



---

## Tinjauan Teori Kriminologi Dalam Kejahatan Siber (Kasus Kebocoran Data Nasabah)

Gumelar Rizki Duana<sup>1\*</sup>, Ali Masyar<sup>2</sup>, Cahya Wulandari<sup>3</sup>

Universitas Negeri Semarang, Indonesia

Email: [gumelar@gmail.com](mailto:gumelar@gmail.com)

\*Correspondence

### ABSTRAK

Internet atau mobile banking merupakan aplikasi atau layanan yang menghubungkan perangkat nasabah dengan sistem bank. Layanan internet dan mobile banking memiliki banyak manfaat, terutama memudahkan transaksi yang hanya menggunakan perangkat elektronik yang memiliki akses internet. Namun, dengan adanya kemudahan tersebut juga terdapat risiko dan ancaman bagi para pengguna jasa teknologi tersebut. Dalam beberapa kasus, bank dapat mengalami gangguan pelayanan digital yang disebabkan oleh serangan hacker. Serangan hacker termasuk kedalam kejahatan siber dan pelanggaran hukum. Dengan adanya teori kriminologi dapat digunakan untuk menegakkan hukum pidana karena menawarkan jawaban atas pertanyaan bagaimana atau mengapa orang dan perilaku tertentu dianggap jahat oleh masyarakat. Penelitian ini mencoba mengkaji teori kriminologi yang dapat digunakan dalam kejahatan siber pada kasus kebocoran data nasabah. Dengan metode penelitian yuridis-empiris maka penulis mengharapkan dapat mengkaji teori kriminologi dalam kejahatan siber, sehingga teori tersebut dapat digunakan untuk penanggulangan kejahatan siber pada kasus kebocoran data nasabah. Kesimpulan dari kajian ini yaitu terdapat empat teori kriminologi yang dapat digunakan untuk menganalisis kejahatan siber kasus hacker dalam kebocoran data nasabah, yaitu: teori anomie, asosiasi diferensial, kontrol social, dan netralisasi. Teori kriminologi tersebut dapat digunakan sebagai salah satu strategi pemerintah untuk mengambil langkah-langkah kebijakan penalisasi dan non penal terhadap kejahatan siber di perbankan Indonesia.

**Kata kunci:** kebocoran data; kejahatan siber; tinjauan kriminologi.

### ABSTRACT

*Internet or mobile banking is an application or service that connects a device to a banking system. Internet and mobile banking services have many benefits, especially facilitating transactions that only use electronic devices that have internet access. However, with such facilities there are also risks and threats to the users of the technology services. In some cases, banks may experience digital service disruption caused by hacker attacks. Hacker attacks include cybercrime and violations of the law. Criminological theory can be used to enforce criminal law because it provides answers to the questions of how or why a person and certain behavior are considered evil by society. This study tries to explore criminological theories that can be used in cybercrime in cases of customer data leakage. With the method of juris-empirical research, the author hopes to study the criminological theory in cybercrime, so that the theory can be used to counter its crime in the case of customer data leakage. The conclusion of this study is that there are four criminological theories that can be used to analyze cybercrimes in hacker cases involving customer data leaks, namely: anomie theory, differential association, social control, and neutralization. This criminological theory can be used as a government strategy to take penal and non-penal policy steps against cybercrime in Indonesian banking.*

**Keywords:** data leakage; cybercrime; criminology review.

---

## **PENDAHULUAN**

Perubahan social budaya akibat dari kemajuan teknologi yang berkembang pesat dapat memicu terjadinya kejahatan (Meidiyanto, 2015). Perkembangan tingkat peradaban manusia sejalan dengan berkembangnya kejahatan (Erlina, 2014). Menurut Hartanto (2015), dilihat dari aspek sosiologis dapat disimpulkan kejahatan merupakan salah satu jenis gejala social yang terjadi pada individu atau masyarakat. Sedangkan menurut Mubarak, N. (2017), kejahatan adalah suatu pola tingkah laku merugikan yang didalamnya terdapat korban dan dapat menimbulkan reaksi social dari masyarakat. Banyak faktor yang dapat menyebabkan kejahatan seperti faktor ekonomi, pergaulan, kesempatan yang ada, dan lain sebagainya. Faktor utama terjadinya kejahatan yang dilakukan oleh seseorang atau sekelompok hanya semata-mata untuk memenuhi kebutuhan hidupnya. Selain itu, kejahatan juga dapat terjadi akibat dari seseorang individu ingin mempraktekan perkembangan ilmu teknologi yang dimilikinya dengan cara yang menyimpang.

Teori adalah alat yang berguna yang membantu orang memahami dan menjelaskan dunia di sekitar kita. Dalam kriminologi, teori ini membantu kita memahami cara kerja sistem peradilan pidana dan siapa yang berperan dalam sistem peradilan. Teori memberikan solusi bagaimana memecahkan masalah (Hadisuprpto, 2004). Paulus Hadisaputro mengatakan bahwa dalam konteks kriminologi, asumsi yang dikembangkan itu terarah pada upaya pemahaman terhadap makna perilaku tertentu yang dipersepsi oleh pelakunya sendiri, setelah ia berinteraksi dengan kelompoknya atau masyarakat sekitarnya (*significant others*) (Hadisuprpto, 2004). Teori kejahatan dapat digunakan dalam penegakan hukum pidana karena memberikan jawaban atas pertanyaan tentang bagaimana atau mengapa orang atau tindakan tertentu dianggap jahat oleh masyarakat. Mengapa faktor non-hukum dapat mempengaruhi perilaku dan pendidikan hukum? Bagaimana sumber daya negara dan lokal dapat mengatasi kejahatan?

Teori-teori kriminologi berupaya menjawab pertanyaan ini dengan memahami variabel sosiologis, politik, dan ekonomi yang dapat mempengaruhi keputusan hukum, administratif, dan penegakan hukum dalam sistem peradilan pidana. Beberapa penegak hukum masih banyak yang tidak dapat mengidentifikasi penyebab terjadinya suatu kejahatan. Perlunya strategi dalam penanggulangan dan pencegahan kejahatan memerlukan pertimbangan terhadap faktor penyebab kejahatan. Keadaan yang menyebabkan terjadinya kejahatan tersebut harus dikomunikasikan kepada masyarakat oleh pihak kepolisian agar masyarakat mengetahuinya. Oleh karena itu, teori kriminologi sangat diperlukan untuk menganalisis dan mempertanyakan secara kritis penyebab seseorang melakukan kejahatan. Selain itu, teori kriminologi juga diperlukan untuk menganalisis dan memberikan jawaban mengapa individu atau sekelompok orang mampu mempraktikkan norma social dan hukum, sementara sebagainya lainnya melanggar. Teori kriminologi bermanfaat bagi kegiatan pemerintahan, akademisi dan juga sebagai pendidikan untuk masyarakat.

Beberapa penelitian tentang kejahatan siber di Indonesia, antara lain penelitian tentang pencurian data yang dilakukan oleh hacker (Sulisrudatin, 2018); (Widayanti, 2022). Berdasarkan beberapa artikel sebelumnya telah menjelaskan tindak pidana bagi pelaku kejahatan siber, namun belum adanya artikel yang menjelaskan teori-teori kriminologi pada kejahatan siber. Kejahatan siber tidak hanya meliputi Indonesia, tetapi juga global. Internet banking dan mobile banking memungkinkan masyarakat melakukan transaksi jual beli melalui aplikasi perbankan. Tentu saja, mengingat kemudahan yang dinikmati masyarakat melalui layanan Internet banking dan mobile banking, terdapat risiko dan ancaman yang signifikan bagi pengguna layanan teknologi informasi tersebut. Dalam beberapa kasus,

bank dapat mengalami gangguan pelayanan digital yang disebabkan oleh serangan hacker. Penjahat siber akan mencuri data-data pribadi dari para nasabah, yang nantinya data tersebut dapat digunakan sebagai alat pencucian uang serta berhubungan dengan terorisme (Putri et al., 2023).

Salah satu contoh kejahatan siber kasus kebocoran data nasabah PT Bank Syariah Indonesia Tbk (BSI) pada tanggal 8 Mei 2023. Kemudian, pada tanggal 9 Mei 2023 Direktur Utama BSI Hery Gunardi mengatakan adanya temuan dugaan serangan siber yang menyebabkan gangguan pada layanan BSI. Oleh sebab itu, perseroan melakukan evaluasi dan temporary switch off terhadap sejumlah layanannya. Selanjutnya, terungkap bahwa kelompok hacker LockBit diduga meretas data nasabah BSI dan menyebarkannya di pasar gelap internet atau dark web. Kelompok tersebut juga mengajukan tawaran sebesar Rp 295,61 miliar kepada BSI agar data nasabah dapat dikembalikan. Kelompok hacker LockBit mengaku telah mencuri sekitar 1,5 terabyte data internal BSI, termasuk di dalamnya 15 juta data pengguna BSI. Data yang bocor itu di antaranya adalah nama, nomor ponsel, alamat, saldo di rekening, riwayat transaksi, tanggal pembukaan rekening, informasi pekerjaan, dan beberapa data lainnya. Sebelum data tersebut disebar, LockBit mengaku telah bernegosiasi dengan pihak BSI. PT. Bank Syariah Indonesia menyatakan kesiapan untuk membayar tebusan sebesar 100.000 dollar AS atau setara sekitar Rp 1,48 miliar (asumsi kurs Rp 14.850 per dollar AS). Namun tawaran tersebut ditolak, dan LockBit meminta dana sebesar 20 juta dollar AS (Azarine, 2023).

Selain itu, kasus kebocoran data nasabah PT Bank Pembangunan Daerah Jawa Timur (Bank Jatim) Tbk. Data yang bocor kemudian dijual di forum RAID seharga \$250.000 atau Rp 3,5 miliar. Data tersebut dijual dengan nama pengguna bl4ckt0r dan menurut pelaku berisi data sebesar 378 GB yang berisi 259 database. Menurut Pratama Persada, pakar keamanan siber di Cissrec Research Institute data yang dijual adalah data sensitif seperti data pelanggan, data karyawan, dan data keuangan pribadi (Duana et al., 2023).

Adanya kejahatan siber telah menjadi ancaman stabilitas lintas negara, sehingga pemerintah sulit mengimbangi teknik kejahatan yang dilakukan dengan teknologi komputer, khususnya jaringan internet (Rais & Songkarn, 2022). Hal ini merupakan akibat dari pesatnya perkembangan teknologi informasi, dan setiap perkembangan tersebut pada hakikatnya saling berhubungan dalam bentuk positif dan negatif (Ardjono Reksodiputro, 1998). Penulis meyakini bahwa banyak teori kriminologi yang dapat digunakan dalam memahami kejahatan siber pada kasus kebocoran data nasabah. Secara teoritis, penelitian ini didasarkan pada gagasan bahwa terdapat hubungan antara dalil teori-teori tersebut dengan karakteristik kejahatan, karakteristik pelaku, dan reaksi masyarakat terhadap kejahatan siber di Indonesia. Hasil kajian tersebut dapat digunakan sebagai salah satu bahan pertimbangan untuk merencanakan langkah-langkah kebijakan kriminal terhadap kejahatan siber pada kasus kebocoran data nasabah di Indonesia, terutama dalam penalisasi dan kebijakan non penal. Berdasarkan paparan tersebut rumusan masalah pada artikel ini yaitu: Apa teori kriminologi yang dapat diterapkan dalam kejahatan siber pada kasus kebocoran data nasabah, dan Bagaimana penerapan teori kriminologi tersebut dalam mengkaji penanggulangan kejahatan siber pada kasus kebocoran data nasabah.

## **METODE**

Penelitian ini menggunakan metode penelitian yuridis-empiris. Berdasarkan sifatnya, penelitian ini bersifat deskriptif untuk menguraikan hasil kajian mengenai teori-teori kriminologi dalam kejahatan siber pada kasus kebocoran data nasabah. Berdasarkan bentuknya adalah penelitian evaluatif dan prespektif. Bersifat evaluatif dan prespektif, karena bertujuan untuk memberikan analisis mendalam

yang bertujuan mencegah kejahatan siber pada kasus kebocoran data nasabah. Di sisi lain, kajian normative ini juga akan memberikan solusi yang tepat terhadap upaya pencegahan dan penanggulangan kejahatan siber pada kasus kebocoran data nasabah melalui pendekatan teori kriminologi.

## **HASIL DAN PEMBAHASAN**

Saat ini penggunaan internet dan mobile banking menyediakan kemudahan bagi para nasabah untuk melakukan transaksi tanpa harus datang ke kantor cabang bank. Berdasarkan penelitian yang pernah dilakukan oleh Rahmah (2018) bahwa pemakaian internet banking dan juga mobile banking memiliki pengaruh yang cukup besar kepada kejahatan dunia siber (Rahmah, n.d.). Hal ini membuktikan bahwa kejahatan siber mengancam para nasabah di dunia perbankan. Perlindungan hukum mengenai kejahatan siber terdapat pada Undang-Undang No. 11 Tahun 2008 pada Pasal 33 yang berbunyi “Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya”. Dengan teori-teori kriminologi dapat digunakan untuk menegakkan hukum pidana karena dapat digunakan untuk mengkaji dan menganalisis sebab seseorang melakukan kejahatan siber.

### **Teori Kriminologi dalam Kejahatan Siber Kasus Kebocoran Data Nasabah**

#### **a. Teori Anomia**

J. J. M. van Dick, H. I. Sagel Grande, dan L.G. Toornvliet pendapat bahwa teori anomie tergolong dalam kumpulan teori-teori keterbelakangan masyarakat. Teori lain yang tergolong dalam teori-teori keterbelakangan masyarakat adalah teori subkultur delinkuen, teori Cloard dan Ohlin, dan teori kriminologi ekologis (Dijk et al, 2003) Pendapat Durkheim dikemukakan lebih dulu dibandingkan Merton. Durkheim menggunakan istilah anomie untuk menyebut suatu kondisi yang mengalami deregulasi. Menurutnya perubahan sosial yang cepat dan mencekam dalam masyarakat mempunyai pengaruh besar terhadap semua kelompok dalam masyarakat (Yusril, 2000). Durkheim menggambarkan konsep anomie sebagai kondisi dalam masyarakat yang terjadi keputusasaan atau ketiadaan norma. Anomie juga merupakan akibat dari perubahan sosial yang cepat. Anomie ada di semua masyarakat dan memanifestasikan dirinya tidak hanya dalam kejahatan tetapi juga dalam bunuh diri. Semua itu terjadi akibat lemahnya norma sosial dan pengawasan sosial yang mampu mengendalikan perilaku menyimpang.

Robert Merton selanjutnya mengungkapkan bahwa perilaku menyimpang dianggap sebagai suatu tingkah laku abnormal karena perilaku tersebut berpangkal pada individu. Perilaku menyimpang terjadi karena banyak orang yang merasakan adanya kesenjangan antara tujuan (goals) dan cara untuk mencapainya. Setiap masyarakat mempunyai dua jenis norma sosial: tujuan sosial (social goal) dan sarana yang tersedia (acceptable mean). Tidak semua orang dapat menggunakan sarana yang sah untuk mencapai tujuan mereka. Oleh karena itu, banyak orang yang berusaha memaksakan kehendak dan mencapai tujuannya, meskipun dengan cara melanggar hukum (illegal). Menurut Romli Atmasasmita menyatakan bahwa, perbedaan antara teori anomie yang dikemukakan oleh Durkheim dengan Merton adalah Teori anomie Merton berfokus pada akses diferensial terhadap struktur peluang, sedangkan teori anomie Durkheim berfokus pada tidak adanya norma, dengan tanpa menjelaskan penyebab tidak adanya norma.

#### **b. Teori Asosiasi Diferensial**

Teori Asosiasi Diferensial diusulkan oleh seorang sosiolog Amerika, Edwin H. Sutherland pada tahun 1939 yang kemudian disempurnakan pada tahun 1947. Teori ini didasarkan pada tiga teori, yaitu Ecological and Cultural Transmission Theory dari Shaw dan McKay; Symbolic Interactionism dari George Mead; dan Culture Conflict Theory. Romli Atmasasmita menyatakan bahwa pemahaman sistematis adalah kejahatan karir atau praktik kriminal terorganisir. Definisi praktik kejahatan terorganisir adalah perilaku yang mendukung norma-norma yang telah dikembangkan dalam masyarakat. Pada tahun 1947, Sutherland menggantikan istilah “social disorganization” dengan “differential social organization”. Melalui penggantian istilah, Sutherland ingin menunjukkan keberadaan berbagai kondisi sosial dengan nilai-nilai dan tujuan internal. Aplikasi teori kriminologi dalam pencegahan kejahatan masing-masing digunakan sebagai sarana yang berbeda dalam mencapai tujuan. Teori ini mengakui keberadaan berbagai organisasi sosial yang terpisah, tetapi bersaing satu sama lain berdasarkan norma dan nilai-nilai mereka sendiri (Levin et al., 2012).

Berdasarkan proposisi di atas, Sutherland dengan tegas membantah teori Cesare Lombroso, yang menyatakan bahwa perilaku jahat dibawa oleh seseorang sejak lahir. Menurut Sutherland, perilaku buruk dapat dipelajari dari orang lain melalui proses interaksi dan komunikasi. Pendapat Sutherland mendapat dukungan dari Glaser yang menyatakan bahwa kejahatan tidak hanya belajar melalui interaksi langsung antara individu, tetapi juga dapat dipelajari meskipun individu tidak bertemu, dan media massa menjadi perantara (Anshori, 2021).

Dapat disimpulkan bahwa teori Asosiasi Diferensial diakui adanya sifat dan efek dari pengaruh lingkungan terhadap tingkah laku seseorang. Teori ini bersifat sosiologis karena berfokus pada hubungan sosial seperti frekuensi, kekuatan, dan peran asosiasi. Berdasarkan teori asosiasi diferensial, perilaku jahat dipelajari dalam kelompok melalui interaksi dan komunikasi. Subjek yang dipelajari pada kelompok ini adalah teknik melakukan kejahatan dan alasan (nilai, motivasi, rasionalisasi, dan tindakan) yang mendukung kejahatannya. Teori ini tidak bergantung pada kualitas atau karakteristik individu atau pada karakteristik dunia ilmiah yang nyata dan terlihat. Menurut Sutherland, keberadaan berbagai organisasi sosial di masyarakat sekitar merupakan fakta mendasar sebab terjadinya kejahatan. Artinya, kombinasi individu yang berbeda menimbulkan kejahatan, yang merupakan konsekuensi logis dari prinsip belajar melalui kombinasi tersebut (social learning). Oleh karena itu, teori asosiasi diferensial berlaku untuk kelompok kriminal maupun antikriminal.

### c. Teori Kontrol Sosial

Teori kontrol sosial adalah klasifikasi dari teori yang mengklaim tidak bertanya mengapa orang melakukan kejahatan, tetapi mengapa mereka tidak melakukan kesalahan? Teori-teori ini mengasumsikan bahwa setiap orang memiliki keinginan untuk melakukan tindakan kriminal dan menyimpang, dan berusaha menjawab mengapa beberapa orang menahan diri dari melakukannya. Control Theories. A classification of theories that claim to ask not why do people commit criminal acts, but why do they not commit criminal acts? These theories assume everyone has the desire to commit criminal and deviant acts, and seeks to answer why some people refrain from doing so.

John Hagan menekankan bahwa teori kontrol sosial didasarkan pada premis bahwa semua individu dalam masyarakat mempunyai kesempatan yang sama untuk menjadi pelanggar hukum atau taat hukum. Teori kontrol sosial mengajukan pertanyaan mendasar tentang mengapa setiap orang tidak melanggar hukum, atau mengapa sebagian orang menaati hukum. Reiss membedakan dua jenis kontrol, yaitu:

1. Kontrol pribadi, yaitu kemampuan seseorang untuk menahan diri dari mencapai tujuannya dengan cara yang melanggar norma;
2. Kontrol sosial, yaitu kemampuan masyarakat atau kelompok sosial untuk menerapkan norma atau hukum dan peraturan.

Reiss menyimpulkan bahwa melemahnya kontrol sosial juga mengakibatkan perilaku kejahatan (Anshori, 2021). Baik atau buruknya perilaku seseorang tergantung sepenuhnya pada masyarakat disekitarnya. Siapapun yang lemah atau putus ikatan sosialnya rentan melakukan perbuatan jahat. Hal ini juga terjadi ketika lembaga kontrol sosial, baik formal maupun informal, mengalami kehilangan kewenangan. Peraturan hukum yang dibuat negara untuk mengatur kehidupan warga negaranya disebut lembaga kontrol formal. Lembaga kontrol sosial mencakup aturan-aturan tidak tertulis yang diakui sah oleh masyarakat. Namun, sarana kontrol informal mungkin lebih mengikat dibandingkan tindakan kontrol dalam bentuk hukum tertulis.

d. Teori Netralisasi

Pendapat utama dari teori netralisasi (netralisasi pada teori), bahwa seseorang akan belajar untuk menetralkan moralitas yang mengendalikan perilaku manusia, kemudian melakukan perilakunya yang menyimpang. Selain itu, teori ini menjelaskan bagaimana remaja melakukan penyimpangan, dan bagaimana anak-anak muda ini terlibat dalam perilaku yang menyimpang. David Matza mengkonfirmasi bahwa teori netralisasi menekankan proses belajar orang muda untuk rasionalisasi perilaku kejahatan yang dilakukan sehingga diharapkan untuk menyetatkan kerja nilai-nilai sosial dan norma-norma dalam masyarakat. Larry J. Siegel mengungkapkan, Major premise youth learn ways of neutralizing moral restraint and periodically drift in and out of criminal behavior pattern. Explains way may delinquents do not adult criminals. Explains why youthful law violators can participate in conventional behavior.

Teori Netralisasi mengasumsikan bahwa perilaku manusia dikendalikan oleh pikiran pelaku. Teori ini bertanya, apa yang ada di balik pikiran orang baik yang kadang-kadang membuat mereka berubah menjadi orang yang berperilaku buruk atau menyimpang dari norma-norma sosial? Berdasarkan pertanyaan-pertanyaan ini, teori ini mengasumsikan bahwa kebanyakan orang, melakukan sesuatu tindakan dikendalikan oleh pikiran-pikiran baik, tetapi mengapa orang-orang yang umumnya memiliki pikiran yang baik melakukan tindakan yang menyimpang atau melakukan kejahatan.

Sykes dan Matza menggambarkan 5 (lima) teknik netralisasi yang dapat dilakukan oleh penjahat, sebagai berikut:

1. Penolakan tanggung jawab, di mana pelaku menggambarkan dirinya sebagai orang-orang yang tidak berdaya menghadapi tekanan social.
2. Penolakan cedera, yaitu pelaku berpendapat bahwa tindakan yang dilakukan tidak menimbulkan kerusakan besar bagi masyarakat.
3. Penolakan korban, yaitu pelakunya mengerti dirinya sebagai "penebus", sedangkan korban perbuatannya dianggap bersalah.
4. Penghakiman penjahat, yaitu para pelaku mengasumsikan bahwa orang-orang yang mengutuk tindakan yang telah dilakukan adalah orang munafik, munafik sebagai pelaku kejahatan tersembunyi, dari kecemburuan, dan sebagainya.
5. Penolakan terhadap loyalitas yang lebih tinggi, yaitu pelaku merasa terjebak antara kehendak masyarakat dan ketentuan hukum yang ada dalam masyarakat dengan kebutuhan kelompok yang lebih kecil, yaitu kelompok di mana mereka termasuk atau bergabung.

Dapat disimpulkan bahwa teori netralisasi mengungkapkan bahwa perbuatan menyimpang dan jahat didasarkan pada pemikiran orang tersebut sendiri dan disebabkan oleh berbagai kondisi di luar diri orang tersebut, maka pelaku selalu mencari alasan untuk membenarkan tindakannya melalui proses rasionalisasi.

### **Penerapan Teori Kriminologi untuk Penanggulangan Kejahatan Siber Kasus Kebocoran Data**

Tinjauan kriminologi secara umum bertujuan untuk mempelajari kejahatan dari berbagai aspek (Rochaeti & Sularto, 2017). Kriminologi sangat mementingkan dinamika pemikiran kritis mengenai teori kejahatan untuk memahami bagaimana suatu perbuatan menjadi kejahatan dan bagaimana seseorang menjalani ritual untuk digolongkan melakukan tindak pidana kejahatan. Sehingga dari pemahaman yang benar tentang proses-proses tersebut, selanjutnya dapat dijadikan dasar untuk menetapkan strategi kebijakan yang tepat dalam menanggulangi kejahatan (Odunze, 2018). Berdasarkan penjelasan teori kriminologi di atas, dapat dipahami bahwa penggunaan teori-teori kriminologi sangat diperlukan dalam kasus kejahatan siber terutama pada kasus kebocoran data nasabah karena digunakan sebagai dasar pijakan pengambil keputusan (decision maker) dalam menanggulangi kejahatan siber agar tepat sasaran dan efektif sesuai dengan karakteristik pelaku dan modusnya (Siregar & Sinaga, 2021).

Setiap jenis kejahatan siber mempunyai spesifikasi yang berbeda-beda, sehingga penyebab setiap jenis kejahatan siber belum tentu sama. Demikian pula motif pelaku tidak selalu sama. Namun pada umumnya terdapat persamaan antara satu pelaku kejahatan dengan pelaku kejahatan lainnya, dan antara satu jenis kejahatan dengan jenis kejahatan lainnya. Berdasarkan uraian keempat teori kejahatan di atas, maka dapat diambil kesimpulan untuk langkah penanggulangan kejahatan siber sebagai berikut:

- (1) Teori anomie dapat digunakan sebagai alat analisis untuk mengetahui alasan orang melakukan hacker terhadap suatu sistem. Teori Anomie berpendapat bahwa kejahatan terjadi karena tidak adanya norma dalam masyarakat yang mengatur kegiatan tersebut (kurangnya norma). Berdasarkan uraian Agus Rahardjo, dalam praktik ada sekelompok orang yang menolak kehadiran hukum untuk mengatur kegiatan di dunia maya (virtual). Menurut kelompok ini, dunia virtual adalah ruang yang bebas sehingga pemerintah tidak mempunyai kewenangan campur tangan dalam aktivitas tersebut, termasuk mengatur dengan sarana hukum.
- (2) Teori asosiasi diferensial dapat digunakan sebagai alat analisis untuk mengetahui mengapa orang melakukan sesuatu. Menurut teori ini, kejahatan pada hakikatnya merupakan hasil proses pembelajaran dan komunikasi yang terjadi antara seseorang dalam suatu kelompok intim. Teori tersebut sejalan dengan karakteristik pelaku kejahatan siber, yaitu sebagaimana dikemukakan oleh Sue Titus Reid, bahwa "They may have learned their acts from others in the same employ; thus, differential association cannot be ruled out.
- (3) Teori kontrol sosial dapat digunakan sebagai alat analisis untuk mencari faktor yang mendorong seseorang melakukan kejahatan hacker. Menurut teori ini, pelaku melakukan kejahatan karena ikatan sosial dalam diri seseorang melemah atau orang tersebut tidak lagi mempunyai ikatan sosial dengan masyarakat. Hal tersebut dibuktikan dalam penelitian sebelumnya yang memaparkan hasil wawancara dengan salah seorang hacker yang bangga atas hasil peretasan yang dilakukan sebagai bentuk menyibukan diri akibat kurangnya kegiatan berorganisasi di kehidupan bermasyarakat (Putra, 2019).
- (4) Teori netralisasi dapat digunakan sebagai alat analisis karena beberapa teknik netralisasi yang dikemukakan oleh Sykes dan Mata juga dapat menjadi penyebab terjadinya kejahatan dunia maya

di Indonesia. Berdasarkan penelitian yang mengumpulkan kuesioner dari beberapa pelaku hacker menjelaskan bahwa setiap individual hacker melakukan kegiatan peretasan bertujuan untuk memenuhi kepuasan pribadi mereka masing-masing (Putra, 2019).

Dari penjelasan teori kriminologi terlihat bahwa fenomena kejahatan siber saat ini perlu segera dilakukan evaluasi terhadap penerapan hukumnya. Oleh karena itu, perlu adanya harmonisasi hukum dalam kerangka ketentuan hukum pidana di bidang tindak pidana teknologi Informasi (Nugraha et al., 2022). Mengingat teknologi informasi saat ini berkembang pesat dan terus bermunculan hal-hal baru, serta kesenjangan hukum yang juga semakin banyak, maka pemerintah perlu merespon dengan cepat. Sudarto menyampaikan bahwa kriminalisasi merupakan bagian dari kebijakan hukum pidana, yang pada hakekatnya merumuskan hukum pidana yang baik dan memberikan pedoman bagi penciptaan (kebijakan legislatif), penerapan (kebijakan yudisial), dan pelaksanaan (kebijakan eksekutif) hukum pidana. Hukum pidana internasional mengenai kejahatan siber juga diperlukan untuk menanggulangi kejahatan siber lintas negara. Asas legalitas hukum pidana internasional harus diterapkan secara berbeda dengan hukum pidana nasional yang berkaitan dengan tanggung jawab pada individu atas kejahatan internasional (Puspito & Masyhar, 2023).

## **SIMPULAN**

Dengan menggunakan teori kriminologi, kita dapat memahami pelaku dan bentuk kejahatan siber dalam dunia perbankan. Selain itu dengan teori kriminologi pemerintah dapat menganalisis sebab akibat pelaku kejahatan siber melakukan hacker. Empat teori yang dapat digunakan untuk menganalisis kejahatan siber pada kasus kebocoran data nasabah, antara lain: teori anomie, asosiasi diferensial, kontrol sosial, dan netralisasi. Selain keempat teori tersebut, masih terdapat beberapa teori yang mungkin dapat digunakan dalam kejahatan siber di perbankan. Dalam kriminologi, penulis tidak selalu mempunyai paradigma yang sama, sehingga hampir semua teori mempunyai karakteristik yang berbeda-beda dalam memahami masyarakat. Namun, karena teori adalah “alat”, kebenaran isinya masih dapat diperdebatkan, dibantah, dan disempurnakan berdasarkan penelitian terkini. Oleh karena itu, tulisan ini dapat dijadikan bahan evaluasi untuk merancang pedoman hukum dalam pencegahan kejahatan siber pada kasus kebocoran data nasabah dengan mempertimbangkan teori-teori kriminologi untuk perkembangan hukum di Indonesia.

## DAFTAR PUSTAKA

- Anshori, A. (2021). Cyber Crime In A Criminology Perspective. *International Journal Of Social, Policy And Law*, 2(3), 120–125.
- Azarine, A. M. (2023). Bank BSI Pasca Serangan Siber: Mengungkap Potensi Kompensasi Bagi Nasabah. Retrieved from *Lk2fhui. Law. Ui. Ac. Id/Portofolio/Bank-Bsi-Pasca-Serangan-Siber-Mengungkappotensi-Kompensasi-Bagi-Nasabah*.
- Duana, G. R., Masyar, A., & Wulandari, C. (2023). Tinjauan Teori Kriminologi Dalam Kejahatan Siber (Kasus Kebocoran Data Nasabah): Overview of Criminological Theory in Cyber Crime (Customer Data Leakage Cases). *Jurnal Hukum PRIORIS*, 11(2), 161–174.
- Erlina, E. (2014). Analisa Kriminologi terhadap kekerasan dalam kejahatan. *Al Daulah: Jurnal Hukum Pidana Dan Ketatanegaraan*, 3(2), 217–228.
- Nugraha, A. A., Lukitaningtyas, Y. K. R. D., Ridho, A., Wulansari, H., & Al Romadhona, R. A. (2022). Cybercrime, Pancasila, and Society: Various Challenges in the Era of the Industrial Revolution 4.0. *Indonesian Journal of Pancasila and Global Constitutionalism*, 1(2), 307–390.
- Oduze, D. (2018). Cyber victimization by hackers: A criminological analysis. *Public Policy and Administration Research*, 8(01), 8–15.
- Puspito, B., & Masyhar, A. (2023). Dynamics of Legality Principles in Indonesian National Criminal Law Reform. *Journal of Law and Legal Reform*, 4(1), 109–122.
- Putra, E. H. (2019). Potret Aktivitas Hacker Di Media Sosial Untuk Aktualisasi Diri. *Jurnal Kaganga: Jurnal Ilmiah Sosial Dan Humaniora*, 3(1), 36–47.
- Rochaeti, N., & Sularto, R. B. (2017). Kajian Kriminologi Terkait Penegakan Hukum Pidana Terhadap Tindak Pidana Pembakaran Hutan Dan Lahan Di Provinsi Riau. *Diponegoro Law Journal*, 6(2), 1–15.
- Siregar, G., & Sinaga, S. (2021). The law globalization in cybercrime prevention. *International Journal of Law Reconstruction*, 5(2), 211–227.
- Sulisrudatin, N. (2018). Analisa kasus cybercrime bidang perbankan berupa modus pencurian data kartu kredit. *Jurnal Ilmiah Hukum Dirgantara*, 9(1).
- Widayanti, P. W. (2022). Tindak Pidana Pencurian Data Nasabah Dalam Bidang Perbankan Sebagai Cyber Crime. *Legacy: Jurnal Hukum Dan Perundang-Undangan*, 2(2), 1–21.



© 2025 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY SA) license (<https://creativecommons.org/licenses/by-sa/4.0/>).