BAB I

PENDAHULUAN

A. Latar Belakang

Seiring pekembangan zaman, kemajuan teknologi berkembang pesat, Hal ini terbukti dengan munculnya berbagai inovasi teknologi di seluruh dunia. internet dan media sosial membawa dampak perubahan terhadap perilaku manusia dalam bersosialisasi dan berkomunikasi.

Internet juga mendekatkan yang jauh dan mempererat hubungan seseorang yang telah dekat melalui media sosial yang ada di internet. Banyak sekali dampak positif yang kita dapatkan dari internet khususnya dari media sosial. Media sosial merupakan sarana berkomunikasi satu sama lain dan berlangsung secara online yang memungkinkan masyarakat saling berkomunikasi tanpa dibatasi oleh dampak negatif media sosial[1].

Keamanan di dunia *cyber* saat ini masih sangat rentan karena kemampuan menggunakan teknologi telah menjadi umum. Peretas dapat dengan mudah menembus sistem keamanan yang telah dirancang dengan cermat. Sistem keamanan internet seringkali gagal, sehingga muncul

[1] Rose Mini, *Dampak Internet Dalam Kehidupan Sosial,* (Penebar Swadaya, 2006), h. 17

kejahatan internet disebut dengan kejahatan dunia maya *(cyber Phising)* [2].

Cyber phishing merupakan perilaku menipu seseorang untuk memberikan atau mencuri informasi pribadi biasanya dilakukan dengan menyamar sebagai individu atau entitas terpercaya, seringkali dengan menggunakan situs web atau tautan palsu. Penyerang melakukan serangan *phishing* dengan mengirimkan *email* yang disamarkan sebagai pesan resmi dari penyedia layanan yang dikenal korban. "Silahkan masukkan user ID/Password anda" adalah salah satu dari banyak tautan yang ditemukan di bar subjek. Korban dibawa ke situs web penipuan melalui tautan phising yang dikirimkan melalui *email*. Seringkali, penipuan *phishing* digunakan untuk mendapatkan keuntunganAkibat dari adanya *Cyber phising* ini yaitu kerugian finansial dan mengancam privasi dan keamanan *online* secara keseluruhan. Informasi data data pribadi yang para pelaku dapatkan ini dapat digunakan untuk kegiatan ilegal atau disalahgunakan untuk mengakses layanan *online* yang bersifat sensitif dan bahkan bisa dijual ke pihak lain. Selain itu ada juga kerugian lain yang didapatkan korban seperti pelakunya yang tidak diketahui dimana lokasinya atau lokasi pelaku yang jauh dari lokasi korban, hal tersebut akan membuat penangkapan pelaku akan sangat ribet dan

[2] Aisyah, (Dkk), " *Analisis Perkembangan Digital Forensik dalam Penyidikan Cybercrime di Indonesia secara systematic*", Jurnal Esensi Infokom, Vol. 6 No. 1, (2022), 22-27.

memakan banyak waktu sehingga penanganannya belum terlalu maksimal.[3]

Indonesia tidak luput dari kasus kebocoran data pribadi. Terdapat beberapa kasus pelanggaran data pribadi yang terjadi di Indonesia. Contohnya, pada April 2021, diungkapkan sejumlah 533 juta pengguna Facebook mengalami kebocoran data, meliputi nama lengkap, tanggal lahir, jenis kelamin, kata sandi, lokasi negara, alamat email, dan username ID yang di dalamnya juga terdapat data pribadi masyarakat Indonesia. Selanjutnya, pada Juli 2021, terjadi kebocoran data di ranah perbankan terhadap sejumlah dua juta nasabah asuransi BRI Life. Kebocoran tersebut disebabkan adanya peretasan terhadap sejumlah data seperti foto KTP, rekening bank, laporan hasil pemeriksaan laboratorium nasabah, hingga informasi pajak nasabah[4].

Contoh kasus pencurian data pribadi melalui modus *phising* seperti dialami Baim Wong yang mengaku menjadi korban *phising* atau *hacking* melalui WhatsApp (WA) dan kejadian tersebut bermula saat ia mengklik file gambar dari orang yang menyamar sebagai pengantar paket. Ponsel Baim Wong menampilkan pemberitahuan transfer dari aplikasi keuangan setelah ia mengklik file tersebut. Dana senilai jutaan rupiah

---

[3] Eliasta Ketaren. (2016). *Cyber crime* , Cyber Space, DAN Cyber Law, Jurnal TIMES.

[4] Dicky Prastya, "Kasus Kebocoran Data di Indonesia Selama 2021, Termasuk Sertifikat Vaksin Jokowi", https://www.suara.com/tekno/2022/01/01/015822/daftar-kasus-kebocoran-data-di-indonesiaselama2021-termasuk-sertifikat-vaksin-jokowi?page=2, dilihat pada 27 Apri 2024.

ditransfer dari salah satu rekeningnya ke rekening tak dikenal, sehingga mengejutkannya (CNN Indonesia). Kasus tersebut sampai saat ini belum ada tindakan baik dari pemerintah maupun[5]. Aparat penegak hukum, sehingga menjadi alasan kuat bahwa perlindungan hukum terhadap korban pencurian data pribadi melalui modus kejahatan *phising* ini masih diabaikan. Dalam hukum positif, penipuan juga merupakan perbuatan yang dilarang keras. Pelaku penipuan dapat dijerat dengan Pasal 378 KUHP atau Pasal 492 UU 1/2023 tentang KUHP baru. Untuk penipuan *online*, pelaku dapat dijerat dengan Pasal 28 UU ITE. [6]

Kasus lainnya yang serupa juga terjadi, kasus ini dikutip dari berita online (Sumbar) yaitu warga Simpang Haru, Kecamatan Padang Timur, berjenis kelamin Perempuan. Dia mengalami kerugian sekitar Rp 150 juta. Kronologi penipuan ini berawal saat korban menerima pemberitahuan atas nama BRI, kemudian memberikan link tautan dan diminta menekan link tautan tersebut. Setelah menekan tautan tersebut, korban diarahkan mengisi formulir dan mengikuti panduan yang sudah ada di tautan tersebut. Tak lama setelah itu, korban menyadari ternyata uang dalam rekeningnya sudah berkurang

[5] Olivia Drost, *Kronologi Baim Wong Kena Phising via WA,* dari https://www.cnnindonesia.com/hiburan/20231103231916-234-1019881/kronologi-baim-wong
kena-phising-via-wa diakses pada Senin 19 Februari 2024

[6] UUD, N0.1 Tahun 2023 tentang hukum pidana.

drastis dan selain itu masih banyak lagi kasus *Cyber phising* di Indonesia yang terus meningkat setiap tahunnya.[7]

Informasi data data pribadi yang para pelaku dapatkan ini dapat digunakan untuk kegiatan ilegal atau disalah gunakan untuk mengakses layanan *online* yang bersifat sensitif dan bahkan bisa dijual ke pihak lain. Selain itu ada juga kerugian lain yang didapatkan korban seperti pelakunya yang tidak diketahui dimana lokasinya atau lokasi pelaku yang jauh dari lokasi korban, hal tersebut akan membuat penangkapan pelaku akan sangat ribet dan memakan banyak waktu sehingga penanganannya belum terlalu maksimal.[8]

Sebagaimana kasus serupa yang terjadi di bengkulu pada Agustus 2022, dimana seorang ibu rumah tangga berusia 63 tahun dikota Bengkulu menjadi korban penipuan online. Pelaku mengaku sebagai pegawai bank dan meyakinkan korban bahwa dirinya dapat membantu proses pencairan pinjaman bank senilai 300 juta, korbran kemudian mentransfer uang dalam beberapa tahap, total mencapai 545 juta. Namun pinjaman yang diajukan tidak kunjung cair, dan korban kehilangan seluru uang yang ditransfer[9].

---

[7] Duh, Pasutri Asal Padang Jadi Korban Link *Phishing*, Uang Senilai Rp 150 juta Lenyap Seketika.Disway.Id.dari *https://disway.id/read/419287*/duh-pasutri-asal-padang-jadi-korban link-*phishing*-uang-senilai-RP 150 juta -lebih-lenyap-seketika.

[8] Eliasta Ketaren. (2016). *Cyber crime* , Cyber Space, DAN Cyber Law, Jurnal TIMES.

[9] Diambil dari https://rbtv.disway.id/read/2612/ini-kronologi-kasus-penipuan-online-yang diungkap-satreskrim-polresta-bengkulu-hingga-raih-penghargaan.

Dalam UU Nomor 1 Tahun 2024 tentang ITE (Republik Indonesia), memiliki beberapa pasal yang berbicara tentang *Cyber crime Phising* ini yaitu pasal 28 negara. Meskipun demikian, karena peningkatan transaksi elektronik dan teknologi informasi, kejahatan *Cyber phising* meningkat di Indonesia. *Cyber phishing* adalah jenis pencurian atau mengambil milik orang lain secara ilegal merupakan perbuatan yang tidak terpuji atau disebut pencurian dalam hukum Islam. Ini dapat terjadi dengan cara apapun, seperti ketika seseorang mencuri harta benda dari sebuah rumah saat tuan rumah sedang tidur. Fakta bahwa informasi sensitif seperti kredensial logindapatdengan mudah dialihkan ke pengguna internet lain menjadikan pengguna *online banking* sebagai target umum serangan *phishing*. Dalam *phishing*, penipu mendapatkan akses ketika mengirimkan kredensial login dan kata sandi mereka ke dalam formulir login palsu.[10]

Kasus *Cyber phising* sudah terjadi di MukoMuko hal tersebut dikutip dari cerita warga yaitu pasangan suami istri di desa bunga tanjung kecematan teramang jaya kehilangan uang senilai Rp 600.000 dari rekening bank BRI. Kronologi kejadiannya ini berawal dari pesan yang mengirim link tautan atau link *Phising* ini. Pengirim link tersebut mengaku sebagai pihak bank dan pasangan suami istri ini terpedaya atas link

[10] Kadek Odie Kharisma Putra. "*Tindakan Kejahatan Pada Dunia Dalam Bentuk Phising*" Jurnal *cybersccurity* dan Forensik Digital, Vol. 5 No 2, 2022, hlm. 78.

Phising tersebut dan memberikan data pribadi, akun dan finansialnya. Akibatnya pelakunya bisa mengakses data tersebut dan mengambil uang korban di rekening.

Di dalam Islam, menipu merupakan dosa besar yang akan mendapatkan hukuman yang berat di akhirat. Di dalam Al-Qur'an dan Hadits juga dijelaskan bahwa berbohong adalah perbuatan yang dilarang dan dapat merugikan diri sendiri dan orang lain, Orang yang gemar berbohong sering kali akan menghadapi konsekuensi, baik di dunia maupun di akhirat. Dalam konteks duniawi, mereka mungkin kehilangan kepercayaan orang lain, mengalami kerugian dalam hubungan, atau bahkan menghadapi sangsi hukum tergantung pada sipat kebohongannya. Selain itu juga akan mendapatkan balasan yang setimpal dan azab dari Allah Swt.

Dalam konteks ini, penelitian dapat mengeksplorasi bagaimana implementasi pasal 28 oleh kepolisian di MukoMuko dalam menangani *cyber phising*. Yang dapat memberikan pandangan yang berharga tentang bagaimana penanganan terhadap kasus *cyber phising* seperti perlindungan terhadap korban, penegakan keadilan, dan pencegahan tindakan yang merugikan.

B. Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan di atas, maka dalam mempermudahkan penelitian ini, penulis mengajukan rumusan masalah sebagai berikut:

1. Bagaimana mendeskripsikan implementasi pasal 28 Undang- Undang No.1 Tahun 2024 tentang informasi dan transaksi elektronik terhadap perlindungan korban *cyber phising*?
2. Bagaimana Menjelaskan tentang tinjuan siyasah Tanfidiziah terhadap perlindungan korban *cyber phising* dalam pasal 28 undang-undang informasi dan transaksi elektronik?

C. Tujuan Penelitian

1. Untuk mendeskripsikan implementasi pasal 28 Undang-Undang No.1 Tahun 2024 tentang informasi dan transaksi elektronik terhadap perlindungan korban *cyber phising*.
2. Untuk menjelasakan Bagaimana tinjuan siyasah Tanfidiziah terhadap perlindungan korban *cyber phising* dalam pasal 28 undang-undang informasi dan transaksi elektronik.

D. Manfaat Penelitian

1. Manfaat Teoritis

   Penelitian ini di harap kan dapat menambah wawasan bagi pembaca tentang bagai mana implementasi pasal 28 UU Nomor 1 tahun 2024 tentang informasi dan transaksi elektronik terhadap perlindungan korban *cyber phising*.
2. Manfaat Praktis

   Secara praktis penulisan ini diharapkan dapat di jadikansebagi rujukan atau acuan bagi pembaca dan peneliti, selanjutnya yang ingin mengetahui lebih jauh mengenai mana implementasi pasal 28 UU Nomor 1 tahun

2024 tentang Informasi dan tansaksi elektronik terhadap perlindungan korban *cyber phising*.

E. Penelitian Terdahulu

Kajian penelitian terdahulu ini menjadi salah satu acuan penulis untuk melakukan penelitian agar penulis bisa memperkaya teori, maka dapat digunakan dalam mengkaji penelitian yang dilakukan. Penulis mengangkat beberapa penelitian sebagai referensi atau sumber dalam memperkaya bahan kajian pada penelitian penulis. Penelitian ini tidak dipengaruhi oleh penelitin sebelum nya yang telah di lakukan. Subjek penelitian adalah pasal 28 undang – undang Nomor 1 tahun 2024 tentang informasi dan transaksi elektronik terhadap perlindungan korban *cyber phising*. Berdasarkan dari penelusuran penulis terkait judul yang akan penulis teliti di temukan beberapa penelitian terdahulu yang mengangkat tema yang hampir sama yaitu:

1. Akhamad Fery Hasanudin dan A Basuki Babussalam yang berjudul "perlindungan hukum bagi korban kejahatan *phising* yang menguras saldo *M-Banking*" Penelitian ini merupakan tipe penelitian normatif yang mengunakan analisis kualitatif. Tujuan utama penelitian ini adalah untuk memahami cara operasi kejahatan *phising* di ranah *cyber*, khususnya dalam konteks hukum positif Indonesia. Penelitian ini mengidentifikasi dan menganalisis modus operandi yang digunakan oleh pelaku kejahatan phising,

serta menghubungkannya dengan kerangka hukum yang ada di

Indonesia. Penelitian ini juga mengulas regulasi hukum positif Indonesia yang relevan dalam menangani kejahatan *cyber,* termasuk *phising*, dan mengevaluasi efektivitas kerangka hukum tersebut dalam memberikan perlindungan terhadap individu dan organisasi. Hasil penelitian menunjukkan bahwa pelaku kejahatan *phising* secara cermat memanfaatkan berbagai metode manipulatif untuk mencapai tujuan mereka, dan kerap mengabaikan undang-undang yang mengatur keamanan *cyber* dan privasi data. Penelitian ini juga mengulas regulasi hukum positif Indonesia yang relevan dalam menangani kejahatan siber, termasuk phising, dan mengevaluasi efektivitas kerangka hukum tersebut dalam memberikan perlindungan terhadap individu dan organisasi.

2. Muhammad Adil Mubarak skripsi yang berjudul "perlindungan hukum terhadap korban pidana penipuan dalam transsaksi *E- commerce* tahun 2021 Penelitian ini menggunakan metode pendekatan yuridis normatif. Berdasarkan hasil penelitian ini adalah Untuk melindungi korban *ecommerce*, Undang-Undang Nomor 11 Tahun 2008 tentang Transaksi Elektronik serta regulasi terkait jual beli online diberlakukan. Untuk membantu mereka yang mengalami kerugian karena transaksi *online,* peraturan ini

melibatkan pemerintah dan penegak hukum. Namun, salah satu masalah yang menghalangi penegak hukum untuk melindungi korban jual beli *online* adalah kurangnya pengetahuan mereka tentang teknologi informasi. yang membuat penanganan kejahatan siber lebih sulit. Korban transaksi elektronik disarankan untuk tidak takut untuk melaporkan atau mengadukan pihak berwenang jika pelaku usaha melanggar hak-haknya. Pemerintah juga bertanggung jawab untuk mendidik masyarakat tentang cara menjadi lebih berhati-hati saat berbelanja *online*.

3. Fairuz Rhamdhatul Muthia (dkk) "kajian hukum pidana pada kasus kejahatan mayantara (*cyber crime*) dalam perkara pencemaran nama baik di Indonesia Penelitian ini menggunakan metode yuridis normatif dimana penulis hanya melihat undang-undang berdasarkan kasus pencemaran nama baik. Penelitian ini hanya mengkaji teori-teori hukum yang dihubungkan dengan aturan hukum dan kasus pencemaran nama baik melalui dunia maya Hasil penelitiannya Pasal 27 ayat (3) dan Pasal 310 hingga 321 dari Kitab UndangUndang Hukum Pidana mengatur pencemaran nama, baik sebagai tindak kejahatan siber atau *cyber crime*. Ketika fitnah dan informasi palsu tentang seseorang disebarkan, hal itu disebut pencemaran nama baik, dan inimembahayakan reputasi orang tersebut. Korban

dapat melaporkan pelanggaran pencemaran nama baik, dan pelaku dapat dikenakan hukuman penjara

dan denda. Setiap tahun, pencemaran nama baik meningkat, menjadikannya salah satu kasus kejahatan *cyber* yang paling sering ditangani. Seringkali, pencemaran nama baik dilakukan dengan sengaja untuk merusak kehormatan seseorang di masyarakat. Ini bisa dilakukan secara tulisan atau lisan.

4. M. Riza Addi Sulha dalam sriksi yang berjudul "tindak pidana carding dalam *cyber crime* menurut hukum pidana islam tahun 2020 " Penelitian ini adalah penelitian bersifat kualitatif yang mengkaji tentang tindak pidana carding. Penelitian ini bertujuan untuk menjawab beberapa pertanyaan utama yang dibahas dalam skripsi ini, spesifiknya, 1) cara hukum nasional melihat tindak pidana carding, dan 2) cara hukum Islam melihat tindak pidana carding. Studi ini menggunakan metode penelitian hukum normatif. Bahan hukum primer dan sekunder dari Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik adalah yang digunakan. Selain itu,penelitian dan analisis literatur tentang tindak pidana carding ditambahkan. Peneliti menemukan, bahwa sebagai Sebagai bagian dari kejahatan siber,Undang-Undang Nomor 19 Tahun 2016, yang merupakan perubahan dari Undang-

Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, mengatur tindak pidana carding. Ini mengikuti asas bahwa lex specialis derogat legi generalis, yang berarti bahwa undang-undang khusus mengesampingkan undang-undang umum. Selain itu, penulis menemukan bahwa, berdasarkan unsur-unsurnya, pelanggaran carding dalam hukum pidana Islam dapat diqiyaskan dengan jarimah al-sariqah dan termasuk dalam jarimah hudud.

5. Mohd. Yusuf DM, (dkk) " analisis kejahatan hacking sebagai bentuk *cyber crime* dalam system hukum yang berlaku di Indonesia tahun 2022Hacking adalah penyusup penyusupan atau menerobos program komputer milik orang. Penelitian ini menggunakan penelitian kepustakaan sebagai metode penelitian hukum normatif. Penelitian ini bertujuan untuk mengurangi kasus *Cyber crime* di Indonesia karena diperlukan penegakan hukum yang kuat dalam menangani tindak pidana Hacking untuk melindungi hak korban hacking.

Dari beberapa penelitian terdahulu di atas, maka penelitian yang akan di teliti penulis memiliki persamaan dan perbedaan persamaan nya yaitu sama – sama membahas terkait *cyber crime* naamun terdapat perbedaan dalam penelitian ini yaitu penulis lebih memfokuskan *cyber crime* yang berbentuk phising.

F. Metode Penelitian

Penelitian merupakan sarana pokok dalam pengembangan ilmu pengetahuan dan teknologi, maka metodologi penelitian yang diterapkan harus senantiasa disesuaikan dengan ilmu pengetahuan yang menjadi induknya.

Menurut Soerjono Soekanto, penelitian hukum merupakan suatu kegiatan ilmiah yang disasarkan pada metode sistematika dan pemikiran tertentu yang bertujuan untuk mempelajari satu dan beberapa gejala hukum tertentu dengan cara menganalisisnya. Selain itu juga diadakan pemeriksaan yang mendalam terhadap fakta hukum tersebut untuk kemudian mengusahakan suatu pemecahan atas permasalahan yang timbul[11]

1. Jenis penelitian dan metode pendekatan
   a. Jenis Penelitian

      Jenis Penilitian yang digunakan penyusun menggunakan penelitian hukum empiris dan penelitian lapangan (*field reseacrh*) yaitu penelitian langsung ke lapangan, karena data utamanya diambil langsung dari lapangan. Dari itu selain menelaah kaidah- kaidah dan norma hukumnya, saya juga menggunakan alat tinjau dengan literatur-literatur dari buku buku hukum yang ada.

   b. Metode Pendekatan

---

[11] Soerjono Soekanto, *Penelitian Hukum Normatif*, Jakarta: PT Raja Grafindo, 2012, h. 1.

Pendekatan yang dilakukan dalam penyusunan proposal skripsi ini antara lain pendekatan kualitatif dengan pendekatan studi kasus, penelitian yang bermaksud untuk memahami fenomena tentang apa yang dialami oleh subjek penelitian misalnya perilaku, persepsi, motivasi, dan tindakan, secara holistic dan dengan cara deskripsi dalam bentuk kata-kata dan bahasa, pada suatu konteks khusus yang alamiah dan dengan memanfaatkan berbagai metode alamiah. melalui penelitian ini akan diperoleh gambaran mengenai, *implementasi pasal 28 undang – undang Nomor 1 Tahun 2024 tantang informasi dan transaksi elektronik terhadap perlindungan korban cybber phising*. Sumber data dan bahan penelitian

1) Sumber data Primer

   Data primer adalah data yang diperoleh langsung dari sumber data lapangan. Data yang di peroleh melalui observasi langsung yakni pada kepolisian Polres Mukomuko

2) Sumber data Sekunder

   Data sekunder yaitu semua publikasi tentang hukum yang merupakan dokumen yang resmi, data yang di peroleh dari buku- buku yang tertulis para ahli seperti jurnal, skripsi dan kutipan kutipan dari

hasil wawancara jurnalis dari para narasumber sebagai penguat dari peneltian ini dan lain - lain.[12]

3) Teknik pengumpulan data

Pengumpulan sumber bahan hukum yang telah disebutkan disebelumnya, maka dalam penelitian ini pengumpulan bahan hukum primer (Lapangan), data yang diperoleh langsung darisumber data lapangan. Data yang di peroleh melalui observasi langsung yakni dengan cara : Wawancara, dokumentasi yang di lakukan langsung pada kepolisian Polres Mukomuko

4) Informan Penelitian

Yang menjadi subjek penelitian adalah Kepolisian Polres Mukomuko, dan yang menjadi Informan dalam penelitian adalah penyidik pembantu, dan sebagainya yang berperan dalam menangani kasus *cyber phising*

5) Teori yang digunakan

Teori yang digunakan untuk menganalisis masalah yang diteliti diantara lain:

a) Teori Rekayasa Sosial

Phishing adalah bentuk rekayasa sosial yang menggunakan manipulasi psikologis untuk meyakinkan korban agar menyerahkan

[12] Johnyy Ibrahim, *Teori Dan Metode Penelitian Hukum Normatif Malang*; Bayumediya publishing, 2010, h . 173.

informasi pribadi atau melakukan tindakan tertentu. Pelaku phishing memanfaatkan emosi seperti rasa takut, rasa ingin tahu, atau urgensi untuk mengelabui korban, seperti dalam contoh email palsu yang meminta korban mengklik tautan untuk mengupdate akun[13].

b) Teori kriminologi.

Teori ini membantu memahami akar penyebab kejahatan, termasuk kejahatan siber seperti phishing. Dengan menganalisis faktor-faktor seperti latar belakang pelaku, motivasi, dan konteks sosial, kita dapat memahami mengapa seseorang melakukan phishing[14].

6) Teknik Analisis Data

Mengenai teknik analisis data saya menggunakan dua macam metode, yaitu: Metode deduktif, yaitu metode yang di gunakan untuk menyajikan bahan atau teori yang sifatnya umum untuk kemudian di uraikan dan di terapkan secara khusus dan terperinci. Metode induktif, yaitu metode analisis yang berangkat dari fakta-fakta yang khusus lalu di

---

[13] Rahardjo Satjipto, *Sosiologi Hukum (*Togyakarta : Genta Publishing, 2010).

[14] Ni Made Indah Gayatri; Gede Made Swardhana, "*Teori Kriminologi Dalam Memecahkan Kejahatan Pencurian Beserta Kekerasan Yang Dilakukan Secara Berlanjut (Pasal 365 Kuhp*)", Jurnal Media Akademik (Jma), Vol. 2 No. 1, 2023.

tarik suatu kesimpulan yang bersifat umum. Proses yang digunakan dimulai dengan pengambilan data yang dilakukan dilapangan, dilanjutkan dengan proses pengolahan data yang telah diambil sebelumnya, kemudian setelah itu dilanjutkan dengan memilih dan memilah data-data yang dikira perlu untuk penelitian dan membuang data yang dirasa tidak diperlukan, setelah itu mencoba membuat suatu hipotesa awal dengan menyandingkan data yang ada

7) Teknik Penarikan Kesimpulan

Penarikan kesimpulan dalam penelitian skripsi ini menggunakan logika deduktif.Aturan-aturan hukumdan fakta, data yang bersifat umum dijabarkan (dikonkritisasi) dalam wujud peraturan hukum yang konkrit, sehingga dapat ditafsirkan, dan dapat diperoleh kesimpulan dari pembahasan sebagai upaya untuk mengetahui jawaban dari permasalahan-

permasalahan yang ada dalam skripsi ini[15]

G. Sistematika Penulisan

Agar penulisan penelitian ilmiah (skripsi) dapat terarah dengan tujuan maka diperlukan sistematika penulisan yang terdiri dari 5 (lima) bab, dimana antara 1 (satu) bab, dengan bab

---

[15] Abdulkadir Muhammad, 2004, *Hukum dan Penelitian Hukum*, : PT. Citra Aditya Bakti, Bandung, h.172.

lainnya saling mendasari dan berkaitan. Hal ini guna memudahkan pekerjaan dalam penulisan dan menangkap hasil dari penelitian. Adapun sistematika
penulisan ini terdiri dari bagian pembahasan yang diatur dari lima bab, adalah sebagai berikut :

BAB I : Pada bab ini berisi tentang pendahuluan yang meliputi latar belakang, rumusan masalah, tujuan penelitian, kegunaan penelitian, kerangka teori, metode penelitian, dan statistika penelitian.

BAB II : Berisi tentang landasan teori yang akan di angkat dalam penelitian ini, teori – teori yang diangkat dalam penelitian ini ialah teori-teori yang mencangkup tentang, peran kepolisian untuk perlindungan korban *cyber phising* perspektif siyasah tanfidziah.

BAB III : Pada bab ini akan di uraikan mengenai gambaran umum objek penelitian dengan memfokuskan pada setiap rumusan masalah yang hendak di jawab dalam penelitian ini, yaitu berkaitan dengan implementasi pasal 28 undang – undang nomor 1 tahun 2024 tentang informasi dan transaksi elektronik terhadap perlindungan korban *cyber phising* perspektif siyasah tanfidziah. kemudian dilakukan suatu analisis secara sistematis dan komprehensif terhadap

keseluruhan data informasi yang diperoleh untuk mengurai dan menjawab setiap rumusan masalah dalam penelitian.

BAB IV : Analisis Data, dalam bab ini, penulis berusaha menganilisis data mengenai implementasi pasal 28 undang -undang nomor 1 tahun 2024 tentang informasi dan transaksi elektronik terhadap perlindungan korban *cyber phising* perspektif siyasah tanfidziah

BAB V : Bab terakhir pada penulisan ini berisi kesimpulan atas uraian permasalahan serta pembahasan yang telah di sampaikan pada bab-bab sebelumnya. Selain itu juga, berisi saran-saran yang dapat peneliti berikan atas permasalahan atas yang diteliti oleh peneliti.