BAB I

PENDAHULUAN

A. Latar Belakang

Kemajuan ilmu pengetahuan dan teknologi telah memberikan dampak yang sangat positif bagi peradaban umat manusia. Salah satu fenomena abad moderen yang sampai saat ini masih terus berkembang dengan pesat adalah internet. Internet telah menjadi bagian integral dari kehidupan sehari-hari di era modern ini. Sejak pertama kali dikembangkan pada akhir abad ke-20, internet telah berkembang pesat dan mengubah cara manusia berkomunikasi, bekerja, belajar, dan mengakses informasi. Dengan internet, informasi dari seluruh penjuru dunia dapat diakses dengan mudah dan cepat, memungkinkan terjadinya globalisasi dalam berbagai bidang seperti bisnis, pendidikan, dan hiburan.[1]

Pesatnya revolusi digital telah memberikan dampak yang besar pada berbagai sektor, termasuk dibidang hukum. Walaupun perkembangan teknologi banyak memberikan dampak positif, namun banyak juga dampak negatif yang timbul dari perkembangan teknologi itu sendiri, seperti berkurangnya kontak sosial antar manusia, munculnya rasa ketergantungan terhadap teknologi, ketidakmampuan menyaring informasi pemberitaan yang muncul di media internet, penggunaan media informasi yang tidak semestinya, seperti mengakses website yang seharusnya dilarang.

[1] Ardy, Letfi Aziz Febrika, et all, "*Phishing* Di Era Media Sosial Identifikasi dan Pencegahan Ancaman Di Platform Sosial", *Journal of Internet and Sftware Engineering,* Vol. 1, No.4, 2024, hlm 2.

Dampak negatif teknologi juga disertai dengan terjadinya kejahatan-kejahatan di bidang teknologi itu sendiri, yang bisa dibilang baru dibandingkan kejahatan-kejahatan pada umumnya. Pada dasarnya, teknologi di ciptakan bukan untuk tujuan kejahatan, melainkan dengan sifat yang netral. Namun, seiring perkembangan waktu, dengan semakin luasnya fungsi dan kematangan teknologi informasi, serta meningkatnya globalisasi, pelaku kejahatan semakin terdorong untuk memanfaatkan internet sebagai sarana kejahatan.

Penggunaan media internet saat ini memudahkan manusia mendapatkan informasi dan hal lainnya. Internet telah mempermudah banyak aspek kehidupan, tetapi di balik kemudahan ini, terdapat tantangan keamanan yang signifikan, yang dapat berujung pada kerentanan dan potensi terjadinya berbagai jenis kejahatan yang dapat menimbulkan korban. Oleh karena itu, keselamatan masyarakat, baik sebagai subjek maupun objek penggunaan teknologi, harus mengambil sikap hati-hati. Penting untuk mempertimbangkan bahwa tidak hanya aparat penegak hukum saja yang bertanggung jawab untuk menjaga keamanan masyarakat, tetapi juga masyarakat itu sendiri.[2]

Penegakan hukum merupakan kebutuhan yang sangat penting untuk mencapai keamanan, keadilan, dan kemanfaatan hukum dalam penerapan hukum terhadap kasus kejahatan di bidang teknologi informasi, karna akan menjadi masalah yang sangat meresahkan yaitu terjadinya kejahatan yang di lakukan di dunia maya atau yang biasa di sebut dengan *cybercrime.* Kejahatan tersebut dapat disebabkan oleh kelalaian atau kurangnya kepedulian pengguna komputer dalam

[2] Daud Ahmad, "Kebijakan Penegakan Hukum dalam Upaya Penanggulangan Tindak Pidana Teknologi Informasi". *Lex Crimen*, Vol.3, No.2 2013, hlm 101.

melindungi data sensitif dan pribadinya, terutama data keuangan yang digunakan dalam bentuk *online banking*, dompet elektronik, e-*commerce*, dan *platform* pembayaran.[3]

Perkembangan kejahatan siber yang pesat menjadi tantangan utama dalam menyesuaikan kerangka hukum yang ada. Hukum harus mampu melindungi hak-hak korban, mengejar pelaku kejahatan, dan mencegah kejahatan serupa di masa depan.[4] Di luar upaya regulasi dan penegakan hukum, pencegahan menjadi kunci penting dalam menghadapi tindak pidana *phishing*. Pendidikan dan kesadaran masyarakat terhadap ancaman siber masih perlu ditingkatkan, terutama dalam memahami cara mengenali dan menghindari upaya *phishing*. Pemerintah, lembaga pendidikan, dan sektor swasta dapat berkolaborasi untuk mengadakan kampanye literasi digital yang komprehensif, termasuk pelatihan praktis tentang pengamanan data pribadi dan cara mengenali tanda-tanda *phishing*. Dengan upaya pencegahan yang sistematis, diharapkan potensi korban *phishing* dapat diminimalkan, sehingga keamanan siber nasional semakin kuat.

Badan Siber dan Sandi Negara (BSSN) melaporkan 290 juta kasus serangan siber pada tahun 2019. Angka ini meningkat 25% dibandingkan tahun sebelumnya, ketika kejahatan siber di Indonesia mengakibatkan kerugian sebesar 34,2 miliar dolar AS.[5]

---

[3] Putri, Indah Eka, "Analisis Yuridis Putusan Hakim Dalam Perkara Tindak Pidana *Phishing* Yang Dilakukan Melalui Media Sosial" *Jurnal Hukum Pidana dan Kriminologi: DELICTI,* Vol.1, No.1, 2023, hlm 2.

[4] Utin Indah Permata Sari, "Kebijakan Penegakan Hukum Dalam Upaya Penanganan *Cyber Crime* Yang Dilakukan Oleh *Virtual Police* di Indonesia," Jurnal Studia Legalia Vol.2, No. 01, 2022, hlm 2.

[5] Ganda Arisandi, et all, "Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana *Phising*", Jurnal Penelitian Hukum, Vol.4, No.2, 2024, hlm 15.

Banyaknya kasus ancaman siber yang terjadi di Indonesia menunjukkan bahwa kapasitas teknologi dan keahlian di bidang siber yang dimiliki oleh pemerintah Indonesia masih kurang dibandingkan dengan kapasitas yang dimiliki oleh pelaku ancaman siber tersebut. Perkembangan teknologi yang berkembang semakin canggih juga menyebabkan ancaman-ancaman yang ada dalam ruang siber menjadi lebih canggih pula. Hal tersebut menunjukkan bahwa BSSN sebagai institusi keamanan siber nasional perlu untuk selalu meningkatkan kapasitas keamanan siber di Indonesia serta meningkatkan keahlian dari berbagai pihak yang ada didalamnya. Upaya tersebut penting dilakukan untuk mengurangi tingkat ancaman yang ada dalam ruang siber Indonesia.[6]

Tabel 1.
Jumlah Kasus Phishing di Indonesia Berdasarkan laporan IDADX dan SOCRadar[7]

Tahun	**Jumlah Kasus**
2021	19.919
2022	22.853
2023	64.989

Sumber: Laporan IDADX dan SOCRadar, (27 Juni 2024)

Tabel tersebut menunjukkan jumlah kasus *phishing* yang dilaporkan di Indonesia selama tiga tahun terakhir, berdasarkan data dari IDADX dan SOCRadar. Dari tabel tersebut terlihat adanya peningkatan yang signifikan dalam jumlah kasus *phishing* dari tahun ke tahun. Pada tahun 2021, tercatat sebanyak

[6] Haryanto Agus dan Satya Muhammad Sutra, "Upaya Peningkatan Keamanan Siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) Tahun 2017-2020", *Global Political Studies Journal*, Vol.7, No.1, 2023, hlm 61.

[7] IDADX, Laporan Aktivitas Phishing Domain, *https://idadx.id/*, lihat juga SOCRadar, *https://socradar.io/the-digital-industries-commonly-targeted-by-phishing-attacks-in-indonesia/*, pada tanggal 27 Juni 2024.

19.919 kasus *phishing*. Angka ini mengalami kenaikan sebesar 14,74% pada tahun 2022 menjadi 22.853 kasus. Peningkatan paling tajam terjadi pada tahun 2023, dengan jumlah kasus mencapai 64.989, atau meningkat hampir tiga kali lipat dibandingkan tahun sebelumnya. Lonjakan kasus di tahun 2023 juga dapat menjadi indikasi bahwa pelaku kejahatan siber semakin agresif dalam memanfaatkan perkembangan teknologi untuk menjalankan aksinya. Hal ini mengindikasikan bahwa ancaman *phishing* semakin meningkat seiring dengan pertumbuhan pengguna teknologi digital di Indonesia. Faktor kenaikan ini bisa disebabkan oleh peningkatan aktivitas daring, lemahnya literasi digital, serta kurangnya pengawasan keamanan siber. Di Indonesia, penegakan hukum terhadap tindak pidana *phishing* masih menghadapi berbagai tantangan, mulai dari keterbatasan pengetahuan dan sumber daya hingga kompleksitas hukum *cyber* yang masih berkembang.

Phishing merupakan sebuah upaya untuk mendapatkan informasi sesorang dengan teknik pengelabuan yang merugikan seseorang.[8] Pengelabuan (pemancingan informasi penting) adalah salah satu bentuk tindak pidana yang bermaksud untuk mendapatkan rahasia informasi dari seseorang, seperti nama pengguna, *password*, dan kartu kredit, dengan menyamar sebagai orang lain atau bisnis terpercaya di elektronik resmi komunikasi, seperti surat elektronik dan *instant messages*.[9] Metode yang digunakan dalam *phishing* adalah rekayasa sosial dan manipulasi psikologis untuk membuat korban memberikan informasi yang

[8] Dharani Luh Intan Candhika, et all, "*Perlindungan Hukum terhadap Tindak Pidana Phishing di Media Sosial",* Pekalongan: Penerbit NEM, 2024, hlm 2.

[9] Supriadi, Muhammad Rizal, dan Roni Andarsyah. "*Deteksi Halaman Website Phishing Menggunakan Algoritma Machine Learning Gradient Boosting Classifier"*. Penerbit Buku Pedia, 2023, hlm 1.

diminta. Dalam ranah keamanan komputer, *phishing* dikategorikan sebagai kejahatan *cyber* yang berbentuk penipuan.

Metode *phishing* ini melibatkan penyediaan tautan ke situs *web* yang serupa dengan konten situs *web* lain yang dikirimkan melalui email atau ke akun yang tidak diminta. Korban dapat ditemukan di media sosial, seringkali dalam bentuk pembaruan sistem diterima melalui *website* perbankan *online* dan aplikasi yang menggunakan sistem pembayaran elektronik. Akibatnya, para korban mudah terprovokasi dan dimanipulasi, baik secara sadar maupun tidak sadar, membagikan informasi dan data sensitif mereka. dengan para pelakunya.

Cyber Crime dalam bentuk *phishing* secara normatif di Indonesia belum ada peraturan undang-undang khusus yang mengatur tentang *phishing*. Namun demikian, pelaku masih bisa di kenakan pasal dalam Kitab Undang-Undang Hukum Pidana (KUHP) serta Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan perubahannya, sesuai dengan tindak pidana pelaku.

Belum efektifnya penerapan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) menjadikan kasus tindak pidana *phishing* menjadi dilematis, karena aparat penegak hukum belum bisa memanfaatkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) secara maksimal sebagai garda dan dasar utama untuk menjerat pelaku tindak pidana *phishing* di Indonesia.[10]

---

[10] Septian Araya Budi Mahesa, dan Hervina Puspitosari, "Optimalisasi Undang-Undang Nomor Tahun 2008 Tantang Informasi dan Transaksi Elektronik Dalam Penanganan Perkara Tindak Pidana Phising" *Jurnal Penelitian dan Pengabdian Masyarakat: COMSERVA*, Vol.2, No.2, 2023, hlm 2688.

Pemerintah Indonesia telah mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) sebagai respons terhadap situasi ini yang bertujuan memberikan perlindungan lebih kuat terhadap data pribadi masyarakat Indonesia, mengingat meningkatnya kasus *phishing* yang sering kali melibatkan pencurian data pribadi. UU PDP mengatur sanksi yang lebih berat bagi pelaku yang melakukan penyalahgunaan data pribadi, termasuk dalam kasus *phishing*. Diharapkan bahwa sanksi yang lebih berat akan memberikan efek jera bagi pelaku kejahatan siber. Di samping itu, keterbatasan pengetahuan dan sumber daya penegak hukum merupakan masalah utama dalam penegakan hukum terhadap *phishing*. Untuk mengatasi masalah ini, pemerintah telah memulai berbagai program pelatihan dan peningkatan kapasitas untuk penegak hukum. Ini akan membantu mereka menangani kasus kejahatan siber, termasuk *phishing,* dengan lebih baik.

Berdasarkan paparan latar belakang yang diatas, maka penulis memulai penulisan dengan mengangkat judul skripsi yaitu Aspek Hukum Kejahatan Siber Dalam Tindak Pidana Phishing (Penipuan Informasi) di Indonesia.

B. Rumusan Masalah

1. Bagaimana konsep tindak pidana *phishing* di dalam hukum pidana Indonesia?
2. Bagaimana mekanisme perlindungan korban tindak pidana *phishing* di Indonesia?

C. Tujuan dan Manfaat Penelitian

1. Tujuan Penelitian

Adapun tujuan dari penelitian ini atas dasar permasalahan yang sudah diuraikan di atas ialah:

a. Untuk mengetahui konsep tindak pidana *phishing* di dalam hukum pidana Indonesia.
b. Untuk mengetahui mekanisme perlindungan hukum terhadap korban tindak pidana *phishing* di Indonesia.

2. Manfaat Penelitian

Adapun manfaat pada studi ini adalah:

a. Manfaat Teoristis
    1) Sebagai referensi untuk peneliti selanjutnya yang relevan dengan studi ini, yaitu Aspek Hukum Kejahatan Siber Dalam Tindak Pidana Phishing (Penipuan Informasi) di Indonesia
    2) Sebagai rujukan bagi pengembangan ilmu pengetahuan dan ilmu-ilmu hukum terkait Aspek hukum Kejahatan Dalam Tindak Pidana Phishing (Penipuan Informasi) di Indonesia
b. Manfaat Praktis
    1) Sebagai sumber masukan pada pembaca tentang Aspek Hukum Kejahatan Siber Dalam Tindak Pidana Phishing (Penipuan Informasi) di Indonesia
    2) Dapat menambah pengalaman dan ilmu pengetahuan mengenai Aspek Hukum Kejahatan ISber Dalam Tindak Pidana Phishing (Penipuan Informasi) di Indonesia

D. Ruang Lingkup Penelitian

Penelitian ini akan meneliti aspek hukum kejahatan siber dalam tindak pidana phishing di Indonesia, dengan fokus konsep, karakteristis dan hambatan yang dihadapi dalam pemberantasan phishing. Materi penelitian akan membahas kriminalisasi tindak pidana phishing, mekanisme perlindungan bagi korban, serta evaluasi terhadap kebijakan hukum dalam menanggulangi kejahatan ini.

E. Penelitian Terdahulu

Sebuah penelitian yang solid membutuhkan pondasi yang kuat dari literatur terdahulu. Dalam bagian ini, analis akan meninjau dan menyintesis temuan-temuan kunci berdasarkan penelitian-penelitian sebelumnya yang berkaitan dengan penelitian ini. Dengan memeriksa penelitian sebelumnya dengan seksama, analisis akan menunjukkan hal-hal yang masih belum diketahui dan juga hal-hal yang membedakan dengan penelitian sebelumnya. Berikut beberapa hasil penelitian yang serupa dengan permasalahan yang dianalisis peneliti, namun memfokuskan pada aspek yang berbeda, yaitu sebagai berikut:

1. Skripsi Lutfiyatul Hanifah, Mahasiswa Fakultas Hukum Universitas Islam Sultan Agung, Semarang, Tahun 2023 yang berjudul "Pengaturan Tindak Pidana *Cyber Crime* Dalam Bentuk *Cyber Phishing* Menurut Hukum Pidana Indonesia".[11]

   Persamaan penelitian ini dengan penelitian Lufiyatul Hanifah, adalah sama-sama melakukan penelitian mengenai tindak pidana *cyber* dalam bentuk *cyber phishing* dan juga sama-sama mengunakan pendekatan normatif. Perbedaannya, fokus utama dari skripsi Lutfiyatul Hanifah

[11] Lutfiyatul Hanifah, "Pengaturan Tindak Pidana *Cyber Crime* Dalam Bentuk *Cyber Phishing* Menurut Hukum Pidana Indonesia" Skripsi, Fakultas Hukum Universitas Islam Sultan Agung, 2023.

adalah untuk mengetahui pengaturan tindak pidana *cyber crime*, sementara itu, penelitian ini lebih berfokus pada pengaturan tindak pidana phishing dan juga perlindungan korban.

2. Rhesita Yustitiana dengan judul "Pelaksanaan Pengaturan Hukum Tindak Kejahatan *Fraud Phishing* Transksi Elektronik Sebagai Bagian Dari Upaya Penegakan Hukum di Indonesia Di Kaitkan Dengan Teori Evektivitas Hukum".[12]

   Studi ini membahas tantangan dalam penegakan hukum terkait transaksi elektronik, khususnya dalam memerangi penipuan *phishing* di Indonesia. Faktor-faktor yang mempengaruhi efektivitas penegakan hukum antara lain penegakan hukum yang tidak memadai oleh perbankan, kurangnya pemahaman masyarakat terhadap akibat hukum dalam transaksi elektronik, dan infrastruktur pendukung yang belum memadai. Jurnal ini juga menyoroti pentingnya penegakan hukum yang efektif dan peran berbagai pemangku kepentingan, termasuk lembaga keuangan, dalam memerangi kejahatan transaksi elektronik.

   Persamaan penelitian ini degan penelitian Rhesita Yustitiana adalah metode penelitian yang sama-sama menggunakan pendekatan yuridis normatif, dan juga membahas tentang tindak pidana phishing, dan juga evaluasi terhadap regulasi yang ada. Perbedaan penelitian Rhesita Yustitiana terfokus pada kejahatan penipuan *phishing* dalam transaksi

[12] Rhesita Yutitiana, "Pelaksanaan Pengaturan Hukum Tindak Kejahatan Fraud *Phishing* Transksi Elektronik Sebagai Bagian Dari Upaya Penegakan Hukum di Indonesia Di Kaitkan Dengan Teori Evektivitas Hukum", Jurnal Hukum Visio Justisia, Vol. 1, No.1, 2021.

elektronik di Indonesia, sedangkan penelitian tidak hanya berfokus pada penipuan phishing dalam transaksi elektronik.

3. Naufal Mahira Dewantoro dan Dian Alan Setiawan "Penegakan Hukum Kejahatan Siber Berbasis *Phishing* Dalam Bnetuk *Application Package Kit* (APK) Berdasarkan Undang-Undang Informasi dan Elektronik.[13]

   Persamaan penelitian Naufal Mahira Dewantoro dan Dian Alan Setiawan adalah analisis mengenai kejahatan siber berbasis *phishing* di Indonesia, termasuk faktor-faktor penyebabnya, tantangan dalam penegakan hukum. Jurnal ini menyoroti bahwa motivasi finansial, kerentanan sistem teknologi, dan kurangnya edukasi masyarakat menjadi pendorong bagi pelaku *phishing*. Perbedaan yaitu terletak di fokus utama jurnal Naufal Mahira Dewantoro dan Dian Alan Setiawan adalah kejahatan siber berbasis *phishing* yang dilakukan melalui *Application Package Kit* (APK). Jurnal ini menjelaskan bagaimana pelaku kejahatan siber menggunakan APK untuk menipu korban dengan mengirimkan aplikasi yang tampaknya sah, tetapi sebenarnya dirancang untuk mencuri data pribadi dan informasi sensitif dari perangkat korban. Dalam konteks ini, jurnal menguraikan cara kerja kejahatan *phishing* berbasis APK, di mana pelaku mengirimkan file APK kepada calon korban dengan modus sebagai kurir dari perusahaan ekspedisi. Setelah aplikasi diinstal, aplikasi tersebut dapat membobol dan mentransfer data dari perangkat korban tanpa sepengetahuan mereka.

---

[13] Dewantoro Naufal Mahira dan Dian Alan Setiawan, "Penegakan Hukum Kejahatan Siber Berbasis *Phising* dalam Bentuk *Application Package Kit* (APK) Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik." *Bandung Conference Series: Law Studies*. Vol. 3, No. 2. 2023.

F. Tinjauan Pustaka

1. Hukum *Cyber*

Hukum siber *(Cyber Law)* atau Hukum Mayantara adalah istilah lain yang digunakan untuk menggambarkan hukum yang berkaitan dengan penggunaan teknologi informasi. Istilah lain yang juga di gunakan adalah hukum Teknologi Informasi *(Law of Information Techonology),* Hukum Dunia Maya (*Virtual word Law).* Istilah-istilah ini muncul sebagai akibat dari aktivitas di internet dan penggunaan teknologi informasi berbasis *virtual*. Dalam tesis ini digunakan istilah "*cyberlaws*" karena diasumsikan jika *cyber* diartikan sebagai "*cyberspace*" maka akan menghadapi banyak tantangan pembuktian dan penegakan hukum. Karena lembaga penegak hukum menghadapi tantangan ketika mereka harus membuktikan suatu fakta yang dianggap "virtual", yaitu sesuatu yang tidak dapat dilihat dan bersifat *pseudo-visible*, penting untuk menyadari bahwa hukum siber bukan hanya masalah hukum, namun tetap saja. persoalan hukum itu sendiri.[14]

Cyber law merupakan bidang multidisiplin yang menghubungkan pendekatan teknologi, sosiokultural (etika), dan hukum dengan cabang ilmu lain seperti hukum pidana, hukum perdata, perlindungan konsumen, bisnis, dan administrasi. Perkembangan teknologi informasi khususnya Internet membawa banyak manfaat bagi kehidupan, namun layaknya dua sisi mata uang, Internet juga dapat memberikan dampak negatif dan menjadi jalan bagi sebagian individu untuk melakukan kejahatan dasar dengan maksud merugikan kemanusiaan.[15]

---

[14] Ramli, Ahmad. M, "*Cyber Law dan HAKI Dalam Sistem Hukum Indonesia*", Bandung: Refika Aditama, 2006, hlm. 11.

[15] Ersya, Muhammad Prima "Permasalahan Hukum dalam Menaggulangi *cyber crime* di Indonesia", *Journal of Moraland Civic Education,* Vol.1, No.1, 2017, hlm 51.

Hukum *cyber* merujuk pada peraturan yang mengatur aktivitas di ranah dunia *cyber*. Secara menyeluruh *cyber law* tidak hanya mencakup tindak kejahatan di internet, tetapi juga mencakup peraturan yang melindungi para pelaku *e-commerce, e-learning*, pemegang hak cipta, rahasia dagang, paten, tanda tangan elektronik, dan banyak aspek lainnya. Dalam konteks ini, *cybercrime* dapat diartikan sebagai kejahatan yang dilakukan melalui internet yang didasarkan pada kecanggihan teknologi komputer dan telekomunikasi.[16] Hal ini juga diperkuat oleh adanya globalisasi.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia tidak secara jelas mendefinisikan istilah "*cyber*". Namun, UU ITE mengatur berbagai aspek yang berhubungan dengan dunia maya atau *cyberspace,* termasuk transaksi elektronik, tanda tangan elektronik, dokumen elektronik, penyelenggaraan sistem elektronik, dan tindak pidana terkait teknologi informasi dan komunikasi. Sedangkan menurut para ahli, definisi dari hukum *cyber* adalah sebagai berikut

1. Mohammad S. Adji

   Mohammad S. Adji mendefinisikan *cyber law* sebagai hukum yang mengatur masalah hukum yang muncul akibat pemanfaatan teknologi informasi dan komunikasi, terutama yang berkaitan dengan Internet. Ini meliputi berbagai hal seperti transaksi elektronik, perlindungan data pribadi, dan kejahatan siber.

2. Sutarno

   Sutarno menyatakan bahwa *cyber law* adalah suatu cabang ilmu hukum yang mengatur tentang informasi dan transaksi elektronik serta semua

[16] Yurizal, "*Penegakan Hukum Tindak Pidana Cyber Crime di Indonesia*", Malang: Media Nusa *Creative*, April 2018, hlm 17.

aktivitas yang dilakukan di dalam dunia maya, baik yang bersifat komersial maupun non-komersial.

3. Prof. Dr. Sunaryo

   Sunaryo menjelaskan *cyber law* sebagai hukum yang mengatur penggunaan teknologi informasi dan komunikasi, termasuk aspek-aspek yang berkaitan dengan pelanggaran hukum yang dilakukan melalui teknologi tersebut.

4. Jonathan Rosenoer

   Dalam pandangan internasional, Jonathan Rosenoer mendefinisikan *cyber law* sebagai seluruh hukum dan peraturan yang terkait dengan Internet dan jaringan komputer, termasuk masalah yang berkaitan dengan akses ke dan penggunaan jaringan, serta perlindungan terhadap hak-hak digital.

Cyber crime ini mengancam setiap orang dengan risiko yang sangat rendah untuk tertangkap oleh individu atau kelompok, sehingga menimbulkan kerugian besar bagi masyarakat dan negara. Ciri-ciri *cybercrime* dijelaskan oleh Abdul Wahid dan M. Labid:[17]

a. Tindakan ilegal, tidak sah, atau tidak bermoral tersebut terjadi di dunia maya, yang tidak jelas negara mana yang mempunyai yurisdiksi atas tindakan tersebut.
b. Tindakan tersebut dilakukan dengan memanfaatkan perangkat apa pun yang terhubung ke internet.
c. Tindakan ini mengakibatkan kerugian yang berwujud dan tidak berwujud (misalnya waktu, nilai, jasa, uang, harta benda, harga diri, martabat dan privasi informasi), yang biasanya lebih besar dibandingkan kerugian yang terkait dengan kejahatan konvensional.

[17] Wahid Abdul*, Kejahatan Mayantara*, Refika Aditama, Bandung, 2005, hlm 76.

d. Pelaku adalah individu yang memiliki kemampuan untuk menggunakan internet dan aplikasinya.
e. Perbuatan tersebut sering di lakukan secara transnasional/ melintasi batas negara.

Indonesia sendiri belum memiliki Undang-undang khusus tentang *cyber law* yang mengatur mengenai *cyber crime.* Namun, ada beberapa undang-undang positif lain yang secara umum berlaku dan dapat diterapkan terhadap penjahat dunia maya, khususnya dalam kasus di mana komputer digunakan sebagai alat komunikasi,[18] diantaranya itu Kitab Undang- Undang Hukum Pidana (KUHP), Undang-Undang No 19 Tahun 2002 tentang Hak Cipta, Undang-Undang Nomor 11 Tahun 2008 jo No 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.

a) Bentuk kejahatan *cyber*

1) *Unauthorized Access to Computer System and Service*

Kejahatan yang dilakukan dengan cara membobol sistem jaringan komputer tanpa izin atau sepengetahuan pemiliknya. Peretas biasanya melakukan ini dengan tujuan menyabotase atau mencuri informasi penting dan rahasia. Ada pula yang melakukan hal ini karena merasa tertantang untuk menguji kemampuannya dalam menembus sistem keamanan tinggi. Pekerjaan ini menjadi semakin umum seiring dengan berkembangnya teknologi Internet.

2) *Cyber Espionage*

[18] Edrisy, I.F, "*Pengantar Hukum siber*", Lampung: Sai Wawai *Publishing*, 2019, hlm 8.

Kejahatan yang memanfaatkan internet untuk melakukan kegiatan pengintaian terhadap pihak lain dengan cara menembus sistem jaringan komputer sasarannya.

3) *Offense Against Intellectual Property*

Kejahatan ini menargetkan Hak atas Kekayaan Intelektual milik pihak lain di internet. Hal ini termasuk, misalnya, menyalin secara ilegal tata letak situs *web* asing dan menyebarkan informasi di Internet yang merupakan rahasia dagang pihak lain.

4) *Infringements of Privacy*

Kejahatan ini menyasar informasi yang bersifat sangat pribadi dan rahasia. Pelanggaran-pelanggaran ini umumnya menyasar informasi pribadi seseorang yang disimpan dalam bentuk berbasis komputer, yang jika diungkapkan kepada orang lain, dapat menimbulkan kerugian materiil atau immateriil bagi korbannya, seperti nomor kartu kredit, ATM. PIN, dan sebagainya.[19]

2. **Tindak Pidana *Phishing***

Phishing merupakan bentuk penipuan online di mana pelaku berusaha untuk memperoleh informasi sensitif seperti nama pengguna, kata sandi, nomor kartu kredit, atau informasi pribadi lainnya dengan menyamar sebagai entitas yang tepercaya dalam komunikasi elektronik. Metode yang diterapkan untuk melakukan penipuan dengan cara menipu target melalui alamat situs *web* palsu, dengan tujuan mencuri data pribadi target.

---

[19] Maskun, "*Kejahatan Siber (Cryber Crime) Suatu Pengantar*", Makasar: Prenada Media, 2013, hlm.51-54.

Sejarah phising telah mengganggu dunia maya selama lebih dari 2 dekade, dimulai pada tahun 1995 dengan America Online (AOL) Istilah *phishing* adalah variasi dari istilah memancing di mana tindakan *phishing* menyerupai penangkapan ikan dengan cara berikut: penyerang "memancing" korban menggunakan "umpan" dan "memancing" untuk informasi pribadi atau rahasia korban. Studi komprehensif tentang definisi *phishing* dilakukan oleh Lastdrager dimana dia mengidentifikasi definisi *phishing* yang disepakati: "*Phishing* adalah tindakan penipuan yang dapat diskalakan di mana peniruan identitas digunakan untuk mendapatkan informasi dari target"

Phising berasal dari istilah dalam bahasa Inggris yaitu *fishing* yang artinya "memancing", istilah 'memancing' yang digunakan di sini mengacu pada tindakan memancing korban ke dalam perangkap untuk memasukkan data pribadi dengan maksud tertentu. *Phishing* sendiri sering disebarkan oleh pelaku melalui *email* korban, menggunakan *email* tersebut untuk mempromosikan *website* palsu dengan maksud untuk menjebak korban yang dituju.".[20]

Phishing biasanya menyasar pengguna layanan perbankan *online*, karena melibatkan pengisian data seperti ID pengguna dan kata sandi. Namun, hal ini juga bisa menargetkan pengguna layanan *online* lainnya. Ketika pengguna memasukkan data ID dan kata sandi mereka ke dalam *form login* palsu, pelaku kejahatan siber yang melakukan *phishing* akan mendapatkan informasi tersebut. Tercatat secara global, jumlah penipuan bermodus *phising* 42% (empat puluh dua persen) dari modus selain *phising* yang dinyatakan dalam *website* Anti-*Phising*

[20] Muhammad, Faiz Emery. Beniharmoni Harefa, "Pengaturan Tindak Pidana Bagi Pelaku Penipuan *Phisning* Barbasis *Web*", Fakultas Hukum Universitas Pembangunan Nasional Veteran Jakarta, Vol.6, No.1, 2023, hlm 227.

Working Group (APWG). Hal ini menunjukkan bahwa kejahatan internet dalam bentuk *phishing* sangat meluas secara global. *Phishing* biasanya juga terjadi melalui media sosial yang terhubung dengan internet, seperti *email* dan *website.*[21]

Beberapa aspek utama yang dapat menyebabkan timbulnya *phishing cybercrime* yaitu:

1. Semakin maju suatu negara, namun tak diimbangi kesejahteraan masyarakatnya, makin besar potensi kesenjangan social muncul.
2. *Lifestyle*.
3. Minimnya sosialisasi / arahan baik dari akademi umum misal sekolah / edukasi dari orang tua tentang kegunaan internet, sehingga beragam penyalahgunaan muncul.
4. Makin banyak sosmed, media elektronik, serta media penyimpanan virtual *(cloud)*, menjadikan manusia makin tergandrungi dengan akses internet di kehidupanya.
5. Lalai.
6. Muncul hasrat pengakuan dari manusia lain.
7. Semakin maju teknologi serta mudahnya melakukan akses jaringan internet *anytime anywhere* tanpa terbatas masa.[22]

Untuk mengetahui lebih lanjut mengenai *phishing*, berikut adalah jenis-jenis *phishing* yang paling umum, yakni:

---

[21] Suhardi Rustam, "Analisa *clustering phishing* Dengan K-Means Dalam Meningkatkan Keamanan Komputer", ILKOM Jurnal Ilmiah, Vol.10, No.2, 2018, hlm 175.

[22] Hariyono Akbar Galih & Frans Simangunsong, "Perlindungan Hukum Korban Pencurian Data Pribadi (*Phishing cybercrime*) Dalam Perspektif Kriminologi", *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance*, Vol. 3, No. 1, 2023, hlm 437.

a) *Email Phising*. *Email phishing* menggunakan *email* sebagi cara untuk menjangkau calon korban. Data menunjukkan bahwa sekitar 3,4 miliar *email* palsu di kirim setiap hari. Tidak sulit untuk membayangkan jumlah korban yang mungkin terlibat dalam tindakan ini.

b) *Spear Phising*. *Spear phising* merupakan salah satu bentuk dari *email phishing*. Berbedanya *spear phishing* menarget korban acak. Teknik ini biasanya digunakan setelah informasi penting tentang calon korban di kumpulkan, seperti nama dan alamat.

c) *Whaling*. *Whaling* adalah jenis *phishing* yang menargetkan individu dengan otoritas tinggi dalam suatu organisasi, seperti pemilik bisnis, direktur perusahaan, atau manajer personalia. Tujuannya adalah untuk mengincar orang-orang dengan akses penting atau data sensitif.

d) *Web Phising*. *Web phishing* mengacu pada penggunaan situs *web* palsu untuk menipu calon korban. Situs *web phishing* menyerupai situs *web* resmi dan menggunakan nama domain yang serupa. Ini dikenal sebagai *spoofing domain*.[23]

Pengaturan hukum terhadap kejahatan siber berupa *phishing* sebelumnya diatur dalam Pasal 378 KUHP tentang penipuan, karena *phishing* secara umum merupakan tindakan penipuan. Penipuan yang terdapat dalam Pasal 378 KUHP adalah:

> "Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan,

[23] Dodi Parlagutan, et all, "Penegakan Hukum Terhadap Tindak Pidana *Phishing* Ditinjau Berdasarkan Hukum Yang Berlaku Di Indonesia", Fakultas Hukum Universitas Pembangunan Nasional Veteran Jakarta, 2023, hlm 4.

> menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi hutang maupun menghapuskan piutang, diancam karena penipuan dengan pidana penjara paling lama empat tahun".[24]

Penggunaan Pasal KUHP dalam pemidanaan pada kasus *cyber crime* hanya dilakukan berdasarkan penafsiran dikarenakan terdapat perbedaan terhadap jenis tindak pidana *cyber crime* dengan tindak pidana konvensional yang ada, walaupun metode *phishing* dan penipuan dalam KUHP memiliki kesamaan unsur perbuatannya akan tetapi tetap memiliki perbedaan mulai dari mulai dari bentuk tindak pidana, penentuan *locus delicti* sampai tempos delicti-nya. Oleh karena itu, tindak pidana *cyber crime* merupakan pengelompokkan dari jenis tindak pidana yang tergolong baru, dikarenakan *cyber crime* hadir mengikuti perkembangan teknologi yang baru berkembang pesat.[25]

Tahun 2008 menjadi momen penting dengan disahkannya sebuah peraturan perundang-undangan di Indonesia tentang Informasi dan Transaksi Elektronik, yang di dalamnya mencantumkan larangan terhadap perbuatan-perbuatan tertentu dalam transaksi elektronik beserta ketentuan pidananya. Seiring berkembangnya zaman, ketika internet masuk kedalam bagian dari sebuah jaringan komputer, perbuatan-perbuatan hukum yang berkembang didalamnya menjadi pengelompokkan penanganan menggunakan undang-undang ini, salah satunya yaitu *phishing*.[26]

---

[24] Pasal 378 Kitab Undang- Undang Hukum Acara Pidana.

[25] Leticia Malunsenge, et all, "Penegakan Hukum Terhadap Pelaku dan Korban Tindak Pidana *Cyber Crime* Berbentuk *Phishing* di Indonesia", *Lex Crime,* 2022, hlm 3.

[26] *Ibid,* hlm 4

Pasal 28 Ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik juga bisa digunakan untuk menangkap pelaku tindak pidana *Cyber crime Phishing* ini. Bunyi Pasal 28 Ayat (1) yaitu:

> "Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik".[27]

3. Regulasi Hukum *Cyber* di Indonesia

Regulasi adalah salah satu norma atau aturan hukum yang Harus dipatuhi regulasi mengandung arti mengendalikan perilaku manusia atau masyarakat dengan aturan atau pembatasan.[28] Regulasi hukum *cyber* di Indonesia adalah seperangkat aturan dan kebijakan yang dirancang untuk mengatur aktivitas di dunia maya atau siber. Regulasi ini mencakup berbagai aspek hukum yang mengacu pada penggunaan teknologi informasi dan komunikasi, termasuk transaksi elektronik, perlindungan data pribadi, keamanan informasi, dan pencegahan serta penanggulangan kejahatan siber.

Penting bagi setiap negara untuk memiliki regulasi hukum yang mampu mengatur dan mengawasi aktivitas di dunia siber. Oleh Karena itu, negara dalam hal ini memfasilitasi pemamfaatan teknologi informasi yang sekaligus memberikan perlindungan bagi kepentingan *public*, dalam hal ini masyarkat luas, dari segala bentuk gangguan akibat bentuk gugatan akibat penyalahgunaan informasi elektronik.[29] Regulasi hukum siber di Indonesia terutama diatur oleh

---

[27] Pasal 28 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

[28] Subekhan, "*Perspektif Regulasi Manajemen Keselamatan Kapal Niaga di Indonesia*", Damera Press, Jakarta Selatan, 2023, hlm 1.

[29] Endah Dewi Nawangsasi, "*Hukum Administrasi Negara Dalam Perspektif Cyber Law Terkait Data Privasi dan Beschikking Digitalisasi*", PT Alumni, Bandung, 2021, hlm.184.

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang disahkan pada tahun 2008 dan telah beberapa kali direvisi, dengan revisi terakhir pada tahun 2016. UU ITE mencakup berbagai aspek hukum terkait teknologi informasi dan transaksi elektronik.

Banyak peraturan lainnya yang mengatur tentang hukum *cyber*, peraturan peraturan tersebut di antaranya:

1) Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik yang telah di ubah menjadi Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
2) Undang-Undang No 27 tahun 2022 tentang Perlindungan Data Pribadi.
3) Peraturan Menteri Komunikasi dan Informatika (PERMENKOMINFO)
    a) Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016.
    b) Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020.

Regulasi-regulasi tersebut membentuk kerangka hukum yang komprehensif untuk mengatur berbagai aspek aktivitas siber di Indonesia. UU ITE sebagai dasar utama memberikan definisi dan sanksi terhadap berbagai jenis kejahatan siber, termasuk *phishing*, *malware*, dan akses ilegal ke sistem informasi. Sementara itu, Undang-Undang Perlindungan Data Pribadi (UU PDP) menambah lapisan perlindungan terhadap hak individu atas data pribadi mereka, memastikan

bahwa setiap pengumpulan, penyimpanan, dan pemrosesan data dilakukan secara sah dan etis.[30]

Perkembangan teknologi yang semakin pesat menuntut regulasi hukum siber di Indonesia untuk beradaptasi demi menghadapi berbagai tantangan baru. Teknologi seperti kecerdasan buatan (AI), *blockchain*, dan *Internet of Things* (IoT) membawa risiko baru, termasuk serangan siber yang semakin canggih dan sulit diidentifikasi. Oleh karena itu, regulasi seperti UU ITE dan UU Perlindungan Data Pribadi (UU PDP) perlu diperbarui secara berkala agar tetap relevan dengan kebutuhan zaman. Dalam pelaksanaannya, kolaborasi antara pemerintah, pelaku usaha, dan masyarakat sangat diperlukan agar regulasi ini bisa berjalan efektif dan menciptakan lingkungan digital yang aman.

Kementerian Komunikasi dan Informatika (Kominfo) memainkan peran sentral dalam merumuskan kebijakan, mengawasi pelaksanaan regulasi, serta melakukan sosialisasi kepada masyarakat mengenai pentingnya keamanan siber. Selain itu, aparat penegak hukum seperti Kepolisian Republik Indonesia (Polri) dan Badan Siber dan Sandi Negara (BSSN) bertugas untuk menangani kasus-kasus kejahatan siber, melakukan investigasi, dan menindak pelaku kejahatan sesuai dengan ketentuan hukum yang berlaku. Kementerian Pertahanan, TNI, Polri, BIN, Kemenkominfo, Lembaga Sandi Negara, dan berbagai instansi terkait lainnya adalah lembaga-lembaga pemerintah yang perlu disinergikan untuk menangkis, menangkal, dan mencegah serangan *cyber* baik yang dilakukan oleh

[30] Daeng Yusuf, et all, "Perlindungan Data Pribadi Dalam Era Digital: Tinjauan Terhadap Kerangka Hukum Perlindungan Privasi" *Innoveative Journal of Social Science Research,* Vol. 3, No. 6, 2023, hlm 4.

state maupun *non-state actor* yang berasal dari dalam negeri maupun negara lain.[31]

Kerja sama antarnegara sangat penting untuk mengatasi kejahatan siber yang sering melibatkan pelaku lintas negara. Di dalam negeri, pemerintah juga perlu memperkuat kemampuan aparat penegak hukum dalam menyelidiki kejahatan siber, termasuk keahlian di bidang forensik digital. Dengan pembaruan regulasi dan peningkatan kerja sama, Indonesia diharapkan dapat lebih siap menghadapi ancaman siber sekaligus melindungi masyarakat dari risiko dunia maya.

Keberadaan regulasi yang cukup komprehensif belum mampu mengatasi tantangan signifikan dalam penegakan hukum siber di Indonesia. Salah satu tantangan utama adalah kurangnya sumber daya manusia yang terampil dalam bidang keamanan siber, baik di sektor pemerintah maupun swasta. Selain itu, perkembangan teknologi yang cepat sering kali membuat regulasi yang ada menjadi kurang relevan atau sulit untuk diimplementasikan secara efektif. Itulah kenapa diperlukan edukasi lebih mengenai kejahatan di dunia siber dan bagaimana penanggulangannya. Di sisi inilah kemudian peran pemerintah juga diperlukan guna menutupi kekurangan yang dimiliki untuk meningkatkan *awareness* di masyarakat sebagai pengguna internet.[32]

---

[31] Chotimah Hidayah Chusnul, "Tata Kelola Keamanan Siber Dan Dimplomasi Siber Di Indonesia Di Bawah Kelemabgaan Badan Siber dan Sandi Negara" Jurnal Politica Dinamika Masalaha Politik Dalam Negeri dan Hubungan Internasional, Vol. 10, No. 2, 2019, hlm 121.

[32] Mahendra Yustika Citra dan Ni Komang Desy Setiawati Arya Pinatih, "Strategi Penangangan Keamanan Siber (*Cyber Security*) Di Indonesia", Jurnal Review Pendidikan dan Pengajaran, Vol. 6, No. 4, 2023, hlm 1946.

G. Metode Penelitian

Penelitian adalah suatu proses penyelidikan ilmiah di mana data dikumpulkan, diolah, dianalisis, dan ditarik kesimpulan berdasarkan pendekatan, metode, dan teknik tertentu untuk memecahkan suatu masalah.[33] Teknik penelitian adalah cara-cara untuk menghadapi apa dan bagaimana yang mungkin diterapkan dalam penelitian.[34] Setiap pemeriksaan bergantung pada sejauh mana informasi yang mendasari latihan penelitian. Teknik pemeriksaan adalah suatu pendekatan untuk mencapai suatu dengan menggunakan penalaran yang cermat melalui melihat, mencatat, merencanakan dan menyelidiki untuk membuat laporan.[35] Untuk memudahkan penyusunan penelitian ini, peneliti menggunakan metode penelitian sebagai berikut:

1. Jenis, Pendekatan, dan Sifat Penelitian
   a. Jenis Penelitian dan Pendekatan Penelitian

      Jenis penelitian yang peneliti gunakan ialah yuridis normatif. Penelitian yuridis normatif adalah jenis penelitian hukum yang berfokus pada studi dokumen hukum dan teori hukum untuk menemukan aturan hukum yang berlaku serta bagaimana aturan-aturan tersebut diterapkan dalam berbagai kasus. Penelitian ini terutama mengandalkan bahan-bahan hukum primer seperti undang-undang, peraturan, keputusan pengadilan, literatur hukum, jurnal, dan karya ilmiah. Penelitian hukum normatif adalah penelitian yang

---

[33] Arifin, Zainal, "*Penelitian Pendidikan Metode dan Paradigma Baru"*, Bandung: PT Remaja Rosdakarya, 2012, hlm. 2.

[34]Fakultas Hukum Universitas Malikussaleh, *"Buku Panduan Akademik"*, Lhokseumawe, 2016, hlm.106.

[35] Narbuko, Chalid, *"Metode Penelitian",* Jakarta: Bumi Aksara, 2007, hlm.2.

bertujuan untuk menemukan, mendeskripsikan, dan menganalisis norma hukum yang ada dalam sistem hukum positif.[36]

Penelitian ini menggunakan dua pendekatan yaitu pendekatan hukum dan pendekatan konseptual. Pendekatan hukum merupakan suatu metode penelitian dimana dokumen hukum berupa peraturan perundang-undangan menjadi dokumen acuan utama penelitian. Pendekatan konseptual merupakan suatu metode penelitian dalam ilmu hukum yang menawarkan sudut pandang hukum terhadap aspek konsep-konsep dasar hukum atau bahkan terhadap nilai-nilai yang terkandung dalam pengembangan suatu peraturan yang berkaitan dengan konsep-konsep hukum tersebut.[37] Dengan menggunakan kedua pendekatan tersebut, penelitian ini bertujuan untuk memberikan pandangan yang komprehensif tentang Penegakan Hukum Terhadap Tindak Pidana *Phishing* Dalam hukum *Cyber* di Indonesia.

b. Sifat Penelitian

Penelitian deskriptif adalah jenis penelitian yang bertujuan untuk memaparkan dan menjelaskan fenomena yang terjadi dalam suatu konteks tertentu secara sistematis, faktual, dan akurat.

2. Sumber Data

Sumber data sangat penting dalam penelitian karena data yang dikumpulkan digunakan untuk menjawab pertanyaan penelitian atau

---

[36] Salim H. S, "*Penerapan Teori Hukum pada Penelitian Tesis dan Disertasi*", Jakarta, Raja Grafindo Persada, 2013, hlm 19.

[37] SAP, Pendekatan Perundang-undangan (Pendekatan Status) Dalam Penelitian Hukum, *https://www.saplaw.top/pendekatan-perundang-undangan-statute-approach-dalam-penelitian-hukum/* , pada tanggal 1 Agustus 2024.

mengembangkan teori. Dalam penelitian ini penulis menggunakan tiga sumber data hukum yaitu:

1. Bahan hukum primer

   Bahan hukum primer adalah sumber-sumber hukum yang memiliki kekuatan hukum mengikat dan merupakan dasar utama dalam pembentukan dan penegakan hukum. Berikut ini merupakan peraturan perundang-undangan terkait tindak pidana *phishing* dalam konteks hukum *cyber* yang ada didalam penelitian ini:

   1) Undang-undang Nomor 11 Tahun 2008 jo Undang-Undang Nomor 19 Tahun 2016 jo Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik
   2) Undang-undang No 27 tahun 2022 tentang Perlindungan Data Pribadi
   3) Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.

2. Bahan hukum sekunder

   Bahan hukum sekunder adalah sumber-sumber yang memberikan penjelasan atau analisis mengenai penjelasan dan analisis mengenai bahan hukum primer, seperti buku, artikel, dan jurnal yang membahas Tindakan *phishing* dalam konteks hukum *cyber*.

3. Bahan hukum tersier

   Bahan hukum tersier merupakan pelengkap yang memberikan tambahan informasi dan klarifikasi terhadap dokumen hukum primer dan sekunder.

3. Teknik Pengumpulan Data

Metode pengumpulan data yang digunakan merupakan studi Kepustakaan. Dalam studi kepustakaan penulis memakai metode pengumpulan data melalui membaca, mencatat, dan mempelajari bahan-bahan hukum tersebut di atas mengenai penuntutan pelanggaran *phishing* dalam konteks hukum *cyber* di Indonesia.

4. Teknik Analisis Data

Analisis data adalah suatu proses mempelajari persamaan, perbedaan, dan perbandingan data yang telah disiapkan dan menggunakan mode data untuk mendapatkan informasi tambahan. Analisis data yang digunakan analisis kualitatif. Penelitian kualitatif merupakan jenis penelitian deskriptif yang cenderung menggunakan analisis untuk memperoleh makna lebih dari penelitian.

H. Sistematika Penulisan

Sistematika penulisan skripsi ini dibagi menjadi beberapa bab, yaitu:

Bab pertama, dalam bab ini secara keseluruhan memuat tentang latar belakang permasalahan yang menjelaskan hal-hal yang menjadi dasar dibuatnya tulisan ini. Dalam bab ini juga dapat dibaca pokok permasalahan, tujuan penelitian, manfaat penelitian, tinjauan pustaka, metode penelitian, dan sistematika penulisan.

Bab kedua, dalam bab ini berisikan tentang jawaban dari hasil pertanyaan yang disebutkan dalam rumusan masalah yang pertama, yaitu bagaimana konsep mengenai tindak pidana *phishing* di dalam hukum pidana Indonesia.

Bab ketiga, dalam bab ini berisikan tentang jawaban dari hasil pertanyaan yang disebutkan dalam rumusan masalah kedua, yaitu mekanismes perlindungan korban tindak pidana *phishing* di Indonesia.

Bab keempat, dalam bab ini diakhiri dengan memuat kesimpulan dan saran-saran yang diharapkan dapat memberikan kesimpulan yang jelas dari beberapa penjelasan yang telah dipaparkan oleh penulis pada bagian sebelumnnya