BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Tindakan penanggulangan terhadap tindak pidana menjadi hal yang sangat mendesak, mengingat pola kejahatan yang semakin rumit dan beragam, khususnya dalam perkembangan pesat teknologi digital masa kini. ”Percepatan transformasi digital di masa revolusi industri 4.0 membawa dampak signifikan terhadap berbagai lini kehidupan masyarakat, termasuk industri perbankan. Segala sesuatu akan berubah sebagai hasil dari transisi digital yang sedang berlangsung”.[1] Di tengah laju perkembangan digitalisasi yang kian cepat dan dinamis, industri perbankan menjadi salah satu sektor yang sangat dependen terhadap teknologi informasi dan komunikasi. Digitalisasi layanan perbankan, seperti *e-banking, m-banking,* serta sistem pembayaran elektronik semakin memudahkan masyarakat dalam melakukan transaksi keuangan. Namun, kemajuan ini juga membawa dampak negatif berupa meningkatnya *cybercrime* yang kian kompleks dan sulit ditangani.

Pesatnya evolusi teknologi di era digital ini membawa implikasi yang signifikan dalam industri perbankan. *Cybercrime* menjadi salah satu ancaman utama yang terus meningkat seiring dengan meningkatnya digitalisasi layanan keuangan. *Cybercrime* merupakan jenis kriminalitas terorganisir yang

[1]Dennys Megasari br Nababan, Sahuri Lasmadi, dan Erwin, “Pertanggungjawaban Pidana Terhadap Penyalahgunaan Data Pribadi Pada Tindak Pidana Dunia Maya”, *PAMPAS: Journal of Criminal Law,* Volume 4 Nomor 2, 2023, hlm. 233. (https://repository.unja.ac.id/59997/1/4.%20Pertanggungjawaban%20Pidana%20Terhadap%20Penyalahgunaan%20Data.pdf)

dilakukan oleh perseorangan maupun kelompok tertentu dengan kemampuan khusus dalam bidang teknologi informasi yang memanfaatkan kelemahan pada sistem perbankan maupun nasabah sehingga menimbulkan kerugian.[2] Berdasarkan laporan dari Badan Siber dan Sandi Negara (BSSN), dalam rentang waktu Januari hingga Agustus tahun 2024 telah terjadi 122,79 juta serangat siber atau anomali trafik internet di Indonesia.[3] Angka serangan siber yang begitu tinggi tersebut menunjukkan betapa seriusnya ancaman *cybercrime* terhadap stabilitas sektor perbankan di Indonesia. Hal ini merupakan hasil dari kebutuhan masyarakat global yang terus berkembang serta pengaruh informasi dan teknologi terhadap pergeseran dan tuntutan rakyat.[4]

Berdasarkan survei Mandiant M-Trends, pada tahun 2023, target utama serangan *cybercrime* adalah industri perbankan dan keuangan. Hal tersebut menandakan rentannya sektor perbankan akan ancaman serangan *cybercrime*.[5] Salah satu bentuk serangan *cyber* yang kerap terjadi adalah tindak pidana gangguan terhadap sistem elektronik dengan modus serangan *Distributed Denial of Service* (DDoS). Serangan DDoS adalah wujud final

[2]I Made Adi Medhyana Putra, "Perlindungan Hukum atas Hak Nasabah Bank Sebagai Konsumen Layanan Internet Banking Dari Ancaman Cybercrime", *Jurnal Kertha Wicara,* Volume 9 Nomor 4, 2020, hlm. 36. (https://ojs.unud.ac.id/index.php/kerthawicara/article/download/58241/34179)

[3]Lihat Irawati, "Ngeri! Ada 122,79 Juta Serangan Siber ke RI, Sektor ini Target Utamanya", Infobanknews, 2024, https://infobanknews.com/ngeri-ada-12279-juta-serangan-siber-ke-ri-sektor-ini-target-utamanya/

[4]Lihat Dina Elisa Putri Dina, Elly Sudarti, dan Elizabeth Siregar, "Tindak Pidana Penipuan Melalui Aplikasi Digital (Gagasan Pemikiran Pertanggungjawaban oleh Bank", *PAMPAS: Journal of Criminal Law,* Volume 5 Nomor 1, 2024, hlm. 73-74. (https://online-journal.unja.ac.id/Pampas/article/download/31716/17630/)

[5]Lihat Kemal Idris Balaka, Aulia Rahman Hakim, dan Frygyta Dwi Sulistyany, "Pencurian Informasi Nasabah di Sektor Perbankan: Ancaman Serius di Era Digital", *Yustitiabelen,* Volume 10 Nomor 2, 2024, hlm. 109. (https://journal.unita.ac.id/index.php/yustitia/article/download/1167/672/)

dari aktivitas *cracking* yang memiliki efek serius terhadap suatu sistem. *Cracking* sendiri adalah upaya seseorang untuk menerobos sistem milik pihak lain dengan tujuan merusaknya.[6] Serangan DDoS merupakan bentuk *cybercrime* yang menyasar *server* dengan tujuan mengganggu kinerjanya. Teknik yang digunakan adalah membanjiri server dengan lalu lintas yang sangat padat hingga *server* tidak mampu menangani permintaan akses dari pengguna secara efektif.[7]

Serangan DDoS dapat menyebabkan gangguan besar pada sistem perbankan, membuat layanan menjadi tidak tersedia dan menimbulkan ketidakpercayaan masyarakat terhadap keamanan sektor finansial di dunia maya. Serangan tersebut tidak hanya berdampak pada kerugian finansial, tetapi juga merusak reputasi perbankan serta menurunkan kepercayaan nasabah terhadap layanan yang mereka gunakan. Data terbaru dari Gcore Radar juga menunjukkan bahwa jumlah serangan DDoS mengalami peningkatan mencolok pada paruh pertama 2024, yakni sebesar 46% dan 12% di antaranya berasal dari industri keuangan. Jumlah serangan tersebut meningkat sebanyak 34% dibandingkan data kuartal ketiga dan keempat pada tahun 2023.[8] Lebih lanjut, data tersebut juga didukung dengan laporan dari perusahaan keamanan global Kaspersky yang menyatakan bahwa jenis

[6]Lihat Cheny Berlian, "DOS Attack Sebagai Tindak Pidana Siber Dalam Pengaturan Hukum di Indonesia", *Journal Equitable,* Volume 7 Nomor 1, 2022, hlm. 3. (https://ejurnal.umri.ac.id/index.php/JEQ/article/view/3686/1828)

[7]Lihat Tonny Rompi dan Harly Stanly Muaja, "Tindak Kejahatan Siber di Sektor Jasa Keuangan dan Perbankan", *Lex Privatum,* Volume 9 Nomor 4, 2021, hlm. 185. (https://ejournal.unsrat.ac.id/index.php/lexprivatum/article/view/33358/31553)

[8]"Lihat DDoS Attack Trends for Q1-Q2 2024: Insights from Gcore Radar Report", Gcore Radar, 2024, https://gcore.com/blog/radar-q1-q2-2024-insights/.

cybercrime yang kerap menyasarIndonesia adalah DDoS.[9]Hal ini menunjukkan betapa rentannya industri perbankan terhadap *cybercrime* yang semakin meningkat dan regulasi yang ada pada saat ini belum mampu secara efektif mengatasi masalah ini.

Cybercrime pada industri perbankan telah menimbulkan kerugian besar, baik bagi institusi keuangan maupun masyarakat sebagai pengguna jasa perbankan. Hal yang paling efektif untuk dilakukan adalah melalui pencegahan dan penanggulangan terjadinya suatu perbuatan tercela.[10] Tindakan tidak terpuji tersebut merupakan bentuk perbuatan melawan hukum di dunia maya yang menimbulkan kekhawatiran serius, mengingat tindakan *carding,* peretasan*,* pembobolan sistem*,* penipuan, dan lain-lain telah menjadi hal yang lumrah dilakukan oleh pelaku kejahatan di dunia maya.[11] Oleh sebab itu, penanggulangan tindak pidana *cyber* menjadi suatu urgensi yang tidak dapat diabaikan.

"Cybercrime merupakan hasil dari revolusi teknologi informasi yang berbeda dari kejahatan konvensional biasa".[12] Berbeda dengan kejahatan konvensional yang efeknya lebih mudah dilokalisasi dan nilai kerugian

---

[9]Lihat Nikita Dewi Kurnia Salma, "Tantangan dan Hambatan Besar yang Dihadapi CSIRT-BSSN Indonesia", CSIRT Indonesia, 2024, https://csirt.or.id/pengetahuan-dasar/tantangan-csirt-bssn

[10]Lihat Andika Rifqi Fadilla, Haryadi, dan Mohamad Rapik, "Plagiarisme Karya Ilmiah Dalam Kacamata Hukum Pidana", *PAMPAS: Journal of Criminal Law,* Volume 4 Nomor 1, 2023, hlm. 151. (https://mail.online-journal.unja.ac.id/Pampas/article/download/24074/15732/)

[11]Lihat Ardi Saputra Gulo, Sahuri Lasmadi, dan Kabib Nawawi, "Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik", *PAMPAS: Journal of Criminal Law,* Volume 1 Nomor 2, 2020, hlm. 70. (https://repository.unja.ac.id/18131/1/9574-Article%20Text-28027-1-10-20201010.pdf/)

[12]Puan Maharani, Hafrida, dan Mohamad Rapik, "Pertanggungjawaban Pidana Hacktivist dalam Perspektif Hukum Pidana di Indonesia", *PAMPAS: Journal of Criminal Law,* Volume 5 Nomor 2, 2024, hlm. 243. (https://online-journal.unja.ac.id/Pampas/article/download/33291/18279)

terbesarnya sering kali merupakan nilai yang dikaitkan dengan korban kejahatan, *cybercrime* ini dapat merugikan dan merusak sistem perekonomian dunia.[13] Salah satu sektor yang paling mudah menjadi sasaran *cybercrime* adalah sektor keuangan, termasuk perbankan.

Penegakan hukum terhadap *cybercrime* di industri perbankan pada pelaksanaanya mengalami kendala, baik yang bersifat teknis maupun struktural. Salah satu kendala yang bersifat teknis adalah kurangnya infrastruktur yang memadai untuk mendeteksi dan mencegah serangan *cyber*. Di samping itu, minimnya tenaga ahli yang kompeten di bidang keamanan siber turut menjadi kendala utama dalam upaya pencegahan dan penanggulangan serangan digital. Pada sisi yang lain, kendala penegakan hukum secara struktural terhadap tindak pidana *cybercrime* sering kali terhambat oleh minimnya kerjasama internasional, mengingat banyak pelaku *cybercrime* beroperasi lintas batas negara. Meskipun Peraturan Otoritas Jasa Keuangan Nomor 22 Tahun 2023 telah mengatur terkait transaksi keuangan digital lintas negara, tetapi peraturan tersebut tidak merincikan perlindungan konsumen terkait transaksi digital ataupun proteksi hukum lintas negara. Lebih lanjut, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi juga belum sepenuhnya menjawab kebutuhan sektor perbankan dalam menghadapi ancaman *cyber* secara langsung.

[13]Lihat Narto Yabu Ninggeding, Rihantoro Bayuaji, dan Dwi Elok Indriastuty, "Penegakan Hukum Terhadap Cyber Crime di Bidang Perbankan di Indonesia", *Jurnal Ilmu Hukum Wijaya Putra,* Volume 1 Nomor 2, 2023, hlm. 217-218. (http://jurnal.uwp.ac.id/fh/index.php/jurnalilmuhukum/article/view/107/42/)

Dalam konteks permasalahan ini, Menurut Barda Nawawi Arief, penanggulangan kejahatan dapat diupayakan dengan pendekatan penal dan non-penal. Pendekatan penal berfokus pada upaya hukum pidana untuk memberikan sanksi tegas kepada pelaku, sementara pendekatan non-penal lebih pada pencegahan, seperti edukasi masyarakat dan peningkatan keamanan sistem, guna mengurangi peluang terjadinya kejahatan.[14] Dalam permasalahan *cybercrime* pada industri perbankan, pendekatan penal menjadi sangat penting untuk memastikan bahwa individu atau kelompok yang melakukan kejahatan melalui jaringan digital menghadapi konsekuensi hukum yang jelas dan tegas. Hal ini mencakup penerapan ketentuan pidana yang tercantum dalam ketentuan hukum yang berlaku.

Ketentuan hukum yang mengatur permasalahan *cybercrime* pada sektor perbankan tersebut tidak diatur secara khusus dalam undang-undang terkait perbankan. Namun karena modus kejahatannya memanfaatkan media cyber, maka Undang-undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Undang-Undang ITE) dapat dijadikan dasar dalam pertanggungjawaban pelaku pidana *cybercrime* pada sektor perbankan. Dalam Pasal 33 Undang-Undang ITE tersebut telah mengatur terkait larangan terhadap segala tindakan yang berpotensi mengganggu sistem elektronik, dengan norma yang berbunyi "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apapun yang berakibat

[14]Lihat Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana (Perkembangan Penyusunan Konsep KUHP Baru),* Semarang: Fajar Interpratama, 2011. Hlm. 46-48.

terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya". Namun demikian, dalam permasalahan ini norma tersebut masih menjadi persoalan tersendiri.

Dalam rumusan Pasal 33 Undang-Undang ITE ini masih kurang jelas dan menimbulkan multitafsir di kalangan praktisi hukum. Formulasi pasal ini terlalu luas, sehingga penerapannya dalam kasus serangan sistem elektronik menjadi kurang tepat sasaran. Hal tersebut didukung dengan penelitian yang dilakukan oleh Silvi Ardianing Yulianita di Universitas Gadjah Mada yang menyoroti bahwa istilah "gangguan sistem elektronik" masih memiliki makna yang terlalu luas, sehingga diperlukan interpretasi yang tepat dalam penerapannya. Ketiadaan definisi yang jelas dalam Pasal 33 Undang-Undang ITE membuka ruang bagi berbagai interpretasi yang tidak seragam, baik di tingkat penyidikan, penuntutan, ataupun pengadilan. Sebagai dampaknya, baik pelaku maupun korban dalam kasus tersebut sering kali harus menghadapi situasi hukum yang tidak pasti.[15] Dalam konteks serangan sistem elektronik, cakupan istilah ini dapat mencakup tindakan yang disengaja maupun akibat kelalaian, tanpa adanya batasan eksplisit untuk membedakan tingkat keseriusan gangguan

Dalam rumusan delik pada Pasal 33 Undang-Undang ITE menyatakan larangan atas setiap tindakan yang "dengan sengaja dan tanpa hak atau melawan hukum" yang "berakibat terganggunya Sistem Elektronik". Namun, frasa "mengganggu Sistem Elektronik" mencakup berbagai bentuk gangguan

[15]Lihat Silvi Ardianing Yulianita, *Penyertaan dalam Tindak Pidana Gangguan Terhadap Sistem Elektronik (Modus Serangan Distributed Denial Of Services),* (Skripsi Universitas Gadjah Mada), Yogyakarta, 2022.

yang belum dibatasi dengan jelas. Cakupan yang terlalu luas ini memungkinkan tindakan seperti akses ilegal, penyusupan, atau modifikasi data juga dianggap sebagai gangguan sistem elektronik, meskipun dampak masing-masing tindakan berbeda secara signifikan. Kurangnya batasan jelas pada definisi "gangguan" menimbulkan dilema dalam praktiknya, khususnya bagi penegak hukum yang harus menentukan apakah gangguan pada sistem elektronik harus bersifat total atau cukup mengakibatkan ketidakstabilan sementara.

Unsur "dengan sengaja" atau *mens rea* dalam pasal ini pun menambah kompleksitas pembuktian, sebab pada kasus *cybercrime*, terutama yang bersifat anonim dan kompleks, niat pelaku sering kali sulit dibuktikan. Kompleksitas ini muncul karena niat pelaku tidak selalu terlihat secara eksplisit, hal ini dikarenakan niat atau kesengajaan merupakan sesuatu yang sifatnya subjektif dan tersembunyi dalam pikiran pelaku.[16]Situasi tersebut membuat pihak aparat penegak hukum mengalami kesulitan dalam menentukan dan mengambil keputusan terkait apakah tindakan tersebut benar-benar dilakukan dengan niat untuk mengganggu atau merusak.

Kekaburan dalam unsur niat menyebabkan perbedaan pemahaman di kalangan aparat penegak hukum dalam menentukan tingkat kesengajaan pelaku yang sering kali memengaruhi hasil penyidikan dan putusan kasus, bahkan pada kasus dengan konteks serupa. Disparitas ini tidak hanya menciptakan ketidakpastian hukum, melainkan juga berpotensi menurunkan

[16]Lihat Aris Munandar Ar, dkk, "Peran Niat (*Mens rea) dalam Pertanggungjawaban Pidana di Indonesia*", *JIMMI: Jurnal Ilmiah Mahasiswa Multidisiplin,* Volume 1 Nomor 3, 2024, hlm. 240-252. (https://jurnal.fanshurinstitute.org/index.php/jimmi/article/view/140/94)

kepercayaan publik terhadap integritas sistem peradilan.[17] Selain itu, perbedaan dalam pemahaman tentang *mens rea* dapat melemahkan upaya preventif dan represif dalam menghadapi *cybercrime*, sebab ketidakjelasan standar pembuktian membuat pelaku sulit dijerat atau justru dikenakan sanksi yang tidak proporsional terhadap niat mereka.

Dalam konteks rumusan Pasal 33 Undang-Undang ITE khususnya dalam frasa "mengganggu/terganggunya" tersebut dapat menimbulkan multitafsir terhadap pemaknaan norma. Sebab frasa "mengganggu/terganggunya" ini memiliki cakupan penafsiran yang luas sehingga menyebabkan inkonsistensi dalam penerapan hukum, di mana aparat hukum yang berbeda dapat menafsirkan tindakan "mengganggu" secara berbeda pula. Kerumitan pembuktian unsur *mens rea* dalam Pasal 33 ini berdampak pada ketidakpastian hukum dalam penanganan kasus *cybercrime*. Aparat penegak hukum perlu memastikan bahwa tindakan pelaku tidak hanya memenuhi unsur perbuatan (*actus reus*) tetapi juga dilakukan dengan niat yang jelas untuk mengganggu atau merusak sistem elektronik.

Dalam pertanggungjawaban pidana, unsur *actus reus* dan *mens rea* sangatlah penting dalam membuktikan suatu perbuatan pidana. Kedua unsur ini harus terbukti secara bersamaan agar seseorang dapat dinyatakan bersalah atas suatu tindak pidana, termasuk juga pada pembuktian tindak pidana yang melanggat Pasal 33 Undang-Undang ITE. Namun demikian, dalam dunia

[17]Lihat Gilbert Winata dan Ade Adhari, "Konsistensi Pemberatan Pidana dalam Pemidanaan Pelaku Tindak Pidana Pencucian Uang dengan Narkotika Sebagai *Predicate Crime*", *JIHHP: Jurnal Ilmu Hukum, Humaniora, dan Politik,* Volume 5 Nomor 2, 2024, hlm. 240-252. (https://dinastirev.org/JIHHP/article/download/3453/1920/13993)

cyber niat ini bisa kabur karena sifat tindakan yang tidak langsung atau bahkan diatur oleh perangkat otomatis yang diprogram sebelumnya tanpa interaksi langsung dari pelaku. Oleh karena itu, multitafsir sering kali terjadi dalam menerjemahkan unsur niat dalam Pasal 33 Undang-Undang ITE, di mana satu tindakan tertentu mungkin dianggap disengaja oleh satu pihak, tetapi tidak dianggap demikian oleh pihak lain.

Undang-Undang ITE juga tidak memberikan pedoman teknis yang memadai bagi aparat hukum dalam menangani *cybercrime* yang kompleks, sehingga banyak penyidik yang tidak memiliki kemampuan teknis cukup mendalam untuk memahami sifat gangguan yang terjadi. Hal ini semakin diperparah dengan banyaknya kasus *cybercrime* lintas negara, yang menambah tantangan dalam pembuktian dan kerja sama antar-negara dalam penyidikan. Dengan adanya kekaburan hukum dalam Pasal 33 Undang-Undang ITE ini, reformulasi terhadap pasal tersebut menjadi penting untuk memperjelas lingkup tindakan yang dapat dikenakan sanksi, definisi gangguan yang lebih konkret, serta mempertegas pembuktian unsur kesengajaan.

Seiring dengan pesatnya perkembangan teknologi yang juga akan berdampak pada keamanan sektor perbankan, maka regulasi yang ada perlu terus diperbarui agar tetap relevan dalam menghadapi ancaman yang semakin kompleks sebagai bentuk penanggulangan. Penanggulangan ini dilakukan dengan penguatan regulasi dan penerapan sanksi yang lebih ketat untuk memastikan mitigasi risiko *cyber* yang lebih baik dalam industri perbankan.

Dalam menghadapi *cybercrime* yang semakin kompleks, kebijakan penal masa depan perlu difokuskan pada penguatan regulasi teknis dan pengembangan kompetensi otoritas yang bertanggung jawab untuk menegakkan hukum. Salah satu langkah yang dapat dilakukan ke depan adalah mereformulasi Pasal 33 Undang-Undang ITE khususnya dalam penjelasan mengenai frasa "mengganggu/terganggunya" sehingga tidak akan menimbulkan multitafsir. Hal ini juga sebagai penerapan prinsip legalitas hukum pidana, yaitu lex certa yang menekankan rumusan undang-undang yang jelas dan mudah dipahami, serta lex stricta yang menegaskan pada rumusan undang-undang yang harus ditafsirkan secara ketat dan tidak boleh diperluas.

Berdasarkan latar belakang yang telah diuraikan di atas, maka penulis mengkaji penelitian tentang **"Penanggulangan Tindak Pidana *Cybercrime* Pada Industri Perbankan dalam Perspektif Peraturan Perundang-Undangan Indonesia".** Penelitian ini difokuskan pada pembahasan rumusan Pasal 33 Undang-Undang ITE sebagai landasan hukum dalam pertanggungjawaban pidana pelaku *cybercrime* dalam sektor perbankan. Tidak adanya penjelasan dan pembatasan mengenai frasa "mengganggu/terganggunya" dalam Pasal 33 Undang-Undang ITE ini akan menimbulkan multitafsir dan ketidakpastian hukum sehingga penelitian ini menjadi penting untuk dilakukan.

B. Rumusan Masalah

Berdasarkan uraian latar belakang di atas, maka yang menjadi rumusan masalah dalam penelitian ini adalah:

1. Bagaimana pengaturan penanggulangan *cybercrime* pada industri perbankan berdasarkan perspektif peraturan perundang-undangan Indonesia?
2. Bagaimana kebijakan hukum dalam mereformulasi rumusan Pasal 33 Undang-Undang ITE yang berkaitan dengan penanggulangan *cybercrime* pada industri perbankan?

C. Tujuan Penelitian

Dengan merujuk pada latar belakang dan masalah yang telah diuraikan sebelumnya, maka tujuan dari penelitian ini adalah:

1. Untuk mengetahui dan menganalisis pengaturan penanggulangan *cybercrime* pada industri perbankan berdasarkan perspektif peraturan perundang-undangan Indonesia.
2. Untuk mengetahui dan menganalisis kebijakan hukum dalam mereformulasi rumusan Pasal 33 Undang-Undang ITE yang berkaitan dengan penanggulangan *cybercrime* pada industri perbankan

D. Manfaat Penelitian

Sesuai dengan tujuan penelitian sebagaimana yang telah diuraikan di atas, maka diharapkan penelitian ini dapat bermanfaat secara:

1. Secara Teoretis

Secara teoretis, hasil penelitian ini diharapkan dapat memberikan kontribusi pengetahuan bagi pengembangan ilmu hukum, khususnya dalam bidang hukum pidana yang berkaitan dengan *cybercrime* di industri perbankan.

2. Secara Praktis

Secara praktis, hasil penelitian ini diharapkan dapat memperluas pemahaman, pengetahuan, wawasan, keterampilan, dan kemampuan dalam menganalisis lebih lanjut untuk masyarakat. Selain itu, temuan dan hasil dari penelitian ini dapat menjadi referensi, sumber informasi, dan bahan rujukan bagi mahasiswa yang ingin mempelajari dan meneliti terkait *cybercrime* pada industri perbankan.

E. Kerangka Konseptual

Kerangka konseptual dalam penelitian ini berperan sebagai pedoman untuk memahami dan menjelaskan konsep-konsep utama yang digunakan, serta memberikan definisi yang jelas terkait istilah-istilah yang terdapat dalam judul skripsi ini. Kerangka konseptual tersebut antara lain mencakup:

1. Tindak Pidana

Dalam bahasa Belanda, frasa "tindak pidana" berasal dari kata *straafbaarfeit*yang merupakan perbuatan yang tercantum dalam ketentuan hukum yang berlaku sebagai suatu perbuatan yang dilarang kemudian memiliki suatu akibat, yakni diancam dengan hukuman. Tindak pidana dan norma hukum sangat erat kaitannya karena tindak pidana merupakan unsur

utama dalam sistem hukum pidana yang bertujuan untuk melarang atau memerintahkan perilaku tertentu.[18] "Simons mendefinisikan *strafbaarfeit* sebagai tindakan melanggar hukum yang telah dianggap sebagai tindakan criminal oleh hukum yang dilakukan oleh seseorang yang bertanggung jawab atas tindakannya, baik secara sengaja maupun tidak sengaja. Kata "*feit"* dalam bahasa Belanda berarti "sebagian dari suatu kenyataan" atau "*een gedeelte van de werkelijkheid",* sedang "*strafbaar"* berarti dapat dihukum". Secara harfiah, istilah"*strafbaarfeit"* dapat diterjemahkan sebagai "Sebagian dari suatu kenyataan yang dapat dihukum". Namun, terjermahan ini kurang tepat karena pada akhirnya kita mengetahui bahwa yang dapat dihukum adalah individu sebagai pribadi, bukan kenyataan, perbuatan, atau tindakan itu sendiri".[19]

Menurut pandangan Moeljatno, tindak pidana merupakan suatu perbuatan yang dilarang oleh ketentuan hukum, di mana pelanggaran terhadap larangan tersebut diiringi dengan ancaman hukuman pidana tertentu bagi siapa pun yang melanggarnya. Tindak pidana juga dapat dimaknai sebagai perbuatan yang dikenai larangan oleh hukum dan disertai sanksi pidana, dengan catatan bahwa larangan tersebut berlaku atas tindakan itu sendiri (yakni kondisi atau akibat yang ditimbulkan oleh tindakan seseorang),

[18]Lihat Muhammad Ainul Syamsu, *Penjatuhan Pidana dan Dua prinsip Dasar Hukum Pidana,* Jakarta: Kencana, 2016. Hlm. 16-20.

[19]Lamintang, *Dasar-Dasar Hukum Pidana Indonesia,* Bandung: PT Citra Aditya Bakti. Hlm. 181.

sementara ancaman pidananya diperuntukkan bagi pelaku dari perbuatan tersebut.[20]

2. *Cybercrime*

"Cybercrime atau kejahatan siber dapat diartikan sebagai bentuk tindak kriminal yang memanfaatkan teknologi modern dan dilakukan di ruang digital melalui jaringan internet".[21] Definisi sempit dan luas dari *cybercrime* adalah dua kategori yang diklarifikasi oleh Widodo. Dalam pengertian yang paling terbatas, *cybercrime* merujuk pada tindak kejahatan yang secara langsung menyasar atau menyerang sistem komputer. Di sisi lain, *cybercrime* secara luas mengacu pada kejahatan yang melibatkan komputer serta kejahatan terhadap jaringan atau sistem komputer.[22]

Abdul Wahid dan Mohammad Labib berpendapat bahwa *cybercrime* mempunyai karakter sebagai berikut:

a. Tindakan yang dilakukan secara tidak sah, melanggar hukum, atau tidak etis di ranah siber, sehingga menimbulkan kesulitan dalam menetapkan yurisdiksi negara mana yang berwenang menanganinya;
b. Aksi tersebut dilakukan melalui pemanfaatan perangkat apa pun yang terhubung atau berkaitan dengan jaringan internet;
c. Dampak dari perbuatan ini menimbulkan kerugian, baik secara materiil maupun immateriil yang umumnya melebihi kerugian akibat tindak kriminal konvensional;

[20]Lihat Evi Hartanti, *Tindak Pidana Korupsi,* Jakarta: Sinar Grafika, 2007. Hlm. 7.

[21]Miftakhur Rokhman Habibi-Isnatul Liviani, "Kejahatan Teknologi Informasi (*Cyber Crime*) dan Penanggulangannya dalam Sistem Hukum Indonesia", *Al-Qanun: Jurnal Pemikiran dan Pembaharuan Hukum Islam,* Volume 23 Nomor 2, 2020, hlm. 407. (https://jurnalfsh.uinsa.ac.id/index.php/qanun/article/download/1132/825/5285)

[22]Lihat Widodo, *Sistem Pemidanaan dalam Cyber Crime,* Yogyakarta: Laksbang Meditama, 2009. Hlm. 24.

d. Pelaku merupakan individu yang menguasai akses dan penggunaan internet terhadap internet serta aplikasi-aplikasinya;
e. Perbuatan semacam ini kerap kali dilakukan dengan pola atau metode yang meyerupai tindak kejahatan konvensional.[23]

3. Industri Perbankan

Mengacu pada Undang-Undang Perbankan, bank merupakan suatu badan usaha yang berperan dalam mengumpulkan dana dari masyarakat dan menyalurkannya kembali melalui pemberian kredit dan/atau berbagai bentuk lainnya, dengan tujuan untuk meningkatkan kesejahteraan hidup masyarakat secara luas. Perbankan, khususnya bank umum merupakan inti dari sistem keuangan setiap negara. Menurut A. Abdurrachman, bank adalah sejenis organisasi keuangan yang menjalankan sejumlah fungsi, termasuk pemberian pinjaman, peredaran mata uang, pengawasan perusahaan, dan banyak lagi.[24]

4. Peraturan Perundang-undangan

Pasal 1 angka 2 Undang-Undang Nomor 15 Tahun 2019 tentang Perubahan Atas Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-Undangan memberikan acuan bahwa peraturan perundang-undangan merupakan ketentuan tertulis yang berisi norma hukum bersifat mengikat secara umum, yang dibentuk atau ditetapkan oleh lembaga negara atau pejabat yang memiliki kewenangan, melalui prosedur yang telah diatur dalam sistem perundang-undangan yang berlaku.

[23]Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime),* Jakarta: PT. Refika Aditama, 2005. Hlm. 76.
[24]Lihat Thomas Suyanto, dkk. *Kelembagaan Perbankan*, Jakarta: PT. Gramedia Pustaka Utama, 2007. Hlm. 1.

Menurut Bagir Manan, peraturan perundang-undangan adalah setiap putusan tertulis yang dirancang, disahkan, dan dikeluarkan oleh lembaga atau pejabat negara yang menjalankan fungsi legislatif, sesuai dengan prosedur yang telah ditentukan.[25]Adapun elemen-elemen yang membentuk peraturan perundang-undangan meliputi:

a. Bentuknya berupa ketentuan tertulis;
b. Dibuat oleh lembaga atau pejabat negara yang berwenang;
c. Disusun melalui tata cara yang diatur dalam peraturan perundang-undangan;
d. Memiliki kekuatan mengikat yang bersifat umum.[26]

F. Landasan Teori

1. Teori Penanggulangan

Kebijakan atau langkah-langkah dalam penanggulangan kejahatan pada hakikatnya merupakan bagian tak terpisahkan dari upaya perlindungan terhadap masyarakat (*social defence*) serta usaha dalam mewujudkan kesejahteraan sosial (*social welfare*). Oleh karena itu, dapat disimpulkan bahwa tujuan pokok dari politik kriminal adalah memberikanperlindungan kepada masyarakatgunamencapai kondisi masyarakat yang sejahtera.[27] Kebijakan dalam menanggulangi kejahatan (*criminal policy*) merupakan salah satu elemen dari kebijakan penegakan hukum (law *enforcement policy*). Sementara itu, kebijakan penegakan hukum merupakan bagian dari kebijakan

[25]Lihat Bagir Manan, *Peraturan Perundang-Undangan dalam Pembinaan Hukum Nasional,* Bandung: Armico, 1987. Hlm. 13.
[26]Rachmat Trijono, *Dasar-Dasar Ilmu Pengetahuan Perundang-Undangan,* Jakarta: Papas Sinar Sinanti, 2014. Hlm. 15.
[27]Lihat Andi Hamzah, *Asas-Asas Hukum Pidana,* Jakarta: Rineka Cipta, 2014. Hlm. 12.

sosial (*social policy*) dan juga termasuk dalam kebijakan legislatif (*legislative policy*). Secara umum, politik kriminal merupakan unsur krusial dalam kebijakan sosial yang berfokus pada upaya-upaya untuk mendorong terciptanya kesejahteraan masyarakat.[28]

Muladi menekankan bahwa cakupan dan kerumitan kebijakan kriminal, terutama dalam pencegahan kejahatan sangatlah luas. Hal ini wajar mengingat kejahatan merupakan persoalan sosial dan kemanusiaan yang memerlukanpemahaman mendalam. Sebagai persoalan sosial, kejahatan adalah fenomena yang terus berubah, berkembang, dan terhubung dengan gejala serta struktur sosial lainnya yang rumit, sehingga dapat dianggap sebagai masalah sosial-politik (*socio-political problems*).[29]

Pada prinsipnya, menurut Barda Nawawi, penanggulangan hukum dapat dilaksanakan dalam dua jenis pendekatan, yakni dengan kebijakan:

a. Kebijakan Penal

Upaya penanggulangan melalui jalur penal dapat dipahami sebagai pendekatan yang mengandalkan hukum pidana. Pendekatan ini lebih menekankan pada tindakan represif, yaitu langkah-langkah yang diambil setelah terjadinya kejahatan, seperti penegakan hukum dan pemberian sanksi terhadap pelaku. Selain itu, dalam pendekatan penal, upaya untuk menanggulangi kejahatan juga mencakup pembinaan dan rehabilitasi bagi pelaku tindak pidana.[30]

---

[28]Barda Nawawi Arief, *Op. Cit*. Hlm. 2.

[29]Lihat Paulus Hadisuprapto, *Juvenile Deliquency,* Bandung: Citra Aditya Bakti, 1997. Hlm. 72.

[30]Barda Nawawi Arief, *Op. Cit.* Hlm. 46

b. Kebijakan Non-Penal

Kebijakan non-penal dalam teori penanggulangan kejahatan pada prinsipnya merupakan kebijakan yang sasaran utamanya adalah untuk dapat menyelesaikan faktor-faktor yang kiranya dapat menyebabkan terjadinya suatu kejahatan. Pendekatan ini akan lebih memusatkan perhatian pada masalah sosial yang ada, baik yang secara langsung maupun tidak langsung dapat memicu terjadinya kejahatan. Oleh karena itu, maka tampak jelas bahwa kebijakan non penal dimaksudkan untuk menanggulangi sebab-sebab yang dapat menimbulkan kejahatan secara lebih strategis.[31]

2. Teori Kepastian Hukum

Dalam suatu negara berlandaskan hukum, asas kepastian hukum merupakan salah satu asas yang sangat fundamental. Prinsip kepastian hukum memberikan pedoman bagi individu dalam berperilaku serta dasar bagi tindakan yang dapat diambil negara terhadap individu. Kepastian hukum tidak hanya mencakup peraturan-peraturan yang tercantum dalam undang-undang, tetapi juga mencakup konsistensi dalam putusan hakim, di mana putusan yang diambil harus sejalan dengan putusan-putusan sebelumnya untuk kasus-kasus serupa.[32]

Terdapat empat hal penting yang memiliki keterkaitan erat dengan makna kepastian hukum, yaitu:

a. Hukum merupakan hal yang bersifat positif, yang berarti hukum itu sendiri berupa undang-undang;

---

[31]*Ibid.*

[32]Lihat Peter Mahmud Marzuki, *Pengantar Ilmu Hukum,* Jakarta: Kencana, 2008. Hlm. 158.

b. Hukum didasarkan pada fakta, yang berarti hukum harus berlandaskan pada kenyataan yang ada;
c. Fakta-fakta yang dinyatakan dalam hukum harus dinyatakan dengan jelas untuk mencegah kesalahpahaman tentang makna atau interpretasi dan untuk membuatnya mudah diterapkan;
d. Hukum yang bersifat positif tidak boleh diubah dengan mudah.[33]

Teori ini sangat relevan dengan permasalahan yang diteliti. Sebab, isu yang diangkat berkaitan dengan permasalahan mulititafsirnya rumusan Pasal 33 Undang-Undang ITE. Permasalahan multitafsir ini akan berdampak pada timbulnya ketidakpastian hukum terhadap penerapan suatu norma dalam undang-undang. Jika masalah multitafsir ini terus terjadi, maka hal ini dapat bertentangan dengan prinsip-prinsip dalam asas legalitas hukum pidana, yaitu lex stricta atau undang-undang yang ketat dan tidak boleh diperluas dengan analogi, serta lex certa yaitu undang-undang yang jelas.[34]

3. Teori Kebijakan Hukum Pidana

Secara umum, kebijakan hukum pidana dapat dipahami sebagai hukum, aturan, atau pedoman yang dirancang oleh negara untuk mencegah terjadinya tindakkriminal. "Prinsip-prinsip umum dan prosedur yang menjadi landasan dan respons terhadap pelanggaran norma hukum melalui hukuman disebut sebagai kebijakan kriminal (*penal policy*). Operasi umum aparat penegak hukum yang mencakup operasi pengadilan dan polisi juga dikenal sebagai kebijakan hukum pidana (*criminal law policy*)".[35] "Teori Kebijakan Hukum Pidana adalah teori yang memanfaatkan hukum pidana sebagai alat untuk

[33]Sajipto Rahardjo, *Ilmu Hukum,* Bandung: PT Citra Aditya Bakti, 2012. Hlm. 20.
[34] Zainal Arifin Mochtar dan Eddy O.S. Hiariej, *Dasar-Dasar Ilmu Hukum,* Depok: Rajawali Pers, 2023. Hlm. 155
[35]M. Ali Zaidan, *Kebijakan Kriminal,* Jakarta: Sinar Grafika, 2016. Hlm. 124.

menanggulangi kejahatan. Dalam konteks ini, terdapat perdebatakan mengenai apakah kejahatan sebaiknya ditanggulangi, dicegah, atau dikendalikan melalui penerapan sanksi pidana".[36]

Menurut Hanafi Amrani, ada beberapa indikasi yang mendukung pentingnya kebijakan hukum pidana, antara lain:

a. KUHP dianggap tidak lagi mencerminkan perkembangan dinamika hukum pidana nasional Indonesia.
b. Sistem hukum pidana yang terkandung dalam KUHP telah mengalami perubahan seiring dengan perkembangan hukum pidana di luar KUHP, baik itu hukum pidana administrasi maupun hukum pidana khusus. Hal ini menyebabkan munculnya berbagai sistem hukum pidana nasional.
c. Terjadi tumpang tindih norma hukum pidana antara yang terdapat dalam KUHP dengan yang ada dalam undang-undang di luar KUHP.[37]

G. Orisinalitas Penelitian

Berdasarkan hasil penelusuran, penulis menemukan sejumlah penelitian terdahulu yang memiliki relevansi dengan topik yang dibahas dalam penelitian ini, yaitu:

1. Penelitian yang berjudul "Perlindungan Hukum Terhadap Nasabah Atas Pembobolan Rekening Melalui *Mobile Banking* di Indonesia" oleh Nira Faridatul Maymuna, Fakultas Syariah Universitas Islam Negeri Maulana Malik Ibrahim, 2024. Penelitian ini mengkaji jenis-jenis pembobolan rekening melalui *mobile banking* serta bentuk perlindungan hukum yang diberikan kepada nasabah bank terkait dengan kasus pembobolan tersebut.

[36]Abintoro Prakoso, *Kriminologi dan Hukum Pidana,* Yogyakarta: Laksbang Pressindo, 2017. Hlm. 176.
[37]Hanafi Amrani, *Politik Pembaruan Hukum Pidana,* Yogyakarta: UII Press, 2019. Hlm. 6.

2. Penelitian yang berjudul "Perlindungan Hukum Terhadap Nasabah Bank Syariah Indonesia Dari Serangan *Cybercrime*" oleh Ballqish Amelia Assifa, Fakultas Syariah dan Hukum Universitas Islam Negeri Syarif Hidayatullah, 2023. Penelitian tersebut mengkaji terkait perlindungan hukum terhadap nasabah bank syariah dari serangan *cybercrime*di industri perbankan, khususnya peretasan dengan cara menyebarluaskan virus ataupun cara lainnya. Sedangkan, penelitian ini menganalisis terkait penanggulangan terhadap tindak pidana *cybercrime*pada industri perbankan berdasarkan perspektif peraturan perundang-undangan. Sedangkan, penelitian ini menganalisis penanggulangan tindak pidana *cyber*di industri perbankan dengan berfokus pada tinjauan dari sudut pandang peraturan perundang-undangan.
3. Penelitian yang berjudul "Perlindungan Hukum Nasabah Bank Korban Pencurian Data Kartu (*Carding*) Sebagai Bentuk Tindak Pidana Dunia Maya (*Cyber Crime*) oleh Vilda Pritipal, Fakultas Hukum Universitas Andalas, 2020. Penelitian tersebut membahas tentang bentuk dan pengaturan perlindungan hukum nasabah bank korban *cybercrime*berupa *carding* atau pencurian data. Sedangkan, penelitian ini membahas mengenai penanggulangan terhadap tindak pidana *cybercrime*pada industri perbankan berdasarkan perspektif peraturan perundang-undangan.

H. Metode Penelitian

1. Tipe Penelitian

Penelitian ini menggunakan metode penelitian normatif, yaitu pendekatan yang menganalisis hukum sebagaimana tercantum dalam teks-teks otoritatif, seperti undang-undang, yurisprudensi, traktat, keputusan pemerintah, teori hukum, serta pendapat ahli. Dalam pendekatan penelitianyuridis normatif, hukum dipandang sebagai ketentuan yang tercantum dalam peraturan perundang-undangan (*law in book*) serta sebagai seperangkat norma dan kaidah yang berfungsi sebagai acuan dalam bertingkah laku.[38]Penelitian normatif juga dapat diartikan sebagai telaah terhadap norma-norma hukum yang mencakup analisis terhadap asas-asas hukum, struktur sistem hukum, tingkat keselarasan antar peraturan, studi perbandingan hukum, serta aspek historis hukum, dengan tujuan untuk memperoleh pemahaman mengenai hukum dalam konteks situasi tertentu.[39]Proses mengidentifikasi doktrin, norma, dan prinsip hukum dikenal sebagai penelitian normatif.[40]Penelitian ini difokuskan secara eksklusif pada peraturan hukum yang bersifat tertulis atau pada sumber-sumber hukum lainnya.[41] Penelitian ini berfokus pada penanggulangan terhadap tindak

[38]Lihat Jonaedi Efendi dan Johny Ibrahim, *Metode Penelitian Hukum: Normatif dan Empiris,* Jakarta: Kencana, 2018. Hlm. 124.

[39]Lihat Bahder Johan Nasution, *Metode Penelitian Hukum,* Bandung: Mandar Maju, 2008. Hlm. 86-87.

[40]*Ibid.* Hlm. 90.

[41]Lihat Sintia Febriani dan Sahuri Lasmadi, "Pengembalian Kerugian Negara Melalui Pembayaran Uang Pengganti", *PAMPAS: Journal of Criminal Law,* Volume 1 Nomor 1, 2020, hlm. 9. (https://online-journal.unja.ac.id/Pampas/article/download/8277/9887)

pidana *cybercrime* pada industri perbankan berdasarkan perspektif peraturan perundang-undangan.

2. Pendekatan Penelitian

a. Pendekatan Perundang-undangan (*Statute Approach*)

Pendekatan perundang-undangan merupakan suatu metode yang digunakan dengan cara mengkaji berbagai ketentuan hukum, termasuk norma dan prinsip-prinsip hukum yang sedang berlaku dalam masyarakat. Dalam pendekatan ini, penting untuk memperhatikan susunan norma secara hierarkis, apakah norma tersebut berada dalam peraturan yang bersifat eksklusif atau inklusif, serta terkait apakah aturan tersebut masih baru atau sudah usang dan tidak lagi berlaku.[42]

b. Pendekatan Konsep (*concept approach*)

Pendekatan konsep merupakan metode yang digunakan dengan mengeksplorasiberagam pandangan serta doktrin yang berkembang dalam ranah hukum. Melalui telaah terhadap pemikiran-pemikiran tersebut, peneliti dapat menggaligagasan-gasgasan yang berkaitan denganpermasalahan hukum yang sedang diteliti, sehingga memberikan pemahaman yang lebih mendalam tentang cara penerapan atau interpretasi hukum yang tepat.

3. Pengumpulan Bahan Hukum

Jenis penelitian yang digunakan dalam skripsi ini adalah penelitian hukum normatif, yang menitikberatkan pada studi kepustakaan melalui

[42]Lihat I Made Pasek Diantha, *Metodologi Penelitian Hukum Normatif dalam Justifikasi Teori Hukum,* Jakarta: Kencana, 2017. Hlm. 156-159.

analisis terhadap berbagai sumber dan materi hukum.[43] Bahan-bahan hukum tersebut berfungsi sebagai sumber penelitian hukum untuk menganalisis permasalahan hukum yang dikaji. Jenis dan sumber bahan hukum yang digunakan dalam penelitian ini terdiri dari:

a. Bahan Hukum Primer

Bahan hukum primer merupakan bahan hukum utama yang berupa aturan tertulis yang bersifat autoritatif. Dalam penelitian ini, bahan hukum primer yang digunakan adalah:

1) Undang-Undang Negara Republik Indonesia Tahun 1945
2) Kitab Undang-Undang Hukum Pidana
3) Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan
4) Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen
5) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi
6) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2009 tentang Informasi dan Transaksi Elektronik
7) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik
8) Peraturan Otoritas Jasa Keuangan Nomor 22 Tahun 2023 tentang Perlindungan Konsumen dan Masyarakat

[43]Lihat Marzuki, *Penelitian Hukum,* Jakarta: Kencana, 2005. Hlm. 44.

b. Bahan Hukum Sekunder

Bahan hukum sekunder dalam penelitian ini berperan sebagai pelengkap dan penjabaran atas bahan hukum primer, serta dimanfaatkan untuk memperkokoh analisis yang disampaikan. Sumber bahan ini mencakup buku, jurnal akademik, artikel, makalah, dan laporan hasil penelitian yang memiliki keterkaitan dengan topik yang dikaji.

c. Bahan Hukum Tersier

Bahan hukum tersier merupakan referensi yang memberikan penjelasan atau pengertian atas bahan hukum primer maupun sekunder, yang diperoleh dari sumber-sumber seperti Kamus Hukum, Kamus Besar Bahasa Indonesia, serta ensiklopedia.

4. Analisis Bahan Hukum

Bahan hukum yang telah terkumpul kemudian diidentifikasi dan diklasifikasikan sesuai dengan kategori masing-masing. Setelah itu, bahan-bahan tersebut akan diolah dan dianalisis secara sistematis oleh penulis menggunakan pendekatan analisis kualitatif. Proses pengolahan dan analisis akan dilakukan berdasarkan teori-teori hukum yang relevan, dengan tujuan untuk menemukan solusi atas permasalahan hukum yang menjadi fokus utama dalam penelitian ini.

I. Sistematika Penulisan

Untuk mempermudah penulis dalam memberikan gambaran umum perihal setiap bagian dari pembahasan yang ada di dalam skripsi ini, penulis

membagi skripsi ini menjadi 4 (empat) bagian yang terdiri atas 4 (empat) bab, yaitu:

BAB I PENDAHULUAN

Bab ini menjelaskan mengenai latar belakang permasalahan, rumusan masalah, tujuan penelitian, manfaat penelitian, kerangka konseptual, landasan teori, metode penelitian, dan sistematikan penulisan.

BAB II TINJAUAN UMUM

Bab ini memuat uraian mengenai tinjauan umum tentang tindak pidana, *cybercrime*, dan industri perbankan.

BAB III PEMBAHASAN

Pada bab ini penulis akan menguraikan dan menganalisis pembahasan yang menjadi rumusan masalah pada penelitian ini, yakni memuat bagaimana bentuk-bentuk *cybercrime* yang dapat menyerang industri perbankan dan pengaturan sistem sanksi sebagai bentuk penanggulangan tindak pidana *cybercrime*dalam industri perbankan berdasarkan hukum positif Indonesia.

BAB IV PENUTUP

Bab ini merupakan bab penutup yang berisikan kesimpulan dari hasil penelitian yang diuraikan pada bab pembahasan sebagai pokok permasalahan dari penelitian serta memuat saran yang diharapkan akan memberikan manfaat bagi penulis dan para pihak lainnya.