

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Perkembangan teknologi modern telah membawa perubahan yang sangat signifikan dalam berbagai aspek kehidupan masyarakat modern. Kemajuan teknologi *digital*, khususnya melalui pemanfaatan internet, media sosial, serta berbagai sistem transaksi elektronik, telah menciptakan pola interaksi baru dalam aktivitas sosial maupun ekonomi masyarakat. Kehadiran teknologi tersebut tidak hanya mempermudah proses komunikasi antarindividu maupun kelompok, tetapi juga memperluas ruang interaksi yang sebelumnya terbatas oleh faktor geografis dan waktu.

Selain itu, teknologi *digital* membantu masyarakat untuk melakukan berbagai kegiatan secara lebih mudah dan efisien, seperti berkomunikasi, mengakses informasi, melakukan transaksi perdagangan, hingga menjalankan berbagai aktivitas ekonomi lainnya tanpa harus bertatap muka secara langsung. Perkembangan ini juga telah mendorong terjadinya transformasi *digital* dalam berbagai sektor kehidupan, termasuk dalam bidang perdagangan, jasa, dan keuangan. Dengan semakin luasnya penggunaan teknologi *digital* tersebut, ekonomi *digital* pun berkembang pesat dan mendorong meningkatnya penggunaan transaksi elektronik dalam kehidupan masyarakat sehari-hari.¹

¹ Muhammad Safrizal Dwi Prayoga et al., "Transformasi Pembayaran Digital Di Era Ekonomi Digital: Analisis Efisiensi Dan Dampaknya Terhadap UMKM," *Nusantara Entrepreneurship and Management Review* 3, no. 1 (2025): 29–38, <https://doi.org/10.55732/nemr.v3i1.1563>.

Perkembangan teknologi *digital* tidak hanya memberikan berbagai manfaat dan kemudahan bagi masyarakat dalam menjalankan aktivitas sehari-hari, tetapi juga menimbulkan tantangan baru berupa munculnya berbagai bentuk kejahatan yang memanfaatkan teknologi informasi sebagai sarana pelaksanaannya. Seiring dengan meningkatnya penggunaan internet dan sistem elektronik dalam berbagai bidang kehidupan, peluang terjadinya penyalahgunaan teknologi juga semakin besar. Kejahatan yang dilakukan dengan memanfaatkan sistem elektronik tersebut dikenal sebagai kejahatan siber (*cybercrime*).

Perkembangan *cybercrime* menunjukkan bahwa teknologi *digital* tidak hanya digunakan untuk tujuan yang bersifat positif, tetapi juga dapat dimanfaatkan oleh pihak-pihak tertentu untuk melakukan berbagai tindakan melawan hukum. Modus kejahatan ini sering kali dilakukan dengan memanfaatkan celah atau kelemahan dalam sistem *digital*, serta memanfaatkan rendahnya tingkat literasi *digital* masyarakat yang membuat sebagian pengguna teknologi menjadi lebih rentan terhadap berbagai bentuk kejahatan berbasis teknologi.²

Kejahatan *cybercrime* yang semakin berkembang dalam masyarakat adalah *scamming*, yaitu tindakan penipuan yang dilakukan melalui media elektronik dengan tujuan memperoleh keuntungan secara tidak sah dari korban.

Praktik *scamming* umumnya dilakukan melalui berbagai platform *digital*

² Gita Eka Sila and Cevi Mochamad Taufik, "Literasi Digital Untuk Melindungi Masyarakat Dari Kejahatan Siber," *Komversal* 5, no. 1 (2023): 112–23, <https://doi.org/10.38204/komversal.v5i1.1225>.

seperti media sosial, aplikasi pesan instan, *marketplace*, maupun situs web tertentu. Pelaku biasanya menggunakan identitas palsu, manipulasi informasi, serta teknik rekayasa sosial untuk meyakinkan korban agar menyerahkan sejumlah uang atau informasi pribadi kepada pelaku.³ Fenomena penipuan *digital* menunjukkan bahwa perkembangan teknologi informasi telah melahirkan bentuk kejahatan baru yang memiliki karakteristik berbeda dengan kejahatan konvensional.

Kejahatan berbasis teknologi informasi seringkali dilakukan secara anonim dengan memanfaatkan identitas *digital* yang sulit dilacak. Kondisi tersebut menyebabkan proses penegakan hukum terhadap pelaku kejahatan siber menjadi lebih rumit dibanding dengan kejahatan konvensional. Proses pembuktian dalam kejahatan *digital* juga memerlukan pemahaman terhadap sistem elektronik serta bukti *digital* yang digunakan dalam proses penegakan hukum.⁴

Kebutuhan masyarakat saat ini tidak terlepas dari peran utama teknologi informasi yang terus mengalami perubahan signifikan. Perkembangan teknologi, terutama dalam sektor informasi dan komunikasi, tidak hanya berdampak pada cara orang berinteraksi dan memperoleh layanan, tetapi juga secara signifikan mengubah pola kehidupan sosial, ekonomi, serta budaya masyarakat modern.

³ Ande Aditya Iman Ferrary, Sri Hartini, and Prihatini Purwaningsih, "Kajian Hukum Terhadap Tindak Pidana Cyber Phising Yang Digunakan Untuk Mengambil Data Pribadi Pada Situs Digital Trading Dihubungkan Dengan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Transa," *Yustisi* 10, no. 2 (2023): 1–12, <https://doi.org/10.32832/yustisi.v10i2.14314>.

⁴ Elvina Tanoto et al., "Kekuatan Alat Bukti Elektronik Dalam Proses Pembuktian Di Peradilan Pidana," *Jurnal Ilmu Hukum* 2, no. 1 (2024): 90–96, <https://doi.org/10.62017/syariah>.

Internet, yang awalnya merupakan alat terbatas dalam konteks akademik dan militer, kini telah menjadi infrastruktur penting dalam kehidupan sehari-hari. Akses internet kini bukan hanya sekadar layanan tambahan, tetapi telah menjadi kebutuhan mendasar dalam struktur masyarakat digital masa kini.

. Peningkatan kasus penipuan *digital* menunjukkan bahwa kejahatan berbasis teknologi informasi telah menjadi salah satu permasalahan hukum yang cukup serius di Indonesia.

Data dari Indonesia Anti-Scam Center (IASC) yang berada di bawah koordinasi Otoritas Jasa Keuangan menunjukkan bahwa hingga tahun 2025 terdapat sekitar 297.217 laporan penipuan online dengan total kerugian masyarakat mencapai sekitar Rp7 triliun.⁵ Data tersebut menunjukkan bahwa praktik penipuan *digital* tidak hanya terjadi secara sporadis, tetapi telah berkembang secara luas dan menimbulkan kerugian yang cukup besar bagi masyarakat. Data tersebut menunjukkan bahwa praktik penipuan *digital* tidak hanya terjadi secara sporadis, tetapi telah berkembang secara luas dan menyeluruh.

Peningkatan kasus penipuan *digital* tersebut menunjukkan bahwa ruang *digital* yang seharusnya memberikan kemudahan bagi masyarakat juga menghadirkan risiko baru berupa penyalahgunaan teknologi informasi. Kondisi tersebut mendorong negara untuk membentuk regulasi yang dapat mengatur aktivitas masyarakat di ruang *digital* sekaligus memberikan

⁵ Devi Anjheli, "Privasi Digital Dan Kejahatan Phishing Di Indonesia : Evaluasi Kritis Terhadap Efektivitas UU ITE Dan UU PDP Berdasarkan Laporan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) Tahun 2023 , Lebih Dari 215 Juta Penduduk Telah Terhubung" 4, no. 1 (2024).

perlindungan hukum bagi pengguna teknologi informasi. Upaya negara dalam mengatur aktivitas di ruang *digital* diwujudkan melalui pembentukan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik yang merupakan perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-undang ini menjadi dasar hukum untuk beragam aktivitas yang berlangsung di dalam lingkup sistem elektronik. Salah satunya adalah mengatur tindak pidana yang menggunakan teknologi informasi.

Ketentuan yang berkaitan dengan penipuan dalam transaksi elektronik diatur dalam Pasal 28 ayat (1) yang menyatakan bahwa setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik. Pelanggaran terhadap ketentuan tersebut dikenakan sanksi pidana sebagaimana diatur dalam Pasal 45A ayat (1) dengan ancaman pidana penjara paling lama enam tahun dan/atau denda paling banyak satu miliar rupiah.⁶

Pengaturan lain yang berkaitan dengan kejahatan *digital* terdapat dalam Pasal 35 Undang-Undang Informasi dan Transaksi Elektronik yang mengatur mengenai manipulasi, penciptaan, perubahan, penghilangan, atau perusakan informasi elektronik dengan tujuan agar data tersebut dianggap sebagai data yang autentik. Pelanggaran terhadap ketentuan tersebut dapat dikenakan sanksi pidana sebagaimana diatur dalam Pasal 51 ayat (1) dengan ancaman pidana penjara paling lama dua belas tahun dan/atau denda paling banyak dua belas

⁶ Altje Agustin Musa and Ronald Elrik Rorie, "Vol. 15 No. 5 (2025): Lex Privatum Jurnal Fakultas Hukum Unsrat" 15, no. 5 (2025).

miliar rupiah.⁷

Pengaturan mengenai tindak pidana penipuan dalam sistem hukum pidana Indonesia juga diatur dalam Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana. Ketentuan mengenai penipuan diatur dalam Pasal 492 KUHP yang menyatakan bahwa setiap orang yang dengan maksud menguntungkan diri sendiri atau orang lain secara melawan hukum menggunakan nama palsu, tipu muslihat, atau rangkaian kebohongan untuk membujuk orang lain menyerahkan barang, memberikan utang, atau menghapuskan piutang dapat dipidana. Ketentuan tersebut menunjukkan bahwa praktik *scamming* memiliki unsur yang sejalan dengan tindak pidana penipuan dalam hukum pidana, meskipun dilakukan melalui media elektronik.

Keberadaan berbagai ketentuan hukum tersebut menunjukkan bahwa sistem hukum di Indonesia telah memberikan dasar hukum yang mengatur terhadap berbagai bentuk penyalahgunaan teknologi informasi yang terjadi dalam masyarakat. Melalui pengaturan tersebut, negara berupaya menciptakan kerangka hukum yang dapat mengatur penggunaan teknologi informasi secara bertanggung jawab serta mencegah terjadinya berbagai tindakan yang melanggar hukum di ruang *digital*.

Kajian hukum mengenai *cybercrime* juga menjelaskan bahwa perkembangan teknologi *digital* yang berlangsung sangat cepat menuntut adanya kemampuan adaptasi dari sistem hukum agar tetap relevan dan mampu menjangkau berbagai bentuk kejahatan. Dalam konteks ini, hukum tidak hanya

⁷ Dokumen Elektronik, "Vol. 15 No. 4 (2025): Lex Privatum Jurnal Fakultas Hukum Unsrat" 15, no. 4 (2025).

berguna sebagai alat pengendali sosial, tetapi juga memiliki peran penting dalam memberikan kepastian hukum serta menjamin perlindungan bagi masyarakat sebagai pengguna teknologi informasi. Dengan adanya kepastian dan perlindungan hukum tersebut, diharapkan masyarakat dapat memanfaatkan teknologi *digital* secara aman, tertib, dan bertanggung jawab.⁸

Meskipun demikian, pengaturan hukum mengenai penipuan yang dilakukan dengan memanfaatkan teknologi informasi masih menimbulkan sejumlah persoalan yuridis dalam praktik penerapannya. Permasalahan tersebut terutama berkaitan dengan bagaimana norma hukum yang berlaku dalam peraturan perundang-undangan dapat diterapkan secara tepat terhadap berbagai bentuk praktik *scamming* yang dilakukan melalui sistem elektronik. Modus penipuan yang memanfaatkan teknologi *digital* umumnya memiliki karakteristik yang berbeda dengan penipuan konvensional, karena pelaku sering menggunakan identitas palsu, melakukan manipulasi informasi, serta memanfaatkan berbagai media elektronik sebagai sarana untuk menipu korban. Kondisi ini menimbulkan tantangan tersendiri dalam proses penegakan hukum, khususnya dalam menentukan apakah suatu perbuatan telah memenuhi unsur-unsur tindak pidana sebagaimana diatur dalam peraturan yang berlaku.

Oleh karena itu, muncul pertanyaan yuridis mengenai bagaimana ketentuan dalam Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik dapat digunakan untuk menilai terpenuhinya unsur perbuatan pidana, unsur kesalahan, serta bentuk pertanggungjawaban

⁸ Fakultas Hukum et al., "Transformasi Digital Dan Keamanan Siber : Upaya Penanggulangan Kejahatan Di Era Teknologi Di Indonesia" 06, no. 01 (2025): 341–47.

pidana pelaku dalam tindak pidana penipuan yang dilakukan melalui pemanfaatan teknologi informasi.¹⁰

Berdasarkan uraian tersebut, penting untuk dilakukan kajian hukum mengenai pengaturan hukum terhadap praktik *scamming* serta bagaimana pertanggungjawaban hukum pelaku *scamming* terhadap korban berdasarkan ketentuan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Oleh karena itu, penelitian ini dilakukan agar dapat menjawab permasalahan mengenai pertanggungjawaban hukum pelaku *scamming* terhadap korban dalam aturan hukum positif yang berlaku di Indonesia.

Berdasarkan uraian tersebut, peneliti tertarik untuk melakukan penelitian dalam bentuk skripsi yang berjudul **“Pertanggungjawaban Hukum Pelaku *Scammer* Terhadap Korban *Scamming* Berdasarkan Undang-Undang Nomor 1 Tahun 2024 Tentang Informasi Dan Transaksi Elektronik”**.

B. Rumusan Masalah

Berdasarkan latar belakang permasalahan yang telah diuraikan, maka rumusan masalah dalam penelitian ini dirumuskan sebagai berikut :

1. Bagaimanakah pengaturan hukum mengenai tindak pidana *scamming* dalam sistem hukum di Indonesia berdasarkan Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik?
2. Bagaimanakah pertanggungjawaban hukum bagi pelaku *scammer* terhadap korban berdasarkan ketentuan Undang-Undang Nomor 1 Tahun 2024

tentang Informasi dan Transaksi Elektronik?

C. Tujuan penelitian

Dalam penelitian ini, peneliti merumuskan 2 tujuan penelitian sesuai dengan rumusan masalah yang diteliti :

1. Mengetahui pengaturan hukum yang berkaitan dengan praktik *scamming* dalam sistem hukum di Indonesia, khususnya yang diatur dalam Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik. Tujuan ini diarahkan untuk memahami ketentuan hukum yang mengatur penggunaan sistem elektronik dalam aktivitas masyarakat serta norma hukum yang dapat digunakan untuk menilai perbuatan penipuan yang dilakukan melalui media elektronik, termasuk ketentuan mengenai penyebaran informasi menyesatkan dalam transaksi elektronik, manipulasi informasi elektronik, serta ketentuan pidana yang berkaitan dengan penyalahgunaan teknologi informasi dalam praktik penipuan *digital*.
2. Mengetahui bentuk pertanggungjawaban hukum bagi pelaku *scamming* terhadap korban dalam tindak pidana penipuan yang dilakukan melalui sistem elektronik. Tujuan ini dimaksudkan untuk memperoleh pemahaman mengenai bagaimana ketentuan hukum pidana dapat diterapkan terhadap pelaku *scamming*, termasuk penilaian terhadap unsur perbuatan, unsur kesalahan, serta penerapan sanksi pidana berdasarkan ketentuan dalam Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik, sehingga dapat memberikan gambaran mengenai pertanggungjawaban hukum pelaku penipuan *digital* dalam sistem hukum

positif di Indonesia.

D. Manfaat Penelitian

1. Manfaat Teoritis

Penelitian ini diharapkan dapat memberikan peran terhadap pengembangan ilmu pengetahuan di bidang hukum, khususnya dalam kajian hukum pidana yang berkaitan dengan tindak pidana yang dilakukan melalui media elektronik. Pembahasan mengenai pertanggungjawaban hukum pelaku *scamming* diharapkan dapat memperkaya pemahaman mengenai penerapan ketentuan pidana terhadap perbuatan penipuan yang dilakukan melalui sistem elektronik sebagaimana diatur dalam Undang- Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik. Selain itu, penelitian ini diharapkan dapat menjadi referensi akademik bagi penelitian selanjutnya yang berkaitan dengan penipuan tindak pidana berbasis teknologi informasi serta penerapan pertanggungjawaban pidana terhadap pelaku kejahatan di ruang *digital*.

2. Manfaat Praktis

a. Bagi Pemerintah (Regulator/OJK):

Penelitian ini diharapkan dapat memberikan masukan bagi pemerintah dalam upaya meningkatkan efektivitas pengaturan hukum yang berkaitan dengan tindak pidana penipuan melalui media elektronik. Hasil penelitian ini juga diharapkan dapat menjadi bahan pertimbangan dalam upaya penguatan kebijakan hukum yang berkaitan dengan penanggulangan praktik *scamming* yang memanfaatkan perkembangan teknologi informasi.

b. Bagi Aparat Penegak Hukum (Kepolisian, Jaksa, Hakim):

Penelitian ini diharapkan dapat memberikan pemahaman yang lebih jelas mengenai penerapan ketentuan hukum terhadap pelaku *scamming* yang melakukan penipuan melalui sistem elektronik. Hasil penelitian ini juga diharapkan dapat menjadi bahan pertimbangan bagi aparat penegak hukum dalam menerapkan ketentuan pidana yang diatur dalam Undang-Undang Nomor 1 Tahun 2014 tentang Informasi dan Transaksi Elektronik sehingga proses penegakan hukum terhadap pelaku penipuan *digital* dapat dilakukan secara tepat sesuai dengan ketentuan Hukum yang berlaku.

C. Metode penelitian

1. Jenis penelitian

Penelitian ini menggunakan metode normatif pendekatan yang fokus pada kajian norma-norma hukum yang berlaku terkait masalah tersebut. Metode ini menggunakan studi kepustakaan dengan menganalisis peraturan perundang-undangan, asas-asas hukum, doktrin, dan putusan pengadilan yang relevan dengan pelanggaran *cybercrime*. Penelitian normatif berarti meneliti aspek internal hukum positif, bukan perilaku atau situasi sosial empiris di lapangan. Penelitian ini memilih metode normatif karena fokus pada analisis terhadap peraturan hukum yang relevan dengan perlindungan korban terkait insiden kejahatan siber. Penelitian normatif mengacu pada norma-norma hukum yang terdapat dalam perundang-undangan serta norma-norma yang

berlaku dalam masyarakat atau praktik umum yang ada dalam masyarakat.⁹

2. Metode Pendekatan

Pada Penelitian ini peneliti menggunakan metode pendekatan sebagai berikut :

a. Pendekatan Undang-Undang (*Statute Approach*):

Menganalisis peraturan perundang-undang dan regulasi yang berkaitan dengan isu hukum yang diteliti. Dalam penelitian ini, fokus utama adalah menganalisis Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik. Peneliti akan mengkaji pasal-pasal kunci seperti Pasal 28 ayat (1) mengenai berita bohong yang merugikan konsumen, Pasal 35 mengenai manipulasi informasi elektronik, serta Pasal 45A mengenai sanksi pidananya. Selain itu, pendekatan ini juga merujuk pada Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP) untuk melihat delik penipuan konvensional dengan delik siber.

b. Pendekatan Kasus (*Case Approach*):

Menganalisis kasus hukum atau putusan pengadilan yang relevan dengan kejahatan siber untuk melihat bagaimana konstruksi pertanggung jawaban bank dan penerapan pembuktian di dalam praktik peradilan.

c. Pendekatan Konseptual (*Conceptual Approach*):

Pendekatan ini merujuk pada doktrin dan pandangan para ahli hukum

⁹ Paulana Christian Suryawin et al., “Kajian Penegakan Hukum Tindak Pidana *Cybercrime* Di Indonesia : Analisis Implementasi Uu Iti Dan Tantangan Dalam Praktik” 2, No. 2 (2026): 145–58.

dalam literatur untuk melengkapi definisi teknis *scamming* yang belum diatur secara mendalam dalam undang-undang. Peneliti menggunakan Teori Pertanggungjawaban Pidana, Asas Kepastian Hukum di Ruang Siber, dan Teori Perlindungan Hukum sebagai fondasi untuk membangun argumen mengenai beban tanggung jawab pelaku terhadap kerugian materiil maupun immaterial korban.

3. Sumber Bahan Hukum

Penelitian ini menggunakan sumber bahan hukum sebagai berikut:

- a. Bahan Hukum Primer: Berupa Undang-Undang Nomor 19 Tahun 2016, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, serta perubahan terbarunya dalam Undang-Undang Nomor 1 Tahun 2024. Selain itu, peneliti juga merujuk pada Undang-Undang Nomor 1 Tahun 2023 tentang KUHP, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, serta kumpulan Putusan Pengadilan yang telah berkekuatan hukum tetap terkait perkara *scamming*.
- b. Bahan Hukum Sekunder: Berupa hasil penelitian, jurnal hukum, buku-buku teks hukum siber, jurnal hukum mengenai kejahatan komputer, serta hasil penelitian atau tesis yang relevan. Selain itu, peneliti juga menyertakan doktrin atau pendapat para ahli hukum terkemuka yang dipublikasikan dalam artikel ilmiah maupun makalah seminar untuk memperkuat analisis mengenai pertanggungjawaban pidana pelaku.

- c. Bahan Hukum Tersier: Berupa kamus hukum, ensiklopedia, dan kamus besar bahasa Indonesia sebagai pendukung dalam menjelaskan istilah-istilah teknis.

4. Proses Pengumpulan Bahan Hukum

Dalam melaksanakan pengumpulan data, maka peneliti mengklasifikasikan serta mengumpulkan data yang diambil yaitu sebagai berikut: Studi Pustaka (*Library Research*): Mencari dan mengumpulkan data dari bahan hukum primer, sekunder, dan tersier melalui penelusuran dokumen hukum, literatur buku di perpustakaan, maupun melalui repositori jurnal *digital* yang kredibel.

5. Analisis Bahan Hukum

Analisis data adalah proses mencari dan menyusun data secara sistematis dari bahan hukum yang diperoleh dengan cara mengelompokkan data ke dalam kategori, menjabarkan secara mendalam, dan menarik kesimpulan. Analisis data yang penulis gunakan dalam penelitian ini adalah Deskriptif Analitis. Deskriptif analitis adalah suatu analisis yang menjelaskan atau menggambarkan aturan hukum mengenai pertanggungjawaban hukum bagi pelaku *scammer* terhadap korban *scamming* sesuai hukum yang berlaku, penulis tidak hanya memaparkan pasal-pasal normatif dalam Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagai aturan hukum positif belaka namun juga mengkaitkan dengan realita permasalahan kejahatan siber di lapangan, untuk kemudian ditarik kesimpulan mengenai efektivitas perlindungan hukum korban kejahatan siber.

D. SISTEMATIKA PENULISAN

penulisan disusun guna memberikan kemudahan dalam memahami serta menelaah keseluruhan penelitian. Pada laporan penelitian ini, susunan penulisan dibagi ke dalam empat bab, yang masing-masing bab memuat pembahasan pokok sebagaimana dijelaskan secara ringkas sebagai berikut ini:

BAB 1: PENDAHULUAN

Pada bab pertama terdiri dari latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, metode penelitian dan sistematika penulisan

BAB II : TINJAUAN PUSTAKA

Bab kedua menjelaskan tentang Tinjauan Umum *Scamming*, Konsep Kejahatan *Scamming* dalam Hukum Pidana, Perlindungan Hukum dalam perspektif Hukum, Perlindungan Hukum terhadap Masyarakat dalam bersosial media.

BAB III : PEMBAHASAN

Bagian penjelasan menjawab dari rumusan masalah yang diteliti yaitu, Bagaimana konsep *Scamming* (unsur kesalahan/niat jahat) dalam hukum pidana dan Bagaimana bentuk perlindungan hukum yang dapat diberikan kepada korban *scamming* dalam permasalahannya tersebut.

BAB IV : PENUTUP

Bagian keempat merupakan penutup yang memuat kesimpulan dan saran dari penelitian.