Jurnal Riset Ilmu Hukum (JRIH)
e-ISSN 2798-6055 | p-ISSN 2808-3156
https://journals.unisba.ac.id/index.php/JRIH

Tersedia secara online di
Unisba Press
https://publikasi.unisba.ac.id/

Analisis Kriminologis Terhadap Peningkatan Kejahatan Siber di Masa Pandemi Covid-19

Alfiyan Umbara, Dian Alan Setiawan*

Prodi Ilmu Hukum, Fakultas Hukum, Universitas Islam Bandung, Indonesia.

ARTICLE INFO

Article history :
Received : 13/8/2022
Revised : 29/11/2022
Published : 20/12/2022

Volume : 2
No. : 2
Halaman : 81 - 88
Terbitan : **Desember 2022**

ABSTRAK

Pandemi Covid-19 yang terjadi di berbagai belahan dunia Khususnya Indonesia sebagai salah satu negara yang terdampak wabah tersebut. Beberapa negara mencatat terdapat penurunan kejahatan, akan tetapi terdapat kejahatan yang meningkat secara signifikan yakni Kejahatan Siber. Berdasarkan fenomena tersebut, maka permasalahan dalam penelitian ini dirumuskan sebagai berikut: (1) Apakah faktor-faktor yang menyebabkan meningkatnya kejahatan siber di masa pandemi covid-19? (2) Bagaimana langkah preventif yang harus dilakukan supaya mengurangi kejahatan siber di Indonesia?. Peneliti menggunakan metode pendekatan Yuridis Normatif yaitu pendekatan yang dilakukan berdasarkan bahan hukum utama dengan cara menelaah teori-teori, konsep-konsep, asas-asas hukum serta peraturan perundang-undangan yang berhubungan dengan penelitian ini. Pendekatan yang digunakan adalah studi kepustakaan yang meliputi Bahan Hukum Primer, bahan hukum sekunder, dan bahan hukum tersier. Untuk mendukung bahan sekunder, maka data-data dari BSSN (Badan Sandi dan Siber Negara) dan Kominfo terhadap peristiwa meningkatnya kejahatan siber di masa pandemi di gunakan untuk melengkapi data penelitian. Analisis data yang digunakan adalah analisis data kualitatif. Hasil dari penelitian ini adalah : bahwa kejahatan siber ditinjau dari aspek kriminologis terjadi akibat faktor ekonomi dan sosial selama masa pandemi, langkah penanggulangan dan pencegahannya menggunakan dua sarana yaitu penal dan non penal.

Kata Kunci : Pandemi; Kejahatan Siber; Kriminologi.

ABSTRACT

COVID-19 pandemic occurring in various parts of the world, especially Indonesia, as one of the countries affected by the outbreak. Some countries recorded a decrease in crime, but there was a significant increase in crime, namely cyber crime. Based on this phenomenon, the problems in this research are formulated as follows: (1) What are the factors that caused the increase in cyber crime during the COVID-19 pandemic? (2) What are the preventive steps that must be taken to reduce cyber crime in Indonesia? The researcher uses a normative juridical approach, which is an approach based on the main legal material by examining theories, concepts, legal principles, and legislation related to this research. The approach used is a literature study, which includes primary legal materials, secondary legal materials, and tertiary legal materials. To support secondary material, data from BSSN (National Cyber and Crypto Agency) and The Ministry of Communication and Informatics regarding the increasing incidence of cyber crime during the pandemic is used to complement the research data. The data analysis used is qualitative data analysis. The results of this study show that cyber crime, in terms of criminological aspects, occurs due to economic and social factors during the pandemic. Prevention and control measures use two means, namely penal and non-penal.

Keywords : Pandemic; Cyber Crime; Criminology.

Corresponding Author : Email : dianalan.setia@yahoo.com
Indexed : Garuda, Crossref, Google Scholar
DOI : https://doi.org/10.29313/jrih.v2i2.1324

A. Pendahuluan

Kejahatan siber adalah segala aktivitas illegal yang digunakan oleh pelaku kejahatan dengan menggunakan teknologi sistem informasi jaringan komputer yang secara langsung menyerang teknologi sistem informasi dari korban. Kejahatan siber dapat dibedakan menjadi dua kategori, yaitu kejahatan terhadap sistem komputer dan kejahatan yang menggunakan jaringan computer (Widodo, 2009). Kejahatan dalam bidang komputer ini merupakan sisi gelap dari kemajuan teknologi yang mempunyai dampak sangat luas bagi seluruh sendi kehidupan modern ini (Maskun, 2013).

Kebijakan pembatasan sosial berskala besar sebagai upaya pencegahan penyebaran kasus covid-19 yang menyebabkan orang berada di rumah baik untuk beribadah, belajar, berkerja, dan lain-lain. Oleh karenanya semakin mengandalkan internet untuk mengakses layanan kehidupan yang biasanya didapatkan secara offline. Di masa Pandemi Covid-19, kejahatan siber mengalami peningkatan yang sangat signifikan, hal ini dipicu oleh presentase populasi masyarakat yang terhubung ke internet dan waktu yang dihabiskan untuk online, dikombinasikan dengan rasa kecemasan dan ketakutan yang ditimbulkan akibat pandemi telah memberi peluang lebih banyak bagi pelaku kejahatan untuk mengambil keuntungan dari situasi ini dan menghasilkan lebih banyak uang atau menciptakan gangguan yang masif.

Berdasarkdan data dari BSSN (Badan Sandi dan Siber Negara), sepanjang bulan januari-agustus 2020, terdapat hampir 190 juta upaya serangan siber di Indonesia, naik empat kali lipat dibanding periode yang sama pada tahun lalu hanya tercatat 39 juta (Heniarti et al., 2015). Menurut data POLRI, bulan April 2020 setidaknya da 937 kasus yang dilaporkan. Ada tiga kasus dengan angka tertinggi yaitu kasus Provocative, hate content and hate speech sebanyak 473, Penipuan online 259 kasus, dan Konten pornografi 82 kasus.

Ruang lingkup kejahatan siber menjadi sangat penting guna memberikan batasan, patut disadari bahwa perkembangan internet yang begitu cepat berbanding lurus dengan modus kejahatan yang mucul. Ada beberapa ruang lingkup kejahatan siber, yaitu: pembajakan, penipuan, pencurian, pornografi, pelecehan, pemfitnahan, dan pemalsuan (Bestari, n.d.).

Kejahatan siber secara persebaran mempunyai modus yang berbeda-beda dan seiring berjalannya waktu semakin beragam dan diperbarui modus operandi nya, yang paling banyak digunakan adalah rekaya sosisal (social engineering) yakni kejahatan yang memanipulasi psikologi korban, baik disadari atau tidak agar melakukan tindakan tertentu yang menguntungkan pelaku. Media yang digunakan dalam social engineering seperti telepon, SMS, e-mail maupun berbagai media sosial (Rahardjo, 1976).

Upaya untuk mencegah dan menanggulangi peningkatan kejahatan siber ini perlu untuk dilakukan. Pemerintah, masyarakat dan semua stake holder yang ada harus bersama-sama memerangi kejahatan siber ini, karena sifat dari kejahatan siber sendiri yang berbahaya. Dalam kasus kejahatan siber, baik korban maupun pelaku tidak berhadapan langsung dalam satu tempat kejadian perkara (Golose, 2007). Dalam beberapa kasus, baik korban maupun pelaku dapat berada pada negara yang berbeda. Hal tersebut menggambarkan bahwa kejahatan siber merupakan salah satu bentuk kejahatan lintas negara (*transnational crime*), tak terbatas (*borderless*), tanpa kekerasan (*non-violence*), tidak ada kontak fisik (*no physically contact*) dan tanpa nama (*anonomity*).

Berdasarkan latar belakang yang telah diuraikan, maka perumusan masalah dalam penelitian ini sebagai berikut: "Apakah faktor-faktor yang menyebabkan peningkatan kejahatan siber selama pandemi covid-19?" dan "bagaimana langkah preventif yang dilakukan guna mengurangi kejahatan siber di Indonesia?". Selanjutnya, tujuan dalam penelitian ini diuraikan dalam pokok-pokok sebagai berikut: (1) Untuk mengetahui faktor-faktor apa saja yang menyebabkan terjadinya peningkatan kejahatan siber di masa pandemi covid-19; (2) Menentukan dan sebagai referensi langkah penanggulangan apa saja yang bisa dilakukan guna mengurangi terjadinya kejahatan siber di Indonesia.

B. Metode Penelitian

Peneliti menggunakan metode hukum normatif yaitu pendekatan yang dilakukan berdasarkan bahan utama hukum dengan cara menelaah teori-teori konsep-konsep, asas-asas hukum serta peraturan perundang-undangan yang berhubungan dengan penelitian ini. Pendekatan yang digunakan adalah studi kepustakaan yang meliputi Bahan Hukum Primer, bahan hukum sekunder, dan bahan hukum tersier.

Dengan teknik pengumpulan data yang digunakan dalam penelitian ini adalah observasi, dan studi pustaka. Adapun teknik analisis data yang digunakan dalam penelitian ini adalah teknis normatif kualitatif yaitu dengan cara menjabarkan data-data yang diperoleh berdasarkan norma-norma hukum, teori-teori, serta doktrin dan kaidah yang relevan dengan pokok permasalahan guna dilakukan pembahasan yang komprehensif.

C. Hasil dan Pembahasan

Data dan Fakta Kasus Kejahatan Siber di Indonesia Selama Masa Pandemi Covid-19

Adanya pandemi covid-19 memaksa dan menyadarkan kita bahwa segala hal menjadi mungkin tuntuk dilakukan melalui internet, meski tanpa interaksi tatap muka secara langsung. Hal ini mendorong masyarakat berinteraksi melalui ruang siber dalam berbagai aspek kehidupan, mulai dari bersosialisasi, Pendidikan, mencari nafkah, mengisi waktu luang, dan lain sebagainya. Perubahan secara sistemik dalam cara kita menjalani kehidupan dan penggunaan internet yang sangat tinggi mendorong maraknya kejahatan elektronik. Teknik kejahatan siber yang umum seperti halnya *phishing* telah mengalami lonjakan. *Phishing* adalah praktik penipuan yang mendorong individu untuk mengungkapkan informasi pribadi, seperti kata sandi dan nomor kartu kredit melalui situs web atau email palsu. Meskipun banyak organisasi yang telah menerapkan sistem keamanan untuk memblokir serangan *phishing*, namun penyerang juga semakin memiliki peralatan *phishing* yang lebih canggih. Pusopskamsinas 2020 mendeteksi terhadinya emaik phishing sebanyak 2549 kasus dengan peningkatan jumlah kasus email phishing terjadi di bulan maret-mei 2020. Sebanyak 55,53% dikirim pada jam kerja (09.00-17.00) dan 44,37% dikirim di luar jam kerja.

Menurut survey Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada tahun 2019 hingga kuartal II tahun 2020, jumlah pengguna internet di indonesia adalah sebanyak 196,7 juta jiwa, setara dengan 73.7% dari populasi penduduk di indonesia. Angka tersebut menjadi cerminan bahwa ruang siber, kini tidak lagi hanya menjadi milik kelompok masyarakat yang "melek internet", tetapi juga menjadi ruang gerak baru bagi mereka yang terdorong untuk menggunakannya karena pandemi. Di satu sisi, hal ini menjadi merupakan berita baik atas meningkatnya kapabilitas masyarakat dalam beradaptasi dengan perkembangan teknologi. Di sisi lain, ancaman keamanan pun semakin meningkat karena semakin besarnya jumlah pengguna yang masih awam terhadap keamanan siber. Pandemi Covid-19 menjadi topik utama dalam tren keamanan siber. indonesia bahkan semakin diuji dengan adanya kasus kebocoran data 91 juta pengguna situs belanja online Tokopedia, yang tidak lama kemudian disusul oleh kebocoran data 1,2 juta pengguna situs Bhinneka. Selain kasus tersebut, pada pertengahan 2020 di masa pemilihan umum, adanya akun yang mengakui telah membobol 2,3 juta data warga Indonesia dari Komisi Pemilihan Umum (KPU).

Kebocoran data ini tentu akan berdampak panjang jika kesadaran masyarakat akan keamanan siber sangat rendah. Setidaknya mitigasi pertama pengguna ketika terjadi kebocoran data adalah mengubah kata sandi. Jika hal itu tidak dilakukan, dampak dan kerugiannya menjadi tidak terbatas.

Berikut adalah data peningkatan kasus kejahatan siber selama pandemi covid-19 dan sebelum adanya pandemi covid-19:

Tabel 1. Data Peningkatan Kasus Kejahatan Siber Selama Pandemi Covid-19

NO	JENIS KEJAHATAN	2018-2019	2020-2021
1	Hate Speech	473	575
2	Penipuan Online	259	390
3	Pornografi	82	126
4	Akses Ilegal	53	85
	Total Kejahatan	**867**	**1.176**

Sumber : Badan Pusat Statitstika.

Faktor-Faktor yang Menyebabkan Terjadinya Peningkatan Kejahatan Siber di Masa Pandemi Covid-19 Berdasarkan Aspek Kriminologi

Cybercrime merupakan kejahatan yang tergolong baru karena muncul seiring berkembangnya ilmu teknologi informasi dan komunikasi. Kejahatan ini dapat ditujukan kepada fasilitas umum, kelompok organisasi/lembaga, maupun terhadap target individu. Ditinjau dari aspek kriminologi Ditinjau dari aspek kriminologi yang dikaji melalui beberapa pendekatan teori. Dalam teori Social Control, kejahatan siber dapat muncul karena lemahnya kontrol sosial. Pada beberapa kasus yang hadir, pelaku dari kejahatan siber ini tidak tampak secara fisik dan identitasnya cenderung sulit untuk di identifikasi sehingga kontrol terhadap perilakunya sangatlah sulit untuk dilakukan. Menurut Travis Hirschi, terdapat empat bentuk *social bonds* yaitu *attachment, commitment, involvement,* dan *belief*.

Attachment adalah kemampuan manusia untuk melibatkan dirinya terhadap orang lain. Kalau attachment sudah terbentuk, maka orang tersebut akan pekaterhadap pikiran, perasaan, dan kehendak orang lain. Kaitan attachment dengan penyimpangan adalah sampai sejauh mana orang tersebut peka terhadap pikiran, perasaan, dan kehendakorang lain sehingga ia dapat dengan bebas melakukan penyimpangan. Attachment dibgai menjadi dua, yaitu: (1) Attachment Total, adalah suatu keadaan dimana seorang individu melepas rasa ego yang terdapat dalam dirinya dan diganti dengan rasa kebersamaan.rasa kebersamaan inilah yang mendorong seseorang untuk selalu menaati aturan-aturan, karena pelanggaran terhadap aturan tersebut berarti menyakiti perasaan orang lain; (2) Attachment Partial, adalah hubungan antara seorang individu dengan lainnya, dimana hubungan tersebut tidak didasarkan pada peleburan ego dengan ego yang lain tetapi karena hadirnya orang lain yang mengawasi.

Lalu *Commitment* adalah keterikatan seseorang pada sub sistem konvensional seperti sekolah, pekerjaan, organisasi-organisasi dan sebagainya. Segala kegiatan yang dilakukan oleh seorang individu tersebut, akan mendatangkan manfaat bagi orang tersebut, yang dapat berupa harta, benda, reputasi, masa depan, dan sebagainya.

Segala investasi tersebutlah yang mendorong orang untuk taat pada aturan-aturan yang berlaku. maka segala investasi yang diperoleh akan lenyap begitu saja. Investasi tersebut dapat digunakan sebagai rem untuk melakukan devian.

Involvment adalah aktivitas seseorang dalam sub sistem konvensional. Jika seseorang berperan aktif dalam organisasi maka kecil kecenderungannya untuk melakukan deviasi (penyimpangan). Bila orang aktif dalam segala kegiatan maka orang tersebut akan menghabiskan segala waktu dan tenaganya dalam kegiatan tersebut, sehingga dia tidak sempat lagi memikirkan hal-hal yang bertentangan dengan hukum. Dengan demikian segala aktivitas yang dapat mendatangkan manfaat, akan mencegah orang untuk melakuakan perbuatan yang bertentangan dengan hukum.

Belief adalah aspek moral yang terdapat dalam ikatan sosial. Belief merupakan kepercayaan seseorang pada nilai-nilai moral yang ada. Kepercayaan seseorang kepada norma-norma yang ada akan menimbulkan kepatuhan terhadap norma. Kepatuhan terhadap norma tersebut akan mengurangi keinginan untuk melanggar, tetapi bila orang tidak mematuhi norma-norma maka lebih besar kemungkinan orang tersebut melakukan pelanggaran.

Teori *Kontol Sosial* berasumsi bahwa semakin kuat ikatan-ikatan sosial tersebut maka semakin kecil kemungkinan terjadi delinkuensi, begitupun sebaliknya. Sehingga lemahnya ikatan dan hubungan sosial individu dengan masyarakat dapat menjadi faktor penyebab munculnya kejahatan, salah satunya cybercrime.

Kemudian dalam teori *differential association* dari Sutherland, dimana kejahatan dapat muncul dari adanya proses yang dipelajari. Cybercrime bukan tergolong kejahatan yang mudah untuk dilakukan setiap orang karena perlu adanya teknik dan keterampilan tertentu dalam bidang teknologi dan jaringan. Hal tersebut menunjukkan bahwa terdapat proses "belajar" atau "Latihan" yang dilakukan oleh pelaku dalam melakukan tindak kejahatan. Selain itu, teori ini juga mengemukakan bahwa kejahatan dipelajari melalui partisipasi bersama orang lain, baik dalam komunikasi verbal maupun non-verbal. Dalam beberapa kasus, cybercrime umumnya dilakukan bukan oleh individu, melainkan kelompok tertentu yang antar anggotanya saling belajar dan bekerjasama satu sama lain.

Teori anomi beranggapan bahwa kejahatan muncul karena dalam masyarakat tidak ada norma yang mengatur suatu aktivitas tersebut *(normlesness).* 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. Selanjutnya dijelaskan bahwa pendapat pro dan kontra tentang ada atau tidak adanya hukum yang dapat mengatur kejahatan siber *(cyber crime)* tersebut berpangkal pada kesenjangan antara karakteristik kejahatan dengan hukum pidana konvensional. Karakteristik penggunaan internet sebagai basis kegiatan bersifat lintas batas sehingga sulit untuk diketahui yurisdiksinya, padahal hukum pidana konvensnional yang berlaku di Indonesia banyak yang bertumpu pada batasan-batasan tentorial. Ketentuan hukum pidana konvensional tersebut ternyata tidak dapat menyelesaikan kasus dalam aktivitas dan internet secara optimal (Golose, 2007).

Beberapa faktor utama yang menyebabkan timbulnya kejahatan siber itu sendiri adalah sebagai berikut: (a) Kurangnya sosialisasi atau pengarahan baik dari akademisi umum seperti sekolah atau edukasi dari orang tua mengenai manfaat internet, sehingga banyak penyalahgunaan yang terjadi; (b) Semakin maju sebuah negara, tapi tidak diimbangi kesejahteraan masyarakatnya, maka makin besarnya kesenjangan sosial terjadi; (c) Makin maraknya sosial media, media elektornik, dan media penyimpanan virtual (cloud), sehingga membuat manusia menjadi makin tergandrungi akan akses internet di dalam kehidupannya; (d) Gaya hidup; (e) Kelalaian daripada manusianya itu sendiri; (f) Adanya keinginan pengakuan dari orang lain; (g) Bertambah majunya teknologi dan mudahnya mengakses jaringan internet anytime anywhere tanpa ada batasan waktu.

Dalam sudut pandang yang lebih luas, latar belakang terjadinya kejahatan siber ini terbagi menjadi dua faktor penting, yaitu: (1) Faktor Teknis, Saling terhubungnya antara jaringan yang satu dengan yang lain memudahkan pelaku kehjahatan untuk melakukan aksinya. Kemudian tidak meratanya penyebaran teknologi menjadikan pihak yang satu lebih kuat dari pihak yang lain; (2) Faktor Ekonomi, Kejahatan siber dapat dipandang sebagai produk ekonomi. Isu global yang kemudian dihubungkan dengan kejahatan tersebut adalah keamanan jaringan. Keamanan jaringan merupakan isu global yang muncul bersamaan dengan internet. Sebagai komoditi ekonomi, banyak negara yang tentunya sangat membutuhkan perangkat keamanan jaringan. Melihat kenyataan seperti itu cyber crime berada dalam skenario besar dari kegiatan ekonomi dunia.

Motif Kejahatan siber pada umumnya dapat dikelompokkan menjadi dua (2) katergori, yaitu sebagai berikut: (a) Motif Intelektual, kejahatan yang dilakukan hanya untuk kepuasan pribadi dan menunjukkan bahwa dirinya telaah mampu untuk merekayasa dan mengimplementasikan bidang teknologi informasi. Kejahatan dengan motif ini pada umumnya dilakukan oleh seseorang secara individual. (b) Motif ekonomi, politik dan kriminal yaitu kejahatan yang dilakukan untuk keuntungan pribadi atau golongan tertentu yang berdampak pada kerugian secara ekonomi dan politik pada pihak lain. Karena memiliki tujuan yang dapat berdampak besar, kejahatan dengan motif ini pada umumnya dilakukan oleh sebuah korporasi.

Kemudian Berdasarkan analisis yang dilakukan oleh penulis terhadap peningkatan kejahatan siber ini ada beberapa hal yang pada akhirnya menjadi faktor terjadinya peningkatan kejahatan siber selama masa pandemic covid-19 di Indonesia, diantaranya adalah sebagai berikut:

Kurangnya kesadaran hukum masyarakat, kesadaran hukum sendiri merupakan kesadaran tentang apa yang seharusnya atau tidak seharusnya kita lakukan berkaitan dengan aturan atau hukum yang berlaku di masyarakat. Saat ini kesadaran hukum masyarakat masih dinilai kurang terkait aktivitas cybercrime, hal tersebut dikarenakan kurangnya pemahaman terkait cybercrime baik itu tindakan maupun efek yang ditimbulkan. Tingkat Kesadaran masyarakat atas teknologi dan aktivitas di dunia maya juga sangat mempengaruhi apa yang terjadi di dalamnya. Semakin kurangnya kesadaran atas teknologi, maka semakin besar pula peluang untuk dapat dimanfaatkan oleh pelaku kejahatan (Setiawan, 2018). Melalui pemahaman mengenai cybercrime, masyarakat sangat berperan penting dalam upaya penanggulangan cybercrime, tanpa pemahaman pelaku cybercrime akan merajalela karena masyarakat tidak tahu apa yang sesungguhnya mereka lakukan hingga pada akhirnya mereka tertipu, rekening mereka dibobol dan berbagai kerugian lainnya.

Keamanan, media yang digunakan oleh pelaku cybercrime berbeda dengan pelaku tindak pidana pada umumnya, pelaku cybercrime menggunakan akses internet yang dapat digunakan dimana saja baik di tempat tertutup maupun terbuka. Namun, sistem keamanan yang dimiliki oleh internet masih belum dapat

dikatakan aman, sehingga dapat membuat siapa pun bebas melakukan aktivitasnya di dunia maya tanpa sadar akan batasan yang dapat mendorong pertumbuhan cybercrime.

Aparat penegak hukum, tidak dapat dipungkiri bahwa adanya kemungkinan sebagian dari aparat penegak hukum masih minim pengetahuan akan teknologi yang menjadi tempat yang digunakan pelaku untuk melakukan kejahatan cybercrime, sehingga dapat dimungkinkan pelaku cybercrime jauh lebih hebat dibandingkan aparat penegak hukum yang mengakibatkan semakin meningkatnya intensitas cyber crime di Indonesia.

Perundang-undangan yang kurang ditegakkan, saat ini Indonesia memang belum memiliki undang-undang khusus yang mengatur mengenai mengenai cybercrime. walaupun sudah ada hukum yang berlaku umum dan dapat dikenakan bagi para pelaku cybercrime seperti aturan dalam KUHP dan Undang-undang ITE yang sebenarnya sudah sangat membantu, sayangnya mengaplikasinya dari peraturan yang ada kurang dijalankan oleh para aparat penegaka hukum.

Hal ini dipengaruhi oleh kurangnya pengetahuan atau kemampuan mereka dalam dunia maya. hukum pidana berfungsi mengatur dan menyelenggarakan akan kehidupan masyarakat agar dapat tercipta dan terpeliharanya ketertiban umum. Sehingga peraturan yang ada dalam bidang kejahatan siber harusnya perlu di mutakhirkan dengan perkembangan hari ini dan juga di pertegas dalam ranah penegakkannya.

Langkah-Langkah preventif yang Dilakukan sebagai Upaya Mengurangi Kejahatan Siber di Indonesia

Kegiatan siber meskipun bersifat virtual dapat dikategorikan sebagai tindakan dan perbuatan hukum yang nyata dalam transaksi dan aplikasi. Penggunaan hukum pidana teknologi komputer dalam mengatur masyarakat (lewat peraturan perundang-undangan pidana) pada hakikatnya merupakan bagian dari suatu langkah kebijakan *(policy)*.

Selanjutnya untuk menentukan bagaimana suatu usaha yang rasional dalam melakukan kebijakan tidak dapat pula dipisahkan dari tujuan kebijakan pembangunan itu sendiri secara integral. Hukum pada prinsipnya harus mengantisipasi kecepatan perkembangan teknologi informasi dan internet. Jika mengacu kepada teori preventif yang dikemukakan dalam ilmu kriminologi, ada beberapa cara yang dapat dilakukan dalam pencegahan dam penanggulangan kejahatan siber yaitu sebagai berikut : mengamankan sistem, membuat undang-undang khusus untuk kejahatan siber, peningkatan sumber daya manusia (SDM), dan Meningkatkan Kerjasama antar negara. Upaya penanganan cyber crime membutuhkan keseriusan semua pihak mengingat teknologi informasi khususnya internet dijadikan sarana untuk membangun masyarakat yang berbudaya informasi. Keberadaan undang-undang yang mengatur cyber crime memang diperlukan, akan tetapi apalah arti undang-undang jika pelaksana dari undang-undang tidak memiliki kemampuan atau keahlian dalam bidang itu dan masyarakat yang menjadi sasaran dari undang-undang tidak mendukung tercapainya tujuan pembentukan hukum tersebut (Yurizal, 2018).

Penanggulangan kejahatan dengan menggunakan hukum pidana merupakan bagian dari kebijakan kriminal. Kebijakan dengan sarana penal adalah upaya penanggulangan kejahatan dengan menggunakan sarana pidana. Dalam hal ini telah terjadi semacam perumusan pidana dan pemidanaan yang telah dilegalkan melalui perundang-undangan. Sehingga, telah ada kepastian hukum dalam melakukan penanggulangan maupun pemecahan terhadap pelanggaran atau kejahatan yang dilakukan oleh para pelaku kejahatan siber. Sedangkan sarana non penal artinya upaya penanggulangan kejahatan dengan tidak melakukan hukum pidana atau dapat diartikan juga sebagai upaya preventif terhadap kejahatan (Rasso, 2014).

Menurut analisis penulis ada beberapa Langkah preventif yang bisa dilakukan guna mengurangi peningkatan kejahatan siber di Indonesia, yakni sebagai berikut:

Pertama, meningkatkan kualitas dan kuantitas aparat penegak hukum yang menguasai teknologi informasi termasuk internet. Bisa digunakan semacam patroli siber terpadu yang dilakukan secara massif yakni suatu bentuk penanggulangan terhadap kejahatan siber yang lebih komprehensif mencakup Edukasi/kampanye siber, deteksi untuk pencegahan dan penegakan hukum terhadap tindak pidana yang terjadi.

Kedua, Meningkatkan sarana dan prasarana pendukung bagi penyidikan dan penyelidikan kasus-kasus kejahatan siber. Karena cyber crime merupakan kejahatan trans nasional dan juga masuk dalam kategori kejahatan yang tak kasat mata, maka perlunya penguatan sarana dan prasarana guna mempercepat kinerja

dalam penanganan atas kasus-kasus yang terjadi dan dengan cepat mengurangi penyebaran kejahatan siber yang terjadi. Khususnya alat-alat pendeteksi kejahatan siber agar lebih tanggap dalam rangka penanggulangan.

Ketiga, Menyusun undang-undang khusus yang mengatur tentang kejahatan siber. Indonesia sebagai negara hukum, haruslah mempunyai peraturan yang jelas dan tegas terkait kejahatan siber ini, karena jika tidak ada ketentuan yang mengaturnya, terlalu jauh berbicara penanggulangan, Langkah penegakan saja sudah melemah karena kekosongan hukum. walaupun memang hadirnya Undang-Undang tentang Informasi dan Transaksi Elektronik sudah ada, namun perlu adanya aturan yang lebih khusus mengenai tindak pidana siber ini guna memperkuat Langkah penanggulangan kejahatan siber.

Keempat, Edukasi dan Literasi Publik yang harus di tingkatkan perihal siber ini, khususnya cerdas dalam menggunakan media sosial sehingga hal-hal kecil seperti misalnya phishing ataupun konten pornografi online bisa di hindari, lebih jauh daripada itu penggunaan platform e-commerce juga menjadi faktor utama hari ini, sehingga literasi yang di berikan juga harus bisa dipahami dengan mudah oleh public sehingga tidak terjadi lagi di masa depan penipuan online.

D. Kesimpulan

Cyber crime merupakan kejahatan tergolong baru karena muncul seiring berkembangnya ilmu teknologi informasi dan komunikasi. Kejahatan ini dapat ditujukan kepada fasilitas umum, kelompok organisasi/Lembaga, maupun target individual. Dengan meningkatnya aktivitas penggunaan internet di saat pandemi Covid-19 potensi terjadinya perilaku kejahatan mengalami peningkatan yang sangat siginifikan. Ditinjau dari aspek kriminologi, dalam teori Social Control, kejahatan siber muncul karena lemahnya kontrol sosial. Pada beberapa kasus, pelaku dari kejahatan siber ini tidak tampak secara fisik dan identitasnya sulit untuk di identifikasi sehingga kontrol terhadap perilakunya sangatlah sulit. semakin kuat ikatan-ikatan sosial tersebut maka semakin kecil kemungkinan terjadi delinkuensi, lemahnya ikatan dan hubungan sosial individu dengan masyarakat menjadi faktor munculnya kejahatan, salah satunya cybercrime. Kemudian teori differential association, kejahatan dapat muncul dari adanya proses yang dipelajari. Cybercrime bukan tergolong kejahatan yang mudah untuk dilakukan setiap orang karena perlu adanya teknik dan keterampilan tertentu dalam bidang teknologi dan jaringan. sehingga terdapat proses "belajar" atau "Latihan" yang dilakukan oleh pelaku. kejahatan dipelajari melalui partisipasi bersama orang lain, baik komunikasi verbal maupun non-verbal. Cybercrime umumnya dilakukan oleh kelompok tertentu yang antar anggotanya saling belajar dan bekerjasama satu sama lain.

Pencegahan dan penanggulangan terhadap kejahatan siber membutuhkan pendekatan penal dan non penal yang integral dan terpadu. Kebijakan dengan sarana penal adalah upaya penanggulangan kejahatan dengan menggunakan sarana hukum pidana. Sedangkan sarana non penal dapat diartikan sebagai upaya preventif terhadap kejahatan siber, yakni sebagai berikut : Meningkatkan kualitas dan kuantitas aparat penegak hukum yang menguasai teknologi informasi termasuk internet, Meningkatkan sarana dan prasarana pendukung bagi penyidikan dan penyelidikan kasus-kasus kejahatan siber, Menyusun undang-undang khusus yang mengatur tentang kejahatan siber, dan Memberikan edukasi serta literasi yang masif kepada publik terkait kejahatan siber dan bagaimana upaya pencegahannya agar tidak terperangkap dalam modus pelaku kejahatan siber.

Daftar Pustaka

Bestari, N. P. (n.d.). *Mengenal Social Edan 4 Modus Bobol Rekening*. cnbcindonesia.com/tech/20220621062955-37-348746/mengenal-social-engineering-dan-4-modus-bobol-rekening

Golose, P. R. (2007). *Penegakan Hukum Cyber Crime dalam Sistem Hukum Indonesia*.

Heniarti, D. D., Syawali, H., & Wiyanti, D. (2015). Kebijakan Kriminal Penanggulangan Kejahatan Telematika. *Ethos Jurnal Penelitian Dan Pengabdian Kepada Masyarakat*, *3*(2).

Maskun. (2013). *Kejahata Siber (Cyber Crime)*. Kencana, Jakarta.

Rahardjo, A. (1976). *Cyber crime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*.

Rasso, V. S. N. (2014). Upaya Kriminalisasi dalam Hal Penanggulangan Kejahatan Cyber Crime. *Lex Administratum, 9*(4).

Setiawan, D. A. (2018). Perkembangan Modus Operandi Kejahatan Skimming dalam Pembobolan Mesin ATM Bank sebagai Bentuk Kejahatan Dunia Maya (Cyber Crime). *Era Hukum (Jurnal Ilmiah Ilmu Hukum), FH Universitas Tarumanegara, 16*(2).

Widodo. (2009). *Sistem Pemidanaan dalam Cyber Crime*. Laksbang Meditama: Yogyakarta.

Yurizal. (2018). *Penegakan Hukum Tindak Pidana Cyber Crime di Indonesia*. Media Nusa Creative, Malang.