan rekening bank nasabah melalui sistem elektronik.

4. Sumber Data Penelitian

Jenis penelitian ini adalah penelitian yuridis-empiris. Sumber data yang diperlukan dalam penelitian ini yaitu menggunakan data primer dan sekunder. Sebagai berikut:

a. Data primer adalah data yang diperoleh penulis secara langsung dari subjek penelitian yang dapat berupa hasil wawancara yang dilakukan kepada Satuan Reserse dan Kriminal (Satreskrim) Polisi Daerah Istimewa Yogyakarta.
b. Data sekunder adalah data yang diperoleh dari bahan-bahan hukum primer, sekunder dan tersier.
    1) Bahan Hukum Primer adalah bahan hukum yang bersifat kekuatan mengikat (*binding*). Pada penelitian ini menggunakan beberapa bahan hukum primer yaitu:
        a) Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;
        b) Kitab Undang-Undang Hukum Pidana;

c) Undang-Undang Nomor 10 tahun 1998 tentang perubahan atas Undang-Undang Nomor 7 tahun 1992 tentang Perbankan.

d) Undang-Undang Republik Indonesia Nomor 8 Tahun 1981 Tentang Hukum Acara Pidana

2) Bahan hukum sekunder merupakan sumber informasi yang tidak bersifat mengikat secara langsung, namun berperan penting dalam menjelaskan dan mendukung pemahaman terhadap bahan hukum primer. Contohnya meliputi buku-buku teks hukum, jurnal ilmiah, artikel hukum, hasil penelitian, dan karya ilmiah lainnya yang relevan dengan topik penelitian. Sumber-sumber ini membantu memperluas perspektif dan memberikan konteks yang lebih mendalam terhadap peraturan perundang-undangan atau ketentuan hukum yang menjadi fokus kajian.

3) Bahan hukum tersier merupakan referensi penunjang yang memberikan pedoman dan penjelasan mengenai bahan hukum primer dan sekunder. Contohnya termasuk kamus hukum, Kamus Besar Bahasa Indonesia (KBBI), ensiklopedia hukum, dan

sumber sejenis yang membantu memperjelas istilah atau konsep hukum utama.

5. Subjek Penelitian

Subjek penelitian dalam penelitian ini adalah Satuan Reserse dan Kriminal (Satreskrim) Polisi Daerah Istimewa Yogyakarta.

6. Lokasi Penelitian

Polisi Daerah Istimewa Yogyakarta di Jl. Ring Road Utara, Sanggrahan, Condongcatur, Kec. Depok, Kabupaten Sleman, Daerah Istimewa Yogyakarta 55283.

7. Teknik Pengumpulan data

Metode pengumpulan data yang digunakan pada penelitian yaitu:

a. Wawancara adalah teknik pengumpulan data berupa interaksi tanya jawab secara langsung antara peneliti dan responden atau narasumber. Tujuannya adalah menggali informasi yang relevan dengan masalah penelitian dari sumber primer yang diwawancarai.
b. Studi dokumen adalah teknik pengumpulan data yang dilakukan melalui penelaahan dan analisis dokumen baik berupa tulisan, gambar, maupun media elektronik. Dokumen yang dikumpulkan dipilih sesuai dengan fokus penelitian, kemudian diuraikan, dibandingkan, dan disintesiskan hingga membentuk hasil kajian yang sistematis, terpadu, dan

menyeluruh. Teknik ini tidak sekadar mengutip, tetapi melaporkan hasil analisis kritis terhadap dokumen tersebut.

c. Studi pustaka adalah metode pengumpulan data yang dilakukan dengan menelaah sumber-sumber pustaka meliputi membaca, mencatat, serta mengolah materi penelitian. Aktivitas ini bertujuan untuk mengumpulkan informasi dari berbagai koleksi seperti buku, jurnal, ensiklopedi, artikel, atau media lain yang relevan, dan diolah hingga menghasilkan pemahaman yang komprehensif terhadap topik yang diteliti.

8. Teknik Analisis Data

Analisis data merupakan tahapan penelitian yang dilakukan dengan menelaah hasil pengolahan data menggunakan landasan teori yang telah diperoleh sebelumnya. Data yang dikumpulkan dari studi kepustakaan maupun penelitian lapangan kemudian dianalisis secara deskriptif kualitatif, yakni dengan menghimpun, mengolah, dan menafsirkan data sesuai dengan permasalahan penelitian. Hasil analisis tersebut disusun secara sistematis, dikaji secara mendalam, lalu ditarik kesimpulan untuk menjawab rumusan masalah dalam penelitian ini.

I. Sistematis Penulisan

1. BAB I PENDAHULUAN

BAB I ini berisi penjabaran mengenai latar belakang permasalahan, rumusan masalah, tujuan dan manfaat penelitian, orisinalitas studi, tinjauan pustaka, definisi operasional, metode penelitian, serta sistematika penulisan karya ilmiah.

2. BAB II TINJAUAN UMUM

   BAB II ini memuat penjelasan mengenai tindak pidana *cyber crime*, pembobolan rekening bank elektronik, modus operandi dalam kejahatan siber, penegak hukum.

3. BAB III PENELITIAN DAN PEMBAHASAN

   BAB III dalam penulisan ini akan berisi hasil penelitian dan analisis jawaban dari rumusan masalah yang sedang diangkat oleh penulis yaitu Bagaimana penegakan hukum pidana oleh Kepolisian Daerah Istimewa Yogyakarta dalam mencegah dan memberantas kejahatan pembobolan rekening bank nasabah melalui sistem elektronik dan Bagaimana modus operandi yang digunakan dalam tindak pidana pembobolan rekening bank melalui akses ilegal terhadap sistem elektronik di Kepolisian Daerah Istimewa Yogyakarta.

4. BAB IV PENUTUP

   BAB IV akan disampaikan kesimpulan atas hasil penelitian disertai dengan saran.

BAB II