JURNAL HUKUM
Universitas Sulawesi Barat

Volume 6 Nomor 2, Juni, 2023
e-ISSN : 2716-0203
p-ISSN : 2548-8724

PERSPEKTIF HUKUM PIDANA DALAM KEJAHATAN CYBER CRIME

Muh. Chaerul Anwar, Muh. Arfhani Ichsan AH, Fadli Yasser Arafat J

Universitas Sulawesi Barat, Majene, Indonesia

Correspondent email : m.chaerulanwar@unsulbar.ac.id

Abstrak

Dalam penelitian ini adalah untuk memahami kebijakan regulasi hukum pidana terhadap tindak pidana teknologi informasi saat ini dalam menangani cyber crime, menganalisa dan menggambarkan kebijakan regulasi hukum pidana terhadap tindak pidana teknologi dalam menangani kasus cyber crime di masa yang akan datang, mengetahui dan meneliti apa saja kasus cyber crime yang pernah terjadi di Indonesia yang memiliki dan yang tidak memiliki ketentuan hukumnya. Dalam Fakta hukum sebagaimana yang ada pada saat ini, dampak perkembangan ilmu pengetahuan dan teknologi yang telah disalahgunakan sebagai sarana kejahatan ini menjadi teramat penting untuk diantisipasi bagaimana kebijakan hukumnya, sehingga cyber crime yang terjadi dapat dilakukan upaya penanggulangannya dengan hukum pidana, termasuk dalam hal ini adalah mengenai sistem pembuktiannya karena dalam penegakan hukum pidana dasar pembenaran seseorang dapat dikatakan bersalah atau tidak melakukan tindak pidana.

Kata Kunci : ***Cyber Crime, Hukum Pidana***

A. PENDAHULUAN

Dalam era globalisasi saat ini Perkembangan Internet yang semakin hari semakin meningkat baik teknologi dan penggunaannya, membawa banyak dampak baik positif maupun negatif. Dampak yang positif karena banyak manfaat dan kemudahan yang didapat dari teknologi ini. Namun, tidak dapat dipungkiri bahwa teknologi Internet membawa dampak negatif yang tidak kalah banyak dengan manfaat yang ada. Internet membuat kejahatan yang semula bersifat konvensional seperti pengancaman, pencurian dan penipuan kini dapat dilakukan dengan menggunakan media komputer secara online dengan risiko

Volume 6 Nomor 2, Juni, 2023
e-ISSN : 2716-0203
p-ISSN : 2548-8724

tertangkap yang sangat kecil oleh individu maupun kelompok dengan akibat kerugian yang lebih besar baik untuk masyarakat maupun negara disamping menimbulkan kejahatan-kejahatan yang baru.

Cybercrime adalah salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian luas dari kejahatan masa kini yang mendapat perhatian luas dari dunia internasional. *Volodymyr Golubev* menyebutnya sebagai *the new form of anti-social behavior*. Kekhawatiran terhadap ancaman (*threat*) *cybercrime* telah terungkap dalam makalah *Cybercrime* yang disampaikan dalam ITAC *(Information Technology Association of Canada)* pada *International Information Industry Congress (IIIC) 2000 Millenium Congress di Quebec* pada *tanggal 19 September 2000, yang menyatakan bahwa cybercrime is a real growing threat to economic and social development aspect of human life and so can electronically enabled crime*[1]

Dewasa ini kita dapat melihat bahwa hampir seluruh kegiatan manusia mengandalkan teknologi yang menghadirkan kemudahan bagi penggunanya berupa akses bebas yang dapat dilakukan oleh siapapun, kapanpun dan dimanapun tanpa sensor serta ditunjang dengan berbagai penawaran internet murah dari penyedia jasa layanan internet. Kemudahan yang ditawarkan oleh aktivitas siber itu sendiri contohnya ketika melakukan jual-beli barang atau jasa tidak memerlukan lagi waktu yang lama untuk bertemu langsung dengan penjual atau pembelinya, sehingga waktu yang digunakan lebih cepat. Indonesia telah menggeser kedudukan Ukraina sebagai pemegang presentasi tertinggi terhadap cybercrime. Data tersebut berasal dari penelitian Verisgin, perusahaan yang memberikan pelayanan intelejen di dunia maya yang berpusat di California, Amerika Serikat. Hal ini juga ditegaskan oleh Staf Ahli Kapolri Brigjen Anton Tabah bahwa jumlah cybercrime di Indonesia adalah yang tertinggi di dunia. Indikasinya dapat dilihat dari banyaknya kasus pemalsuan kartu kredit, penipuan

[1] Barda Nawawi Arief, Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime Di Indonesia, PT Raja Grafindo Persada: Jakarta, 2006, hlm. 2.

Volume 6 Nomor 2, Juni, 2023
e-ISSN : 2716-0203
p-ISSN : 2548-8724

perbankan, judi online, terorisme, dan lainlainnya.[2]

Memanfaatkan teknologi dalam kehidupan sehari-hari telah menjadi gaya hidup masyarakat kita, akan tetapi penggunaan teknoligi tersebut tidak didukung dengan pengetahuan untuk menggunakannya dengan baik. Hasil Lembaga Riset Telematika Sharing Vision menempatkan Tahun 2013 Indonesia menjadi negara urutan pertama target kejahatan dunia maya. Hasil riset itu menyebutkan selama Tahun 2013 ada 42 ribu serangan cyber saban harinya. Dimitri Mahayana dalam seminar 'Indonesia Cyber Crime Summit 2014' di ITB menyebutkan bahwa saat ini masyarakat Indonesia menduduki peringkat pertama dunia dengan persentase sebesar 23,54 persen sebagai pengguna internet terbesar.[3]

Salah satu bentuk kejahatan yang ditimbulkan oleh perkembangan dan kemajuan teknologi informasi atau telekomunikasi adalah kejahatan yang berkaitan dengan aplikasi internet. Kejahatan ini dalam istilah asing disebut Cybercrime. Barda Nawawi Arief menggunakan istilah tindak pidana mayantara untuk menunjuk jenis kejahatan ini atau identik dengan "tindak pidana siber" (cyberspace).[4]

Dalam beberapa pandangan ahli, terdapat perbedaan dalam menafsirkan tentang cyber crime. Muladi dalam "Bunga Rampai Hukum Pidana" berpendapat bahwa sudut pandang cyber crime adalah dengan menggunakan pendekatan computer crime. Namun adapula yang berpendapat bahwa sebenarnya cyber crime berbeda dengan computer crime. Walaupun demikian, sesungguhnya memang ada upaya untuk memperluas pengertian komputer agar dapat melingkupi segala kejahatan di internet dengan peralatan apapun, seperti pengertian komputer dalam The Proposed West Virginia Computer Crimes Act: :[5] peralatan pemrosesan

[2] Budi Suhariyanto, Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya, Rajawali Pers: Jakarta, 2013, hlm. 17.
[3] http://www.merdeka.com/peristiwa/hasil-riset-hukum-tahun-2013-Indonesia-target-utamakejahatan-cyber.httml, diakses pada 15 Maret 2017
[4] Barda Nawawi Arief, 2010, Kapita Selekta Hukum Pidana, Citra Aditya Bakti, Bandung, hal 253.
[5] Abdul Wahid dan Mohammad Labib, 2005, Kejahatan Mayantara (cyber crime), Refika Aditama, Bandung, hal 41.

Volume 6 Nomor 2, Juni, 2023
e-ISSN : 2716-0203
p-ISSN : 2548-8724

data listrik, magnetik, optik, elektro kimia, atau peralatan kecepatan tinggi lainnya dalam melakukan logika aritmatika, atau fungsi penyimpanan dan memasukkan beberapa fasilitas penyimpanan data atau fasilitas komunikasi yang secara langsung berhubungan dengan operasi tersebut dalam konjungsi dengan peralatan tersebut tidak memasukkan mesin ketik otomatis atau tipe-setter, sebuah kalkulator tangan atau peralatan serupa lainnya.

Melihat fakta hukum sebagaimana yang ada pada saat ini, dampak perkembangan ilmu pengetahuan dan teknologi yang telah disalahgunakan sebagai sarana kejahatan ini menjadi teramat penting untuk diantisipasi bagaimana kebijakan hukumnya, sehingga cyber crime yang terjadi dapat dilakukan upaya penanggulangannya dengan hukum pidana, termasuk dalam hal ini adalah mengenai sistem pembuktiannya. Dikatakan teramat penting karena dalam penegakan hukum pidana dasar pembenaran seseorang dapat dikatakan bersalah atau tidak melakukan tindak pidana, di samping perbuatannya dapat dipersalahkan atas kekuatan undang-undang yang telah ada sebelumnya (asas legalitas), juga perbuatan mana didukung oleh kekuatan bukti yang sah dan kepadanya dapat dipertanggungjawabkan (unsur kesalahan). Pemikiran demikian telah sesuai dengan penerapan asas legalitas dalam hukum pidana (KUHP), yakni sebagaimana dirumuskan secara tegas dalam Pasal 1 ayat (1) KUHP "Nullum delictum nulla poena sine praevia lege poenali" atau dalam istilah lain dapat dikenal, "tiada tindak pidana, tidak ada pidana, tanpa adanya aturan hukum pidana terlebih dahulu".

Jika dilihat dari pidananya, Menurut Soedjono Dirdjosisworo menyatakan bahwa: “Perubahan dan penyesuaian sosial serta perkembangan tekhnologi selama setengah abad sejak 1985 (UU No.73/58) demikian pesatnya, dan kepesatan perkembangan sosial dan teknologi serta semakin berpengaruhnya globalisasi yang terus didorong oleh teknologi informasi dan komunikasi sangatlah terasa bahwa Kitab Undang-Undang Hukum Pidana sudah sejak lama tidak mampu secara sempurna mengakomodasi dan mengantisipasi kriminlitas yang meningkat, baik kualitatif, maupun kuantitatif dengan jenis, pola dan modus

Volume 6 Nomor 2, Juni, 2023
e-ISSN : 2716-0203
p-ISSN : 2548-8724

operandi yang tidak terdapat dalam Kitab Undang–Undang Hukum Pidana.

Sebenarnya dalam persoalan cyber crime, tidak ada kekosongan hukum, ini terjadi jika digunakan metode penafsiran yang dikenal dalam ilmu hukum dan ini yang mestinya dipegang oleh aparat penegak hukum dalam mengahadapi perbuatan-perbuatan yang berdimensi baru yang secara khusus belum di atur dalam undang-undang. Persoalan menjadi lain jika ada keputusan politik untuk menetapkan cyber crime dalam perundang-undangan tersendiri di luar KUHP atau undang-undang khusus lainya. Sayangnya dalam persoalan mengenai penafsiran ini, para hakim yang menafsirkan masuk dalalm kategori penipuan, ada pula yang memasukkan dalam kategori pencurian. Untuk itu sebetulnya perlu dikembangkan pemahaman kepada para hakim mengenai teknologi informasi agar penafsiran mengenai suatu bentuk cyber crime ke dalam pasal-pasal dalam KUHP atau undang-undang lain tidak membingungkan

Kejahatan cybercrime telah menjadi isu semakin penting di Indonesia, seiring dengan kemajuan teknologi dan informasi dan komunikasi dan beberapa permasalahan yang muncul dalam kejahatan cyber crime di Indonesia yaitu yang pertama Keterbatasan Undang-Undang yang Tepat: Salah satu permasalahan utama adalah bahwa undang-undang yang ada belum sepenuhnya mampu mengatasi berbagai bentuk kejahatan siber. Meskipun Indonesia memiliki beberapa undang-undang yang relevan, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Perlindungan Data Pribadi, undang-undang ini masih memerlukan penyesuaian dan penyempurnaan agar dapat mengatasi berbagai jenis kejahatan siber yang terus berkembang.

Permasalahan yang kedua Kurangnya Kesadaran dan Kapasitas Penegakan Hukum: Kejahatan siber seringkali melibatkan pelaku yang memiliki pengetahuan teknis yang mendalam dan mampu menyembunyikan jejak digital mereka. Namun, kesadaran dan kapasitas penegakan hukum dalam mengatasi kejahatan siber masih relatif rendah di

Volume 6 Nomor 2, Juni, 2023
e-ISSN : 2716-0203
p-ISSN : 2548-8724

Indonesia. Diperlukan pelatihan yang lebih baik dan peningkatan kolaborasi antara lembaga penegak hukum, sektor swasta, dan pihak-pihak terkait lainnya untuk meningkatkan kemampuan dalam menghadapi kejahatan siber.

Perlindungan Data Pribadi yang Lemah: Kejahatan siber seringkali melibatkan pencurian dan penyalahgunaan data pribadi. Meskipun Indonesia memiliki Undang-Undang Perlindungan Data Pribadi, pelaksanaannya masih perlu ditingkatkan untuk memastikan bahwa data pribadi warga negara Indonesia terlindungi dengan baik. Hal ini melibatkan pemantauan yang lebih ketat terhadap perusahaan dan organisasi yang mengumpulkan dan mengelola data pribadi, serta penegakan hukum yang tegas terhadap pelanggaran.

Selanjutnya permasalahan yang ketiga Kejahatan siber sering kali melintasi batas negara dan melibatkan pelaku dari berbagai negara. Pelaku kejahatan seringkali dapat menggunakan alat dan teknik untuk menyembunyikan identitas dan lokasi fisik mereka, membuat sulit bagi penegak hukum untuk mengejar dan menghukum mereka. Diperlukan kerjasama internasional yang lebih baik dalam hal pertukaran informasi, ekstradisi, dan penuntutan pelaku kejahatan siber.

Kemudian adapun permasalahan yang terakhir yaitu Salah satu tantangan dalam penegakan hukum pidana dalam kejahatan siber adalah menentukan hukuman yang proporsional dengan kejahatan yang dilakukan. Seiring dengan kemajuan teknologi, jenis kejahatan siber yang berbeda-beda muncul, dan adakalanya undang-undang yang ada tidak dapat memberikan hukuman yang memadai. Penting untuk terus memperbarui dan menyesuaikan undang-undang pidana

Berdasarkan uraian di atas, maka penulis menetapkan judul tulisan ini yaitu Cyber Crime Dalam Sudut Pandang Hukum Pidana. Rumusan masalah yang penulis bahas adalah: Bagaimana permasalahan Perspektif Hukum Pidana dalam Kejahatan Cyber Crime di Indonesia?

Volume 6 Nomor 2, Juni, 2023
e-ISSN : 2716-0203
p-ISSN : 2548-8724

B. METODE PENELITIAN

Metode pendekatan yang dilakukan dalam penelitian hukum ini adalah dengan menggunakan metode pendekatan yuridis normatif. Penelitian hukum normatif merupakan penelitian yang mengutamakan data kepustakaan yaitu penelitian terhadap data sekunder. Data sekunder tersebut dapat berupa bahan hukum primer, sekunder maupun tersier. Penelitian ini meliputi penelitian mengenai ketentuan hukum positif yang berlaku di Indonesia yang berkaitan perspektif hukum pidana dalam kejahatan cyber crime

C. HASIL DAN PEMBAHASAN

Dalam hukum pidana, sesuatu yang dikatakan sebagai kejahatan apabila tindakan jahat tersebut dirumuskan dalam suatu delik atau tindak pidana, dan bagi pelanggarnya dapat dijatuhi pidana. Istilah tindak pidana atau strafbaarfeit di dalam bahasa Belanda ialah Strafbaar "dapat dihukum" dan Feit "sebagian dari suatu kenyataan". Menurut beberapa ahli hukumdapat disebutkan sebagai berikut[6]:

1. HAZEWINKEL SURINGA, strafbaarfeit merupakan suatu perilaku manusia yang pada suatu saat tertentu telah ditolak di dalam sesuatu pergaulan hidup tertentu dan dianggap sebagai perilaku yang harus ditiadakan oleh hukum pidana dengan menggunakan sarana-sarana yang bersifat memaksa yang terdapat didalamnya.
2. POMPE, strafbaarfeit merupakan suatu tindakan yang menurut sesuatu rumusan Undangundang telah dinyatakan sebagai tindakan yang dapat dihukum.
3. SIMONS, strafbaarfeit merupakan suatu tindakan melanggar hukum yang telah dilakukan dengan sengaja oleh seseorang yang dapat dipertanggungjawabkan atas tindakannya dan yang oleh undang-undang telah dinyatakan sebagai suatu tindakan yang dapat dihukum.

Menurut SIMONS, bahwa strafbaarfeit dirumuskan sebagai berikut :

[6] P.A.F Lamintang, 1997, Dasar-dasar Hukum Pidana Indonesia, Citra Aditya Bakti, Bandung, hal 182-185.

Volume 6 Nomor 2, Juni, 2023
e-ISSN : 2716-0203
p-ISSN : 2548-8724

a. Untuk adanya suatu strafbaarfeit disyaratkan bahwa harus terdapat suatu tindakan yang dilarang ataupun yang diwajibkan oleh undang-undang, dimana pelanggaran terhadap larangan atau kewajiban semacam itu telah dinyatakan sebagai suatu tindakan yang dapat dihukum;

b. Agar sesuatu tindakan itu dapat dihukum, maka tindakan tersebut harus memenuhi semua unsur dari delik seperti yang dirumuskan dalam undang-undang, dan

c. Setiap strafbaarfeit sebagai pelanggaran terhadap larangan atau kewajiban menurut undang-undang itu, pada hakikatnya merupakan suatu tindakan melawan hukum atau merupakan suatu "onrechtmatige handeling"

Pada intinya bahwa suatu perbuatan yang dilakukan serta melawan hukum namun dilanggar oleh seseorang, maka perbuatan yang bersangkutan dapat dikenakan suatu sanksi pidana menurut suatu peraturan yang berlaku.

Kebijakan Hukum Pidana Terhadap Tindak Pidana Teknologi Informasi Berdasarkan Hukum Positif Saat ini Definisi kata kebjakan berasal dari bahasa inggris yaitu pilcy atau dalam bahasa belanda disebut politiek yang dimana secara umum dapat diistilahkan sebagai dasar-dasar umum yang berfungsi untuk mengarahlan pemerintah, dalam pengertian luas termasuk pula didalamnya unsur aparat penegak hukum dalam hal mengelola, mengatur, atau menyelesaikan kepentingan-kepentingan umum, persoalan-persoalan masyarakat atau permasalahan penyusunan peraturan perundang-undangan dan pengaplikasikan hukum atau peraturan dengan tujuan umum yang menjurus kepada upaya mewujudkan kesejahteraan ataupun keadilan dalam masyarakat[7]

Cyber Crime merupakan jenis baru dalam dunia kriminal. KUHP memiliki yurisdiksi yang jelas bahwa sesuai Pasal 2 KUHP menyebutkan bahwa ketentuan pidana dalam perundang-undangan Indonesia diterapkan bagi setiap orang yang melakukan sesuatu delik di

[7] Aloysius Wisnubroto, Kebijakan Hukum Pidana Dalam Penanggulangan Penyalahgunaan Komputer Atmajaya Yogyakarta, Yogyakatya, 1999, Hal. 10

Volume 6 Nomor 2, Juni, 2023
e-ISSN : 2716-0203
p-ISSN : 2548-8724

Indonesia. Hal ini menurut saya menjadi hambatan dalam penegakan kejahatan siber (cyber crime) karena bisa jadi pelakunya melakukan kejahatan tersebut di luar Indonesia sedangkan korbannya adalah orang Indonesia. Sedangkan apabila sebaliknya, negara kita seakan tidak mampu karena belum adanya perjanjian mutual legal assistant dalam bidang hukum pidana (ekstradisi). Penjelasan di atas merujuk pada definisi bahwa ruang cyber bersifat global, tidak terikat pada yurisdiksi nasional suatu negara. Hal ini karena cyber space tercipta melalui ruang internet. Pendapat bahwa cyber crime sama dengan computer crime terkadang tidak relevan lagi karena pelaku dapat menggunakan media atau alat lain dalam melakukan kejahatan tersebut.

Bentuk-bentuk cyber crime pada umumnya yang dikenal dalam masyarakat dibedakan menjadi 3 (tiga) kualifikasi umum, yaitu[8] :

1. Delik-delik yang berkaitan dengan kerahasiaan, integritas dan keberadaan data dan sistem komputer.

a. Illegal access (akses secara tidak sah terhadap sistem komputer)

b. Data interference (mengganggu data komputer)

c. System interference (mengganggu sistem komputer)

d. Illegal interception in the computers, systems and computer networks operation (intersepsi secara tidak sah terhadap komputer, sistem, dan jaringan operasional komputer)

e. Misuse of devices (menyalahgunakan peralatan komputer)

2. Delik-delik yang berhubungan dengan komputer: pemalsuan dan penipuan (computer related offences; forgery and fraud).

3. Delik-delik yang bermuatan pornografi anak (content-related offences, child phornography).

[8] Abdul Wahid dan Mohammad Labib,op.cit.hal 74.

Volume 6 Nomor 2, Juni, 2023
e-ISSN : 2716-0203
p-ISSN : 2548-8724

4. Delik-delik yang berhubungan dengan hak cipta (offences-related of infringements of copyright).

Dalam Kitab Undang-Undang Hukum Pidana Kitab Undang–Undang Hukum Pidana yang biasa disingkat menjadi KUHP merupakan sistem utama bagi peraturan-peraturan hukum pidana di Indonesia. Perumusan tindak pidana yang tercantum dalam KUHP mayoritas masih bersifat konvensional dan belum secara langsung dikaitkan dengan perkembangan dari cyber crime itu sendiri. Beberapa peraturan perundang- undangan yang berhubungan dengan tindak pidana teknologi informasi diluar dari pengaturan KUHP yaitu:

1)Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi

2)Undang-Undang Nomor 19 Tahun 2002 Tentang Hak Cipta

3)Undang-Undang Nomor 25 Tahun 2003 Tentang Perubahan atas Undang- Undang Nomor 15 Tahun 2002 Tentang Tindak Pidana Pencucian Uang

4)Undang-Undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme

Dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Seiring dengan perkembangan zaman, dan dalam mengatur cyber space dan cyber crime telah terbit peraturan yang khusus mengatur tentang tindak pidana teknologi informasi yang tercantum dalam UU Nomor 19 Tahun 2016 Tentang Perubahan Atas UU Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. UU ITE ini diharapkan dapat menjadi kekuatan pengendali dan penegak ketertiban bagi kegiatan pemanfaatan teknologi informasi

Pembentukan peraturan perundangundangan di dunia siber pun, berpangkal pada keinginan masyarakat untuk mendapatkan jaminan keamanan, keadilan dan kepastian hukum. Sebagai norma hukum siber atau cyber law akan bersifat mengikat bagi tiap-tiap individu untuk tunduk dan mengikuti segala kaidah-kaidah yang terkandung didalamnya. Sebelum

Volume 6 Nomor 2, Juni, 2023
e-ISSN : 2716-0203
p-ISSN : 2548-8724

diundangkannya Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang mengatur secara khusus tentang pemanfaatan teknologi informasi, sebenarnya Indonesia dalam persoalan cybercrime tidak ada kekosongan hukum, ini terjadi jika digunakan metode penafsiran yang dikenal dalam ilmu hukum dan ini yang mestinya dipegang oleh aparat penegak hukum dalam menghadapi perbuatan-perbuatan yang berdimensi baru yang secara khusus belum diatur dalam undang-undang.

Upaya menafsirkan cybercrime ke dalam perundang-undangan KUHP dan khususnya undang-undang yang terkait dengan perkembangan teknologi informasi telah dilakukan oleh penegak hukum dalam menangani cybercrime selama ini. Sebelum UU ITE diundangkan ada beberapa ketentuan hukum positif yang dapat diterapkan dengan keberanian untuk melakukan terobosan dengan penafsiran hukum yang berkaitan dengan teknologi

Dalam upaya menangani kasus kejahatan dunia maya, terdapat beberapa pasal dalam KUHP yang mengkriminalisasi cybercrime dengan mengggunakan metode interpretasi ekstensif (perumpamaan dan persamaan) terhadap pasal-pasal yang terdapat dalam KUHP. Mengacu pada Kitab Undang-Undang Hukum Pidana (KUHP), pengertian secara luas mengenai tindak pidana siber ialah semua tindak pidana yang menggunakan sarana atau dengan bantuan Sistem Elektronik. Itu artinya semua tindak pidana konvensional dalam Kitab Undang-Undang Hukum Pidana (KUHP) sepanjang dengan menggunakan bantuan atau sarana Sistem Elektronik seperti pembunuhan, perdagangan orang, dapat termasuk dalam kategori tindak pidana siber dalam arti luas[9]. Namun, hukum pidana (KUHP) menurut sebagian berpendapat tidak dapat menjangkau kejahatan ini, sementara sebagian yang lain berpendapat bahwa hukum pidana positif dapat menjangkau kejahatan ini. Untuk membahas cyber crime dalam perspektif hukum pidana maka saya akan mengkaitkan dengan delik yang diatur dalam KUHP. Ada beberapa contoh tindak pidana cyber crime yang dapat saya

[9] "Landasan Hukum Penanganan Cyber Crime di Indonesia" – www.hukumonline.com.htm diakses tanggal 18 Maret 2013.

Volume 6 Nomor 2, Juni, 2023
e-ISSN : 2716-0203
p-ISSN : 2548-8724

berikan, diantaranya:

1. Pencurian (Pasal 362)

Barang siapa mengambil barang sesuatu, yang seluruhnya atau sebagian kepunyaan orang lain, dengan maksud untuk dimiliki secara melawan hukum, diancam karena pencurian,dengan pidana penjara paling lama lima Tahun atau pidana denda paling banyak sembilan ratus rupiah. Ketentuan Pasal di atas dapat digunakan dalam kasus pencurian nomor kartu kredit orang lain dengan menggunakan internet untuk melakukan transaksi. Setelah barang dikirimkan, penjual tidak dapat mencairkan uangnya karena pemilik kartu bukanlah orang yang melakukan transaksi.

2. Penipuan (Pasal 378)

Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi hutang maupun menghapuskan piutang, diancam karena penipuan dengan pidana penjara paling lama empat tahun. Ketentuan pasal di atas dapat digunakan untuk kasus penipuan dengan seolah-olah menawarkan dan menjual suatu produk atau barang dengan memasang iklan di salah satu website sehingga orang tertarik untuk membelinya lalu mengirimkan uang kepada pemasang iklan. Tetapi, pada kenyataannya, barang tersebut tidak ada. Hal tersebut diketahui setelah uang dikirimkan dan barang yang dipesankan tidak datang sehingga pembeli tersebut menjadi tertipu.

3. Pemerasan dan Pengancaman Pasal 335

(1) Diancam dengan pidana penjara paling lama satu tahun atau denda paling banyak empat ribu lima ratus rupiah:

1. barang siapa secara melawan hukum memaksa orang lain supaya melakukan, tidak melakukan atau membiarkan sesuatu, dengan memakai kekerasan,

Volume 6 Nomor 2, Juni, 2023
e-ISSN : 2716-0203
p-ISSN : 2548-8724

sesuatu perbuatan lain maupun perlakuan yang tak menyenangkan, atau dengan memakai ancaman kekerasan, sesuatu perbuatan lain maupun perlakuan yang tak menyenangkan, baik terhadap orang itu sendiri maupun orang lain;

2. barang siapa memaksa orang lain supaya melakukan, tidak melakukan atau membiarkan sesuatu dengan ancaman pencemaran atau pencemaran tertulis.

(2) Dalam hal sebagaimana dirumuskan dalam butir 2, kejahatan hanya dituntut atas pengaduan orang yang terkena. Ketentuan pasal di atas dapat digunakan dalam kasus pengancaman dan pemerasan yang dilakukan melalui e-mail yang dikirimkan oleh pelaku untuk memaksa korban melakukan sesuatu sesuai dengan apa yang diinginkan oleh pelaku dan jika tidak dilaksanakan akan membawa dampak yang membahayakan. Hal ini biasanya dilakukan karena pelaku mengetahui rahasia korban.

4. Pencemaran nama baik Pasal 311 ayat (1)

Jika yang melakukan kejahatan pencemaran atau pencemaran tertulis dibolehkan untuk membuktikan apa yang dituduhkan itu benar, tidak membuktikannya, dan tuduhan dilakukan bertentangan dengan apa yang diketahui, maka dia diancam melakukan fitnah dengan pidana penjara paling lama empat tahun. Ketentuan Pasal di atas dapat digunakan pada Kasus pencemaran nama baik dengan menggunakan media Internet. Modusnya adalah pelaku menyebarkan email kepada teman-teman korban tentang suatu cerita yang tidak benar atau mengirimkan email ke suatu mailing list sehingga banyak orang mengetahui cerita tersebut.

5. Judi online Pasal 303 ayat (1) butir 1 (1)

Diancam dengan pidana penjara paling lama sepuluh tahun atau pidana denda paling banyak dua puluh lima juta rupiah, barang siapa tanpa mendapat izin: 1. dengan sengaja menawarkan atau memberikan kesempatan untuk permainan judi dan menjadikannya sebagai pencarian, atau dengan sengaja turut serta dalam suatu

Volume 6 Nomor 2, Juni, 2023
e-ISSN : 2716-0203
p-ISSN : 2548-8724

perusahaan untuk itu; Pasal 303 KUHP dapat dikenakan untuk menjerat permainan judi yang dilakukan secara online (ex: judi bola online) di Internet dengan penyelenggara dari Indonesia.

6. Pornografi Pasal 282

Barang siapa menyiarkan, mempertunjukkan atau menempelkan di muka umum tulisan, gambaran atau benda yang telah diketahui isinya melanggar kesusilaan, atau barang siapa dengan maksud untuk disiarkan, dipertunjukkan atau ditempelkan di muka umum, membikin tulisan, gambaran atau benda tersebut, memasukkannya ke dalam negeri, meneruskannya, mengeluarkannya dari negeri, atau memiliki persediaan, ataupun barang siapa secara terang-terangan atau dengan mengedarkan surat tanpa diminta, menawarkannya atau menunjukkannya sebagai bisa diperoleh, diancam dengan pidana penjara paling lama satu tahun enam bulan atau pidana denda paling tinggi empat ribu lima ratus rupiah. Dapat dikenakan untuk penyebaran pornografi maupun website porno yang banyak beredar dan mudah diakses di Internet. Walaupun berbahasa Indonesia, sangat sulit sekali untuk menindak pelakunya karena mereka melakukan pendaftaran domain tersebut diluar negeri dimana pornografi yang menampilkan orang dewasa bukan merupakan hal yang ilegal. kasus penyebaran foto atau film pribadi seseorang yang vulgar di Internet .

7. Hacking Pasal 406

Barang siapa dengan sengaja dan melawan hukum menghancurkan, merusakkan, membikin tak dapat dipakai atau menghilangkan barang sesuatu yang seluruhnya atau sebagian milik orang lain, diancam dengan pidana penjara paling lama dua tahun delapan bulan atau pidana denda paling banyak empat ribu lima ratus rupiah. Pasal di atas dapat digunakan pada kasus deface atau hacking yang membuat sistem milik orang lain, seperti website atau program menjadi tidak berfungsi atau dapat digunakan

Volume 6 Nomor 2, Juni, 2023
e-ISSN : 2716-0203
p-ISSN : 2548-8724

sebagaimana mestinya.

Dalam]meningkatkan upaya penanggulangan kejahatan siber atau cyber crimes yang semakin meningkat Polri dalam hal ini Bareskrim Mabes Polri telah berupaya melakukan sosialisasi mengenai kejahatan cyber dan cara penanganannya kepada satuan di kewilayahan (Polda). Sosialisasi tersebut dilakukan dengan cara melakukan pelatihan (pendidikan kejuruan) dan peningkatan kemampuan penyidikan anggota Polri dengan mengirimkan personel-nya ke berbagai macam kursus yang berkaitan dengan cyber crime. Selain upaya dari kepolisian, kesadaran hukum masyarakat sangat diperlukan dalam berteknologi dan rendahnya kesadaran hukum para masyarakat ini menjadikan penegakan hukum terhadap cyber crime tidak berjalan optimal. Tidak adanya kesadaran hukum para masyarakat ini terlihat pada pemanfaatan sarana internet untuk melakukan berbagai jenis tindak pidana salah satunya memperjualbelikan layanan seks dan berbagai jenis tindak pidana lainnya.

Kendala dalam mengungkap kasus *cybercrime* ini yaitu karena si korban beranggapan bahwa pihak polisi sulit menangkap si pelaku dan tidak melaporkan ke pihak terkait, penghilangan barang bukti oleh pelaku, dan mengingat bahwa kasus *cybercrime* memiliki cakupan wilayah yang sangat luas tidak hanya antar provinsi di Indonesia tetapi juga lintas negara. Beberapa kendala tersebut di atas dapat mengurangi kefektifan gerak dan kegiatan pihak kepolisisan untuk menanggulangi kejahatan *cybercrime*, oleh karena itu pemenuhan atas kendala di atas segera teratasi seperti koordinasi yang cepat dan terarah, pemenuhan alat-alat yang mendukung untuk menanggulangi kasus *cybercrime*. Untuk itu peran aktif masing-masing pihak sangat diperlukan dalam menanggulangi tindak pidana *cybercrime* dan pihak yang diberi tanggungjawab dapat melaksanakan tanggungjawabnya secara optimal dan diatasi dengan baik.

Berbagai contoh kasus yang dikaitkan dengan tindak pidana cyber crime maka

Volume 6 Nomor 2, Juni, 2023
e-ISSN : 2716-0203
p-ISSN : 2548-8724

seyogyanyaa masih terdapat beberapa kekurangan dalam upaya penegakan hukumnya, pada kenyataannya sanksi yang dikenakan apabila menggunakan KUHP memang ringan. Padahal beberapa kasus yang terjadi mengakibatkan kerugian yang besar sehingga tidak sepadan dengan akibat yang ditimbulkan. Disamping itu, delik yang berkaitan dengan cyber crime dalam KUHP membutuhkan penafsiran yang luas, padahal hukum pidana menganut asas legalitas yang nantinya berpengaruh dalam upaya menjerat pelaku, jadi perlu dengan penafsiran secara luas mengingat hukum pidana hanya menerima penafsiran secara otentik saja.

D. KESIMPULAN

Di era globalisasi saat sekarang ini banyak persoalan-persoalan yang baru terhadap perbuatan pidana di dunia maya dengan adanya Undang-Undang Tramsaksi Elektronik dapat memayungi kejahatan telematika. Namun dalam Undang-undang ini mempunyai kendala yuridis. Dalam definisi cyber crime hingga saat ini belum memiliki yang baku. Beberapa berpendapat cyber crime identik dengan computer crime namun ada pula yang berpendapat berbeda karena tidak semua cyber crime tersebut menggunakan komputer sebagai alat, namun biasa menggunakan juga alat yang lain. Yurisdiksi juga ini mempengaruhi kinerja aparat penegak hukum untuk melakukan proses peradilan karena cyber crime melintasi batas antar negara. Hukum pidana belum mampu memberikan keefektifan dalam penegakan hukumnya, karena pasal yang terdapat dalam KUHP yang berkaitan dengan cyber crime sanksi yang dikenakan cukup ringan. Dalam beberapa kasus yang terjadi mengakibatkan kerugian yang besar sehingga tidak sepadan dengan akibat yang ditimbulkan. KUHP dalam cybercrime mempunyai penafsiran yang luas sebagai salah satu tujuan hukum yaitu menuju kepastian hukum.

Volume 6 Nomor 2, Juni, 2023
e-ISSN : 2716-0203
p-ISSN : 2548-8724

DAFTAR PUSTAKA

Abdul Wahid dan Mohammad Labib, 2005, *Kejahatan Mayantara (cyber crime)*, Refika Aditama, Bandung

Aloysius Wisnubroto, 1999, *Kebijakan Hukum Pidana Dalam Penanggulangan Penyalahgunaan Komputer,* Universitas Atmajaya Yogyakarta, Yogyakarta

Barda Nawawi Arief, 2010, *Kapita Selekta Hukum Pidana*, Citra Aditya Bakti, Bandung

Budi Suhariyanto, 2013, *Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya*, Rajawali Pers: Jakarta

Barda Nawawi Arief, 2010, *Kapita Selekta Hukum Pidana*, Citra Aditya Bakti, Bandung

P.A.F Lamintang, 1997, *Dasar-dasar Hukum Pidana Indonesia*, Citra Aditya Bakti

Landasan Hukum Penanganan Cyber Crime di Indonesia" – www.hukumonline.com.htm diakses tanggal 18 Maret 2013.

http://www.merdeka.com/peristiwa/hasil-riset-hukum-tahun-2013-Indonesia-target-utamakejahatan-cyber.httml, diakses pada 15 Maret 2017