# BAB I

# PENDAHULUAN

## 1.1 Latar Belakang

Perkembangan teknologi, informasi, dan komunikasi telah membawa perubahan besar dalam kehidupan masyarakat modern. Pemanfaatan internet, sistem elektronik, dan teknologi digital tidak hanya memberikan kemudahan dalam bidang ekonomi, pendidikan, pemerintahan, dan komunikasi, melainkan melahirkan berbagai bentuk kejahatan baru yang dilakukan melalui media elektronik. Perkembangan tersebut mendorong munculnya kejahatan siber yang berkaitan dengan kerahasiaan data yang memerlukan perhatian khusus sebab karakteristiknya berbeda dengan tindak pidana konvensional.[1] Menurut United Nations Office on Drugs and Crime (UNODC), kejahatan siber merupakan tindak pidana yang dilakukan dengan menggunakan sistem komputer atau jaringan sebagai alat, sasaran, atau tempat terjadinya kejahatan.[2] Kejahatan siber tidak hanya menimbulkan kerugian ekonomi, tetapi juga mengancam keamanan nasional, stabilitas sosial, serta perlindungan data pribadi masyarakat.

Perkembangan kejahatan siber di Indonesia menunjukkan peningkatan yang signifikan seiring meningkatnya penggunaan teknologi digital dalam kehidupan masyarakat. Kejahatan siber dikategorikan dalam tiga ketegori

[1]Budiyanto, *Pengantar Cybercrime dalam Sistem Hukum Pidana di Indonesia*, PT Sada Kurnia Pustaka, Banten, 2023, hlm. 4.

[2]United Nations Office on Drugs and Crime, "Comprehensive Study on Cybercrime", diakses pada 16 Juni 2025.

utama, yaitu kejahatan siber terhadap individu, kejahatan siber terhadap properti, dan kejahatan siber terhadap pemerintah.[3] Salah satu bentuk kejahatan siber yang banyak terjadi dalam praktik adalah tindak pidana akses ilegal (*illegal access*), yaitu perbuatan mengakses sistem elektronik milik orang lain tanpa hak atau melawan hukum. Tindak pidana tersebut umumnya dilakukan untuk memperoleh data elektronik, menguasai akun digital korban, dan mengambil keuntungan ekonomi.

Salah satu modus yang berkembang dalam tindak pidana akses ilegal adalah *phishing*. *Phishing* merupakan metode penipuan berbasis rekayasa sosial (*social engineering*) yang dilakukan dengan cara mengelabui korban agar memberikan data pribadi, kode OTP, *username*, *password*, maupun informasi rahasia lainnya melalui tautan elektronik palsu yang menyerupai situs resmi.[4] Modus *phishing* berkembang melalui berbagai media elektronik, seperti pesan singkat, surat elektronik, media sosial, dan aplikasi percakapan daring. Kejahatan ini tidak hanya menimbulkan kerugian materiil bagi korban, tetapi juga berdampak pada penyalahgunaan data pribadi dan penguasaan sistem elektronik secara melawan hukum.

Secara yuridis, pengaturan mengenai tindak pidana akses ilegal diatur dalam Undang-Undang Nomor 11 Tahun 2008 *jo.* Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE). Pasal 30 UU ITE mengatur bahwa setiap orang dengan sengaja dan tanpa hak

---

[3]Ferry Irawan Febriansyah, *Cybercrime Kejahatan di Balik Layar Digital*, Najaha, Ponorogo, 2025, hlm. 14.

[4]Kiki Kristanto dan Rakhmat Baihaki, *Tindak Pidana Informasi dan Transaksi Elektronik*, PT Media Penerbit Indonesia, Medan, 2025, hlm. 30.

mengakses komputer dan/atau sistem elektronik milik orang lain, sedangkan Pasal 32 ayat (2) UU ITE mengatur bahwa setiap orang dengan sengaja dan tanpa hak memindahkan atau mentransfer informasi elektronik dan/atau dokumen elektronik milik orang lain. Selain itu, pengaturan mengenai perlindungan data pribadi juga diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Pasal 65 ayat (1) UU PDP melarang setiap orang dengan sengaja dan tanpa hak memperoleh atau mengumpulkan data pribadi yang bukan miliknya. Ketentuan tersebut menunjukkan bahwa tindak pidana akses ilegal dengan modus *phishing* melalui tautan elektronik memiliki keterkaitan erat dengan pelanggaran terhadap sistem elektronik dan penyalahgunaan data pribadi korban.

Penerapan ketentuan hukum mengenai tindak pidana akses ilegal dapat dilihat dalam Putusan Nomor 293/Pid.Sus/2023/PN Mjk pada kasus Ahmad Saleh. Dalam perkara tersebut, terdakwa melakukan tindak pidana akses ilegal dengan modus *phishing* melalui pengiriman tautan elektronik palsu yang menyerupai situs resmi layanan keuangan kepada sejumlah warga negara Jepang.[5] Tautan tersebut digunakan untuk memperoleh akses secara tanpa hak terhadap data pribadi dan informasi elektronik milik korban. Dalam proses penegakan hukum, terdakwa didakwa berdasarkan Pasal 30 dan Pasal 32 Undang-Undang Nomor 11 Tahun 2008 *jo.* Undang-Undang Nomor 19 Tahun

[5]Fendy Hermasyah, *Jawapos.com* (*online*), 5 September 2023, "Hacker Pencuri Data Warga Jepang Divonis Berat PN Mojokerto", dalam https://radarmojokerto.jawapos.com/hukumkriminal/822929339/hacker-pencuri-data-warga-jepang-divonis-berat-pn-mojokerto, diakses pada 2 Juni 2025.

2016 tentang Informasi dan Transaksi Elektronik karena terdakwa tidak hanya mengakses sistem elektronik tanpa hak, melainkan menguasai dan memindahkan data elektronik milik korban. Perkara tersebut menunjukkan bahwa tindak pidana akses ilegal dengan modus *phishing* tidak hanya berkaitan dengan sistem elektronik, melainkan penyalahgunaan data pribadi dan penguasaan informasi elektronik yang melawan hukum.

Penanganan tindak pidana akses ilegal dengan modus *phishing* memerlukan kemampuan teknis penyidik dalam melakukan pelacakan digital, pemeriksaan perangkat elektronik, identifikasi alamat IP (*internet protocol address)*, serta pengamanan alat bukti elektronik agar tetap memiliki kekuatan pembuktian di persidangan. Dalam praktiknya, penyidikan kejahatan siber menghadapi berbagai kendala, antara lain keterbatasan sarana dan prasarana forensik digital, rendahnya kompetensi di bidang teknologi informasi, penggunaan VPN *(virtual private network)* dari server luar negeri oleh pelaku, serta sulitnya koordinasi antarinstansi maupun koordinasi lintas negara.[6] Kondisi tersebut menunjukkan bahwa mekanisme penyidikan tindak pidana siber memiliki kompleksitas yang berbeda dengan penyidikan tindak pidana konvensional.

Selain aspek teknis, perlindungan data pribadi dalam proses penyidikan juga menjadi isu penting dalam penegakan hukum kejahatan siber. Penggeledahan dan penyitaan perangkat elektronik berpotensi menimbulkan

[6]*Ibid*., hlm. 18.

pelanggaran hak privasi apabila tidak dilakukan sesuai prosedur hukum.[7] Oleh karena itu, mekanisme penyidikan tindak pidana akses ilegal tetap memperhatikan prinsip *due process of law,* yaitu penegakan hukum yang dilakukan sesuai prosedur hukum dan perlindungan hak asasi manusia. Meskipun demikian, pengaturan mengenai mekanisme penyidikan elektronik, standar forensik digital, dan perlindungan data pribadi dalam proses penyidikan masih belum diatur secara rinci dan terpadu dalam peraturan perundang-undangan. Kondisi tersebut menimbulkan perbedaan penerapan dalam praktik penyidikan tindak pidana akses ilegal pada setiap kasus.

Sistem hukum pidana Indonesia pada dasarnya mengatur mekanisme penyidikan dengan mengacu pada Kitab Undang-Undang Hukum Acara Pidana (KUHAP) sebagai hukum acara pidana umum serta Peraturan Kepala Kepolisian Nomor 6 Tahun 2019 tentang Penyidikan Tindak Pidana sebagai pedoman teknis pelaksanaan penyidikan. Akan tetapi, kedua pengaturan tersebut belum mengatur secara rinci mekanisme penyidikan elektronik, khususnya terkait standar pembuktian digital, tata cara pengamanan barang bukti elektronik, dan perlindungan data pribadi dalam proses penyidikan. Kondisi tersebut menunjukkan adanya kekaburan norma dalam mekanisme penyidikan tindak pidana akses ilegal, terutama yang dilakukan melalui media elektronik. Selain itu, mekanisme penyidikan tindak pidana akses ilegal juga

[7]Muhammad Syaukani, dkk., *Hukum Digital dan Privasi Data*, CV Al-Haramain Lombok, Mataram, 2025, hlm. 62.

masih menghadapi berbagai permasalahan, baik dari aspek pengaturan maupun aspek penegakan hukum.

Berdasarkan data Direktorat Reserse Siber Kepolisian Daerah Jawa Timur yang telah direkapitulasi selama periode Januari hingga Desember 2024, tercatat sejumlah pengaduan masyarakat terkait tindak pidana akses ilegal. Data tahun 2024 digunakan karena merupakan data terbaru yang telah terdokumentasi dan tersedia secara resmi pada saat penelitian dilakukan pada tahun 2025 sebagai berikut:

| No. | Pengaduan Masyarakat | Jumlah |
|---|---|---|
| 1 | Mengakses sistem elektronik milik orang lain tanpa izin (Pasal 30 ayat (1) UU ITE) | 6 |
| 2 | Mengakses dan mengambil alih sistem elektronik milik orang lain (Pasal 30 ayat (2) UU ITE) | 6 |
| 3 | Mengakses sistem elektronik milik orang lain dengan cara apapun (Pasal 30 ayat (3) UU ITE) | 5 |

Tabel 1: Rekapitulasi Tindak Pidana Siber di Direktorat Reserse Siber Kepolisian Daerah Jawa Timur Periode Januari hingga Desember 2024
Sumber: Data sekunder diperoleh dari Direktorat Reserse Siber Kepolisian Daerah Jawa Timur Tahun 2024.

Pengaduan tersebut didominasi oleh perbuatan mengakses sistem elektronik milik orang lain dengan sengaja dan tanpa hak sebagaimana diatur dalam Pasal 30 ayat (1) dan ayat (2) UU ITE, sedangkan Pasal 30 ayat (3) UU ITE menunjukkan adanya variasi cara dalam melakukan tindak pidana akses ilegal. Data tersebut menunjukkan bahwa tindak pidana akses ilegal masih menjadi salah satu bentuk kejahatan siber yang memerlukan penanganan secara efektif, khususnya pada tahap penyidikan.

Berdasarkan uraian tersebut, dapat dipahami bahwa tindak pidana akses ilegal dengan modus *phishing* merupakan bentuk kejahatan siber yang memiliki kompleksitas tinggi dalam proses penanganannya. Meskipun telah terdapat berbagai regulasi yang mengatur tindak pidana siber, dalam praktik penyidikan masih ditemukan berbagai kendala dan perbedaan penerapan hukum yang menunjukkan adanya kekaburan norma dalam mekanisme penyidikan elektronik. Oleh karena itu, penulis tertarik melakukan penelitian dengan judul **"Mekanisme Penyidikan Tindak Pidana Akses Ilegal Dengan Modus *Phishing* Melalui Tautan Elektronik (Studi Kasus Di Direktorat Reserse Siber Kepolisian Daerah Jawa Timur)".**

## 1.2 Rumusan Masalah

Berdasarkan uraian latar belakang di atas, maka penulis merumuskan rumusan masalah sebagai berikut:

1. Bagaimana mekanisme penyidikan tindak pidana akses ilegal di Direktorat Reserse Siber Kepolisian Daerah Jawa Timur?
2. Bagaimana kendala dan upaya penanganan penyidikan tindak pidana akses ilegal di Direktorat Reserse Siber Kepolisian Daerah Jawa Timur?

## 1.3 Tujuan Penelitian

Berdasarkan rumusan masalah di atas, maka penulis merumuskan tujuan penelitian sebagai berikut:

1. Penelitian ini bertujuan untuk menganalisis mekanisme penyidikan tindak pidana akses ilegal di Direktorat Reserse Siber Kepolisian Daerah Jawa Timur.

2. Penelitian ini bertujuan untuk menganalisis kendala dan upaya penanganan penyidikan tindak pidana akses ilegal di Direktorat Reserse Siber Kepolisian Daerah Jawa Timur.

## 1.4 Manfaat Penelitian

Berdasarkan tujuan penelitian di atas, maka penelitian ini memiliki manfaat sebagai berikut:

1. Manfaat Teoritis:

   Hasil penelitian diharapkan dapat memberikan kontribusi dalam pengembangan ilmu hukum, khususnya terkait mekanisme penyidikan tindak pidana akses ilegal. Penelitian ini diharapkan dapat menjadi bahan referensi penelitian selanjutnya yang berkaitan dengan penyidikan tindak pidana siber, khususnya akses ilegal.

2. Manfaat Praktis:

   a. Sebagai tambahan referensi bagi mahasiswa yang akan melakukan penelitian serupa.

   b. Sebagai salah satu syarat untuk memperoleh gelar Sarjana Hukum pada Program Studi Hukum Fakultas Hukum Universitas Pembangunan Nasional “Veteran” Jawa Timur.

## 1.5 Keaslian Penelitian

Penelitian yang ditulis oleh penulis memiliki perbedaan dengan penelitian terdahulu. Berikut penelitian-penelitian terdahulu yang menjadi penunjang dalam penulisan Skripsi ini:

| Analisis Penelitian Terdahulu | | | |
|---|---|---|---|
| **No.** | **Nama, Tahun, Judul** | **Rumusan Masalah** | **Perbedaan** |
| 1. | Hermawan Bayu Aji Pratama, 2020, Pelaksanaan Perlindungan Hukum Korban Tindak Pidana *Illegal Access.*[8] | 1. Bagaimana modus operandi tindak pidana akses ilegal?<br>2. Bagaimana bentuk perlindungan hukum tindak pidana akses ilegal?<br>3. Apa upaya hukum yang dapat dilakukan oleh korban? | 1. Penelitian terdahulu membahas mengenai modus operandi tindak pidana akses ilegal, sedangkan penelitian yang dilakukan oleh penulis membahas mengenai mekanisme penyidikan tindak pidana akses ilegal dengan modus *phishing* berdasarkan KUHAP dan Peraturan Kepala Kepolisian Nomor 6 Tahun 2019 tentang Penyidikan Tindak Pidana di Direktorat Reserse Siber Kepolisian Daerah Jawa Timur.<br>2. Penelitian terdahulu membahas mengenai bentuk perlindungan hukum dan upaya hukum yang dialami oleh korban tindak pidana akses ilegal, sedangkan penelitian yang dilakukan oleh penulis membahas mengenai kendala dan upaya penanganan penyidikan tindak pidana akses ilegal di Direktorat Reserse Siber Kepolisian Daerah Jawa Timur. |
| 2. | Dian Eka Kusuma Wardani, 2021, Penegakan Hukum Oleh Kepolisian Republik Indonesia Terhadap Kejahatan *Skimming* Di Indonesia.[9] | 1. Bagaimana mekanisme penegakan hukum oleh kepolisian dalam menangani kejahatan *skimming* yang terkait akses ilegal terhadap data elektronik? | 1. Penelitian terdahulu membahas mengenai kejahatan *skimming* (pencurian data pada kartu elektronik), sedangkan penelitian yang dilakukan oleh penulis membahas mengenai mekanisme penyidikan tindak pidana akses ilegal yang menggunakan modus *phishing* (penipuan online dengan mencuri data sensitif) berdasarkan KUHAP dan |

[8]Hermawan Bayu Aji, "Pelaksanaan Perlindungan Hukum Korban Tindak Pidana *Illegal Access*", *Skripsi,* Program Sarjana Universitas Muhammadiyah Magelang, Magelang, 2020.

[9]Dian Eka Kusuma, "Penegakan Hukum Oleh Kepolisian RI Terhadap Kejahatan *Skimming* Di Indonesia", *Disertasi,* Program Doktor Universitas Hasanuddin, Makassar, 2021.

| | | | |
|---|---|---|---|
| | | 2. Apa kendala hukum dan teknis yang dihadapi dalam proses penyidikan kejahatan ini?<br>3. Bagaimana upaya peningkatan kemampuan penyidik dan sarana teknologi penunjang dalam penyidikan tindak pidana siber? | Peraturan Kepala Kepolisian Nomor 6 Tahun 2019 tentang Penyidikan Tindak Pidana di Direktorat Reserse Siber Kepolisian Daerah Jawa Timur.<br>2. Penelitian terdahulu memiliki ruang lingkup lebih luas karena melibatkan beberapa instansi penegak hukum dan beberapa kasus *skimming* di Indonesia. Sementara itu, penelitian yang dilakukan oleh penulis memiliki ruang lingkup lebih spesifik dengan fokus pada mekanisme penyidikan tindak pidana akses ilegal dengan modus *phishing* pada Direktorat Reserse Siber Kepolisian Daerah Jawa Timur. Maka dari itu, penelitian ini lebih menitikberatkan pada aspek mekanisme penyidikan dan kendala penegakan hukum dalam satu jenis delik dan satu instansi. |
| 3. | Muh Akbar Ismail, Hambali Thalib, dan Anggreany Arief, 2024, Efektivitas Penyidikan Terhadap Pelaku Tindak Pidana *Illegal Access* di Kepolisian Resor Soppeng.[10] | 1. Bagaimana efektivitas penyidikan terhadap pelaku tindak pidana akses ilegal di Kepolisian Resor Soppeng?<br>2. Bagaimana kendala yang dihadapi pada tindak pidana akses ilegal oleh Kepolisian Resor Soppeng? | 1. Penelitian terdahulu membahas mengenai penyidikan akses ilegal di Kepolisian Resor Soppeng, sedangkan penelitian yang dilakukan oleh penulis membahas mengenai mekanisme penyidikan tindak pidana akses ilegal dengan modus *phishing* berdasarkan KUHAP dan Peraturan Kepala Kepolisian Nomor 6 Tahun 2019 tentang Penyidikan Tindak Pidana di Direktorat Reserse Siber Kepolisian Daerah Jawa Timur.<br>2. Penelitian terdahulu membahas evaluasi kinerja penyidikan dalam wilayah hukum Kepolisian Resor Soppeng yang memiliki cakupan penanganan |

[10]Ismail, M.A., Thalib, H., dan Arief., A, "Efektivitas Penyidikan Terhadap Pelaku Tindak Pidana *Illegal Access* di Kepolisian Resor Soppeng", *Journal of Lex Philosophy*, Vol. 5, No. 1, Juni 2024.

| | | | |
|---|---|---|---|
| | | | perkara pada tingkat wilayah kepolisian resor di bawah kepolisian daerah. Sementara itu, penelitian yang dilakukan oleh penulis berfokus pada mekanisme penyidikan tindak pidana akses ilegal di Direktorat Reserse Siber Kepolisian Daerah Jawa Timur yang memiliki kewenangan dan cakupan penanganan tindak pidana siber lebih luas serta didukung unit khusus di bidang kejahatan siber. |

Tabel 2: Perbandingan Penelitian Terdahulu
Sumber: Skripsi, Disertasi, dan Jurnal Terdahulu, diolah sendiri.

Berdasarkan tabel penelitian terdahulu, dapat diketahui bahwa penelitian sebelumnya memiliki persamaan dengan penelitian penulis, yaitu mengkaji tindak pidana akses ilegal sebagai bagian dari kejahatan siber serta menggunakan pendekatan hukum empiris dalam melihat praktik penegakan hukum. Persamaan tersebut menunjukkan bahwa penelitian penulis masih berada dalam ruang lingkup kajian penyidikan tindak pidana siber. Adapun perbedaannya terletak pada fokus dan ruang lingkup penelitian. Penelitian yang dilakukan oleh penulis secara khusus membahas mekanisme penyidikan tindak pidana akses ilegal dengan modus *phishing* melalui tautan elektronik termasuk kendala dan upaya penanganan penyidikan. Dengan demikian, penelitian penulis memiliki kebaruan pada fokus kajian mengenai mekanisme penyidikan tindak pidana akses ilegal dengan modus *phishing* melalui tautan elektronik serta analisis terhadap kekaburan norma dalam praktik penyidikan elektronik. Penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan kajian hukum siber, khususnya terkait efektivitas mekanisme penyidikan tindak pidana akses ilegal di Indonesia.

## 1.6 Metode Penelitian

### 1.6.1 Jenis dan Sifat Penelitian

Jenis penelitian yang akan penulis gunakan dalam penelitian ini yaitu yuridis empiris atau penelitian hukum empiris. Penelitian tersebut merupakan penelitian lapangan yang mengkaji ketentuan hukum yang berlaku dengan kenyataan yang berada dalam masyarakat. Dalam penelitian yuridis empiris, penulis melakukan penelitian lapangan di Direktorat Reserse Siber Kepolisian Daerah Jawa Timur untuk meneliti secara langsung mengenai mekanisme penyidikan tindak pidana akses ilegal dengan modus *phishing* melalui tautan elektronik pada Putusan Nomor 293/Pid.Sus/2023/PN Mjk.

Sifat dari penelitian yang digunakan dalam penelitian ini yaitu deskriptif analitis. Penelitian deskriptif analitis merupakan penelitian yang bertujuan untuk menggambarkan suatu kondisi atau keadaan yang sedang terjadi dalam masyarakat dengan tujuan untuk memberikan data yang terperinci atas objek yang diteliti.[11] Sehingga penelitian ini akan memberikan penjelasan atas topik pembahasan yang diangkat guna menemukan jawaban atas permasalahan yang ada.

### 1.6.2 Pendekatan

Pendekatan yang digunakan dalam penelitian ini yaitu pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual

[11]Jonaedi Efendi dan Johnny Ibrahim, *Metode Penelitian Hukum Normatif dan Empiris*, Kencana, Jakarta, 2021, hlm. 16-17.

(*conceptual approach*). Berikut penjelasan mengenai pendekatan yang digunakan oleh penulis dalam penelitian ini:

1. Pendekatan perundang-undangan adalah pendekatan yang digunakan melalui undang-undang yang berkaitan dengan topik permasalahan yang diangkat. Pendekatan perundang-undangan sangat penting untuk dilakukan oleh penulis melalui KUHAP, UU ITE beserta perubahannya, UU PDP, dan Peraturan Kepala Kepolisian Nomor 6 Tahun 2019 tentang Penyidikan Tindak Pidana.
2. Pendekatan konseptual adalah pendekatan dalam penelitian hukum yang berfokus pada analisis terhadap konsep-konsep hukum, asas, dan doktrin yang berkembang dalam ilmu hukum.[12] Pendekatan ini digunakan untuk memahami konsep-konsep yang berkaitan dengan mekanisme penyidikan tindak pidana akses ilegal, seperti konsep penyidikan, alat bukti elektronik, serta kewenangan penyidik dalam hukum siber. Selain itu, pendekatan ini juga digunakan untuk menganalisis permasalahan berdasarkan teori sistem hukum yang dikemukakan oleh Lawrence M. Friedman yang meliputi struktur hukum, substansi hukum, dan budaya hukum.

### 1.6.3 Bahan Hukum

Bahan hukum yang digunakan penulis dalam penelitian yuridis empiris merupakan data primer yang diperoleh dari narasumber secara

[12]Nur Solikin, *Pengantar Metodologi Penelitian Hukum*, CV. Penerbit Qiara Media, Pasuruan, 2021, hlm 60.

langsung, data sekunder yang diperoleh dari studi kepustakaan, dan data tersier dari penjelasan terkait bahan hukum primer serta bahan hukum sekunder. Dalam penelitian ini, sumber data yang digunakan sebagai berikut:

1. Data Primer adalah data melalui wawancara secara langsung kepada penyidik Direktorat Reserse Siber Kepolisian Daerah Jawa Timur sebagai pelaksana penyidikan terhadap tindak pidana akses ilegal.
2. Data Sekunder adalah data yang diambil dari peraturan perundang-undangan, buku, dan hasil penelitian yang mempunyai keterkaitan dengan objek penelitian. Berikut bahan hukum sekunder yang digunakan penulis pada penelitian ini:
    a. Bahan Hukum Primer yakni bahan hukum yang memiliki sifat pengaturan. Berikut penelitian ini menggunakan bahan hukum primer:
        1) Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (Lembar Negara Republik Indonesia Tahun 2008 Nomor 76, Tambahan Lembaran Negara Republik Indonesia Nomor 3209);
        2) Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana (Lembar Negara Republik Indonesia Tahun 2025 Nomor 188, Tambahan Lembaran Negara Republik Indonesia Nomor 7149);

3) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843);
4) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952);
5) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905);
6) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820);
7) Peraturan Kepolisian Negara Republik Indonesia Nomor 3 Tahun 2024 tentang Perubahan Atas Peraturan Kepolisian Negara Republik Indonesia Nomor 14 Tahun

2018 tentang Susunan Organisasi dan Tata Kerja Kepolisian Daerah;

8) Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 6 Tahun 2019 tentang Penyidikan Tindak Pidana;

9) Putusan Pengadilan Negeri Mojokerto Nomor 293/Pid.Sus/2023/PN Mjk.

b. Bahan hukum sekunder yakni dokumen kamus hukum, jurnal hukum, dan putusan hakim.[13]

c. Bahan hukum tersier yakni penjelasan terhadap bahan hukum sebelumnya yang dapat berupa ensiklopedia dan kamus.

### 1.6.4 Prosedur Pengumpulan Bahan Hukum

Untuk memperoleh bahan hukum yang diperlukan dalam penulisan penelitian ini diperoleh dengan metode wawancara dan studi kepustakaan. Berikut penjelasan mengenai prosedur pengumpulan bahan hukum yang digunakan oleh penulis dalam penelitian ini:

1. Wawancara bertujuan untuk memperoleh informasi mengenai mekanisme penyidikan akses ilegal dengan modus *phishing* melalui tautan elektronik dengan sudut pandang dari penyidik dalam menangani perkara. Dalam upaya penulis menggunakan pedoman wawancara terstruktur sebagai sarana guna memastikan ketepatan arah pertanyaan. Selanjutnya, penulis menyusun beberapa pertanyaan untuk melakukan wawancara kepada penyidik yang

[13]Muhaimin, *Metode Penelitian Hukum*, Mataram University Press, Mataram, 2020, hlm. 59.

menangani tindak pidana akses ilegal di Direktorat Reserse Siber Kepolisian Daerah Jawa Timur.

2. Studi kepustakaan atau studi literatur dilakukan dengan cara mengumpulkan data dokumen melalui penelusuran bahan pustaka yang dapat berupa literatur termasuk buku, peraturan perundang-undangan, dan jurnal yang terkait.

### 1.6.5 Analisis Bahan Hukum

Analisis bahan hukum dalam penelitian ini merupakan yuridis empiris yang dilakukan melalui pendekatan normatif dan pendekatan empiris. Secara normatif, analisis dilakukan terhadap bahan hukum primer dan bahan hukum sekunder dengan menggunakan pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Pendekatan perundang-undangan digunakan untuk menelaah ketentuan dalam KUHAP lama, KUHAP baru sebagai *ius constituendum*, UU ITE, UU PDP, dan Peraturan Kepala Kepolisian Nomor 6 Tahun 2019 tentang Penyidikan Tindak Pidana. Pendekatan konseptual digunakan untuk memahami dan menganalisis konsep-konsep hukum yang relevan, seperti konsep penyidikan, alat bukti elektronik, perlindungan data pribadi, serta *integrated criminal justice system* (ICJS), yaitu sistem peradilan pidana terpadu yang mengintegrasikan kerja sama antar aparat penegak hukum guna memberikan landasan teoritis dalam menganalisis permasalahan yang diteliti.

Secara empiris, analisis dilakukan terhadap data primer yang diperoleh melalui wawancara dengan pihak Direktorat Reserse Siber Kepolisian Daerah Jawa Timur. Data tersebut dianalisis secara kualitatif dengan cara mengelompokkan dan menghubungkan fakta yang diperoleh di lapangan dengan ketentuan hukum yang berlaku. Hasil analisis tersebut kemudian digunakan untuk menarik kesimpulan mengenai mekanisme penyidikan tindak pidana akses ilegal serta mengidentifikasi kendala dan upaya penanganan yang dilakukan penyidik dalam praktik penyidikan.

### 1.6.6 Lokasi Penelitian

Untuk memperoleh data yang diperlukan dalam penulisan Skripsi ini berada di Direktorat Reserse Siber Kepolisian Daerah Jawa Timur yang beralamat di Jalan Jenderal Ahmad Yani Nomor 116, Surabaya, Jawa Timur. Penentuan pengambilan lokasi tersebut berdasarkan pembahasan pada penelitian ini, yaitu instansi kepolisian yang menangani perkara tindak pidana akses ilegal dengan modus *phishing* melalui tautan elektronik pada perkara Putusan Nomor 293/Pid.Sus/2023/PN Mjk.

### 1.6.7 Sistematika Penulisan

Sistematika penulisan penelitian hukum disusun untuk memberikan gambaran yang sistematis mengenai isu penelitian sesuai ketentuan penulisan hukum yang berlaku serta memudahkan pembaca

dalam memahami keseluruhan isu penelitian. Dalam penelitian ini, sistematika penulisan dibagi menjadi empat bab sebagai berikut:

Bab *Pertama,* menguraikan pendahuluan yang memuat topik permasalahan yang diangkat oleh penulis. Bab I terdiri atas tujuh subbab, yaitu latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, keaslian penelitian, metode penelitian, dan tinjauan pustaka.

Bab *Kedua,* menguraikan pembahasan dari rumusan masalah pertama yaitu mekanisme penyidikan tindak pidana akses ilegal di Direktorat Reserse Siber Kepolisian Daerah Jawa Timur. Bab II ini terdiri atas dua subbab, subbab pertama berisi tentang pelaksanaan penyidikan tindak pidana akses ilegal berdasarkan KUHAP dan Peraturan Kepala Kepolisian Nomor 6 Tahun 2019 tentang Penyidikan Tindak Pidana serta subbab kedua berisi tentang analisis penulis terhadap pelaksanaan penyidikan tindak pidana akses ilegal di Direktorat Reserse Siber Kepolisian Daerah Jawa Timur.

Bab *Ketiga,* menguraikan pembahasan dari rumusan masalah kedua yaitu kendala dan upaya penanganan penyidikan tindak pidana akses ilegal di Direktorat Reserse Siber Kepolisian Daerah Jawa Timur. Bab III ini terdiri atas dua subbab, subbab pertama berisi tentang kendala terkait pelaksanaan penyidikan tindak pidana akses ilegal di Direktorat Reserse Siber Kepolisian Daerah Jawa Timur dan subbab kedua berisi tentang upaya penanganan terkait pelaksanaan penyidikan tindak pidana akses ilegal di Direktorat Reserse Siber Kepolisian Daerah Jawa Timur.

Bab *Keempat,* memuat akhir dari penyusunan penelitian. Bab IV ini terdiri atas dua subbab, subbab pertama berisi tentang kesimpulan penelitian dan subbab kedua berisi tentang saran dari penulis terkait penelitian ini.

### 1.6.8 Jadwal Penelitian

| No | Jadwal Penelitian | 2025 | | | | | | | | | | | 2026 | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Feb | Mar | Apr | Mei | Jun | Jul | Ags | Spt | Okt | Nov | Des | Jan | Feb | Mar | Apr | Mei |
| 1 | Pengajuan Judul | ■ | | | | | | | | | | | | | | | |
| 2 | Pengumpulan Data | ■ | ■ | | | | | | | | | | | | | | |
| 3 | Penyusunan Proposal | ■ | ■ | | | | | | | | | | | | | | |
| 4 | Bimbingan Proposal | | | | ■ | | | | | | | | | | | | |
| 5 | Seminar Proposal | | | | ■ | | | | | | | | | | | | |
| 6 | Revisi Proposal | | | | | ■ | | | | | | | | | | | |
| 7 | Pengumpulan Proposal | | | | | ■ | | | | | | | | | | | |
| 8 | Pengumpulan Data | | | | | | | ■ | | | | | | | | | |
| 9 | Bimbingan Skripsi | | | | | | ■ | | | ■ | ■ | | | ■ | | | |
| 10 | Sidang Skripsi | | | | | | | | | | | | | | | ■ | |

Tabel 3: Jadwal Penelitian
Sumber: Diolah sendiri.

## 1.7 Tinjauan Pustaka

### 1.7.1 Tinjauan Umum Penyidikan

#### 1.7.1.1 Pengertian Penyidikan

Penyidikan dalam Kamus Besar Bahasa Indonesia (KBBI) berasal dari kata sidik yaitu rangkaian tindakan penyidik yang diatur oleh undang-undang untuk mencari dan mengumpulkan bukti pelaku tindak pidana, proses, cara, dan perbuatan penyidik.[14] Berdasarkan Pasal 1 ayat 2 Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana *jo.* Pasal 1 angka 10 Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia, penyidikan adalah serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam undang-undang ini untuk mencari serta mengumpulkan bukti yang dengan bukti itu membuat terang tentang tindak pidana yang terjadi dan guna menemukan tersangkanya. Penyidikan adalah suatu proses awal dalam tindak pidana yang memerlukan penyelidikan serta pengusutan secara tuntas di dalam sistem peradilan pidana.[15]

---

[14] KBBI, "Arti kata sidik - Kamus Besar Bahasa Indonesia (KBBI) Online", https://kbbi.web.id/sidik#google_vignette, diakses pada 15 Mei 2025.

[15] Uswatun Hasanah dan Yulia Monita, "Sidik Jari sebagai Pendukung Alat Bukti dalam Proses Penyidikan Perkara Pidana", *PAMPAS: Journal of Criminal Law*, Vol. 1, No. 3, 2020, hlm. 141.

#### 1.7.1.2 Tahapan Penyidikan

Tahapan umum penyidikan menurut KUHAP dan praktik di kepolisian sebagai berikut:

a. Penerimaan Laporan atau Informasi

   Tahapan awal dimulai dengan masuknya laporan dari korban atau informasi dari pihak lain terkait dugaan tindak pidana.

b. Penyelidikan

   Dilakukan oleh penyelidik untuk menentukan dugaan tindak pidana. Apabila terdapat bukti permulaan yang cukup maka proses dinaikkan ke tahap penyidikan.

c. Penerbitan Surat Perintah Penyidikan

   Penyidik sebagai perwira polisi menerbitkan penerbitan surat perintah penyidikan sebagai dasar hukum untuk memulai tindakan penyidikan secara formal.

d. Pengumpulan Alat Bukti

   Dalam hal ini penyidik mengumpulkan alat bukti sebagaimana diatur dalam Pasal 184 KUHAP, yaitu keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa.

e. Pemeriksaan Saksi, Ahli, dan Tersangka

   Penyidik memeriksa saksi-saksi, ahli, dan apabila ditemukan tersangka dilakukan pemanggilan beserta

pemeriksaan tersangka.

f. Penetapan Tersangka

Penetapan tersangka dilakukan apabila penyidik telah memperoleh sekurang-kurangnya dua alat bukti yang sah sebagaimana diatur dalam KUHAP. Berdasarkan alat bukti tersebut, penyidik menentukan seseorang yang diduga sebagai pelaku tindak pidana dan bertanggung jawab secara hukum atas perbuatan yang disangkakan.

g. Upaya Paksa

Dalam penyidikan tindak pidana termasuk kejahatan siber, penyidik berwenang melakukan upaya paksa terhadap tersangka atau barang bukti untuk kepentingan penyidikan seperti penggeledahan, penyitaan, dan penahanan.

h. Pembuatan Berkas Perkara (BAP)

Setelah alat bukti dinyatakan cukup, penyidik melakukan penyusunan berkas perkara termasuk keterangan saksi, keterangan ahli, keterangan tersangka, dan barang bukti yang telah dikumpulkan selama proses penyidikan. Berkas perkara tersebut kemudian diserahkan kepada penuntut umum untuk dilakukan penelitian lebih lanjut sebagai bagian dari proses penegakan hukum.

i. Pelimpahan Berkas Kepada Jaksa Penuntut Umum

Terdapat dua tahap, yaitu pada tahap I, penyidik

menyerahkan berkas hasil penyidikan kepada penuntut umum untuk diteliti kelengkapan formil dan materiilnya. Pada tahap II, penyidik menyerahkan tersangka dan barang bukti apabila berkas dinyatakan sudah lengkap (P-21).

### 1.7.2 Tinjauan Umum Tindak Pidana Akses Ilegal

#### 1.7.2.1 Pengertian Tindak Pidana Akses Ilegal

Akses ilegal merupakan salah satu bentuk kejahatan siber tanpa hak yang dilakukan dengan memasuki, mengakses, atau menerobos sistem elektronik milik orang lain untuk memperoleh, mengubah, memindahkan maupun melihat informasi di dalamnya.[16] Menurut Pasal 30 Undang-Undang Nomor 11 Tahun 2008 *jo.* Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, definisi akses ilegal mencakup perbuatan mengakses sistem elektronik milik orang lain, mengakses dengan melampaui kewenangan, dan menerobos sistem pengaman. Ketentuan ini menjelaskan bahwa tindak pidana akses ilegal tidak hanya mencakup perbuatan tanpa izin, melainkan juga termasuk tindakan menembus mekanisme keamanan sistem.

Menurut teori hukum pidana Indonesia, Moeljatno menjelaskan bahwa akses ilegal merupakan tindakan melawan

[16]Danrivanto Budhijanto, *Cybersecurity Law Perlindungan Data Virtual Dan Infrastruktur Informasi Vital*, Logoz Publishing, Bandung, 2022, hlm. 240.

hukum yang bertentangan dengan ketentuan hukum yang berlaku ketika seseorang memasuki sistem elektronik tanpa izin. Batasan konsep "akses" dalam ranah kejahatan siber tidak hanya memasuki secara fisik ke komputer, melainkan juga interaksi digital seperti menggunakan tautan palsu, pencurian kata sandi, dan manipulasi jaringan. Maka dari itu, tindak pidana akses ilegal tidak selalu memerlukan kerusakan sistem, melainkan cukup dengan masuk atau berinteraksi dengan sistem milik orang lain.

#### 1.7.2.2 Bentuk-Bentuk Tindak Pidana Akses Ilegal

Tindak pidana akses ilegal memiliki berbagai bentuk dan modus operandi (cara pelaksanaan kejahatan) yang berkembang seiring dengan kemajuan teknologi informasi. Bentuk-bentuk tersebut dapat dikelompokkan menjadi dua kategori, yaitu akses ilegal secara langsung dan modus operandi yang mengarah pada terjadinya akses ilegal:

A. Bentuk Langsung Tindak Pidana Akses ilegal

1. Akses Tanpa Hak (*Unauthorized Access*)

   Bentuk dasar tindak pidana akses ilegal yang secara tanpa hak dilakukan secara langsung melalui komputer atau jaringan tanpa izin dari pihak berwenang, baik melalui jaringan lokal ataupun jarak jauh melalui internet.[17]

[17]Thomas J. Holt dan Adam Bossler, "Cybercrime Beyond Borders," *Journal of Digital Forensics*, Vol. 9, No. 2, 2017, hlm. 89.

Perbuatan ini merupakan pelanggaran terhadap sistem keamanan elektronik yang dilindungi oleh hukum karena dilakukan tanpa izin yang sah.

2. *Cracking*

   Tindakan membobol atau meretas sistem keamanan perangkat lunak atau komputer untuk memperoleh akses yang tidak sah, menghilangkan proteksi, atau memodifikasi sistem.[18] Tindakan ini umumnya dilakukan dengan teknik tertentu untuk melewati sistem keamanan yang telah dipasang oleh pemilik sistem.

3. *Hacking*

   Tindakan mengakses atau memasuki sistem komputer maupun jaringan tanpa hak dengan memanfaatkan kelemahan keamanan sistem untuk memperoleh informasi atau kendali terhadap sistem tertentu.[19] Dalam konteks kejahatan siber, *hacking* tidak hanya bertujuan untuk mengakses, tetapi juga dapat digunakan untuk menguasai, mengambil, atau memanipulasi data dan sistem.

B. Modus Operandi Tindak Pidana Akses Ilegal

1. *Phishing*

   Tindakan penipuan dengan cara memancing korban untuk

[18]George Curtis, *The Law of Cybercrimes and Their Investigations*, CRC Press, Boca Raton, 2011, hlm. 3.

[19]Dedik Kurniawan*, Ilmu Hacking*, Elex Media Komputindo, Jakarta, 2023, hlm. 61.

memberikan informasi pribadi seperti *username*, kata sandi, nomor kartu kredit, dan data akun perbankan. Modus yang digunakan oleh pelaku yaitu dengan menyamar sebagai pihak resmi seperti bank, perusahaan, dan institusi pemerintah melalui email, pesan teks, atau media sosial.[20]

2. *Carding*

   Tindakan pencurian informasi kartu kredit milik orang lain untuk melakukan transaksi ilegal.[21] Informasi kartu kredit diperoleh melalui metode *phishing, malware* atau melalui situs web yang tidak aman hal ini menyebabkan kerugian finansial bagi korban maupun institusi keuangan. Setelah mendapatkan informasi terkait kartu, pelaku menggunakannya untuk mencairkan dana ataupun menjual kembali data kepada pihak lain.

3. *Malware* (*Malicious Software*)

   Sebuah program berbahaya yang dirancang untuk menyusup ke dalam sistem komputer tanpa sepengetahuan pengguna dengan tujuan mencuri data, merusak sistem, melakukan sabotase, pemerasan dan

[20]*Ibid.*, hlm. 92.

[21]Alamsyah, Edy Santoso, dan Nugraha Pranadita, "Kajian Terhadap Kejahatan Carding Sebagai Bentuk Cybercrime Di Indonesia", *Iustitia Omnibus: Jurnal Ilmu Hukum*, Vol. 6, No. 2, 2025, hlm 63.

mengambil alih kendali perangkat elektronik.[22] Jenis *malware* meliputi virus, *worm, trojan*, *ransomware*, serta *spyware*. Program ini dapat disebarkan melalui lampiran email, tautan palsu, atau file yang diunduh dari situs tidak terpercaya, setelah berhasil masuk ke dalam sistem, *malware* memungkinkan pelaku untuk mengambil alih kontrol sistem atau mencuri informasi sensitif.[23]

### 1.7.3 Tinjauan Umum Direktorat Reserse Siber

#### 1.7.3.1 Struktur Organisasi Direktorat Reserse Siber

Direktorat Reserse Siber memiliki struktur organisasi yang diatur dalam Peraturan Kepolisian Negara Republik Indonesia Nomor 3 Tahun 2024 tentang Perubahan Atas Peraturan Kepolisian Negara Republik Indonesia Nomor 14 Tahun 2018 tentang Susunan Organisasi dan Tata Kerja Kepolisian Daerah, yang memuat tugas setiap bagian di antaranya sebagai berikut:

1. Subbagrenmin (Subbagian Perencanaan dan Administrasi)
   Menyusun perencanaan kerja beserta anggaran, menangani manajemen personel logistik, melakukan pelayanan administrasi, serta melakukan ketatausahaan.
2. Bagbinopsnal (Bagian Pembinaan Operasional)

[22]Teodor Sommestad dan Henrik Karlzén, "The Unpredictability of *Phising* Susceptibility: Results from a Repeated Measures Experiment", *Journal of Cybersecurity*, Vol. 10, No. 1, 2024, hlm 1-3.

[23]Fatmawati dan Raihana, "Analisis Yuridis Terhadap Artificial Intelligence Pada Tindak Pidana Penyebaran Malware Di Indonesia", *Innovative: Journal Of Social Science Research*, Vol. 3, No. 2, 2023.

Memeriksa, membimbing, menyatukan, memelihara, mengelola data, melaksanakan pelatihan fungsi, serta melakukan dokumentasi. Dalam melaksanakan tugasnya bagbinopsnal dibantu oleh dua subbagian sebagai berikut:

a. Subbagminopsnal (Subbagian Administrasi Operasional) bertugas merencanakan pelatihan fungsi, mengarsipkan berkas perkara, dan melakukan administrasi penyelidikan.
b. Subbaganev (Subbagian Analisis dan Evaluasi) bertugas menganalisis, mengevaluasi tugas Direktorat Reserse Siber, mengumpulkan data, mengelola data, memaparkan informasi, dan memaparkan dokumentasi.

3. Bagwassidik (Bagian Pengawasan Penyidikan)

   Mengawasi administrasi, mengawasi materi, memberikan bantuan penyelidikan dan melakukan penyidikan.

4. Sikorwas PPNS (Seksi Koordinasi dan Pengawasan Penyidik Pegawai Negeri Sipil)

   Berkoordinasi dan mengawasi penyidikan, memberikan bimbingan teknik, strategi, serta konsultasi penyidikan kepada penyidik pegawai negeri sipil.

5. Subdit (Sub Direktorat)

   Melakukan penyelidikan dan penyidikan di daerah hukum kepolisian daerah, melakukan pemberkasan sesuai dengan

ketetapan yang berlaku, menerapkan manajemen penyelidikan dan penyidikan tindak pidana siber, melakukan pencegahan dengan mengedukasi terkait tindak pidana siber, serta melakukan kerja sama perusahaan atau organisasi yang memiliki tujuan yang sama. Subdit memiliki tiga struktur organisasi sebagai berikuts:

a. Subdit I bertugas melaksanakan penyelidikan dan penyidikan pada sistem elektronik tindak pidana siber.
b. Subdit II bertugas melaksanakan penyelidikan dan penyidikan pada sarana elektronik serta penyebaran konten ilegal terkait tindak pidana siber.
c. Subdit III

   Memberikan bantuan teknis pada tahapan penyelidikan dan penyidikan tindak pidana siber.

**1.7.3.2 Tugas Penyidikan Direktorat Reserse Siber**

Berdasarkan Peraturan Kepolisian Negara Republik Indonesia Nomor 3 Tahun 2024 tentang Perubahan Atas Peraturan Kepolisian Negara Republik Indonesia Nomor 14 Tahun 2018 tentang Susunan Organisasi dan Tata Kerja Kepolisian Daerah, Direktorat Reserse Siber memiliki tugas dan menjalankan fungsi di antaranya sebagai berikut:

1. Melakukan penyelidikan dan penyidikan tindak pidana siber.
2. Mendeteksi dan menganalisis tindak pidana siber.

3. Melakukan patroli siber, mencegah, dan mengedukasi terkait literasi digital tindak pidana siber.
4. Mengawasi penyidikan tindak pidana siber pada lingkungan kepolisian daerah.
5. Mengolah data, memaparkan informasi, memaparkan dokumentasi, melakukan analisis, serta melakukan evaluasi.
6. Berkoordinasi atas pengawasan kepada penyidik negeri sipil.