JERAT PIDANA TERHADAP PELAKU PERETAS SISTEM KOMPUTER SECARA ILEGAL (*HACKER*) DALAM PERPSEKTIF HUKUM PIDANA INDONESIA

Bramanta Aryo Wijoseno, Fakultas Hukum Universitas Udayana,
e-mail: bramanta.aryo@gmail.com
I Gusti Agung Ayu Dike Widhiyaastuti, Fakultas Hukum Universitas Udayana,
e-mail: dikewidhyaastuti2@gmail.com

ABSTRAK

Perkembangan teknologi di era globalisasi ini dapat memberikan peluang bagi pelaku kejahatan, kejahatan yang semakin merajalela salah satunya adalah kejahatan siber. Peretasan atau hacking termasuk dalam kejahatan mayantara. Tulisan ini akan membahas mengenai pengertian dari hacker, sanksi pidana dan upaya penanggulangannya guna mengetahui akibat hukum terjadi akibat perbuatan yang dilakukan oleh pelaku peretasan dalam perspektif hukum pidana di Indonesia. Metode penelitian dalam studi ini adalah penelitian hukum normatif, dimaksudkan untuk menganalisisi kaidah hukum berkaitan dengan perkara pidana hacking, yang bersumber dari bahan hukum primer maupun sekunder selanjutnya dianalisis dengan cara kualitatif guna mendapat jawaban atas permasalahan. Hasil studi menunjukkan bahwa kejahatan dunia maya yang menggunakan data atau informasi di internet semakin meningkat sebagai akibat dari kemajuan teknologi informasi berbasis komputer. Pelaku peretas jika terbukti melakukan tindak pidana dapat dikenakan pasal 30 UU ITE dengan hukuman maksimal 8 tahun penjara dan/ atau denda maksimal Rp. 800.000.000. Banyak unsur yang perlu dibenahi untuk mengatasi kejahatan siber, yang dapat dilakukan diantaranya dengan melakukan penyempurnaan perangkat hukum pidana indonesia, meningkatkan sumber daya manusia dari para penyidik, membangun fasilitas forensic computing, serta melakukan upaya penanggulangan pencegahan.

Kata Kunci: Kepastian Hukum, Tindak Pidana, Peretas, Kejahatan Dunia Maya.

ABSTRACT

In this age of globalization, technological advancement may offer possibilities for criminals, one of which is cybercrime. Hacking is included in cybercrime. This paper will discuss the definition of hacking, criminal sanctions and countermeasures in order to learn the repercussions of actions on the law committed by the perpetrators of hacking in the perspective of criminal law in Indonesia. The research method used in this study is normative legal research methods intended to analyze legal rules related to criminal cases of hacking, which are sourced from primary law and secondary legal materials and then analyzed in a qualitative way to get answers to problems. The study's findings indicate that cybercrime using data on the internet is increasing as a result of advances in computer-based information technology. Hackers if proven to have committed a criminal offense can be subject to article 30 of the ITE Law with a maximum sentence of 8 years in prison and/or a maximum fine of Rp. 800,000,000. Many elements need to be addressed to overcome cybercrime, which can be done by improving the Indonesian criminal law apparatus, increasing the human resources of investigators, building forensic computing facilities, and conducting preventive countermeasures.

Key Words: Legal Certainty, Criminal Act, Hacking, Cybercrime.

1. Pendahuluan

1.1. Latar Belakang Masalah

Globalisasi disebut sebagai fenomena khusus yang tidak bisa dihindari dan dicegah. Kemajuan dan perkembangan teknologi di era globalisasi tampaknya semakin terikat erat dengan kehidupan manusia. Perkembangan teknologi yang pesat memberikan banyak dampak positif maupun negatif bagi kehidupan masyarakat.[1] Satu sisi, kemajuan teknologi berdampak positif dengan membawa pengaruh yang menguntungkan, seperti terlihat dari adanya penggunaan surat elektronik (*e-mail);* jual beli secara *online* (*e-commerce);* pembelajaran secara *online (e-learning);* transaksi perbankan (*Internet Banking); Online Business* dan masih banyak lagi. Dengan adanya *Internet*, telah menciptakan wawasan baru bagi kehidupan manusia, khususnya di bidang komunikasi internasional dan berbagi informasi serta penyebaran pengetahuan maupun gagasan di antara para ilmuwan di seluruh dunia.[2] Namun, kemajuan teknologi komunikasi tidak selalu menimbulkan hal positif dalam segala aspek, munculnya beberapa jenis kejahatan teknologi tinggi (*high tech crime)* dan kejahatan mayantara (*cybercrime)* merupakan indikasi dari hal ini, yang secara ilegal sering disalahgunakan untuk kepentingan pelakunya. Jika dibandingkan dengan jenis kejahatan tradisional lainnya, fenomena maraknya kejahatan teknologi informasi merupakan jenis kejahatan yang relatif baru. Misalnya saja media *internet*, yang merupakan salah satu kreasi sebagai hasil kemajuan teknologi informasi yang berdampak signifikan terhadap pemberdayaan informasi dan telekomunikasi. Setiap orang memiliki akses ke *internet*, namun bagi individu tertentu dalam hal ini pelaku peretasan atau biasa disebut *hacker*, *internet* dijadikan ruang untuk melakukan tindakan kejahatan untuk kepentingannya sendiri yang pada akhirnya dapat merugikan beberapa pihak, seperti meretas akun media sosial bahkan sampai meretas situs-situs rahasia milik pemerintah.

Semakin banyaknya individu yang melakukan kejahatan dalam penggunaan teknologi sebagai media yang berbasis *internet* menjadikan hal yang wajar.[3] Maraknya kejahatan yang dilakukan oleh para *hacker* di *internet* adalah buktinya. Sebagai contoh, pada tahun 2007 silam, tepatnya di Estonia telah terjadi Pembobolan besar-besaran terjadi di Estonia. Serangan peretas Rusia terhadap Estonia, yang melumpuhkan perekonomian negara tersebut, benar-benar merupakan babak kelam dalam jagat cyber dan membuat negara Estonia mengalami kerugian baik secara materi maupun non-materi. Hal ini dipicu oleh konflik dan perselisihan mengenai politik. Estonia, yang baru saja memperoleh kemerdekaan dari Uni Soviet, ingin menyingkirkan segala pengaruh Soviet dan memiliki rencana untuk menurunkan patung-patung perunggu pahlawan Soviet dari jantung kota Talinn. Hal ini dikecam oleh warga Estonia keturunan Rusia, yang kemudian melakukan protes di jalanan dan memulai kerusuhan. Banyak situs web yang sepenuhnya dihapus sebagai akibat dari serangan cyber yang mempengaruhi beberapa situs web yang dioperasikan oleh pemerintah Estonia. Bahkan situs web Presiden, Menteri, dan anggota parlemen pun dihapus oleh para peretas. Bersama dengan situs-situs media Estonia, sektor finansial juga diretas.

[1] Ngafifi, M. "Kemajuan Teknologi dan Pola Hidup Manusia dalam Perspektif Sosial Budaya." *Jurnal Pembangunan Pendidikan: Fondasi dan Aplikasi*, 2 No. 1 (2014): 33-47.

[2] Widyopramono, Hadi Widjojo. "Cybercrime dan Pencegahannya." *Jurnal Hukum Teknologi, Fakultas Hukum Universitas Indonesia*: 7.

[3] Afitrahim. "Yurisdiksi Dan Transfer of Proceeding Dalam Kasusu Cybercrime." *Tesis, Universitas Indonesia,* (2012): 2.

Hansabank, bank terbesar di Estonia, terpaksa menutup layanan online-nya pada hari Kamis, 10 Mei 2007, sebagai akibat dari serangan data yang intens pada infrastruktur Internet Estonia. Hansabank mengalami kerugian sebesar $1.000.000, atau sekitar Rp 8,5 miliar. Aksi peretasan ini berlangsung dalam 21 hari, di mana Estonia harus menjalani hidup tanpa internet dalam jangka waktu tersebut. Serangan ini begitu besar hingga dinamakan "Web War One," sebuah plesetan dari World War One. Estonia menuduh Rusia sebagai dalang di balik *cyber crime* ini, yang pada akhirnya diketahui bahwa orang Rusia-lah yang 'memutus' hubungan Estonia dari dunia luar dengan cara memutus internetnya, namun ternyata sang hacker tidak disponsori oleh Pemerintah Rusia. Meski demikian, peretasan ini tetap jadi perhatian dunia karena sebelumya tidak pernah terjadi kasus peretasan yang menyerang suatu negara dengan merusak segala infrastruktur dalam satu negara. Pemerintah Estonia, dengan segala upaya untuk memerangi hal ini sejak awal, kini telah mengalokasikan sejumlah besar dana publik untuk meningkatkan keamanan siber di Estonia.

Dewasa ini, ramai diperbincangkan di Indonesia mengenai seorang *Hacker* yang menyebut dirinya sebagai "Bjorka" yang meretas situs rahasia milik pemerintah Indonesia dan membagikannya di laman telegram miliknya. Akun terebut telah membocorkan mengenai data-data rahasia milik sejumlah instansi, salah satunya adalah data dari *SIM Card*. Selain itu Bjorka juga merupakan sosok yang mengungkap surat yang ditujukan kepada presiden Indonesia. Selain itu Bjorka juga diduga mengungkap dalang dibalik kasus pembunuhan Munir. Hal tersebut sempat menggemparkan jagat dunia maya. Salah satu tersangka pada kasus ini bernama Muhammad Agung Hidayatullah (21). Peran tersangka adalah sebagai anggota dari "organisasi" Bjorka yang berperan dalam mengelola saluran telegram. Tersangka memiliki motif yakni menjadikan "Bjorka" agar dapat terkenal dan mendapatkan uang. Menurut pernyataan Kombes Ade Yaya Suryana, tersangka tidak ditahan namun dikenakan wajib lapor. Pada akhirnya kasus ini lenyap dari pandangan publik dikarenakan tidak ditemukannya sosok dari "Bjorka" tersebut.

Kendati *cybercrime* ini sering terjadi, namun hingga sekarang belum adanya pilar hukum yang mampu mencegah kasus-kasusnya, justru kejahatan mayantara semakin sering terjadi. Sistem hukum Indonesia telah memiliki Undang-Undang yang mengatur mengenai ITE atau Informasi dan Transaksi Elektronik yakni Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, namun implementasi penegakkan hukum terhadap kejahatan mayantara dirasa belum efektif. Mengingat teknologi informasi telah berkembang menjadi suatu bentuk komunikasi yang canggih, maka upaya penanggulangan cybercrime dalam kategori hacker menuntut keseriusan dari semua pihak. Keberadaan undang-undang a quo yang mengatur mengenai *cybercrime* khususnya dalam klasifikasi *hacker* sangatlah diperlukan, masih banyak *hacker* di luar sana yang menjadi sosok menakutkan bagi masyarakat, karena bisa saja perlindungan data pribadi masyarakat bisa terancam. Gambaran mengenai individu, atau semua informasi tentang individu biasa disebut data pribadi. Namun demikian, jika pelaksanaan daripada undang-undang tersebut tidak memiliki kemampuan dan dalam teknologi informasi, tujuan pembentukan undang-undang tersebut tidak akan tercapai. Adapun sebelumnya terdapat penelitian hukum mengenai hacker diantaranya berjudul "HACKER DALAM PERSPEKTIF HUKUM

INDONESIA" karya Bambang Hartono[4] yang membahas mengenai pengaturan hacking ditinjau dari perspektif hukum indonesia. Sementara dalam penelitian ini, menitikberatkan hacker yang ditinjau dari perspektif hukum pidana dan bagaimana upaya penanganannya.

1.2. Rumusan Masalah

Dengan memperhatikan informasi latar belakang yang telah diuraikan, penulisan ini akan membahas:

1. Apa yang dimaksud dengan peretasan atau *hacking?*
2. Apa saja bentuk sanksi pidana yang akan dijatuhkan kepada pelaku peretasan ini?
3. Bagaimanakah upaya pencegahan serta penanganan yang dapat dilakukan terhadap kejahatan cyber ini?

1.3. Tujuan Penulisan

Tujuan dari penulisan ini adalah untuk mengetahui apa saja akibat hukum yang dapat dijatuhkan kepada seseorang yang secara hukum terbukti melakukan pidana peretasan. Untuk mengetahui bagaimana upaya penanganan pemerintah Indonesia terhadap kejahatan cyber di era globalisasi ini.

2. Metode Penelitian

Metode penelitian merupakan serangkaian langkah metodis untuk memecahkan rantai kausalitas dan menemukan solusi terhadap suatu permasalahan. Penulisan ini menggunakan penelitian hukum yuridis normatif, dimaksudkan untuk mengkaji kaidah hukum berkaitan dengan perkara pidana *hacking* dengan berfokus pada pengumpulan bahan hukum melalui studi kepustakaan antara lain, bahan hukum primer, terdiri atas, peraturan perundang-undangan, yurisprudensi dan juga traktat. Lalu bahan hukum sekunder, yang terdiri atas data serta informasi yang berasal dari buku, skripsi, maupun tesis yang berkaitan dengan objek penelitian. Selain itu juga data dari bahan hukum tersier. Dari data-data yang telah diperoleh kemudian dianalisis menggunakan metode kualitatif. Hasil dari analisis data kemudian dijelaskan secara deskriptif.

3. Hasil dan Pembahasan

3.1. Pengertian *Hacking*

Kemajuan juga perkembangan teknologi informasi dan komunikasi berdampak signifikan pada hampir setiap aspek peradaban modern. Pemanfaatan teknologi semakin mudah karena tidak terbatas oleh batas-batas negara (*borderless*), yang menyebabkan mudah diaksesnya suatu teknologi.[5] Hal tersebut dipengaruhi dengan munculnya teknologi yang dinamakan *internet* yang bisa menjangkau aktivitas dari benua satu ke benua lainnya. *Internet* secara harfiah diartikan sebagai jaringan kecil komputer yang membentuk jaringan yang lebih besar dengan struktur jaringan yang berbeda.[6] Dari jaringan inilah nantinya dapat dijadikan celah untuk melakukan

[4] Hartono, Bambang. "Hacker dalam Perspektif Hukum Indonesia." *Jurnal Masalah-Masalah Hukum, Fakultas Hukum Universitas Diponegoro,* 43 No. 1 (2014).
[5] Widodo. *Aspek Hukum Pidana Kejahatan Mayantara* (Yogyakarta, Aswaja, 2013), 17.
[6] Maskun. *Kejahatan Siber Cyber Crime* (Jakarta, Kencana, 2013), 46.

peretasan. Peretasan atau *hacking* yaitu aktivitas yang berupaya mendapatkan akses secara ilegal perangkat digital, misalnya seperti komputer, ponsel cerdas, tablet, bahkan seluruh jaringan. Orang yang melakukan peretasan disebut dengan *hacker*. *Hacker* merupakan orang atau kelompok yang dengan pengetahan yang lebih mendalam tentang komputer, jaringan, pemrograman, atau perangkat keras. Untuk merusak pertahanan keamanan siber, *Hacker* menggunakan segala keterampilan teknis yang ia kuasai. *Hacking* ditetapkan sebagai tindak pidana tingkat pertama dalam Kongres PBB ke X di Wina. Hal ini disebabkan oleh karakteristik unik dari kejahatan ini, yang memberikan keunggulan dibandingkan kejahatan mayantara konvensional lainnya. Keunggulan dan keunikan yang dimaksud adalah mereka yang mampu melakukan kejahatan siber semacam ini, tidak diragukan lagi, mungkin juga akan melakukan kejahatan mayantara lebih lanjut. Selanjutnya, dibandingkan dengan jenis kejahatan siber lainnya, tindakan peretasan berkualitas memiliki dampak yang lebih negatif. Misalnya, untuk menyebarluaskan konten yang berbau pornografi tidak perlu keahlian khusus tentang meretas sistem, hanya perlu paham mengenai internet saja. Lain halnya dengan *hacking*, yang diperlukan keahlian khusus untuk melakukannya.

Pada awalnya, *hacking* merupakan suatu bentuk aktivitas seorang *hacker* untuk menguji sistem, meningkatkan performa sistem, atau menemukan *bug* di dalam sistem (suatu kecacatan teknis dalam sebuah aplikasi yang mengakibatkan terjadinya malfungsi) program komputer dan *internet*. *Hacking* dilakukan dengan memodifikasi, mengubah *software* atau *hadware* komputer.[7] Ternyata budaya *hacking* dapat juga memberikan manfaat, karena dengan *hacking* memungkinkan hacker menemukan kelemahan produk *software* maupun *hardware.* Tidak selamanya kegiatan *hacking* ini termasuk kegiatan yang merugikan masyarakat. Terdapat dua istilah kategori *hacker* yakni hacker baik atau *white hat* dan hacker jahat atau *black hat.*

1. *White hat hacker* merupakan sebutan untuk menggambarkan peretas yang mengungkap suatu kerentanan sistem komputer secara sah. Berbeda dengan *black hat* yang lebih berfokus pada cara menghancurkan sistem, white hat seringkali lebih berfokus pada cara menjaga sistem.
2. *Black hat hacker* merupakan istilah yang digunakan untuk menggambarkan peretas yang secara ilegal memasuki sistem keamanan komputer yang bertujuan untuk mendapatkan akses ke setiap komputer yang terkoneksi ke jaringan tersebut.[8] **M**encuri data identitas seseorang, menjatuhkan sistem, bahkan menyanderanya dengan imbalan uang tebusan adalah bentuk kejahatan yang dapat dilakukan oleh *Black hat hacker*.

Seorang hacker tidak semata mata meretas suatu jaringan. Modus operasi dari *cybercrime* ini sangatlah bermacam-macam dan terus berkembang seiring dengan kemajuan teknologi. Dalam Undang-Undang tentang Informasi Dan Transaksi Elektronik pada pasal 30 dijelaskan mengenai modus operandi dari *hacking* yang biasanya disebut "*Unauthorized Acces to Computer System and Service*" yang memiliki arti tindakan kejahatan yang secara ilegal dilakukan dengan mengakses atau menembus ke dalam jaringan komputer tanpa sepengetahuan dari pemilik sistem. Biasanya pelaku melakukan modus sebagaimana dimaksud guna men-sabotase atau

[7] Riskawati. "Penanganan Kasus Cyber Crime di Kota Makassar (Studi pada Kantor Kepolisian Resort Kota Besar Makassar)." *Jurnal Tomalebbi* Makassar,1 No. 1 (2014): 97.

[8] Wijaya, Tubagus Heru Dharma. "Penerapan sanksi sosial sebagai alternatif pemidanaan terhadap pelaku tindak pidana kejahatan siber (cyber crime)." *Al-Qisth Law Review*, 5 No. 2 (2022): 371-404.

mencuri data dan informasi rahasia, namun, sebagian orang melakukannya hanya karena mereka ingin mencoba keahliannya dengan mencoba masuk ke dalam sistem dengan keamanan tinggi.

3.2. Sanksi yang Dapat Dikenakan Kepada Hacker

Tindak pidana sering disebut delik atau tindak pidana dalam beberapa literatur. Kejahatan yang hanya dapat terjadi hanya dengan menggunakan sistem jaringan komputer dikenal sebagai kejahatan mayantara, atau secara sederhananya kejahatan yang meggunakan komputer sebagai media utamanya dalam tindak kejahatan.[9] *Cybercrime* mempunyai spesialisasi tersendiri dalam mengidentifikasi pelakunya dan melakukan tindak kejahatannya, berbeda dengan kejahatan menurut KUHP bahwa proses pengungkaan dan pembuktian tindak kejahatan maupun pelakunya mengacu pada ketentuan dalam KUHAP. Atas dasar perbuatan itulah pelaku dapat dikenakan pidana. Sesuai dengan asas hukum pidana, yakni suatu perbuatan tidak dapat dijatuhi pidana, kecuali jika sebelumnya terdapat kekuatan ketentuan perundang-undangan pidana atau disebut juga *Nullum delictum nulla poena sine praevia lege poenalli*. Karena hal tersebut, seseorang hanya dapat dimintai pertanggungjawaban pidana apabila ia melakukan perbuatan yang secara khusus dilarang oleh undang-undang.[10]

Pemerintah Indonesia ini telah berusaha menangani kasus *hacking* ini dengan membentuk suatu payung hukum yang menaungi mengenai perkara ini, diantarnya Undang-Undang No. 36 tentang 1999 tentang Telekomunikasi, Undang-Undang No. 19 Tahun 2002 tentang Hak Cipta, Undang-Undang No. 15 Tahun 2003 tentang Pemberantasan Terorisme, Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta Undang-Undang No. 19 Tahun 2016 tentang Perubahan Atas Undang-Undang No. 11 Tahun 2008. Undang-undangan yang telah dibentuk ini mengkriminalisasi bentuk kejahatan mayantara disertai juga dengan ancaman sanksi pidana bagi individu yang melanggarnya.[11] Namun masih banyak para *hacker* di luar sana yang tetap melancarkan aksinya untuk meretas baik akun pribadi hingga situs pemerintah. Hal ini dapat terjadi karena kejahatan mayantara sulit diidentifikasi secara pasti mengingat dilakukan di lingkungan elektronik dan dunia maya. Sistem hukum pidana Indonesia menjelaskan ketentuan hukumnya hanya berlaku bagi warga negara dan yurisdiksinya sendiri, yang disebut juga asas teritorial dan asas personal/nasional aktif. Faktor yang sering menjadi hambatan dalam penegakan hukum dalam memerangi kejahatan transnasional, termasuk kejahatan dunia maya, adalah penentuan yurisdiksi. Faktor hambatan dalam penentuan yurisdiksi terkait kejahatan mayantara ini dapat diatasi dengan adanya ketentuan pada pasal 2 Undang-Undang tentang Informasi dan Transaksi Elektronik yang dapat diberlakukan bagi siapapun

[9] Nurdiani, Iftah Putri. "Pencurian Identitas Digital Sebagai Bentuk Cyber Related Crime." *Jurnal Kriminologi Indonesia,* 16 No. 2 (2020): 3.

[10] Setiawan, Beni. "Penegakan hukum pidana terhadap akses sistem komputer secara ilegal (hacking) dan menimbulkan kerusakan (cracking) dalam kejahatan dunia maya (cybercrime) menurut perspektif undang-undang nomor 19 tahun 2016 tentang perubahan atas undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik." *Jurnal Universitas Batanghari* (2019).

[11] Thantawi. "Perlindungan Korban Tindak Pidana Cyber Crime dalam Sistem Hukum Pidana Indonesia." *Jurnal Ilmu Hukum Pascasarjana Universitas Syiah Kuala,* 2 No. 1 (2014): 37.

yang melakukan perbuatan hukum yang ditetapkan dalam peraturan ini, baik di dalam maupun di luar yurisdiksi Indonesia, memiliki akibat hukum di dalam dan/atau di luar yurisdiksi Indonesia dan merugikan kepentingan Indonesia. Dengan adanya ketentuan ini, diharapkan dapat menyelesaikan permasalahan jikalau pelaku berasal dari luar wilayah hukum Indonesia, tetap dapat dikenakan pidana.

Undang-Undang tentang Informasi dan Transaksi Elektronik pasal 30 menjelaskan ketentuan yang secara spesifik mengatur terkait definisi tindak pidana peretasan yang menafsirkan bahwa siapapun yang mencoba mengakses sistem elektronik ataupun komputer milik orang lain dengan sengaja dan melawan hukum dengan tujuan untuk mendapatkan informasi atau dokumen elektronik. Lalu lebih lanjut dijelaskan dalam pasal 46 UU ITE mengenai ancaman pidana yang dapat dijatuhkan kepada pelaku *hacking*. Pasal 46 ayat (1) menyebutkan bahwa setiap orang yang memenuhi kriteria dalam pasal 30 ayat 1 dapat dijatuhi hukuman penjara maksimal 6 tahun penjara dan/atau denda maksimal Rp 600.000.000,00. Lalu dalam pasal 46 ayat (2) menyebutkan bahwa setiap orang yang memenuhi kriteria dalam pasal 30 ayat 2 dapat dijatuhi hukuman penjara maksimal 7 tahun penjara dan/atau denda maksimal Rp 700.000.000,00. Selanjutnya dalam pasal 46 ayat (3) disebutkan bahwa setiap orang yang memenuhi kriteria dalam pasal 30 ayat 3 dapat dijatuhi hukuman penjara maksimal 8 tahun penjara dan/ atau denda maskimal Rp 800.000.000,00.

Terdapat pemberatan pidana atas kejahatan peretasan, selain ancaman pidana yang dijelaskan di Pasal 46 UU ITE. Pemberatan pidana dalam perkara ini dibedakan sesuai dengan subjek dan objeknya. Berdasarkan objeknya disebutkan dalam Pasal 52 ayat (2) UU ITE, yang memperberat pengenaan hukuman jika sistem elektronik yang diretas adalah kepunyaan pemerintah atau sistem pelayanan publik. Pemberatan pidana tersebut berupa pidana pokok ditambah sepertiga. Pasal 52 ayat (3) UU ITE juga menjelaskan apabila yang diretas adalah website milik negara yang memiliki hubungan langsung dengan keamanan dan stabilitas negara, maka akan dikenakan pemberatan sanksi pidana. Pemberatan pidana dalam pasal 52 ayat (3) berupa ancaman pidana pokok setiap pasal ditambah dua pertiga. Lalu berdasarkan subjeknya, disebutkan dalam Pasal 52 ayat (4) UU ITE, yaitu apabila peretas adalah korporasi atau perusahaan, pemberatan penjatuhan hukuman pidana akan diterapkan yakni pidana pokok ditambah dua pertiga.

Penegakan hukum membutuhkan sejumlah sub-sistem yang saling berhubungan untuk mencapai ketertiban dan keamanan, khususnya pada tahap perumusan hukum yang menitikberatkan pada bagaimana menciptakan hukum yang baik, tahap penegakan hukum, dan tentu saja sebagai bentuk budaya hukum, tingkat kesadaran hukum masyarakat itu sendiri.[12] Sehingga penting untuk mempertimbangkan keseimbangan yang proporsional ketika memeriksa bagaimana penegakan hukum dilaksanakan. Meskipun dalam praktiknya tidak mudah membuat keseimbangan dari komponen tersebut pada penegakan hukum.

3.3. Upaya Penanggulangan Kejahatan *Hacking* di Masa yang Akan Datang

Sekarang yang jadi permasalahan adalah bagaimana cara untuk menanggulangi dampak dari *cybercrime* ini. Penegakan hukum terhadap kejahatan dunia maya menjadi tidak ideal, karena fasilitas dan sarana penegakan hukum yang

[12] Rosana, E. "Kepatuhan Hukum Sebagai Wujud Kesadaran Hukum Masyarakat." *Jurnal Teropong Aspirasi Politik Islam,* 10 No. 1 (2014): 80.

tidak memadai. Sarana dan fasilitas itu diantaranya kemampuan sumber daya manusia yang ahli dan berpendidikan, peralatan komputer forensik yang memadai, dan lain sebagainya. Penanggulangan terhadap aksi ilegal *hacking* ini harus diimbangi dengan reformasi dan pembaharuan hukum pidana secara menyeluruh, yang berarti struktur dan substansi dari hukum pidana juga perlu diberikan pembaharuan tidak terlepas dari kultur bangsa indonesia itu sendiri. Terdapat banyak kekurangan dan batasan bagaimana KUHP menyikapi kemajuan teknologi dan kejahatan berteknologi tinggi yang sangat bervariasi. Perumusan delik pidana dalam KUHP juga sebagian besar masih bersifat konvensional dan tidak memiliki korelasi langsung dengan perkembangan kejahatan dunia maya. Upaya yang dilakukan untuk memerangi kejahatan ini juga harus diperhitungkan dalam hal potensi kejahatan di masa depan, serta bagaimana penegak hukum dapat menggunakannya untuk merumuskan kebijakan yang efektif.[13] Di dalam hukum Indonesia mengenal Asas culpabilitas yang berarti tidak adanya pidana tanpa adanya kesalahan. Asas ini pun sudah semestinya harus diperhatikan dalam perkara pidana *cybercrime*. Dengan adanya asas ini diharapkan para penegak hukum jeli dalam hal membuktikan kesalahan pelaku kejahatan *hacking* ini.

Penentuan setiap kebijakan hukum pidana dalam upaya untuk menanggulangi perkara *cyber* harus mepertimbangkan nilai-nilai. Walaupun dalam pelaksanaanya, badan *cyber* di Indonesia mungkin menghadapi tantangan yang cukup sulit dalam menangani permasalahan ini karena sulitnya menentukan dan membuktikan adanya unsur kesalahan, dikarenakan *user* berada di lingkungan digital yang sulit diidentifikasi secara akurat dan terdapat kemungkinan melintasi batas-batas negara. Menurut Jhon Sipropoulus kejahatan mayantara bersifat afektif dan memiliki akses yang cepat dan mudah, karena hal itu maka menjadi tantangan yang sulit bagi penegak hukum dalam mengungkap pelaku kejahatan mayantara.[14] Penyidik pada umumnya dilatih agar menjadi ahli hukum, bukan ahli teknologi informasi dan komunikasi. Untuk meningkatkan usaha penanggulangan kejahatan mayantar yakni Bareskrim atau Badan Reserse Kriminal Mabes Polri diharapkan memberikan sosialisasi yang berkaitan dengan kejahatan mayantara dan cara penanganannya dengan cara memberikan pelatihan dan meningkatkan kemampuan penyidikan atau investigasi anggota Polri dengan memberikan berbagai kursus dan binaan terkait *cybercrime* kepada anggotanya. Hal ini dilakukan guna meningkatnya kemampuan dan keahlian penyidik dalam mengungkap kejahatan mayantara termasuk didalamnya menggali informasi tentang alat dan barang bukti yang menyangkut data-data elektronik. Dengan dilakukannya pelatihan tersebut diharapkan penyidik lebih baik lagi dalam menangani kasus kejahatan *cyber* ini agar masyarakat indonesia merasa mendapat perlindungan hukum dari kejahatan *cyber* yang semakin meningkat.

Penyidik juga dapat bekerjasama dengan para *white hat hacker* dalam upaya menanggulangi *cybercrime* ini, dengan cara menggali informasi lebih lanjut dan memanfaatkan keahlian *white hat hacker* ini untuk menemukan segala barang bukti yang dapat digunakan untuk menetapkan pelaku tindak kejahatan. Disamping itu, apabila di masa yang akan datang terdapat suatu kasus kejahatan peretasan yang

[13] Yasmirah, Mandasari S dan Dudung, Abdul. "Perlindungan Data Elektronik Dalam Formulasi Kebijakan Kriminal Di Era Globalisasi." *Jurnal Soumatera Law Review*, 3 No. 2 (2020): 276.

[14] Galuh Kartiko. "Pengaturan Tehradap Yurisdiksi Cyber Crime Ditinjau dari Hukum Internasional." *Jurnal Rechtldee,* 8 No. 2 (2013): 1.

melibatkan oknum hacker yang bekerja sama dengan oknum dari kepolisian untuk meretas suatu sistem komputer, yang dapat dikenakan bagi oknum polisi tentu saja pidana sesuai undang undang ITE dan juga pelanggaran kode etik sesuai pasal 11 Undang-undang Nomor 1 Tahun 2003 tentang Pemberhentian Tidak Dengan Hormat yakni bagi anggota yang melakukan tindak pidana akan dikenakan sanksi berupa diberhentikan tidak dengan hormat.

Perlindungan hukum dapat diartikan sebagai jenis keamanan yang diberikan kepada subyek hukum melalui peraturan perundang-undangan yang sedang berlaku baik tertulis maupun tidak tertulis, yang bersifat preventif maupun represif.[15] Perlindungan hukum preventif yaitu perlindungan hukum dengan maksud guna mencegah sebelum pelanggaran itu terjadi. Setiap penyelenggara sistem elektronik perlu menerapkan peraturan internal atau self-regulation untuk mencegah dari adanya *hacking* diperlukan. Diharapkan dengan adanya aturan yang berkaitan dengan standar *self regulation* yang di berikan oleh pemerintah akan memungkinkan penyelenggara sistem elektronik menjaga keamanan data pribadi konsumen dengan baik dan mencegah peretasan yang mengincar informasi rahasia konsumen.[16] Perlindungan hukum represif merupakan suatu bentuk perlindungan akhir apabila sudah terjadi tindak pidana kemudian memberikan sanksi penjara, denda dan hukuman tambahan.

Pentingnya perlindungan data pribadi dari kejahatan mayantara menjadi semakin penting, seiring dengan meningkatnya penggunaan *smartphone* dan internet. Namun, tidak ada jaminan bahwa perlindungan ini akan efektif. Oleh karenanya terdapat usaha pencegahan yang dapat dilakukan untuk mengatasi serangan *hacker* bagi setiap individu masyarakat antara lain:

a. Langkah pertama adalah dengan rutin meng-*update* kata sandi (*password*) akun anda. Agar tidak mudah ditebak, pastikan juga password memiliki perpaduan angka, huruf kapital, dan lainnya.
b. Langkah kedua, disarankan untuk tidak membuka tautan (*link*) yang mencurigakan di situs manapun.
c. Langkah ketiga, Gunakan perangkat lunak (software) yang legal agar pembaruan sistem (update) selalu tersedia untuk menutup segala potensi celah keamanan atau *bug*.
d. Langkah keempat, disarankan untuk tidak menggunakan koneksi *internet* wireless (Wi-Fi) yang berada ruang publik. Sebab, jaringan Wi-Fi di ruang publik terkadang tidak memiliki jaminan keamanan.
e. Langkah kelima, disarankan untuk pengguna media sosial untuk tidak mengungkapkan informasi pribadi kepada orang lain.

Kebijakan hukum pidana merupakan salah satu cara negara dalam memberantas tindak kejahatan. Mengutip pendapat Sudarto, kebijakan hukum pidana terdiri dari dua hal, yakni: Upaya untuk mewujudkan hukum yang baik sesuai dengan kondisi pada saat itu. Yang kedua, kebijakan negara melalui lembaga-lembaga yang berwenang membentuk suatu undang-undang sesuai dengan kaidah yang terkandung

[15] Islamia, Ayu Anindia. "Perlindungan Hukum terhadap Perdagangan Anak Dengan Modus Pernikahan dalam Perspektif Viktimologis." *Jurnal Litigasi,* 19 No, 1 (2018): 92.
[16] Refaldy, Braif Carundeng. "Perlindungan Hukum Terhadap Data Pribadi Konsumen Yang Diretas Berdasarkan Peraturan Menteri Komunikasi Dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik." *Jurnal Lex Privatum*, 10 No. 1 (2022): 191

dalam masyarakat untuk mencapai apa yang dicita-citakan.[17] Jika *hacker* tersebut menyerang sistem pemerintah maka yang harus dilakukan yaitu memaksimalkan kemampuan Sumber Daya Manusia (SDM) dari penyidik Bareskrim Polri maupun Badan Siber dan Sandi Negara (BSSN) guna memperkuat jagat *cyber* Indonesia. Kendati *cybercrime* ini kerap terjadi, namun hingga dewasa ini, belum ada payung hukum yang ampuh untuk melindungi masyarakat dari para hacker dan pilar hukum untuk menangani kasus-kasusnya, bahkan dapat dikatakan bahwa perkembangan kejahatan di dunia maya semakin dahsyat.

4. Kesimpulan

Perbuatan yang berupaya mengakses perangkat digital secara ilegal, seperti halnya komputer bahkan seluruh sistemnya disebut dengan *Hacking*. Modus operandi kegiatan *hacking* yaitu dengan memasuki sistem jaringan komputer tanpa persetujuan pemilik dan tanpa otoritas hukum untuk melakukannya. Undang-undang yang mengatur peretasan ini telah ditetapkan oleh pemerintah Indonesia. UU No. 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik didalamnya telah mengatur tentang delik hacking. Penegakan hukum terhadap kejahatan dunia maya masih belum mencerminkan penegakan hukum yang efektif. Hambatan yang terdapat dalam mewujudkan penegakan hukum terhadap *cybercrimes* menjadi tidak ideal karena terdapat kurangnya sarana dan fasilitas yang memadai, diantaranya keahlian dan keteramilan sumber daya manusia dalam bidang teknologi informasi, organisasi yang baik, fasilitas komputer forensik yang layak, dan lain sebagainya. Untuk mengatasinya diperlukan upaya diantaranya dengan melakukan penyempurnaan perangkat hukum pidana indonesia, meningkatkan sumber daya manusia dari para penyidik, membangun fasilitas *forensic computing*, serta melakukan upaya penanggulangan pencegah.

DAFTAR PUSTAKA

Buku:

Widodo. *Aspek Hukum Pidana Kejahatan Mayantara* (Yogyakarta, Aswaja, 2013), 17.

Jurnal:

Afitrahim. "Yurisdiksi Dan Transfer of Proceeding Dalam Kasusu Cybercrime." *Tesis, Universitas Indonesia,* (2012): 2.

Galuh Kartiko. "Pengaturan Tehradap Yurisdiksi Cyber Crime Ditinjau dari Hukum Internasional." *Jurnal Rechtldee,* 8 No. 2 (2013): 1

Islamia, Ayu Anindia. "Perlindungan Hukum terhadap Perdagangan Anak Dengan Modus Pernikahan dalam Perspektif Viktimologis." *Jurnal Litigasi,* 19 No, 1 (2018): 92

Kenedi, H. John. *Kebijakan Hukum Pidana: Dalam Sistem Penegakkan Hukum Di Indonesia* (Yogyakarta, Pustaka Pelajar, 2017), 61

Maskun. *Kejahatan Siber Cyber Crime* (Jakarta, Kencana, 2013), 46

[17] Kenedi, H. John. *Kebijakan Hukum Pidana: Dalam Sistem Penegakkan Hukum Di Indonesia* (Yogyakarta, Pustaka Pelajar, 2017), 61

Ngafifi, M. "Kemajuan Teknologi dan Pola Hidup Manusia dalam Perspektif Sosial Budaya." *Jurnal Pembangunan Pendidikan: Fondasi dan Aplikasi*, 2 No. 1 (2014): 33-47.

Nurdiani, Iftah Putri. "Pencurian Identitas Digital Sebagai Bentuk Cyber Related Crime." *Jurnal Kriminologi Indonesia,* 16 No. 2 (2020): 3.

Refaldy, Braif Carundeng. "Perlindungan Hukum Terhadap Data Pribadi Konsumen Yang Diretas Berdasarkan Peraturan Menteri Komunikasi Dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik." *Jurnal Lex Privatum*, 10 No. 1 (2022): 191

Riskawati. "Penanganan Kasus Cyber Crime di Kota Makassar (Studi pada Kantor Kepolisian Resort Kota Besar Makassar)."*Jurnal Tomalebbi* Makassar,1 No. 1 (2014): 97

Rosana, E. "Kepatuhan Hukum Sebagai Wujud Kesadaran Hukum Masyarakat." *Jurnal Teropong Aspirasi Politik Islam,* 10 No. 1 (2014): 80.

Setiawan, Beni. "Penegakan hukum pidana terhadap akses sistem komputer secara ilegal (hacking) dan menimbulkan kerusakan (cracking) dalam kejahatan dunia maya (cybercrime) menurut perspektif undang-undang nomor 19 tahun 2016 tentang perubahan atas undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik." *Jurnal Universitas Batanghari* (2019).

Thantawi. "Perlindungan Korban Tindak Pidana Cyber Crime dalam Sistem Hukum Pidana Indonesia." *Jurnal Ilmu Hukum Pascasarjana Universitas Syiah Kuala,* 2 No. 1 (2014): 37.

Widyopramono, Hadi Widjojo. "Cybercrime dan Pencegahannya." *Jurnal Hukum Teknologi, Fakultas Hukum Universitas Indonesia*: 7.

Wijaya, Tubagus Heru Dharma. "Penerapan sanksi sosial sebagai alternatif pemidanaan terhadap pelaku tindak pidana kejahatan siber (cyber crime)." *Al-Qisth Law Review*, 5 No. 2 (2022): 371-404.

Yasmirah, Mandasari S dan Dudung, Abdul. "Perlindungan Data Elektronik Dalam Formulasi Kebijakan Kriminal Di Era Globalisasi." *Jurnal Soumatera Law Review*, 3 No. 2 (2020): 276.