ANALISIS TINDAK PIDANA *CYBER CRIME* DARI PERSPEKTIF KRIMINOLOGI

Evi Lidia Santri Br Munthe, Fakultas Hukum Universitas Udayana,
e-mail: evimunthe7@gmail.com
I Gusti Ayu Stefani Ratna Maharani, Fakultas Hukum Universitas Udayana,
e-mail: stefaniratnamaharani@unud.ac.id

ABSTRAK

Tujuan penulisan ini untuk menganilisis terkait faktor pendorong dilakukannya tindak pidana cyber crime dari sudut pandang kriminologi dan menelisik terkait upaya yang dapat dilakukan untuk penanggulangan kejahatan cyber crime. Studi ini menggunakan metode penelitian normatif dengan pendekatan konseptual. Hasil dari studi ini menunjukkan bahwa faktor pendorong dilakukkannya tindak pidana cyber crime dapat terjadi karena adanya motivasi, motivasi ini terbagi menjadi dua yaitu intrinsik yang berasal dari dalam diri pribadi seseorang dan ekstrinsik yang berasal dari faktor eksternal,adapun upaya yang dapat dilakukan untuk menanggulangi kejahatan cyber crime adah dengan upaya preventif dengan melakukan edukasi siber dan melengkapi sarana untuk mengimplementasikan keterampilan teknologi yang dimiliki secara legal dan represif yaitu dengan memberi sanksi tegas bagi pelaku kejahatan.

Kata Kunci: Cyber Crime, faktor pendorong, upaya, penanggulangan.

ABSTRACT

The purpose of this writng is to analyze the driving factors behind the commission of cyber crime from a criminological perspective and to explore efforts that can be made to countermeasures cyber crime. This study uses a normative research method with a conceptual approah. The results of this study show that the driving factors behind the commision of cybercrime can occur due to motivation, which is divided into two categories: intrinsic motivation, which comes from within the individual, and extrinsic motivation, which arises from external factors. Efforts to countermeasures cybercrime can be carried out through preventive measures, such as cyber education and equipping individuals with legal means to implement their technological skills, and through repressive measures, such as imposing strict sanctions on the perpetrators of crime.

Key word: Cyber Crime, driving factors, effort, countermeasures.

1. Pendahuluan

1.1. Latar Belakang Masalah

Pada dasarnya perkembangan teknologi digital semakin hari semakin pesat. Perkembangan tesebut dipergunakan untuk memenuhi efesiensi kebutuhan masyarakat sebagai dampak perkembangan zaman. Hal ini tampak pada kondisi dimana kegiatan kehidupan sehari-hari yang pada umumnya dilakukan secara langsung namun saat ini bisa dilakuan secara virtual seperti contoh adalah dengan menggunakan mbanking, masyarakat dapat melakukan transaksi langsung melalui gawai pribadi, telah tersedianya dompet digital, penggunaan aplikasi kesehatan maupun tanda pengenal penduduk, dan masih banyak lagi hal lainnya yang dapat dilakukan melalui teknologi yang berkembang saat ini. Dengan banyak nya aktivitas

yang dilakukan oleh manusia melalui sebuah sistem teknologi informasi dan komunikasi yang dapat menghubungkan setiap orang melalui dunia maya, membentuk suatu perkembangan baru terhadap perbuatan kejahatan.

Tidak dapat dipungkiri bahwa seiring dengan perkembangan zaman ke era yang lebih baru, kejahatan pun ikut serta mengalami perkembangan. Beberapa waktu belakangan masyarakat Indonesia semakin diresahkan dengan suatu bentuk kejahatan berbasis teknologi yang disebut sebagai kejahatan dunia maya atau *Cyber crime*. Kejahatan berbasis teknologi ini sejatinya sudah ada dan terjadi beberapa waktu tahun lalu. Kejahatan *Cyber Crime* berawal dari tragedi yang dilakukan oleh seorang mahasiswa di Amerika Serikat pada tahun 1960 an dengan melakukan manipulasi transkip akademik di Brooklyn Collage New York. Di Indonesia sendiri kejahatan *Cyber Crime* pertama kali terjadi pada tahun 1985 yang ditangani oleh Kepala Kejakasaan Tinggi Aceh Irdam SH,.M. Kasus Cyber Crime tersebut dilakukan dengan pembobolan rekening BNI 1946 cabang New York. Perbuatan tersebut dilakukan oleh Rudy Demsy yang merupakan mantan staf BNI 1946 New York.[1]

Perkembangan teknologi digital dari masa lalu hingga masa sekarang tentunya sangat jauh berbeda begitu pun dengan penggunaan teknologi digital tersebut. Pada masa sekarang manusia sangat bergantung terhadap keberadaan teknologi digital. Hal tersebut karena teknologi digital dianggap sebagai pemenuh kebutuhan hidup manusia di era digital sekarang. Berkembangnya teknologi digital tersebut berbanding lurus dengan makin maraknya kejahatan yang dilakukan melalui dunia maya. Di Indonesia sendiri telah banyak terjadi kasus-kasus *Cyaber Crime.* Sebagai contoh kasus adalah serangan ransomware, serangan ini dilakukan dengan cara membuat kompuer beku, para pelaku menglangsungkan perbuatannya dengan tujuan untuk melakuka pemerasan dengan meminta tebusan. Adapun negara yang menjadi korban adalah seperti Ukraina dan Amerika.[2]

Di Indonesia juga telah mengalami kejahatan ini, sebagai contoh kasus yaitu, *pertama* terjadi peretasan terhadap webiste BPJS kesehatan pada tahun 2021 hal ini membuat web tersebut tidak dapat diakses oleh pengguna hal tersebut juga menjadi dasar kekhawatiran masyarakat karena web tersebut mengelola data-data informasi kesehatan pengguna. *Kedua* pembobolan data pada Kominfo yang terjadi pada tahun 2022, pembobolan ini dilakukan oleh Bjorka dengan mencuri data registrasi kartu SIM yang dikelola oleh Kominfo. Ketiga adalah kasus yang terjadi pada tahun 2017 yang merugikan beberapa negara termasuk Indonesia. Kegiatan yang dilakukan adalah dengan melakukan penyebaran virus WannaCry yang menginfeksi ribuan komputer di seluruh dunia. Di Indonesia sendiri 100 ribu komputer terinfeksi sehingga mengakibatkan kerugian milirian rupiah.Pebuatan tersebut dilakukan agar pelaku mendapat uang tebusan. *Ke empat,* kasus yang sangat meresahkan masyarakat Indonesia adalah terjadinya kebocoran data E-KTP pada tahun 2018. Tidak hanya itu masih banyak kasus lainnya yang terjadi di Indonesia terkait *Cyber Crime* yang

[1] Makmur Dimila. " Cerita Irdam Tangani Kasus *Cyber Crime* Pertama di Indonesia". Diakleksis Tajam dan Strategis (2015), https://www.dialeksis.com/soki/cerita-irdam-tangani-kasus-cybercrime-pertama-di-indonesia/. diakses pada tanggal 26 November 2024.

[2] Abi Tyas. " 17 *Ransomware Examples & How They Occurred"*. Upguard Cybersecurity (2024), https://www.upguard.com/blog/ransomware-examples. Diakses pada tanggal 26 November 2024.

tentunya sangat memberi kerugian secara finansial bagi negara serta keresahan bagi masyarakat.[3]

Cyber Crime adalah suatu tindakan kejahatan yang telah diakui secara universal. Karena perbuatan tersebut dapat dilakukan lintas negara hanya dengan menggunakan seperangkat teknologi komputer. Dalam pendefenisiannya *Cyber Crime* adalah suatu kejahatan yang mempergunakan komputer sebagai alat utamanya dan objek kejahatannya juga terhadap sistem komputer ataupun jaringan komputer.[4] Menurut Widodo, *Cyber Crime* dapat dirtikan sebagai aktivitas yang dilakukan oleh individu, kelompok, atau badan hukum yang menggunakan komputer baik sebagai sarana untuk melakukan kejahatan maupun sebagai target atau objek kejahatan. Lazimnya *Cyber Crime* digolongkan menjadi tiga bentuk yang kerab diketahui oleh masyarakat yaitu, perbuatan berhubungan dengan pelanggaran terhadap kerahasiann, integritas, dan keberlangsungan data maupun sistem komputer, perbuatan yang memanfaatkan komputer sebagai sarana untuk melakukan kejahatan, serta tindakan tersebut berhubungan dengan konten atau atau muatan data dan sistem komputer.[5]

Terbentuknya kejahatan tersebut adalah akibat dari perkembangan ilmu pengetahuan dan teknologi dalam masyarakat. Nyatanya perkembangan tersebut telah digunakan sebagai sarana atau alat untuk melakukan kejahatan. Terdapar dua faktor sebagai dasar yang menyebabkan muncunya *Cyber Crime,* yang *pertama* adalah faktor teknis, dari segi teknis kemajuan teknologi ini mampu menghapus batas geografis antarnegara dan membuat ruang dunia semakin kecil sehigga jarak dirasa semakin dekat, sehingga timbulah konektivitas antarjaringan yang bisa memudahkan pelaku kejahatan dalam menjalankan aktivitas kriminalnya. Kemudian ada faktor sosial ekonomi, dimana ketidakmerataan distribusi teknologi menyebabkan ketimpangan kekuatan antar individu atau kelompok.[6]

Kenyataannya bahwa perbuatan kejahahatan dunia maya ini dilakukan oleh pihak-pihak yang memiliki kemampuan secara teknis di bidang teknologi. Penjahat dunia maya ini kerap disebut sebagai *hacker*. Woodward seorang jurnalis terkenal asal Amerika Serikat mengatakan bahwa para penjahat dunia maya adalah salah seorang yang malas sekaligus pandai, mereka tidak lagi merampok bank dengan senapan. Lebih gampang mencuri melalui dunia virtual.[7] Hacker merupakan salah satu kemampuan yang luarbiasa dalam ilmu komputer, bahkan sistem pemerintahan dalam mempertahankan sistem kemanan suatu negara membutuhkan keahlian ini, yang biasa disebut sebagai *Cyber Security, s*ehingga pada pelaksanannya pemerintah sendiri juga bekerjasama dengan para *hacker* profesional. Namun beberapa pihak lebih menggunakan kemampuan tersebut untuk menggencarkan suatu kejahatan.

---

[3] Achnad Farid. "14 Kasus *Cyber Crime* di Indonesia yang Menggemparkan Warganet". Exabytes (2022), https://www.exabytes.co.id/blog/kasus-cyber-crime-di-indonesia/#:~:text=Peretasan%20terhadap%20website%20BPJS%20Kesehatan,oleh%20akun%20bernama%20%E2%80%9CKotz%E2%80%9D. diakses pada tanggal 26 November 2024.

[4] Aldriano, Muhammad Anthony dan Mas Agus Priyambo. "*Cyber Crime* Dalam Sudut Pandang Hukum Pidana". *Jurnal Kewarganegaraan* 6, no.1 (2022): 2169-2175

[5] *ibid*

[6] Fadli, Muhammad, Dian Widjowati, dan Dwi Andayani. "Pencurian Data Pribadi di Dunia Maya (*Phising Cybercrime)* yang ditinjau dalam Perspektif Kriminologi". *Co-Value: Jurnal Ekonomi, Koperasi & Kewirausahaan* 14, no. 12 (2024): 824

[7] Chris Baraniuk. "Kebanyakan Penjahat Siber Sebenarnya Tidak Cerdas". BBC News Indonesia (2017), https://www.bbc.com/indonesia/vert-fut-41074809 diakses pada tanggal 26 November 2024.

Kriminologi merupakan disiplin ilmu sosial yang berupaya untuk mengidentifikasi penyebab timbulnya kejahatan dengan tujuan untuk mengetahui bagaimana cara pencegahan dan penanggulangan kejahatan tersebut, serta juga berusaha untuk mengurangi angka kejahatan.[8] Dari sudut pandang seorang ahli krimonologi asal Belanda yaitu W.A, Bonger berpendapat bahwasanya kriminologi merupakan ilmu pengetahuan yang dimana bertujuan untuk menyelidiki segala kejahatan seluas-luasnya.[9] Berdasarkan dari hal tersebut maka perlu dilakukan analisis mengenai penyebab kejahatan dunia maya atau *Cyber Crime* yang sebagai akibat dari perkembangan ilmu pengetahuan dan teknologi dari perpektif kriminologi.

Tindak pidana *Cyber Crime* merupakan salah satu bentuk kejahatan yang menarik perhatian para akademisi, sehingga telah ada penelitian terdahulu yang melakukan riset mengenai penelitian ini dan telah dipublikasikan. Penelitian tersebut diantaranya yakni berjudul " Pencurian Data Pribadi di Dunia Maya (*Phising Cybercrime*) yang ditinjau dalam Perspektif Kriminologi" penilitian ini dilaksanakan oleh Muhammad Fadli, Dijan Widjowati, dan Dwi Andayani.[10] Kemudian penelitian yang dilakukan oleh Gumelar Rizki Duana, Ali Masyar dan Cahya Wulandari yang berjudul " Tinjauan Teori Kriminoloi Dalam Kejahatan Siber (Kasus Kebocoran Data Nasabah). Penelitian terdahulu yang telah dipublikasikan memiliki persamaan dan perbedaan dengan penelitian terbaru ini yang berjudul " Analisis Tindak Pidana Cyber Crime dari Perspektif Krminologi".[11] Persamaan penelitian ini dengan penelitian terdahulu adalah tema yang diangkat berkaitan dengan kejahatan dunia maya dan dilihat dari sudut pandang kriminologi. Adapun perbedaannya adalah penelitian terdahulu hanya meniliti secara spesifik dan fokus tentang salah satu golongan atau bentuk dari *Cyber Crime* dan ditinjau hanya dari perspektif teori kriminologi sementara penelitian ini menelisik secara umum mengenai *Cyber Crime* itu tanpa membatasi terhadap salah satu bentuk *Cyber Crime* serta meninjau dari perspektif kriminologi secara mendalam.

1.2. Rumusan Masalah

1. Apa faktor pendorong dilakukannya tindak pidana *cyber crime* dari perspektif kriminologi
2. Bagaimana upaya yang dapat dilakukan untuk menanggulangi tindak pidana *cyber crime*?

1.3. Tujuan Penulisan

Penelitian ini bertujuan untuk mengetahui secara mendalam mengenai faktor pendorong dilakukannya tindak pidan *Cyaber Crime* dari perspektif kriminologi dan

[8] Edrisy, Ibrahim, Kamilatun dan Angelina Putri. *Kriminologi* (Bandar Lampung: Pusaka Media, 2023),9

[9] Widodo, Wahyu. *Kriminologi dan Hukum Pidana* (Semarang: Universitas PGRI SemarangPress, 2015),1

[10] Fadli, Muhammad, Dian Widjowati, dan Dwi Andayani. "Pencurian Data Pribadi di Dunia Maya (*Phising Cybercrime)* yang ditinjau dalam Perspektif Kriminologi". *Co-Value: Jurnal Ekonomi, Koperasi & Kewirausahaan* 14, no. 12 (2024): 824

[11] Gumelar Dauana, Ali Masyar, Cahya Wulandari. "Tinajuan Teori Kriminologi Dalam Kejahatan Siber (Kasus Kebocoran Data Nasabah)". *Comseerva: Jurnal Penelitian Dan Pengabdian Masyarakat* 11 no 2 (2024): 161-174

bagaimana upaya yang dapat diperbuat dalam hal menanggulangi tindak pidana *Cyber Crime* tersebut terutama di Indonesia

2. Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah penelitian hukum yang bersifat normatif. Sifat penelitian ini adalah berupa penelitian deskriptif dengan menggunakan bahan-bahan hukum primer berupa aturan perundang-undangan, dan bahan hukum sekunder dari buku dan jurnal serta bahan hukum tersier berupa literatur lainya yang berbeda dengan bahan hukum primer maupun sekunder yang dirasakan masih ada relevansinya dengan tema penelitian yang dilaksanakan dengan teknik pengumpulam data berupa studi kepustakaan. Pendekatan dalam penelitian ini berupa pendekatan konseptual dengan melihat konsep-konsep hukum yang bermula dari doktrin atau pandangan hukum.

3. Hasil dan Pembahasan

3.1. Faktor pendorong Dilakukannya Tindak Pidana *Cyber Crime* dari Perspektif Kriminologi

Ketika zaman mengalami perubahan dan perkembangan hal tersebut beriringan dengan perkembangan tindak kriminal. Perekembangan tindak kriminal itu tampak dengan diakuinya *Cyaber Crime* sebagai suatu kejahatan yang sangat meresahkan masyarakat. Keberadaan perbuatan kriminal tersebut dikarenakan terdapat kemajuan di bidang teknologi yang sangat memberikan manfaat dalam keberlangsungan kehidupan manusia saat ini baik itu dari segi kecepatan untuk memperoleh informasi, pekerjaan, sebagai sarana berdemokrasi bahkan alat untuk berpartisipasi dalam ranah politik.[12] Penyalahgunaan manfaat dari teknologi informasi dan komunikasi yang berkembang tersebut mengakibatkan timbulnya suatu kejahatan yang disebut kejahatan dunia maya.

Adapun beberapa bentuk kejahatan yang kerap terjadi di dunia maya adalah sebagai berikut:[13]

a. *Illegal acces/unauthorized access to computer system and service*
   Bentuk kejahatan ini dilakukan dengan cara meretas atau menyusup ke dalam sistem jaringan komputer secara ilegal, perbuatan ini dilakukan tanpa meminta atau memperoleh izin dari pemiliknya;
b. *Illegal contents*
   Kejahatan ini dilakukan dengan memasukkan data atau informasi berupa hoax, serta data atau informasi yang disajikan tidak etis. Perbuatan tersebut telah menggangu ketertiban umum bagi pengguna internet;
c. *Data forgey*
   Perbuatan ini dilakukan dengan memalsukan dokumen penting yang tersimpan dalam jaringan internet. Tindakan ini pada umumnya menyerang dokumen *e-commerce;*

[12] Fadli, Muhammad, Dian Widjowati, dan Dwi Andayani. "Pencurian Data Pribadi di Dunia Maya (*Phising Cybercrime)* yang ditinjau dalam Perspektif Kriminologi". *Co-Value: Jurnal Ekonomi, Koperasi & Kewirausahaan* 14, no. 12 (2024): 824

[13] Rokhman, Miftakur&Habibi-Isnatul Liviana. "Kejahatan Teknologi Informasi (*Cyber Crime*) dan Penanggulangannya dalam Sistem Hukum Indonesia". *Al-Oquanun:Jurnal Pemikiran dan Pembaharuan Hukum Islam* 23, no.2 (2020): 401-424

d. *Cyber espionage*
   Perbuatan ini dilakukan dengan tujuan memata-matai target, si pelaku menggunakan jaringan internet dengan menyusup ke sistem jaringan komputer pihak yang ditargetkan;
e. *Cyber sabotage and extortorin*
   Perbuatan ini berupaya untuk merusak data yang terkait ke internet, program komputer, atau sistem jaringan komputer. Perbuatan ini dilaksanakan dengan memasukkan *logic bomv,* virus komputer yang mengakibatkan program komputer tidak dapat digunakan dan pengoperasian komputer tersebut dikendalikan oleh pelaku;
f. *Offense againts intellectual property*
   Perbuatan ini secara spesifik menargetkan hak kekayaan intelektual. Seperti melakukan plagiasi tampilan website pihak lain secara tidak sah;
g. *Infringgements of privacy*
   Kejahatan ini pada umumnya dilakukan dengan membuat informasi pribadi yang tersimpan secara compuerized sebagai objek kejahatannya. Perbuatan ini sangat merugikan baik secara materiil maupun immaterial. Sebagai contoh adalah bocornya informasi pin ATM, KTP, dll.

Tindakan kejahatan dunia maya yang berbasis kejahatan teknologi informasi dan komunikasi ini dikategorikan sebagai *White Crime* hal tersebut berlandaskan karena para pelaku kejahatan ini dianggap memiliki kemampuan, pemahaman dan keahlian dalam menggunakan jaringan internet atau komputer. Individu ataupun kelompok yang memiliki kemampuan atau kecerdasan tersebut dalam mempergunakan teknologi informasi dan komunikasi atau komputer memiliki julukan, adapun julukannya adalah sebagai berikut:

a. *Hacker,* sebutan ini diberikan kepada orang yang ahli dalam bidang komputer dimana mereka mempelajari sistem komputer dan melakukan eksperimen dengan komputer sebagai sarana utamanya. Orang ini memiliki kecerdasan dan kemahiran untuk masuk ke jaringan komunikasi suatu jaringan dunia maya. Kaum ini memiliki pandangan bahwa tujuan seorang hacker adalah untuk memperkuat keamanan jaringan internet
b. *Craker,* sebutan ini diberikan kepada orang yang menggunakan kemampuan dan keterampilannya untuk memasuki atau menyusup dan merusak situs web secara ilegal dengan tujuan sebagai penghiburan dan memperoleh keutungan. Ketika mereka berhasil melakukan perbuatannya ada rasa bangga yang timbul. Berdasarkan info dari Kementerian Pertahanan Amerika terdapat 100 serangan *cracek* perharinya.
c. *Carder,* sebutan ini diperuntukkan untuk orang yang melakukan pembobolan kartu kredit dengan tujuan untuk mencuri nomor kartu orang lain demi memperoleh keuntungan pribadi.
d. *Deface,* sebutan ini diberikan bagi orang yang memasuki situs lain secara ilegal dan kemudian melakukan suatu perbuatan dengan mengganti tampilan halaman situs web untuk tujuan pribadi. Di Indonesia kejadian ini pernah terjadi terhadap situs web TNI dan Polri.
e. *Pheaker,* sebutan ini bagi mereka yang merusak jaringan telepon dengan tujuan untuk melakukan panggilan secara gratis kemana saja.

Dalam ruang teknologi informasi dan komunikasi terdapat dua golongan yakni *Cyber Crime* dan *Cyber Security*. *Cyber Crime* adalah kejahatan yang mengganggu, merusak suatu jaringan internet atau komputer sehingga menimbulkan suatu kerugian

bagi pihak yang menjadi objek kejahatan dan memberikan rasa kepuasan bagi pelaku yang bertindak melakukan kejahatan tersebut. Di sisi lain ada *Cyber Security* yang merupakan sistem yang berupaya untuk memberikan perlindungan keselamatan informasi yang ada dalam jaringan internet ataupun komputer sehingga memberi keamanan dari serangan suatu kejahatan dunia maya.[14] *Cyber Crime* maupun *Cyber Security* merupakan suatu kegiatan atau tindakan yang berhubungan dengan sistem jaringan internet ataupun komputer yang dimana aktor di balik kegiatan tersebut memiliki kemampuan dan keterampilan dibidang teknologi informasi dan komunikasi namun memiliki tujuan yang berbeda dalam pengimplementasian kemampuan serta keterampilan tersebut.

Hadirnya suatu perbuatan yang dianggap sebagai kejahatan oleh khalayak umum penting untuk diidentifikasi penyebab lahirnya suatu perbuatan kejahatan baik dari segi subjektif yaitu pelaku kejahatan maupun dari segi objektif yaitu bentuk perbuatan kejahatan itu sendiri. Dalam ilmu disiplin terdapat ilmu kriminologi yang digunakan untuk mempelajari suatu bentuk kejahatan ataupun pelaku kejahatan. Kriminologi juga sebagai ilmu bantu dalam hukum pidana untuk menentukan apakah suatu perbuatan tersebut layak untuk disebut sebagai tindak pidana dan dapat diberi sanksi pidana.

Menurut pendapat Bonger kriminologi secara teoritis terdiri atas beberapa cabang, diantaranya yaitu:[15]

a. Antropologi kriminal. Ilmu ini mempelajari mengenai manusia yang jahat yang dilihat dari ciri-ciri fisik seseorang yang merupakan ciri khas dari seorang penjahat
b. Sosiologi kriminal. Mempelajari bahwa kejahatan adalah suatu gejala sosial yang memuat faktor-faktor sosial sehingga menimbulkan reaksi kalayak umum dan akibat dari kejahatan itu sendiri. Ilmu ini menjelaskan bahwa keadaan sosial dan ekonomi sebagai musabab timbulnya kejahatan
c. Psikologi kriminal. Ilmu ini mempelajari kejahatan dari sudut ilmu jiwa dimana kejahatan timbul akibat dari adanya penyimpangan dari kondisi kejiwaan individu sehingga dapat mempengaruhi tingkah laku seorang yang menghasilkan suatu perbuatan jahat.
d. Psikopatologi dan Neurapathologi. Ilmu ini mempelajari mengenai penjahat yang diteliti berdasarkan penyimpangan atau ketidasempurnaan susunan urat syaraf sehingga mendorong seseorang untuk berbuat jahat.

Kriminologi secara etimologis berasal dari bahasa Yunani, *crime* cartinya kejahatan dan logos artinya ilmu, sehingga kriminologi adalah ilmu pengetahuan yang mempelajari tentang kejahatan. Istilah tersebut dikemukakan oleh Paul Topinard yang seorang ahli antropologi Prancis. W.A. Bonger seorang ahli kriminologi Belanda mengatakan kriminologi adalah ilmu pengetahuan yang memiliki tujuan untuk mengkaji gejala kejahatan seluas-luasnya. Kriminologi sebagai studi yang berfokus terhadap kejahatan, pelaku kejahatan serta reaksi masyarakat terhadap bentuk kejahatan dan penjahat dalam pelaksanaannya menggunakan suatu metode. Metode yang digunakan dalam penelitian kriminologi salah satunya adalah metode utama

[14] Indah, Febyola & Arista Sidautar, Nurul Annisa. " Peran *Cyber Security* Terhadap Keamanan Dat Penduduk Negara Indonesia (Studi Kasus: Hacker Bjorka). *Jurnal Bidang Penelitian Informatika,*1, no.1 (2022): 1-8

[15] Edrisy, Ibrahim, Kamilatun dan Angelina Putri. *Kriminologi* (Bandar Lampung: Pusaka Media, 2023), 3

yaitu tipologi kejahatan yang dikemukakan oleh Manheim.[16] Tipologi kejahatan merupakan suatu sistem yang bertujuan untuk mengklasifikasikan kejahatan atau penjahat ke dalam kelompok atau tipe tertentu. Seperti penjahat dikelompokkan berdasarkan dari karateritik umur, kelas sosial, kepribadian, situasi pelaku ataupun motif individu atau kelompok untuk melakukan kejahatan.

Tipologi Kejahatan siber dengan kejahatan konvensional yang biasanya terjadi memiliki perbedaan yang signifikan. Hal tersebut terlihat dari media atau sarana yang digunakan dalam melangsungkan kejahatan, target kejahatan, modus operandi serta konsekuensi dari kejahatan yang dilakukan. Untuk mengetahui faktor pendorong dari dilakukannya perbuatan kejahatan dunia maya maka harus diketahui terlebih dahulu tujuan dari dilakukanya kejahatan tersebut. Dalam tipologi kejahatan motivasi atau tujuan dilakukannya kejahatan adalah indikator penting untuk menghasilkan tipologi penjahat.[17] Menurut Farrungton motivasi merupakan keadaan fisiologis ataupun emosional yang menumbuhkan suatu dorongan sehingga menghasilkan energi terhadap individu untuk melakukan suatu pebuatan jahat. Motivasi juga bisa dimaknai sebagai tujuan dari suatu tindakan yang dibutuhkan untuk memuaskan kebutuhannya.

Motivasi oleh pelaku kejahatan pada umum nya terdapat dua jenis yaitu yang *pertama* motivasi intrinsik, yaitu motivasi yang berasal dari dorong dalam diri sendiri untuk melakukan suatu kejahatan tanpa ada intervensi dari faktor luar, *kedua* adalah motivasi ekstrinsik merupakan keinginan berbuat jahat yang di dorong dari keadaan faktor ekternal seperti untuk mendapat keuntungan seperti mendapat imbalan. Dalam perbuatan kejahatan dunia maya atau *Cyber Crime* motivasi yang lebih mendominasi untuk dilakukannya kejahatan adalah model intrinsik. Dorongan untuk melakukan kejahatan itu untuk memenuhi rasa ingin tahu, memiliki gairah untuk merasakan tantangan, karena hal tersebut dianggap menghasilkan rasa penghiburan yang menyenangkan. Adapun motivasi eksintrik pada pelaku kejahatan Cyber Crime adalah untuk membuat orang lain terkesan, sengaja merusak untuk mendapatkan imbalan, dan sebagai sarana balas dendam.[18]

Kejahatan siber merupakan kejahatan intelektual atau kejahatan kecerdasan yang dimana para pelaku kejahatan ini tidak menggunakan kekutan fisik namun lebih menggunakan kecerdasan serta keterampilan yang matang. Apabila dilihat dari tingkat kemampuan kejahatan siber Seebruck mengelompokkan menjadi 8 golongan yaitu; *Hacktivists,* pelaku yang memiliki kemampuan atau keterampilan di level menengah ke bawah, penyerangan yang dilakukan tipe ini adalah dipicu oleh ideologi politik; *Criminals,* pelaku yang memiliki keterampilan level menengah atas, penyerangan yang dilakukannya bertujuan untuk memperoleh keuntungan dan balas dendam; *Cyber warior,* memiliki kemampuan yang sangat terampil, penyerangan dilakukan atas dasar ideologi serta keuntungan; *Insiders,* kemampuan level menengah, dipicu atas rasa balas dendam dan keuntungan; *Crowdsource,* tidak memiliki kemampuan yang memumpuni penyerangan dilakukan sebagai kemauan balas

[16] Martha, Aroma Elmia. *Kriminologi Sebuah Pengantar* (Yogyakarta: Buku Litera, 2020), 31

[17] Wardani, Kusuma, Okta Sinaga,&dkk. " Tipologi White Collar Crime Di Indonesia: Pendekatan Psikologi". *Afeksi: Jurnal Psikologi,* 3, no.3 (2024): 15-24

[18] Sari, Dewi Purnama&Yusti Probowati, dkk. "Penggunaan Criminal Profiling dalam Menentukan Typology Penjahat Konvensional dan Penjhat Siber: Sytematic literature review". *Jurnal Pikologi Tabulrasa,* 19. No.6 (2024): 1-17

dendam dan penghiburan semata; *Novices,* memiliki kemampuan yang masih dasar dan penyerangan dilakukan atas dasar ingin tahu; *Punks,* memiliki kemampuan di level paling rendah, melakukan pernyerangan hanya sebagai keinginan untuk berpartisipasi dalam melakukan perbuatan menyimpang.[19]

Dalam kriminologi klasik terdapat suatu teori kejahatan yang disebut teori pilihan rasional. Landasan teori ini berasal dari filsafat utilitarianisme yang dimana tokoh dalam teori ini adalah seperti Beccaria, Jermy Bentham dan J.S Mill. Bentham dan Mill beranggapan bahwa seseorang berusaha untuk lebih memporeh kebahagian sebesar mungkin dan mencegah penderitaan. Bentham berpendapat bahwa apabila nilai penderitaan dari suatu perbuatan lebih besar daripada nilai kebahagian maka orang akan menghindari perbuatan yang dilarang.[20] Teori pilihan rasional adalah teori yang menjelaskan mengenai timbulnya suatu kejahatan atas dasar pertimbangan pelaku kejahatan yang dimana pelaku tersebut memperkirakan akan keuntungan dan kerugian yang dihasilkan atas perbuatan illegal. Dalam hal ini pelaku kejahatan tersebut akan mempertimbangkan faktor pribadi seperti finansial, balas dendam, sensasi, hiburan, dan ada faktor potensi situasional seperti, keberadaan target, kemungkinan ketahuan oleh polisi serta keamanan.

Teori pilihan rasional merupakan suatu gagasan bahwa individu secara sadar dan sengaja memilih perilaku kriminal dari kehendak bebas yang seseorang miliki. Berdasarkan hal tersebut maka relevan bahwasanya perbuatan *Cyber Crime* dilihat dari perspektif teori pilihan rasional, hal tersebut karena pelaku kejahatan dunia maya yang memiliki kecerdasan dan keterampilan di bidang teknologi memilih untuk mempergunakan keterampilannya melakukan perbuatan jahat, hal tersebut didasarkan atas kehendak bebas yang ada dalam dirinya dan pilihan-pilihan rasional atas besarnya peluang kebahagian yang diperoleh.

Teori pilihan rasional secara harafiah sudah kerap digunakan untuk menjelaskan kejahatan kerah putih. Pelaku kejahatan dunia maya ini berdasarkan teori pilhan rasional sejatinya telah melakukan pertimbangan yang matang untuk melancarkan perbuatannya. Dalam melangsungan perbuatan nya pelaku kejahatan ini biasanya memiliki tolak ukur yang mencakup, kemungkinan ditangkap, ketakutan terhadap konsekuensi, kehilangan kehormatan atau reputasi, pengaruh yang dihasilkan, risiko ataupun keuntungan dari kejahatan yang dilakukan.[21]

3.2. Upaya yang dapat Dilakukan Untuk Menanggulangi Tindak Pidana *Cyber Crime*

Kejahatan dunia maya salah satu kejahatan yang memiliki ruang lingkup yang luas, dimana kejahatan tersebut dapat dilakukan tanpa ada batasan ruang dan waktu. Suatu perbuatan kejahatan dapat timbul ketika ada peluang untuk melakukan kejahatan tersebut. Tindakan *Cyber Crime* akan sangat merugikan apabila ada korban akibat dari perbuatan tersebut, namun suatu kejahatan tanpa korban bukanlah perbuatan yang dapat dihukum. Berdasarkan hal tersebut maka yang harus dilakukan adalah dengan menutup peluang terjadinya suatu tindakan melawan hukum yang menimbulkan korban. Selain dari hal tersebut apabila suatu kejahatan masih terjadi

[19] ibid

[20] Ramadhan, Choky. "Teori Pilihan Rasional untuk Memahami Koruptor di Indonesia" *Jurnal Integritas:Antikorupsi.* 9, no.2 (2023):171-182

[21] Putri, Yuri Ananda. " Analisis Kejahatan Kerah Putih Berdasarkan Tipologi Kejahatan Siber Perorangan". *Makalah Departemen Kriminologi: Fakultas Ilmu Sosial dan Ilmu Politik.* (2016): 1-35

hingga menimbulkan korban maka perlu dilakukan upaya untuk tidak terjadi kembali kejahatan tersebut atau pengulangan kejahatan.

Pada umum nya dalam ranah hukum pidana, penanggulangan suatu kejahatan dapat dilakukan dengan dua upaya, yang *pertama* adalah upaya preventif upaya tersebut adalah suatu usaha untuk melakukan pengendalian dengan pencegahan sebelum terjadinya kejahatan. Hal ini dapat ditempuh dengan menanggalkan kondisi yang dapat menjadi faktor risiko penyebab terjadinya kejahatan. *Kedua* adalah upaya represif, upaya ini dilakukan untuk mengendalikan kejahatan setelah terjadinya perbuatan kejahatan. Tujuan upaya ini adalah untuk mengembalikan kondisi atau keadaan seperti semula dan memberikan kesadaran bagi pelaku kejahatan akibat dari dari perbuatan yang dilakukan.[22]Sejauh ini pemerintah telah melakukan upaya untuk menanggulangi kejahatan dunia maya. Adapun upaya mencolok yang dilakukan pemerintah adalah dengan terbentuknya Badan Siber dan Sandi Negara (BSSN) hal tersebut merupakan salah satu bentuk upaya preventif. Lembaga tersebut memiliki fokus utama terhadap keamanan siber dalam upaya peningkatan ketahanan nasional.[23] Pengendalian kejahatan melalui penegakan hukum Indonesia telah memiliki seperangkat aturan perundang-undang untuk mengatur kejahatan dunia maya yaitu UU ITE No. 1 Tahun 2024 tentang perubahan kedua atas UU ite No. 11 Tahun 2008. Pembentukan seperangkat aturan tersebut adalah implementasi dari upaya represif dengan adanya aturan yang memuat sanksi pidan bagi individu atau kelompok yang melakukan kejahatan dunia maya dan aturan tersebut juga bisa sebagai upaya preventif.

Apabila ditilik dari perspektif kriminologi pelaku kejahatan dengan perbuatan kejahatan adalah satu kesatuan yang berkorelasi. Untuk timbulnya kejahatan maka harus ada pelaku kejahatan, sehingga untuk menanggulangi kejahatan juga penting melakukan pendekatan terhadap pribadi pelaku kejahatan. Rogers mengungkapkan beberapa teori yang membuat kejahatan siber terjadi oleh beberapa penyebab, yaitu :[24]

a. Sosial, dengan menggunakan *learning theory,* teori menyatakan bahwasanya individu belajar melalui proses pembelajaran dan peniruan terhadap lingkungan yang ada di lingkungan sosialnya, hal tersebut memberi peluang seseorang untuk melakukan kejahatan secara mandiri. Mayoritas dari pelaku ini pada daarnya telah menguasai keterampilan dasar, kemudian saling berbagi informasi dan juga saling bersaing dengan tujuan menunjukkan kemampuan guna memperoleh pengakuan atau kerab disebut *reinforcement;*
b. Moral *dis-engagement theory,* pelaku kerap mendapatkan pengakuan atas keberhasilan tindakanya, hal demikian karena pelaku kejahatan siber sulit terdeteksi. Penilian terhadap perbuatan tersebut beralih dan dianggap sebagai penjaga masyarakat yang memiliki peran untuk menjaga kewaspadaan terhadap vendor yang tidak bermoral dan pemerintahan yang tirani. Hal tersebut mengakibatkan pembebasan moral, tidak ada rasa bersalah walaupun telah melakukan tindakan ilegal;

[22] Nebi Oktir. " Analisis Upaya Preventif dan Represif Penagakan Hukum Pidana terhadap Kekerasan Anak di Wilayah Hukum Kepolisian Sektor Jambi". *Parlementer: Jurnal Studi Hukum dan Administrasi Publik,* 1, no.3 (2024): 206-2017

[23] Supanto, Ismunaro, Tika Andarasni Parwitasari&dkk. " Pencegahan dan Penanggulangan Kejahatan Teknologi Infomasi Di Wilayah PDM Kabupaten Klaten Melalui Metode Sosialisasi Interaktif". *Jurnal Gema Keadilan*, 10, no. 3 (2023): 170-182

[24] Agung, Andreas&Hafrida, Erwin. " Pencegahan Kejahatan Terhadap Cybercrime". *Pamppas:Journa of Criminal,* 3, no. 2 (2022): 212-222

c. *Anonymity,* teori ini menyatakan bahwa anonimitas berpotensi menghasilkan kepribadian terburuk pada individu ketika sedang online, hal tersebut akibat dari pandangan bahwasanya mereka tida dapat dikenali bahkan bisa berpua-pura menjadi orang lain dengan samaran. Kondisi ini ditimbulkan karena perilaku online mencerminkan karakter sejati individu yang muncul sewaktu tidak berada dalam pengawasan diri atau karena ada pengaruh dari norma serta tekanan sosial.

Berdasarkan teori yang telah dipaparkan tersebut maka perlu diambil suatu langkah konkrit yang mutlak dilakukan untuk sebagai pencegahan atau penanggulangan tindakan *Cyber Crime* apabila ditilik dari sudut pandang pelakunya yaitu dengan melaksanakan edukasi mengenai *Cyber* itu sendiri. Edukasi siber adalah satu langkah konkrit yang perlu dilaksanakan hal ini bertujuan untuk memperkenalkan siber secara mendalam terhadap masyarakat dan terutama penggiat di bidang teknologi informasi dan komunikasi.[25] Individu atau kelompok yang memiliki keterampilan dalam penggunaan teknologi dan informasi juga harus memiliki pengetahuan tidak hanya terbatas terhadap teknologi tersebut tapi juga pemahaman tentang bahayanya serta kerugian apabila diimplementasikan secara illegal. serta memberi informasi terkait peluang akan diakuinya kemampuan mereka apabila diimplementasikan secara legal.

Dalam kriminologi terdapat suatu teori yang menyatakan tentang alasan timbulnya suatu kejahatan yaitu teori anomie. Teori tersebut dikemukakan oleh Emille Durkheim dan Robert Merton. Teori ini menggambarkan timbulnya suatu perbuatan menyimpang berakaitan dengan keadaan masyarakat atau keterbelakangan masyarakat. Robert Merton mengatakan timbulnya kejahatan dikarenakan terdapat kesenjangan antara cita-cita atau keterapilan yang dimiliki dengan peluang atau cara yang dapat ditempuh untuk mencapai cita-cita atau mengimplementasikan bakat atau kemampuan tersebut. Pada dasarnya setiap individu atau kelompok dalam masyarakat memiliki tujuan yang sama yang ingin dicapai namun tidak semua orang memiliki kesempatan yang sama untuk meraih tujuan tersebut dengan cara yang ilegal. Berdasarkan kondisi tersebut maka orang-orang pun akan melakukan segala cara dan memaksakan kehendaknya untuk meraih keinginanya sekalipun itu melanggar hukum.[26]

Apabila menggunakan pendekatan teori anomie dalam penanggulangan kejahatan *Cyber Crime* maka dapat dilakukan suatu upaya untuk mencegah atau menanggulangi perbuatan tersebut, yaitu pemerintah dapat memberi perhatian bagi individu atau kelompok yang memiliki keterampilan, kemampuan atau kecerdasan di bidang teknologi dan informasi dengan menyediakan sarana, kesempatang atau peluang yang lebih besar, untuk dapat mengimplementasikan keterampilan dan kmampuannya. Perhatian ini terutama bagi pihak yang berasal dari kalangan masyarakat yang kurang mampu sehingga individu atau kelompok tersebut memiliki peluang yang legal untuk mencapai tujuannya sehingga tidak tampak adanya kesenjangan.

---

[25] Rahman, Zulfa Ar. " Pemanfaatan Teknologi Informasi dalam Edukasi Literasi Digital untuk Peningkatan Keamanan Data dan Pencegahan Kejahatan Siber di Masyarakat Rawang Panca Arga". *Merkurius: Jurnal Riset Sistem Informasi dan Teknik Informatika,* 2, no.6 (2024): 82-90

[26] Djanggih, Hardianto&Nurul Qamar. "Penerapan Teori-Teori Kriminologi Dalam Penanggulangan Kejahatan Siber (*Cyber Crime)*". *Jurnal Pandecta,* 13, no.1 (2018): 10-23

4. Kesimpulan

Kejahatan *Cyber Crime* merupakan kejahatan intelektual dimana pelaku kejahatan menggunakan kecerdasan dan keterampilan untuk melangsungkan kejahatannya. Apabila dilihat dari sudut pandang kriminilologi untuk melakukan kejahatan individu ataupun kelompok dapat di dorong oleh motivasi pribadi dalam melakukan kejahatannya. Terdapat dua jenis motivasi yaitu motivasi intrinsik, dimana motivasi ini menjelaskan bahwasanya seseorang melakukan kejahatan karena faktor dorongan dari dalam diri sendiri tanpa dukungan dari luar, kedua ada faktor ekstrinsik, dimana seseorang melakukan kejahatan di dorong dari keadaan eksternal untuk mendapat keuntungan dan imbalan. Adapun beberapa upaya yang dapat dilakukan untuk menanggulangi permasalahan tersebut adalah dengan melakukan upaya preventif sebagai pencegahan seperti melakukan edukasi sibe, melengkapi sarana dan prasana bagi pihak yang memiliki kecerdasan tesebut untuk mengimplementasikan bakat atau kemampuanya secara legal serta upaya represif dengan memberikan sanksi hukuman sesuai dengan peraturan yang telah ada terkait tindak pidana siber.

DAFTAR PUSTAKA

Jurnal:

Aldriano, Muhammad Anthony dan Mas Agus Priyambo. "*Cyber Crime* Dalam Sudut Pandang Hukum Pidana". *Jurnal Kewarganegaraan* 6, no.1 (2022): 2169-2175

Agung, Andreas&Hafrida, Erwin. " Pencegahan Kejahatan Terhadap Cybercrime". *Pamppas:Journa of Criminal,* 3, no. 2 (2022): 212-222

Djanggih, Hardianto&Nurul Qamar. "Penerapan Teori-Teori Kriminologi Dalam Penanggulangan Kejahatan Siber (*Cyber Crime)*". *Jurnal Pandecta,* 13, no.1 (2018): 10-23

Fadli, Muhammad, Dian Widjowati, dan Dwi Andayani. "Pencurian Data Pribadi di Dunia Maya (*Phising Cybercrime)* yang ditinjau dalam Perspektif Kriminologi". *Co-Value: Jurnal Ekonomi, Koperasi & Kewirausahaan* 14, no. 12 (2024): 824

Indah, Febyola & Arista Sidautar, Nurul Annisa. " Peran *Cyber Security* Terhadap Keamanan Dat Penduduk Negara Indonesia (Studi Kasus: Hacker Bjorka). *Jurnal Bidang Penelitian Informatika,*1, no.1 (2022): 1-8

Nebi Oktir. " Analisis Upaya Preventif dan Represif Penagakan Hukum Pidana terhadap Kekerasan Anak di Wilayah Hukum Kepolisian Sektor Jambi". *Parlementer: Jurnal Studi Hukum dan Administrasi Publik,* 1, no.3 (2024): 206-2017

Putri, Yuri Ananda. " Analisis Kejahatan Kerah Putih Berdasarkan Tipologi Kejahatan Siber Perorangan". *Makalah Departemen Kriminologi: Fakultas Ilmu Sosial dan Ilmu Politik.* (2016): 1-35

Rahman, Zulfa Ar. " Pemanfaatan Teknologi Informasi dalam Edukasi Literasi Digital untuk Peningkatan Keamanan Data dan Pencegahan Kejahatan Siber di Masyarakat Rawang Panca Arga". *Merkurius: Jurnal Riset Sistem Informasi dan Teknik Informatika,* 2, no.6 (2024): 82-90

Ramadhan, Choky. "Teori Pilihan Rasional untuk Memahami Koruptor di Indonesia" *Jurnal Integritas:Antikorupsi.* 9, no.2 (2023):171-182

Rokhman, Miftakur&Habibi-Isnatul Liviana. "Kejahatan Teknologi Informasi (*Cyber Crime*) dan Penanggulangannya dalam Sistem Hukum Indonesia". *Al-Oquanun:Jurnal Pemikiran dan Pembaharuan Hukum Islam* 23, no.2 (2020): 401-424

Sari, Dewi Purnama&Yusti Probowati, dkk. "Penggunaan Criminal Profiling dalam Menentukan Typology Penjahat Konvensional dan Penjhat Siber: Sytematic literature review". *Jurnal Pikologi Tabulrasa,* 19. No.6 (2024): 1-17

Supanto, Ismunaro, Tika Andarasni Parwitasari&dkk. " Pencegahan dan Penanggulangan Kejahatan Teknologi Infomasi Di Wilayah PDM Kabupaten Klaten Melalui Metode Sosialisasi Interaktif". *Jurnal Gema Keadilan*, 10, no. 3 (2023): 170-182

Wardani, Kusuma, Okta Sinaga,&dkk. " Tipologi White Collar Crime Di Indonesia: Pendekatan Psikologi". *Afeksi: Jurnal Psikologi,* 3, no.3 (2024): 15-24

Buku:

Edrisy, Ibrahim, Kamilatun dan Angelina Putri. *Kriminologi* (Bandar Lampung: Pusaka Media, 2023)

Martha, Aroma Elmia. *Kriminologi Sebuah Pengantar* (Yogyakarta: Buku Litera, 2020)

Peraturan Perundang-Undangan:

UU ITE No. 1 Tahun 2024 tentang perubahan kedua atas UU ITE No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1

Artikel:

Achnad Farid. "14 Kasus *Cyber Crime* di Indonesia yang Menggemparkan Warganet". Exabytes (2022), https://www.exabytes.co.id/blog/kasus-cyber-crime-di-indonesia/#:~:text=Peretasan%20terhadap%20website%20BPJS%20Kesehatan,oleh%20akun%20bernama%20%E2%80%9CKotz%E2%80%9D

Abi Tyas. " 17 *Ransomware Examples & How They Occurred*". Upguard Cybersecurity (2024), https://www.upguard.com/blog/ransomware-examples

Chris Baraniuk. "Kebanyakan Penjahat Siber Sebenarnya Tidak Cerdas". BBC News Indonesia (2017), https://www.bbc.com/indonesia/vert-fut-41074809

Makmur Dimila. " Cerita Irdam Tangani Kasus *Cyber Crime* Pertama di Indonesia". Diakleksis Tajam dan Strategis (2015), https://www.dialeksis.com/soki/cerita-irdam-tangani-kasus-cybercrime-pertama-di-indonesia/.