BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Perkembangan teknologi informasi telah memberikan dampak yang signifikan terhadap berbagai aspek kehidupan masyarakat, termasuk dalam sektor perbankan yang saat ini semakin mengandalkan sistem elektronik untuk mendukung berbagai layanan transaksi keuangan. Kehadiran mesin Anjungan Tunai Mandiri (ATM) sebagai bagian dari sistem elektronik perbankan telah memberikan kemudahan, kecepatan, dan efisiensi dalam melakukan transaksi.[1] Namun, perkembangan teknologi juga membuka peluang munculnya berbagai bentuk kejahatan baru yang memanfaatkan sistem elektronik sebagai sasaran maupun sarana kejahatan. Salah satu bentuk kejahatan yang mengalami perkembangan cukup pesat adalah kejahatan siber (*cybercrime*), khususnya tindak pidana akses ilegal (*illegal access*) terhadap sistem elektronik.[2]

Salah satu fenomena yang menarik untuk dikaji adalah pembobolan ATM menggunakan metode *jackpotting* yang dilakukan oleh warga negara Bulgaria. Kasus tersebut tidak hanya menimbulkan kerugian materiil, tetapi juga menunjukkan adanya indikasi perkembangan pola kejahatan terhadap sistem elektronik perbankan yang berbeda dari teknik konvensional seperti

[1] "ATM Adalah: Pengertian, Jenis, Manfaat, dan Keuntungan," OCBC, terdapat dalam https://www.ocbc.id/id/article/2022/03/11/atm-adalah, Diakses tanggal 30 Maret 2026.

[2] Rafi Septia Budianto Pansariadi dan Noenik Soekorini, "Tindak Pidana Cyber Crime dan Penegakan Hukumnya," *Binamulia Hukum*, No. 2 Vol. 12, 2023, hlm. 291.

skimming.[3] *Skimming* berfokus pada pencurian data kartu dan informasi pribadi nasabah, sedangkan *jackpotting* menargetkan sistem internal mesin ATM secara langsung sehingga pelaku dapat mengendalikan fungsi mesin untuk mengeluarkan uang tanpa transaksi yang sah. Karena tidak melibatkan transaksi nasabah, pengurasan uang melalui metode ini sulit terdeteksi pada tahap awal. Tindak pidana akses ilegal tersebut diatur dalam Pasal 30 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (yang selanjutnya disebut UU ITE).[4] Dalam kasus ini, tindak pidana tersebut dilakukan oleh empat orang dengan peran yang berbeda: dua pelaku lapangan yang melakukan pembongkaran fisik secara langsung terhadap mesin ATM, satu koordinator yang mengatur operasi sindikat, dan satu operator yang mengendalikan sistem ATM melalui aplikasi *remote access* yang sah dan tersedia secara umum.[5]

Kedua pelaku lapangan telah berhasil ditangkap dan diproses secara hukum, karena *locus delicti* serta alat bukti fisik maupun digitalnya jelas berada di wilayah hukum Indonesia, sehingga penegakan hukum terhadap keduanya tidak menghadapi persoalan yurisdiksi. Persoalan yang kompleks muncul pada koordinator dan operator pengendali sistem yang hingga saat

[3] Victoria Linggoraharjo, "Tanggung Jawab Kejahatan Perbankan Melalui Modus Operandi Skimming," *Jurnal Magister Hukum ARGUMENTUM*, No. 1 Vol. 7, Universitas Surabaya, 2020, hlm. 35.

[4] Arifuddin Aljundani dan Niru Anita Sinaga, "Penegakan Hukum Terhadap Pelaku Tindak Pidana Siber Tentang Akses Ilegal Di Indonesia," *Lex Laguens: Jurnal Kajian Hukum dan Keadilan*, No. 2 Vol. 3, 2025, hlm. 176.

[5] Wawancara dengan Tri Purnomo Sidhi, Pemangku Sementara Kasubnit 1 Satuan Reserse Kriminal Polresta Yogyakarta, di Yogyakarta, 4 Mei 2026.

ini belum tertangkap: keterlibatan koordinator sulit ditindaklanjuti karena statusnya masih Daftar Pencarian Orang (DPO), sedangkan operator pengendali sistem diduga beroperasi dari luar wilayah Indonesia, sehingga penegakan hukum terhadap keduanya terkendala oleh belum dapat dipastikannya identitas dan keberadaan pelaku yang justru menjadi prasyarat bekerjanya mekanisme kerja sama hukum lintas negara.[6] Dengan demikian, kompleksitas hukum dalam kasus ini tidak terletak pada kewarganegaraan asing pada para pelaku yang tertangkap, melainkan pada kesenjangan antara keberhasilan penegakan hukum terhadap pelaku lapangan dan kegagalan menjangkau pelaku yang justru mengendalikan jalannya kejahatan.

Kondisi tersebut menunjukkan adanya pergeseran bentuk kejahatan dari tindakan fisik terhadap objek kejahatan menjadi pengambilalihan kendali terhadap sistem elektronik.[7] Pergeseran ini dapat dijelaskan melalui pendekatan kriminologi *Routine Activity Theory*.[8] Pendekatan ini relevan digunakan untuk menjelaskan pola keterlibatan pelaku yang tidak seragam dalam kasus ini, baik yang bertindak secara fisik terhadap mesin ATM maupun yang mengendalikan sistem dari jarak jauh.

---

[6] Wawancara dengan Tri Purnomo Sidhi, Pemangku Sementara Kasubnit 1 Satuan Reserse Kriminal Polresta Yogyakarta, di Yogyakarta, 4 Mei 2026; Putusan Pengadilan Negeri Yogyakarta No. 391/Pid.Sus/2023/PN Yyk, hlm. 65; Putusan Pengadilan Tinggi Yogyakarta (Putusan Banding) No. 25/PID.SUS/2024/PT YYK, hlm. 11.

[7] Adami Chazawi dan Ardi Ferdian, *Tindak Pidana Informasi dan Transaksi Elektronik*, Bayumedia Publishing, Malang, 2015, hlm. 145.

[8] Mohd. Kharris Maulana dan M. Khasali Hakim, "Analisis Kasus Tindak Pidana Pencurian Uang ATM oleh Petugas Pengisi Uang di Kota Batam Menggunakan Routine Activity Theory (RAT)," *Mahkamah: Jurnal Riset Ilmu Hukum*, Edisi No. 4 Vol. 2, 2025, hlm. 80.

Dalam praktik kejahatan siber perbankan, modus akses ilegal dilakukan dengan mengeksploitasi kelemahan perangkat lunak (*software*) atau sistem operasi yang dijalankan mesin ATM, sehingga memaksa mesin ATM mengeluarkan uang tunai secara terus-menerus tanpa transaksi yang sah, dikenal dengan istilah teknis *jackpotting*.[9] *Jackpotting* dapat dilakukan baik dengan menanamkan perangkat lunak berbahaya (*malware*) yang dirancang khusus untuk sistem operasi ATM, maupun dengan menyalahgunakan perangkat lunak akses jarak jauh (*remote access software*) yang secara umum legal,[10] sebagaimana terjadi dalam kasus tersebut. Modus serupa sebelumnya juga pernah terjadi pada salah satu ATM Bank NTB Syariah yang mengakibatkan kerugian hingga Rp528.000.000,00.[11] Berulangnya modus ini pada perbankan yang berbeda menunjukkan bahwa *jackpotting* bukan sekadar insiden tunggal, melainkan pola kejahatan yang berpotensi terus berkembang pada sistem elektronik perbankan di Indonesia. Istilah *jackpotting* yang digunakan secara konsisten dalam penelitian ini merujuk pada tindak pidana akses ilegal terhadap sistem ATM sebagaimana diatur dalam Pasal 30 UU ITE, sebagaimana dijelaskan di atas.

---

[9] "Tim Tanggap Insiden Siber Nasional, FBI Keluarkan Peringatan Serangan ATM," terdapat dalam https://csirt.or.id/berita/fbi-keluarkan-peringatan-serangan-atm, Diakses tanggal 30 Maret 2026.

[10] "Kenali ATM *Jackpotting*, Serangan yang Bisa Kurasi Uang ATM," CyberHub Indonesia, terdapat dalam https://cyberhub.id/pengetahuan-dasar/mengenal-atm-*jackpotting*, Diakses tanggal 30 Maret 2026.

[11] Uang Rp528 Juta di ATM Bank NTB Syariah Raib akibat Aksi "*Jackpotting*", ANTARA News Mataram, terdapat dalam https://mataram.antaranews.com/berita/252336/uang-rp528-juta-di-atm-bank-ntb-syariah-raib-akibat-aksi-*jackpotting*, Diakses tanggal 31 Maret 2026.

Kompleksitas kasus ini juga tampak dari sifatnya sebagai kejahatan siber lintas negara (*borderless crime*) yang melibatkan sindikat internasional sebagaimana telah diuraikan sebelumnya. Dimensi transnasional tersebut menjadikan kasus ini memenuhi kriteria kejahatan transnasional terorganisasi sebagaimana dimaksud dalam *United Nations Convention Against Transnational Organized Crime* (UNTOC) yang telah diratifikasi Indonesia melalui Undang-Undang Nomor 5 Tahun 2009, khususnya unsur keterlibatan kelompok terorganisasi yang sebagian besar perencanaan dan pengendaliannya berlangsung di luar wilayah Indonesia.[12] Kondisi ini menjadikan kasus tersebut memiliki urgensi akademis yang tinggi untuk dikaji, tidak hanya dari perspektif modus operandi akses ilegal menggunakan metode *jackpotting*, tetapi juga dari perspektif penegakan hukum terhadap jaringan kejahatan lintas negara yang melibatkan pelaku warga negara asing.

Salah satu rangkaian insiden dalam kasus ini terjadi di beberapa lokasi di wilayah Daerah Istimewa Yogyakarta, dengan total kerugian yang ditimbulkan mencapai Rp195.350.000,00.[13] Perkara tersebut ditangani oleh Unit Jatanras Satuan Reserse Kriminal (Satreskrim) Polresta Yogyakarta melalui proses penyelidikan dan penyidikan, termasuk pemeriksaan

[12] Undang-Undang Nomor 5 Tahun 2009 tentang Pengesahan United Nations Convention Against Transnational Organized Crime (Konvensi Perserikatan Bangsa-Bangsa Menentang Tindak Pidana Transnasional yang Terorganisasi).

[13] Dua WNA Bulgaria Bobol ATM di Yogya Pakai *Software* Raup Rp195 Juta, *CNN Indonesia*, terdapat dalam https://www.cnnindonesia.com/nasional/20230628140257-12-967558/dua-wna-bulgaria-bobol-atm-di-yogya-pakai-*software*-raup-rp195-juta, Diakses tanggal 18 April 2026.

terhadap pelaku dan pengamanan barang bukti elektronik dengan analisis bukti digital (*digital evidence*) yang berkaitan dengan sistem ATM.[14] Perkara ini telah diproses hingga berkas perkara dinyatakan lengkap dan dilimpahkan kepada Kejaksaan, serta telah diputus melalui Putusan Pengadilan Negeri Yogyakarta Nomor 391/Pid.Sus/2023/PN Yyk,[15] dan dikuatkan melalui Putusan Pengadilan Tinggi Yogyakarta Nomor 25/PID.SUS/2024/PT YYK pada tingkat banding.[16]

Kejahatan akses ilegal semacam ini, apabila tidak ditangani secara serius, berpotensi menurunkan tingkat kepercayaan masyarakat terhadap keamanan sistem perbankan digital yang saat ini menjadi tulang punggung aktivitas ekonomi modern.[17] Berdasarkan uraian tersebut, penelitian mengenai modus operandi dan penegakan hukum tindak pidana akses ilegal dalam kasus pembobolan ATM menggunakan metode *jackpotting* oleh warga negara Bulgaria di wilayah hukum Polresta Yogyakarta menjadi penting untuk dilakukan. Kajian terhadap modus operandi diperlukan untuk menjelaskan pola keterlibatan pelaku dalam kejahatan ini melalui pendekatan kriminologi, sedangkan analisis terhadap penegakan hukum diperlukan untuk mengetahui proses dan kendala yang dihadapi penyidik Polresta Yogyakarta dalam menangani kasus tersebut. Penelitian ini diharapkan dapat memberikan kontribusi bagi pengembangan hukum

[14] Wawancara dengan Tri Purnomo Sidhi, Pemangku Sementara Kasubnit 1 Satuan Reserse Kriminal Polresta Yogyakarta, di Yogyakarta, 4 Mei 2026.

[15] Putusan Pengadilan Negeri Yogyakarta No. 391/Pid.Sus/2023/PN Yyk.

[16] Putusan Pengadilan Tinggi Yogyakarta No. 25/PID.SUS/2024/PT YYK.

[17] Alfina Ali dan Anggun Okta Fitri, "Keamanan Perbankan di Era Digital: Tantangan dan Solusinya," *Jurnal Bersama Ilmu Ekonomi*, No. 2 Vol. 1, Mei 2025, hlm. 158.

terhadap tindak pidana siber yang terus berkembang seiring dengan kemajuan teknologi informasi.

B. Rumusan Masalah

Berdasarkan uraian latar belakang di atas, maka permasalahan yang menjadi fokus penelitian ini dirumuskan sebagai berikut:

1. Bagaimana modus operandi tindak pidana akses ilegal dalam kasus pembobolan ATM menggunakan metode *jackpotting* oleh warga negara Bulgaria di wilayah hukum Polresta Yogyakarta?
2. Bagaimana penegakan hukum yang dilakukan oleh penyidik Polresta Yogyakarta terhadap pelaku dalam kasus tersebut, serta kendala apa saja yang dihadapi?

C. Tujuan Penelitian

Penelitian yang penulis lakukan ini memiliki tujuan sebagai berikut:

1. Untuk menganalisis modus operandi tindak pidana akses ilegal dalam kasus pembobolan ATM menggunakan metode *jackpotting* oleh warga negara Bulgaria di wilayah hukum Polresta Yogyakarta.
2. Untuk menganalisis penegakan hukum yang dilakukan oleh penyidik Polresta Yogyakarta terhadap pelaku tindak pidana akses ilegal dalam kasus pembobolan ATM tersebut, serta kendala yang dihadapi.

D. Orisinalitas Penelitian

Penulis melakukan penelusuran terhadap penelitian-penelitian sebelumnya yang terdapat temuan dan perbedaan sebagai berikut:

No	Detail Karya Ilmiah	Temuan	Perbedaan
1.	Angelica Gabriel, Dani Robert Pinasang, dan Herlyanty Y. A. Bawole, Penegakan Hukum Terhadap Kejahatan *Skimming* ATM Berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (Jurnal LEX PRIVATUM, No. 5 Vol. 13, 2024).	Penelitian ini membahas penegakan hukum terhadap kejahatan siber yang menyerang sistem ATM serta menggunakan ketentuan dalam UU ITE sebagai dasar analisis hukum. Berfokus pada kejahatan *skimming* ATM yang dilakukan melalui pencurian data kartu nasabah.	Penelitian ini mengkaji modus *jackpotting* yang menargetkan sistem pengendalian mesin ATM tanpa melibatkan data kartu nasabah.
2.	Bhelinda Ramadhani, Tinjauan Yuridis Carding Berdasarkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Kitab Undang-	Penelitian ini mengkaji tindak pidana siber yang memanfaatkan teknologi informasi serta menelaah penerapan ketentuan dalam UU ITE terhadap pelaku	Penelitian ini membahas akses ilegal terhadap sistem ATM melalui metode *jackpotting* terhadap pelaku warga negara asing.

No	Detail Karya Ilmiah	Temuan	Perbedaan
	Undang Hukum Pidana, (Skripsi, Universitas Brawijaya, 2011).	kejahatan elektronik. Berfokus pada tindak pidana *carding* yang berkaitan dengan penyalahgunaan data kartu kredit dalam transaksi elektronik	
3.	Laurencia Adeline dan Hery Firmansyah, Aspek Pembuktian Tindak Pidana *Skimming* ATM Berdasarkan Undang-Undang Nomor 1 Tahun 2024 Tentang Informasi Dan Transaksi Elektronik, (Jurnal Pamulang Law Review, No. 2 Vol. 8, 2025)	Penelitian ini membahas kejahatan terhadap ATM dan penggunaan ketentuan hukum dalam UU ITE, khususnya yang berkaitan dengan tindak pidana berbasis teknologi informasi. Berfokus pada aspek pembuktian tindak pidana *skimming* ATM.	Penelitian ini berfokus pada modus operandi dan penegakan hukum dalam *jackpotting* oleh WNA Bulgaria di wilayah hukum Polresta Yogyakarta.

No	Detail Karya Ilmiah	Temuan	Perbedaan
4.	Arifuddin Aljundani dan Niru Anita Sinaga, Penegakan Hukum Terhadap Pelaku Tindak Pidana Siber Tentang Akses Ilegal Di Indonesia, (LEX LAGUENS: Jurnal Kajian Hukum dan Keadilan, No. 2 Vol. 3, 2025)	Penelitian ini membahas tindak pidana akses ilegal dan penegakan hukum terhadap pelaku berdasarkan peraturan perundang-undangan yang berlaku di Indonesia. Mengkaji akses ilegal secara umum dalam berbagai bentuk tindak pidana siber.	Penelitian ini secara khusus mengkaji akses ilegal dalam kasus pembobolan ATM menggunakan metode *jackpotting* oleh warga negara Bulgaria di wilayah hukum Polresta Yogyakarta.
5.	Oktari Anggi Setya Pratama, Pertanggungjawaban Pidana Pelaku Tindak Pidana Pencurian Data Elektronik Ditinjau Berdasarkan Undang-Undang ITE, (Jurnal Sosial Humaniora Sigli (JSH), No. 1 Vol. 8, 2025)	Penelitian ini membahas tindak pidana dibidang teknologi informasi dan penerapan ketentuan UU ITE terhadap pelaku kejahatan siber. Berfokus pada pertanggungjawaban pidana pelaku pencurian data elektronik.	Penelitian ini menitikberatkan pada kendala penegakan hukum dalam menjangkau pelaku warga negara asing yang belum tertangkap.

Berdasarkan hasil penelusuran terhadap penelitian-penelitian sebelumnya yang terdapat temuan dan perbedaan dapat diketahui bahwa penelitian yang dilakukan oleh penulis adalah orisinal.

E. Tinjauan Pustaka

1. Modus Operandi

Modus operandi dalam hukum pidana merupakan cara atau teknik yang digunakan oleh pelaku dalam melakukan suatu tindak kejahatan. Secara konseptual, modus operandi tidak hanya menggambarkan tindakan fisik pelaku, tetapi juga mencerminkan tingkat kecanggihan, perencanaan, serta pemanfaatan teknologi dalam melakukan kejahatan. Modus operandi pada dasarnya tidak dapat dipisahkan dari kecanggihan teknologi yang terus berkembang, mengingat kejahatan semacam ini turut memanfaatkan jaringan besar (*networking*) dan teknologi terkini dalam pelaksanaannya.[18]

Dalam konteks kejahatan siber (*cybercrime*), modus operandi mengalami perkembangan yang sangat pesat. Hal ini sejalan dengan pendapat Barda Nawawi Arief yang menyatakan bahwa kejahatan berbasis teknologi memiliki sifat dinamis, adaptif, dan cenderung memanfaatkan celah keamanan sistem elektronik. Salah satu bentuk kejahatan tersebut adalah tindak pidana akses ilegal, yaitu perbuatan mengakses sistem elektronik tanpa hak dengan tujuan tertentu, seperti memperoleh data, memanipulasi sistem, atau mengambil keuntungan secara melawan hukum.[19]

---

[18] Alfitra, *Modus Operandi Pidana Khusus di Luar KUHP: Korupsi, Money Laundering, & Trafficking*, Raih Asa Sukses, Jakarta, 2014, hlm. 3.

[19] Barda Nawawi Arief, *Tindak Pidana Mayantara (Cyber Crime): Perkembangan Kajian dan Kebijakan Hukum Pidana*, RajaGrafindo Persada, Jakarta, 2006, hlm. 25.

Modus operandi akses ilegal pada awalnya banyak dilakukan melalui teknik konvensional seperti *phishing*, *hacking* sederhana, atau *skimming* pada mesin ATM.[20] Namun, seiring dengan perkembangan teknologi, modus tersebut mengalami transformasi menjadi lebih kompleks, salah satunya melalui eksploitasi perangkat lunak (*software exploitation*). Dalam konteks pembobolan ATM, pelaku tidak lagi hanya memanfaatkan kelalaian pengguna, tetapi secara langsung menargetkan sistem internal mesin ATM dengan menggunakan perangkat elektronik dan aplikasi khusus.[21]

Modus operandi semacam ini memenuhi unsur tindak pidana akses ilegal sebagaimana diatur dalam Pasal 30 UU ITE, khususnya unsur melawan hukum mengakses sistem elektronik serta unsur melampaui atau menjebol sistem pengamanan yang telah disediakan.[22] Tingkat perencanaan yang matang serta penguasaan teknologi yang tinggi dalam modus ini turut menjadi pertimbangan penting dalam menilai unsur kesengajaan (*dolus*) pelaku, yang merupakan salah satu elemen pokok dalam pembuktian pertanggungjawaban pidana.[23]

Karakteristik utama dari modus operandi ini adalah sasarannya yang tertuju pada sistem pengendalian mesin, bukan pada data kartu

---

[20] Dian Alan Setiawan, "Perkembangan Modus Operandi Kejahatan Skimming Dalam Pembobolan Mesin ATM Bank Sebagai Bentuk Kejahatan Dunia Maya (Cybercrime)," *Era Hukum-Jurnal Ilmiah Ilmu Hukum*, No. 2 Vol. 16, Universitas Tarumanegara, 2018, hlm. 180.

[21] "ATM Malware: Pelajari Cara Menghindarinya," Widya Security, terdapat dalam https://widyasecurity.com/2026/02/01/atm-malware-pelajari-cara-menghindarinya/, Diakses tanggal 31 Maret 2026.

[22] Dian Alan Setiawan, *Op. Cit.* hlm. 185.

[23] Moeljatno, *Azaz-Azaz Hukum Pidana,* Rineka Cipta, Jakarta, 1985, hlm. 173.

maupun kelalaian pengguna, sehingga pengurasan uang tidak terekam sebagai transaksi nasabah dan sulit terdeteksi pada tahap awal. Selain itu, kejahatan ini sering dilakukan secara terorganisasi dan melibatkan jaringan lintas negara, sehingga termasuk dalam kategori kejahatan transnasional (*transnational organized crime*).[24]

Selain dianalisis dari segi pemenuhan unsur pidana, kompleksitas modus operandi semacam ini juga dapat dijelaskan melalui pendekatan kriminologis, yaitu *Routine Activity Theory*, sebagaimana diuraikan pada bagian berikut.

2. *Routine Activity Theory* (RAT)

Routine Activity Theory (RAT) merupakan salah satu pendekatan kriminologis yang dikemukakan oleh Cohen dan Felson, yang menjelaskan bahwa suatu tindak kejahatan terjadi akibat bertemunya tiga unsur secara bersamaan, yaitu pelaku yang termotivasi (*motivated offender*), target yang sesuai (*suitable target*), dan ketiadaan pengawasan yang memadai (*absence of capable guardian*).[25] Pendekatan ini pada mulanya digunakan untuk menjelaskan kejahatan konvensional, namun dalam perkembangannya turut relevan digunakan untuk menganalisis kejahatan yang memanfaatkan teknologi informasi, termasuk tindak pidana terhadap sistem elektronik perbankan seperti

[24] Undang-Undang Nomor 5 Tahun 2009 tentang Pengesahan United Nations Convention Against Transnational Organized Crime.

[25] Lawrence E. Cohen dan Marcus Felson, "Social Change and Crime Rate Trends: A Routine Activity Approach," *American Sociological Review*, No. 4 Vol. 44, 1979, hlm. 589.

mesin ATM.[26] Dalam konteks kasus pembobolan ATM, ketiga unsur tersebut dapat diidentifikasi melalui adanya pelaku yang memiliki kemampuan teknis dan motivasi ekonomi, mesin ATM sebagai target yang menyimpan nilai finansial tinggi, serta lemahnya pengawasan terhadap sistem keamanan ATM yang memungkinkan modus *jackpotting* berjalan tanpa terdeteksi pada tahap awal.

3. Penegakan Hukum Pidana

Kebijakan hukum pidana atau biasa disebut *Penal Policy* merupakan suatu kebijakan yang berorientasi kepada penanggulangan tindak pidana yang menggunakan sarana hukum pidana. *Penal Policy* tersebut terkonsentrasi kepada penanggulangan hukum pidana setelah terjadinya tindak pidana.[27] Penegakan hukum pidana atau lebih dikenal dengan upaya represif merupakan tindakan oleh aparat penegak hukum sesudah terjadi tindak pidana dengan melakukan atau tidak melakukan penyidikan, melakukan atau tidak melakukan penuntutan, menjatuhkan atau tidak menjatuhkan pidana. Upaya represif dilakukan untuk mengurangi jumlah tindak pidana atau pelanggaran dengan cara menjerat pelaku dengan ketentuan pidana, misalnya penjatuhan hukuman penjara,[28] sedangkan upaya preventif dilakukan melalui pencegahan agar tidak terjadi tindak pidana. Penegakan hukum pidana

[26] Mohd. Kharris Maulana dan M. Khasali Hakim, *Op. Cit.* hlm. 80.

[27] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, Kencana Prenada Media Group, Jakarta, 2007, hlm. 21.

[28] Nisrina Ramadhani Daulay, Hafrida, dan Yulia Monita, "Peran Hukum Pidana Dalam Upaya Penegakan Tindak Pidana Pembunuhan Bayi di Wilayah Kota Jambi," *PAMPAS: Journal of Criminal Law*, No. 3 Vol. 4, 2023, hlm. 307-308.

dilaksanakan melalui sistem peradilan pidana yang melibatkan kepolisian, kejaksaan, pengadilan, dan lembaga pemasyarakatan.[29] Keberhasilan penegakan hukum sangat ditentukan oleh profesionalitas aparat penegak hukum dalam mengungkap tindak pidana, mengumpulkan alat bukti, serta menerapkan ketentuan hukum secara tepat dan adil.[30]

Dalam konsep penegakan hukum, polisi memiliki wewenang dalam proses penyelidikan dan penyidikan sebagaimana diatur dalam Pasal 1 angka 2 dan angka 5 Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (yang selanjutnya disebut KUHAP).[31] Wewenang tersebut kemudian berlanjut pada tahap penuntutan oleh kejaksaan dan pemeriksaan perkara oleh pengadilan hingga perkara diputus melalui persidangan, sebagaimana diatur dalam Pasal 1 angka 1 Undang-Undang Nomor 16 Tahun 2004 tentang Kejaksaan Republik Indonesia.[32]

Soerjono Soekanto menjelaskan bahwa ada lima faktor yang memengaruhi penegakan hukum, yakni:[33]

a. Faktor hukum adalah faktor penegakan hukum yang berkaitan dengan aturan hukum. Aturan ini merupakan titik awal dalam

---

[29] Moh. Hatta, *Menyongsong Penegakan Hukum Responsif: Sistem Peradilan Pidana Terpadu (Dalam Konsepsi dan Implementasi)*, Galangpress, Yogyakarta, 2008, hlm. 47.

[30] Soerjono Soekanto, *Faktor-Faktor yang Mempengaruhi Penegakan Hukum*, Rajawali Press, Jakarta, 1983, hlm. 36.

[31] M. Yahya Harahap, *Pembahasan Permasalahan dan Penerapan KUHAP: Penyidikan dan Penuntutan*, Sinar Grafika, Jakarta, 2006, hlm. 101.

[32] *Ibid*. hlm. 121.

[33] Soerjono Soekanto, Faktor-Faktor yang Mempengaruhi Penegakan Hukum, *Op. Cit.* hlm. 8.

proses penegakan hukum. Bisa dikatakan aturan inilah yang menjadi pedoman bagi aparat penegak hukum dan juga masyarakat.

b. Faktor penegak hukum adalah peran aparat penegak hukum dalam menegakkan aturan hukum yang berlaku. Faktor ini juga meliputi bagaimana para aparat bisa menegakkan aturan hukum sesuai dengan tugas dan penggunaan wewenang yang tepat.

c. Faktor sarana dan prasarana adalah ketersediaan sumber daya pendukung dalam proses penegakan hukum. Sarana dan prasarana ini harus dikaji lebih jauh, khususnya tentang kualitas dan kuantitas atau jumlahnya.

d. Faktor masyarakat adalah faktor yang berkaitan dengan masyarakat, khususnya mengenai pemahaman dan pengetahuan soal aturan atau norma hukum. Faktor ini juga meliputi kepercayaan dan pemikiran masyarakat terhadap aparat penegak hukum.

e. Faktor kebudayaan adalah ketetapan tentang apa yang boleh atau harus dilakukan, dan mana yang dilarang. Dalam kaitannya dengan penegakan hukum, faktor kebudayaan mempengaruhi bagaimana perilaku masyarakat sebelum dan setelah mengetahui norma hukum yang ada.

4. Tindak Pidana Akses Ilegal

Tindak pidana akses ilegal merupakan salah satu bentuk kejahatan

siber yang berkembang seiring dengan pesatnya penggunaan teknologi informasi dan sistem elektronik dalam berbagai aktivitas masyarakat. Secara umum, akses ilegal diartikan sebagai perbuatan mengakses komputer, jaringan komputer, atau sistem elektronik milik pihak lain tanpa hak, melawan hukum, atau melampaui kewenangan yang diberikan.[34] Perbuatan tersebut dilakukan dengan tujuan tertentu, seperti memperoleh informasi, mengambil data, mengubah sistem, atau mendapatkan keuntungan secara melawan hukum. Dalam perkembangan kejahatan siber modern, akses ilegal sering menjadi tahap awal untuk melakukan tindak pidana lain, seperti pencurian data, penipuan elektronik, pembobolan rekening, maupun gangguan terhadap keamanan sistem elektronik.[35] Oleh karena itu, tindak pidana akses ilegal dipandang sebagai perbuatan yang mengancam keamanan, kerahasiaan, dan integritas sistem elektronik yang menjadi bagian penting dalam kehidupan digital masyarakat modern.

Dalam perspektif hukum pidana, tindak pidana akses ilegal termasuk dalam kategori kejahatan yang memanfaatkan teknologi informasi sebagai sarana maupun sasaran kejahatan. Kejahatan ini memiliki sifat yang kompleks karena dilakukan dengan menggunakan perangkat teknologi yang terus berkembang, sehingga metode dan modus operandinya sulit dideteksi melalui cara-cara konvensional.

[34] Arifuddin Aljundani dan Niru Anita Sinaga, *Op. Cit.* hlm. 177.
[35] *Ibid.* hlm. 179.

Akses ilegal juga memiliki karakteristik *borderless* atau tanpa batas wilayah, karena pelaku dapat melakukan akses terhadap sistem elektronik dari lokasi yang berbeda dengan tempat sistem tersebut berada. Kondisi tersebut menyebabkan penegakan hukum terhadap tindak pidana akses ilegal memerlukan kemampuan khusus dalam bidang teknologi informasi, terutama dalam aspek pelacakan digital, pengumpulan alat bukti elektronik, dan pembuktian di persidangan.[36]

Pengaturan mengenai tindak pidana akses ilegal di Indonesia diatur dalam UU ITE. Ketentuan mengenai akses ilegal secara khusus diatur dalam Pasal 30 UU ITE yang menyatakan bahwa setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun dilarang.[37] Ketentuan tersebut kemudian dibagi ke dalam beberapa bentuk perbuatan, yaitu akses ilegal biasa, akses ilegal dengan tujuan memperoleh informasi elektronik atau dokumen elektronik, serta akses ilegal dengan cara menerobos, melampaui, atau menjebol sistem pengamanan. Sanksi pidana terhadap perbuatan tersebut diatur dalam Pasal 46 UU ITE yang memberikan ancaman pidana penjara dan denda sesuai dengan tingkat kesalahan dan akibat yang ditimbulkan oleh pelaku.[38]

Selain diatur dalam UU ITE, tindak pidana akses ilegal juga dapat

[36] *Ibid.* hlm. 184.
[37] *Ibid*. hlm. 180.
[38] *Ibid.* hlm. 181.

berkaitan dengan ketentuan dalam Kitab Undang-Undang Hukum Pidana (yang selanjutnya disebut KUHP), terutama apabila perbuatan tersebut menimbulkan kerugian materiil atau dilakukan sebagai sarana untuk melakukan tindak pidana lain, seperti pencurian, penipuan, maupun penggelapan.[39] Dalam praktiknya, penerapan pasal terhadap tindak pidana akses ilegal sering dilakukan secara kumulatif antara UU ITE dengan ketentuan pidana umum dalam KUHP. Hal ini bertujuan agar penegakan hukum dapat menjangkau seluruh aspek perbuatan pelaku, baik terkait akses ilegal terhadap sistem elektronik maupun akibat hukum yang ditimbulkan dari perbuatan tersebut. Dengan demikian, pengaturan hukum mengenai akses ilegal menunjukkan adanya upaya negara dalam memberikan perlindungan terhadap keamanan sistem elektronik serta menjaga kepercayaan masyarakat terhadap penggunaan teknologi informasi dan transaksi digital.[40]

5. *Jackpotting*

Jackpotting merupakan salah satu bentuk kejahatan siber yang menyerang sistem elektronik perbankan, khususnya mesin Anjungan Tunai Mandiri (ATM), dengan cara mengeksploitasi kelemahan perangkat lunak (*software*) atau sistem operasi yang digunakan oleh mesin ATM, baik melalui penanaman perangkat lunak berbahaya (*malware*) maupun penyalahgunaan perangkat lunak (*software*) akses

[39] Mahrus Ali, *Dasar-Dasar Hukum Pidana,* Sinar Grafika, Jakarta, 2011, hlm. 232.
[40] Arifuddin Aljundani dan Niru Anita Sinaga, *Op. Cit.* hlm. 182.

jarak jauh yang secara umum legal. Istilah *jackpotting* digunakan untuk menggambarkan tindakan pelaku yang mampu membuat mesin ATM mengeluarkan uang tunai secara terus-menerus tanpa melalui transaksi yang sah sebagaimana dilakukan oleh nasabah pada umumnya. Berbeda dengan metode konvensional seperti *skimming* yang berfokus pada pencurian data kartu dan informasi pribadi nasabah, *jackpotting* menargetkan sistem internal ATM secara langsung sehingga pelaku dapat mengendalikan fungsi mesin untuk mengeluarkan uang tanpa hak.[41]

Ditinjau dari kedudukannya dalam tipologi kejahatan siber, *jackpotting* merupakan bentuk khusus dari akses ilegal: setiap perbuatan *jackpotting* dengan sendirinya merupakan akses ilegal terhadap sistem elektronik, tetapi tidak setiap akses ilegal merupakan *jackpotting*. Pembedanya terletak pada sasaran serangan dan akibat yang dituju, yaitu sistem pengendalian mesin ATM dan keluarnya uang tunai secara fisik, sedangkan bentuk akses ilegal lain pada umumnya berhenti pada penguasaan data atau gangguan terhadap bekerjanya sistem elektronik.

Perkembangan *jackpotting* tidak terlepas dari meningkatnya ketergantungan sektor perbankan terhadap teknologi informasi dan sistem elektronik. Kemajuan teknologi yang memberikan kemudahan dalam layanan perbankan juga menciptakan risiko baru berupa

[41] "Kenali ATM *Jackpotting*, Serangan yang Bisa Kurasi Uang ATM," CyberHub Indonesia, terdapat dalam https://cyberhub.id/pengetahuan-dasar/mengenal-atm-*jackpotting*, Diakses tanggal 30 Maret 2026.

munculnya berbagai bentuk serangan siber yang menargetkan infrastruktur digital perbankan. Oleh karena itu, *jackpotting* dipandang sebagai salah satu bentuk kejahatan siber yang berbahaya karena dapat menimbulkan kerugian finansial dalam jumlah besar dalam waktu yang relatif singkat serta mengancam kepercayaan masyarakat terhadap keamanan sistem perbankan.

Dalam perspektif hukum pidana di Indonesia, tindakan *jackpotting* dapat dikategorikan sebagai tindak pidana akses ilegal karena pelaku memperoleh akses terhadap sistem elektronik tanpa hak atau melawan hukum. Perbuatan tersebut pada dasarnya memenuhi unsur akses tanpa hak terhadap sistem elektronik sebagaimana diatur dalam Pasal 30 UU ITE.[42] Selain itu, apabila tindakan tersebut dilakukan dengan tujuan memperoleh keuntungan atau menyebabkan kerugian bagi pihak lain, pelaku juga dapat dimintai pertanggungjawaban pidana berdasarkan ketentuan pidana yang diatur dalam peraturan perundang-undangan yang berlaku.

F. Definisi Operasional

1. Modus operandi adalah cara, metode, atau teknik yang digunakan oleh pelaku dalam melakukan suatu tindak kejahatan. Istilah ini menggambarkan pola tindakan pelaku, mulai dari persiapan, pelaksanaan, hingga cara menghindari deteksi.[43]

[42] Arifuddin Aljundani dan Niru Anita Sinaga, *Op. Cit.* hlm. 180.
[43] Ulima Dheani Artanti, *Modus Operandi Dan Problematika Penegakan Hukum Tindak Pidana Penipuan Online*, Skripsi, Universitas Muhammadiyah Magelang, 2020, hlm. 24.

2. *Routine Activity Theory* adalah pendekatan kriminologis yang menjelaskan terjadinya kejahatan akibat bertemunya tiga unsur secara bersamaan, yaitu pelaku yang termotivasi, target yang sesuai, dan ketiadaan pengawasan yang memadai.[44]
3. Penegakan hukum pidana adalah proses dilaksanakannya norma hukum oleh aparat penegak hukum guna mewujudkan ketertiban, kepastian, dan keadilan dalam masyarakat.[45] Penegakan hukum mencakup tindakan preventif (pencegahan) maupun represif (penindakan) terhadap pelanggaran hukum.[46]
4. Tindak pidana akses ilegal adalah perbuatan mengakses atau memasuki suatu sistem elektronik, komputer, jaringan komputer, atau perangkat digital lainnya tanpa hak, tanpa izin, atau secara melawan hukum. Perbuatan ini dilakukan dengan tujuan tertentu, seperti memperoleh informasi, mengubah data, mengganggu sistem, atau memperoleh keuntungan yang tidak sah. Dalam konteks hukum siber, akses ilegal merupakan salah satu bentuk kejahatan yang menyerang keamanan dan integritas sistem elektronik.[47]
5. ATM (Anjungan Tunai Mandiri) merupakan perangkat elektronik yang disediakan oleh bank untuk memudahkan nasabah melakukan transaksi

[44] Lawrence E. Cohen dan Marcus Felson, *Op. Cit.* hlm. 589.

[45] Hasaziduhu Moho, "Penegakan hukum di Indonesia menurut aspek kepastian hukum, keadilan dan kemanfaatan," *Warta Dharmawangsa*, Edisi No. 1 Vol. 13, Universitas Dharmawangsa, 2019, hlm. 34.

[46] Oktir Nebi, "Analisis Upaya Preventif dan Represif Penegakan Hukum Pidana terhadap Kekerasan Anak di Wilayah Hukum Kepolisian Sektor Kota Jambi," *Parlementer: Jurnal Studi Hukum dan Administrasi Publik*, No. 3 Vol. 1, September 2024, hlm. 210.

[47] Arifuddin Aljundani dan Niru Anita Sinaga, *Op. Cit.* hlm. 177.

keuangan secara mandiri tanpa harus datang ke kantor bank. ATM berfungsi untuk melakukan penarikan tunai, transfer dana, pembayaran tagihan, serta pengecekan saldo melalui sistem komputer yang terhubung dengan jaringan perbankan. ATM merupakan mesin yang memberikan kemudahan kepada nasabah dalam melakukan transaksi perbankan secara otomatis selama 24 jam dalam 7 hari termasuk hari libur.[48] Dalam perspektif hukum, ATM termasuk sistem elektronik sebagaimana diatur dalam Pasal 1 angka 5 UU ITE**,** karena merupakan perangkat yang berfungsi mengolah dan menyimpan informasi elektronik dalam kegiatan transaksi keuangan.[49]

6. *Software* atau perangkat lunak adalah sekumpulan instruksi, program, atau data yang digunakan untuk menjalankan perintah tertentu pada perangkat komputer. Dalam konteks kejahatan siber perbankan, *software* memiliki karakter *dual use*, dapat berupa program yang secara umum legal (seperti aplikasi *remote access*) maupun perangkat lunak berbahaya (*malware*) yang dirancang untuk mengeksploitasi kelemahan sistem.[50] Dalam aspek hukum, *software* termasuk program komputer yang dilindungi sebagai kekayaan intelektual sebagaimana diatur dalam Pasal 1 angka 9 Undang-Undang Nomor 28 Tahun 2014

[48] "ATM Adalah: Pengertian, Jenis, Manfaat, dan Keuntungan," OCBC, *Op. Cit.*

[49] Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Pasal 1 angka 5.

[50] "ATM Malware: Pelajari Cara Menghindarinya," Widya Security, terdapat dalam https://widyasecurity.com/2026/02/01/atm-malware-pelajari-cara-menghindarinya/, Diakses tanggal 31 Maret 2026.

tentang Hak Cipta.[51]

7. *Jackpotting* adalah metode kejahatan siber yang membuat mesin ATM mengeluarkan uang tunai secara terus menerus tanpa melalui transaksi sah, dilakukan dengan mengeksploitasi kelemahan pada perangkat lunak atau sistem operasi mesin ATM, baik melalui *malware* maupun penyalahgunaan perangkat lunak akses jarak jauh yang secara umum legal.[52]

G. Metode Penelitian

Metode penelitian menurut Moh. Nazir merupakan cara utama yang digunakan peneliti untuk mencapai tujuan dan menentukan jawaban atas masalah yang diteliti.[53] Metode penelitian juga dapat diartikan dengan cara penelitian. Penelitian merupakan sarana yang digunakan oleh seseorang untuk memperkuat, membina serta mengembangkan suatu ilmu pengetahuan.[54] Penelitian dilakukan dalam rangka suatu kegiatan ilmiah yaitu seseorang berusaha untuk mencari kebenaran dari temuan orang yang dianggap ahli dan dihormati.[55] Pada penelitian ini penulis menggunakan metode:

---

[51] Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta, Pasal 1 angka 9.

[52] "Kenali ATM *Jackpotting*, Serangan yang Bisa Kurasi Uang ATM," CyberHub Indonesia, *Op. Cit.*

[53] Moh. Nazir, *Metode Penel*itian, Ghalia Indonesia, Jakarta, 2014, hlm. 32.

[54] Soerjono Soekanto, *Pengantar Penelitian Hukum*, Penerbit Universitas Indonesia (UI Press), Jakarta, 2014, hlm. 3.

[55] *Ibid.* hlm. 9.

1. Tipologi Penelitian

Penelitian ini berjenis yuridis-empiris, yaitu penelitian hukum mengenai pemberlakuan atau implementasi ketentuan hukum normatif secara *in action* pada setiap peristiwa hukum tertentu yang terjadi dalam masyarakat. Penelitian yuridis-empiris merupakan penelitian lapangan, yaitu suatu penelitian yang meneliti peraturan-peraturan hukum yang kemudian digabungkan dengan data dan perilaku yang hidup di tengah-tengah masyarakat. Sifat penelitian ini adalah deskriptif-analisis, yaitu mendeskripsikan data-data yang didapatkan dan kemudian dilakukan perbandingan dan analisis.[56]

2. Pendekatan Penelitian

Pendekatan yang dilakukan dalam penelitian ini adalah pendekatan sosiologis, yaitu pendekatan yang mengkaji suatu objek penelitian dengan berlandaskan pada kondisi dan fakta sosial yang hidup di masyarakat. Berdasarkan perkembangan ilmu pengetahuan kontemporer, ilmu ini digunakan sebagai salah satu metode dalam rangka memahami dan mengkaji tentang masalah yang diteliti.[57] Pendekatan ini dipilih karena penelitian ini menitikberatkan pada praktik penegakan hukum sebagaimana berlangsung di lapangan, yaitu bagaimana ketentuan hukum diterapkan oleh penyidik dalam menangani perkara tindak pidana akses ilegal dengan metode

[56] Suharsimi Arikunto, *Prosedur Penelitian Suatu Pendekatan Praktek*, Rineka Cipta, Jakarta, 2012, hlm. 126.

[57] Soerjono Soekanto, *Sosiologi Suatu Pengantar*, Rajawali Pers, Jakarta, 2001, hlm. 21-22.

jackpotting di wilayah hukum Kepolisian Resor Kota Yogyakarta.

3. Objek Penelitian

Objek penelitian ini menitikberatkan pada dua aspek pokok. *Pertama,* bagaimana modus operandi tindak pidana akses ilegal dalam kasus pembobolan ATM menggunakan metode *jackpotting* oleh warga negara Bulgaria di wilayah hukum Polresta Yogyakarta. *Kedua*, bagaimana penegakan hukum yang dilakukan oleh penyidik Polresta Yogyakarta terhadap pelaku dalam kasus tersebut, serta kendala apa saja yang dihadapi.

4. Subjek Penelitian

Subjek penelitian adalah informan atau narasumber yang memberikan informasi berkaitan dengan objek penelitian, yang pemilihannya didasarkan pada data yang hendak dicari oleh peneliti.[58] Subjek dalam penelitian ini adalah penyidik Unit Jatanras Satuan Reserse Kriminal (Satreskrim) Polresta Yogyakarta dan pihak vendor pengelola mesin ATM yang mengalami kerugian dalam perkara ini. Penggunaan lebih dari satu subjek dimaksudkan agar data yang diperoleh dapat diuji silang (*triangulasi*), sehingga hasil penelitian tidak bertumpu pada keterangan satu pihak.

5. Lokasi Penelitian

Penelitian ini dilaksanakan di wilayah hukum Kepolisian Resor

[58] Suratman dan H. Phillips Dillah, Metode Penelitian Hukum, Alfabeta, Bandung, 2012, hlm. 127.

Kota (Polresta) Yogyakarta, dengan pertimbangan bahwa perkara tindak pidana akses ilegal dalam kasus pembobolan ATM menggunakan metode *jackpotting* oleh warga negara Bulgaria ditangani oleh Unit Jatanras Satuan Reserse Kriminal (Satreskrim) Polresta Yogyakarta sejak tahap penyelidikan hingga pelimpahan berkas perkara kepada Kejaksaan. Penelitian ini membatasi kajian penegakan hukum pada kewenangan kepolisian, yaitu meliputi upaya pre-emtif, preventif, dan represif berupa penyelidikan dan penyidikan sampai dengan berkas perkara dinyatakan lengkap (P-21), sehingga tidak mencakup tahap penuntutan maupun pemeriksaan di persidangan. Rangkaian peristiwa dalam perkara ini yang sebagian terjadi di luar wilayah administratif Kota Yogyakarta, yaitu di Kabupaten Bantul, merupakan satu kesatuan perkara yang penanganannya tetap berada di bawah kewenangan Polresta Yogyakarta berdasarkan Pasal 84 KUHAP mengenai kewenangan relatif pengadilan dalam perkara yang *locus delicti*-nya meliputi lebih dari satu wilayah hukum, dan dilimpahkan melalui Pengadilan Negeri Yogyakarta.

6. Sumber Data Penelitian

Sesuai dengan tipologi penelitian yuridis-empiris yang digunakan, sumber data dalam penelitian ini terdiri dari data primer dan data sekunder.

a. Data Primer

Data primer adalah data yang diperoleh langsung dari lapangan

melalui wawancara dengan subjek penelitian. Dalam penelitian ini, data primer diperoleh melalui wawancara dengan penyidik Unit Jatanras Satuan Reserse Kriminal (Satreskrim) Polresta Yogyakarta dan pihak vendor pengelola ATM yang mengalami kerugian dalam perkara ini. Data yang diperoleh dari kedua subjek wawancara tersebut turut diuji silang dengan keterangan saksi dan ahli yang tercatat dalam Putusan Pengadilan Negeri Yogyakarta Nomor 391/Pid.Sus/2023/PN Yyk dan Putusan Pengadilan Tinggi Yogyakarta Nomor 25/PID.SUS/2024/PT YYK, guna memastikan validitas dan konsistensi data yang digunakan dalam penelitian ini.

b. Data Sekunder

Data sekunder adalah data yang diperoleh dari studi kepustakaan atau literatur yang memiliki keterkaitan dengan objek penelitian. Dalam penelitian ini, data sekunder bersumber dari bahan hukum yang terbagi menjadi tiga, yakni:

1) Bahan Hukum Primer, yaitu bahan-bahan hukum yang memiliki kekuatan mengikat secara langsung. Dalam penelitian ini menggunakan bahan hukum primer berupa:
   a) Kitab Undang-Undang Hukum Pidana (KUHP)
   b) Kitab Undang-Undang Hukum Acara Pidana (KUHAP)
   c) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

d) Undang-Undang Nomor 5 Tahun 2009 tentang Pengesahan *United Nations Convention Against Transnational Organized Crime*

e) Undang-Undang Nomor 1 Tahun 2006 tentang Bantuan Timbal Balik dalam Masalah Pidana

f) Undang-Undang Nomor 1 Tahun 1979 tentang Ekstradisi

g) Putusan Pengadilan Negeri Yogyakarta Nomor 391/Pid.Sus/2023/PN Yyk

h) Putusan Pengadilan Tinggi Yogyakarta Nomor 25/PID.SUS/2024/PT YYK

2) Bahan Hukum Sekunder, yaitu bahan hukum yang memberikan penjelasan terhadap bahan hukum primer, berupa buku-buku hukum, jurnal ilmiah, hasil penelitian, dan karya ilmiah lainnya yang berkaitan dengan objek penelitian.

3) Bahan Hukum Tersier, yaitu bahan yang memberikan petunjuk maupun penjelasan terhadap bahan hukum primer dan sekunder, berupa kamus besar bahasa Indonesia, kamus hukum, ensiklopedia, dan sumber-sumber lain yang relevan.

7. Teknik Pengumpulan Data

Teknik pengumpulan data yang digunakan pada penelitian yaitu:

a. Wawancara, yaitu mengumpulkan data dan informasi dengan cara melakukan tanya jawab secara langsung dengan responden maupun narasumber. Dalam penelitian ini, wawancara dilakukan

dengan penyidik Unit Jatanras Satuan Reserse Kriminal (Satreskrim) Polresta Yogyakarta dan pihak vendor pengelola ATM untuk mendapatkan data primer yang berkaitan langsung dengan modus operandi dan penegakan hukum dalam kasus yang diteliti.[59]

b. Studi dokumen, yaitu teknik pengumpulan data dengan menghimpun data dan menganalisis dokumen-dokumen resmi yang berkaitan dengan objek penelitian. Dalam penelitian ini, studi dokumen dilakukan terhadap Putusan Pengadilan Negeri Yogyakarta Nomor 391/Pid.Sus/2023/PN Yyk dan Putusan Pengadilan Tinggi Yogyakarta Nomor 25/PID.SUS/2024/PT YYK, serta dokumen resmi lain yang berkaitan dengan proses penyelidikan dan penyidikan dalam perkara ini.

c. Studi pustaka, yaitu serangkaian kegiatan yang berkenaan dengan pengumpulan data dari bahan-bahan kepustakaan berupa buku, jurnal ilmiah, peraturan perundang-undangan, dan sumber tertulis lainnya yang relevan dengan objek penelitian.[60]

8. Teknik Analisis Data

Teknik analisis yang digunakan dalam penelitian ini adalah analisis deskriptif kualitatif, yaitu suatu metode analisis yang dilakukan dengan cara mendeskripsikan, menguraikan, menganalisis data yang

[59] Soerjono Soekanto, *Pengantar Penelitian Hukum*, *Op. Cit.* hlm. 24.

[60] Mestika Zed, *Metode Penelitian Kepustakaan*, Yayasan Obor Indonesia, Jakarta, 2004, hlm. 3.

diperoleh secara sistematis untuk kemudian ditarik kesimpulan yang bersifat kualitatif.[61] Dalam penelitian hukum yuridis-empiris, analisis deskriptif kualitatif dilakukan dengan mengkaji data primer yang diperoleh dari wawancara, kemudian dihubungkan dengan data sekunder berupa putusan pengadilan, peraturan perundang-undangan, doktrin hukum, dan literatur yang relevan, guna menjawab rumusan masalah secara komprehensif dan sistematis.[62]

H. Kerangka Skripsi

Penulisan Skripsi sebagai tugas akhir strata 1 (satu) disusun dalam 4 (empat) bab yang tidak dapat dipisahkan. Uraian kerangka penulisan dalam skripsi ini adalah sebagai berikut:

BAB I PENDAHULUAN

BAB I merupakan pengantar terhadap permasalahan yang diangkat dalam skripsi. Dimulai dengan uraian latar belakang yang menjelaskan fenomena tindak pidana akses ilegal dalam kasus pembobolan ATM menggunakan metode *jackpotting* oleh warga negara Bulgaria di wilayah hukum Polresta Yogyakarta. Selanjutnya dirumuskan permasalahan, tujuan penelitian, orisinalitas penelitian, tinjauan pustaka, definisi operasional, metode penelitian yang digunakan, serta ditutup dengan kerangka skripsi

[61] Soerjono Soekanto, *Pengantar Penelitian Hukum*, *Op. Cit.* hlm. 28-29.

[62] Burhan Ashsofa, *Metode Penelitian Hukum*, Ctk. Pertama, Rineka Cipta, Jakarta, 2004, hlm. 20.

secara umum.

BAB II TINJAUAN UMUM TENTANG MODUS OPERANDI, PENEGAKAN HUKUM PIDANA, DAN TINDAK PIDANA AKSES ILEGAL

BAB II menguraikan tinjauan umum tentang dasar-dasar konseptual yang berkaitan dengan rumusan masalah. Penulis akan menjelaskan mengenai teori-teori yang relevan seperti teori modus operandi, penegakan hukum pidana termasuk bentuk-bentuk upaya penegakan hukum oleh kepolisian dan tindak pidana akses ilegal beserta pengaturannya dalam UU ITE. Selain itu, bab ini memuat penjelasan mengenai tindak pidana akses ilegal dalam kasus pembobolan ATM menggunakan metode *jackpotting* ditinjau dari perspektif Hukum Islam.

BAB III MODUS OPERANDI DAN PENEGAKAN HUKUM TINDAK PIDANA AKSES ILEGAL DALAM KASUS PEMBOBOLAN ATM MENGGUNAKAN METODE *JACKPOTTING* (Studi Kasus Warga Negara Bulgaria di Polresta Yogyakarta)

BAB III merupakan bagian inti dari skripsi yang membahas secara mendalam fenomena tindak pidana akses ilegal dalam kasus pembobolan ATM menggunakan metode *jackpotting* oleh warga negara Bulgaria di wilayah hukum Polresta

Yogyakarta. Penulis akan menguraikan analisis hasil penelitian mengenai modus operandi tindak pidana akses ilegal yang dilakukan dalam kasus tersebut berdasarkan data primer yang diperoleh dari wawancara serta kajian putusan pengadilan, serta penegakan hukum terhadap tindak pidana yang dalam lingkup kewenangan Polresta Yogyakarta yang meliputi upaya pre-emtif, preventif, dan represif berupa penyelidikan dan penyidikan sampai dengan pelimpahan berkas perkara, termasuk analisis yuridis terhadap penerapan UU ITE dan KUHP dalam konstruksi delik yang dirumuskan oleh penyidik.

BAB IV PENUTUP

BAB IV berisi kesimpulan dari hasil analisis yang telah dilakukan, yang menjawab rumusan masalah dalam bentuk narasi padat. Selain itu, bab ini memuat saran-saran dari penulis agar dapat merespons tantangan penegakan hukum mengenai tindak pidana akses ilegal berbasis teknologi secara komprehensif.