IJCLC

Indonesian Journal of Criminal Law and Criminology (IJCLC)
Vol. 1, No. 2, November 2020, 162-169.

E-ISSN: 2745-7184
P-ISSN: 2745-7192

Pusat Kajian Hukum Pidana dan Kriminologi
Fakultas Hukum, Universitas Muhammadiyah Yogyakarta
E-mail: ijclc@umy.university

Penegakan Hukum terhadap Cyber Crime Hacker

Yogi Oktafian Arisandy
Program Studi Hukum, Fakultas Hukum, Universitas Muhammadiyah Yogyakarta
Email : yogi.oktafian.2016@law.umy.ac.id

Info Artikel

Riwayat:
Diajukan : 1 November 2020
Direview : 9 November 2020
Direvisi : 25 November 2020
Diterima : 30 November 2020

Kata Kunci :
crime hacker; kejahatan cyber; penegakan hukum

DOI:
10.18196/ijclc.v1i3.11264

Abstrak

Kasus peretasan marak terjadi di Indonesia. Salah satu kasus peretasan tersebut terjadi di Sleman yang melibatkan hacker berisinial BBA (21) yang melakukan peretasan terhadap server sebuah perusahaan di San Antonio, Texas, Amerika Serikat dengan modus ransomware. Kasus tersebut terjadi disebabkan penegakan hukum terhadap kasus cyber crime hacker ini di rasa masih sangat kurang. Salah satu penyebabnya kurangnya kompetensi aparat penegak hukum dalam memberantas cyber crime hacker. Tulisan ini akan menjelaskan lebih lanjut mengenai penegakan hukum terhadap cyber crime, apa saja komponennya berikut fungsinya, dan mengetahui kendala dalam penegakan hukumnya. Pendekatan penelitian normatif yang bersumber dari bahan hukum yang diperoleh dari studi pustaka dianalisis secara kualitatif untuk mendapatkan jawaban atas permasalahan yang diambil. Berdasarkan hasil penelitian yang dilakukan, dapat disimpulkan bahwa komponen penegak hukum terdiri dari jaksa dan hakim. Kasus peretasan yang dilakukan oleh BBA merujuk pada ketentuan pasal Pasal 49 Jo Pasal 33 dan Pasal 48 ayat (1) Jo Pasal 32 ayat (1) dan Pasal 45 ayat (4) Jo Pasal 27 ayat (4) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang ITE, dan terdakwa dijatuhi hukuman selama tujuh bulan. Adapun pihak kepolisian dalam menjalankan fungsinya memiliki beberapa kendala, yang didasarkan pada aspek kemampuan penyidik, terbatasnya alat bukti, terbatasnya sarana dan prasarana yang ada, dan luasnya yurisdiksi yang ada.

I. Pendahuluan

Penegakan terhadap *cyber crime* di Indonesia masih belum mencerminkan penegakan hukum yang efektif meski Indonesia telah memiliki Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Undang-Undang *a quo* belum bisa mengakomodir *cyber crime* yang semakin marak di Indonesia yang mana meliputi penipuan kartu kredit, penipuan perbankan, *defacing, cracking,* transaksi seks, pornografi, judi online, penyebaran berita bohong melalui internet dan terorisme. Hal tersebut terjadi karena *cyber crime* tidak dibatasi oleh teritorial suatu negara, sehingga menunjukkan penyelarasan dibidang informasi, media, dan informatika berkembang tanpa dapat di bendung.

Salah satu kejahatan yang berkembang dan banyak terjadi adalah pencurian nomor kredit. Menurut Rommy Alkatiry, penyalahagunaan kartu kredit milik orang lain di internet merupakan kasus *cyber crime* terbesar yang berkaitan dengan dunia bisnis internet di Indonesia. Penyalahgunaan kartu kredit milik orang lain memang tidak terlalu rumit dan bisa dilakukan secara fisik atau online. Nama dan kartu kredit orang lain yang diperoleh di berbagai tempat (restaurant, hotel, atau segala tempat yang melakukan transaksi pembayaran dengan kartu kredit) di masukkan di aplikasi pembelian barang di Internet.[1] Hal tersebut lah yang kemudian membuka peluang untuk para *hacker* dapat memasuki, memodifikasi, atau merusak homepage (*hacking*) sehingga kasus *hacking* atau peretasan semakin lama sering terjadi.

[1]Suhariyanto, B. (2014). *Tindak Pidana Teknologi Informasi (Cyber Crime) Urgensi Pengaturan Dan Celah Hukumnya*. Jakarta:Rajawali Pers, h.18.

IJCLC

Indonesian Journal of Criminal Law and Criminology (IJCLC)
Vol. 1, No. 2, November 2020, 162-169.

E-ISSN: 2745-7184
P-ISSN: 2745-7192

Pusat Kajian Hukum Pidana dan Kriminologi
Fakultas Hukum, Universitas Muhammadiyah Yogyakarta
E-mail: ijclc@umy.university

Kasus peretasan umumnya bertujuan untuk mengambil data-data tertentu yang dimiliki target. Tapi ada juga peretasan yang bertujuan menghancurkan data atau sistem tertentu sehingga berdampak seperti kerusakan digital.[2] Dalam peraturan juga disebutkan bahwa kasus *cyber crime* terkait dengan pengambilan data atau sistem elektronik. Kasus pembobolan ATM yang sering terjadi pada korban *cyber crime hacker* bisa dikatakan tindakan peretasan data dan pencurian uang milik korban.

Kasus *cyber crimer hacker* pernah terjadi di Sleman, Daerah Istimewa Yogyakarta. Kasus tersebut melibatkan *hacker* berisinial BBA (21) yang ditangkap karena meretas server sebuah perusahaan di *San Antonio, Texas, Amerika Serikat*.[3] Menurut Kasubdit Direktorat Tindak Pidana Siber Bareskrim Polri, Kombes Rickynaldo Chairul nenyampaikan, pelaku melakukan tindak pidana *hacking* dengan modus *ransomware*. Dia ditangkap pada 18 Oktober 2019 di Yogyakarta. Tersangka ini menyebarkan atau mengirimkan email ke korban, berisi *link* atau tautan, di mana ketika korban mengklik *link* itu, akan menyebabkan server komputer mati. Setelah server komputer sasaranya mati, pelaku kemudian meminta uang tebusan dalam bentuk mata uang *crypto currency bitcoin* sebagai syarat untuk mengembalikan fungsi sistem. Dalam beraksi, BBA bisa memeras hingga 300 bitcoin. Satu btcoin itu kalau ditukar nilainya sekitar Rp 150 juta.

Dalam aksinya, dia mengirimkan tautan email http://ddiam.com/shipping200037315.pdf.exe ke salah satu satu karyawan di perusahaan tersebut. *Link* tersebut mengarahkan pengguna ke *link* lain berisikan *cryptolocker*. BBA juga diketahui melakukan tindak pidana lain berupa *carding* dengan modus membelanjakan kartu kredit orang lain dan memperjualbelikan data kartu kredit orang lain. Atas perbuatannya itu, BBA dikenakan Pasal 49 Jo Pasal 33 dan Pasal 48 ayat (1) Jo Pasal 32 ayat (1) dan Pasal 45 ayat (4) Jo Pasal 27 ayat (4) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang ITE. Pelaku berhasil ditangkap oleh Direktorat Tindak Pidana Siber Badan Reserse Kriminal Kepolisian Republik Indonesia di kediamannya Sleman, Yogyakarta pada Jumat 18 Oktober 2019.

Upaya penanganan *cyber crime* dalam klasifikasi *hacker* dibutuhkan keseriusan seluruh pihak mengingat teknologi informasi telah dijadikan sarana berbudaya komunikasi. Keberadaan undang-undang yang mengatur *cyber crime* terutama dalam klasifikasi *hacker* diperlukan, akan tetapi jika pelaksanaanya tidak memiliki kemampuan dan keahlian dalam bidang tersebut dan masyarakat terus menjadi sasaran, tujuan pembentukan undang-undang tersebut tidak akan tercapai. Menurut ketentuan Pasal 30 dan Pasal 46 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan atau sistem elektronik milik orang lain dengan cara apapun untuk memperoleh informasi elektronik dan atau dokumen elektronik dikenakan sanksi pidana penjara antara 6 (enam) sampai 8 (delapan) tahun dan atau denda sekitar Rp 1.000.000.000,- (satu miliar rupiah) sampai dengan Rp 2.000.000.000,- (dua miliar rupiah).

Meskipun pembentuk Undang-Undang telah merumuskan ketentuan pidana seperti dalam ketentuan peraturan diatas, namun pada kenyataannya penegakan hukum pada *cyber crime hacker* ini di rasa masih sangat kurang. Salah satu penyebabnya adalah tidak semua korban mempunyai keinginan untuk melaporkan meski korban sudah menderita kerugian secara materil. Selain itu kurangnya kompetensi aparat penegak hukum dalam memberantas *cyber crime hacker* juga membawa pengaruh terhadap penegakan hukumnya. Hal tersebut yang kemudian melatar belakangi penulis untuk mengkaji lebih lanjut tentang penegakan hukum terhadap *cyber crime hacker*.

II. Rumusan Masalah

Bagaimana penegakan hukum terhadap *cyber crime hacker* ?

[2]Hadtriyadi, Y. (2014). Kasus.Hacking.Paling.Heboh.Di.2014. Diakses pada tanggal 4 Agustus 2016, http://Tekno.kompas.com.

[3] Kusuma, W. (2019). Hacker Asal Sleman Yang Retas Perusahaan As Dikenal Pribadi Tertutup. Diakses Pada Tanggal 27 November 2019, http://Kompas.com.

IJCLC
Indonesian Journal of Criminal Law and Criminology (IJCLC)
Vol. 1, No. 2, November 2020, 162-169.
E-ISSN: 2745-7184
P-ISSN: 2745-7192
Pusat Kajian Hukum Pidana dan Kriminologi
Fakultas Hukum, Universitas Muhammadiyah Yogyakarta
E-mail: ijclc@umy.university

III. Metode Penelitian

Penelitian ini merupakan penelitian hukum normatif dengan berfokus pada pengumpulan bahan hukum melalui studi kepustakaan antara lain, bahan hukum primer, bahan hukum sekunder dan bahan hukum tersier. Selain itu penulis juga melakukan wawancara dengan Bapak Khairumam selaku Hakim Pengadilan Bantul dan Bapak Kurniawan selaku Polisi *Reserse Unit Cyber Crime* Bantul. Bahan yang dikumpulkan tersebut akan di analisis menggunakan teknik analisis kualitatif, yaitu dengan memberikan pemaparan, mendeskripsikan secara rinci dan menyeluruh mengenai data-data yang diperoleh dari proses penelitian sehingga dapat menjelaskan mengenai penegakan hukum pidana terhadap *cyber crime hacker.*

IV. Hasil dan Pembahasan

Perkembangan ilmu pengetahuan dan teknologi saat ini tidak hanya mampu memberikan dampak yang positif saja namun perkembangan tersebut ternyata disalahgunakan sebagai sarana kejahatan. Hal tersebut sangat penting untuk di antisipasi bagaimana kebijakan hukumnya, sehingga *cyber crime* yang terjadi dapat dilakukan upaya penanggulangannya dengan hukum pidana, termasuk dalam hal ini adalah mengenai sistem penegakannya. Indonesia sendiri sudah memiliki aturan hukum *cyber crime* yang tertuang dalam Undang-Undang Nomor 19 tahun 2016 tentang Informasi dan Transaksi Elektronik yaitu atas perubahan undang-undang nomor 11 tahun 2008.

Penegak hukum merupakan salah satu komponen dalam penegakan hukum. Penegak hukum merupakan mereka yang secara langsung atau tidak langsung berkontribusi di dalam suatu proses penegakan hukum. Pada dasarnya penegak hukum akan menggabungkan antara nilai, kaidah, dan perilaku. Penegak hukum pada umumnya sering melakukan tindakan dan pemeliharaan dalam tercapainya tujuan keadilan. Sikap dari penegak hukum di dalam melaksanakan tugas-tugasnya, tidak jarang melakukan diskresi yang merupakan suatu pengambilan putusan dalam mengatasi masalah yang dihadapi tetapi didalam pengambilan putusan penegak hukum harus tetap berpegang teguh terhadap peraturan, walaupun tidak menutup kemungkinan adanya diskresi yang tanpa berpegang pada peraturan, karena peraturan mengenai masalah tersebut belum ada.[4]

Di Indonesia aparat penegak hukum yang memiliki kewenangan dalam menangani perkara tindak pidana *cyber crime hacker* dibagi menjadi 3 yaitu ;

1. Pengadilan

Pengadilan sebagai instansi resmi negara bertugas untuk melakukan pemeriksaan, memberikan keadilan dengan cara mengadili, memberikan putusan, dan menyelesaikan segala perkara atau permasalahan yang diajukan oleh warga masyarakat. Perkara yang diselesaikan melalui pengadilan akan dapat berjalan sebagaimana mestinya jika semua pihak yang berada atau ikut didalam penyelesaian perkara tersebut. Para pihak yang berperkara atau dari hakimnya sendiri harus mengikuti aturan main (*rule of game*) secara jujur dan sesuai dengan peraturan yang ada.[5]

Pihak yang mengajukan perkara di pengadilan tentunya mempunyai maksud untuk mendapatkan penyelesaian dan pemecahan perkara secara adil dan sesuai dengan harapan dan keinginan para pihak pencari keadilan (*justiciabellen*). Untuk mendapatkan penyelesaian perkara secara adil dan sesuai dengan harapan dan keinginan para pihak pencari keadilan harus melalui proses pembuktian. Proses tersebut bertujuan untuk mengetaui duduk perkara secara jelas, yaitu peristiwa yang benar dan peristiwa yang salah.

Di dalam proses pembuktian para pihak diberikan kesempatan untuk mengemukakan pendapat mengenai peristiwa yang terjadi. Hal tersebut sangat penting karena sebagai dasar untuk meneguhkan hak dan membantah hak dari pihak lain. Dalam hal mengemukakan pendapat para pihak tidak cukup sekedar memberikan pendapatnya secara lisan maupun tertulis saja, tetapi harus didukung dan disertai dengan bukti-bukti yang sah menurut hukum agar kebenarannya dapat dipastikan.

2. Kejaksaan

[4]Soekanto, S. (1990). *Polisi Dan Lalu Lintas (Analisis Menurut Sosiologi Hukum)*. Bandung:Mandar Maju. h. 6.
[5] Wawancara dengan Khairumam selaku Hakim Pengadilan Bantul Pada 28 Juli Pukul 13.00

IJCLC
Indonesian Journal of Criminal Law and Criminology (IJCLC)
Vol. 1, No. 2, November 2020, 162-169.
E-ISSN: 2745-7184
P-ISSN: 2745-7192
Pusat Kajian Hukum Pidana dan Kriminologi
Fakultas Hukum, Universitas Muhammadiyah Yogyakarta
E-mail: ijclc@umy.university

Kejaksaan adalah lembaga pemerintahan yang melaksanakan kekuasaan negara dibidang penuntutan serta kewenangan lain berdasarkan undang-undang. Selain itu kejaksaan merupakan lembaga non departemen, yang berarti kejaksaan tidak berada dibawah kementerian apapun. Kejaksaan dipimpin oleh Jaksa Agung, dimana nantinya Jaksa Agung yang memiliki tanggung jawab terhadap presiden. Tanggung jawab tersebut menjadikan Jaksa Agung memiliki kedudukan setingkat dengan Menteri. Jaksa Agung memimpin kejaksaan yang terbagi ke dalam beberapa daerah hukum mulai dari tingkat Provinsi (jaksa tinggi) sampai dengan tingkat Kabupaten (kejaksaan negeri) di seluruh wilayah Indonesia.

Kejaksaan memiliki tugas utama sebagai salah satu lembaga penegak hukum dalam sistem peradilan pidana Indonesia. Adapun tugasnya untuk melakukan penuntutan dan sebaliknya. Penuntutan merupakan kewenangan satu-satunya yang hanya dimiliki oleh kejaksaan dan tidak dimiliki oleh lembaga penegak hukum lain. Dalam melaksanakan fungsi, tugas, dan wewenangnya, kejaksaan terlepas dari segala pengaruh kekuasaan pemerintah, dan pengaruh dari kekuasaan lainnya. Negara memberikan jaminan kepada jaksa di dalam menjalankan profesinya tanpa adanya intimidasi, gangguan, godaan, dan campur tangan yang tidak sesuai atau pembeberan dari segala sesuatu yang belum teruji kebenarannya, baik terhadap pertanggungjawaban perdata, pidana, maupun lainnya.[6]

3. Kepolisian

Kepolisian merupakan salah satu dari aparat penegak hukum. Tugas dari aparat kepolisian yaitu memelihara keamanan dan ketertiban masyarakat, menegakkan hukum, memberikan perlindungan, pengayoman dan pelayanan terhadap masyarakat. Segala aturan mengenai fungsi kepolisian sendiri sudah diatur didalam Undang-Undang No. 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia. Peraturan tersebut menjelaskan bahwa salah satu fungsi kepolisian adalah menjalankan fungsi pemerintahan negara yang memberikan perlindungan, mewujudkan atau menjaga ketertiban, memberikan pelayanan dan pengayoman terhadap masyarakat, serta melakukan penegakan hukum. Hal tersebut jelas disebutkan didalam Pasal 14 ayat (1) Undang-Undang Kepolisian.

Dalam kasus pidana pada umumnya polisi akan langsung bertindak melakukan penyidikan meskipun tidak ada laporan atau aduan terlebih dahulu. Akan tetapi hal tersebut tentunya memerlukan berbagai pertimbangan terlebih dahulu. Tindakan penyidikan tersebut merupakan tugas dari kepolisian sebagaimana disebutkan didalam Pasal 14 ayat (1) huruf g yang menyatakan bahwa polisi berwenang melakukan penyidikan tindakan pidana sesuai dengan hukum acara pidana dimana sebelumnya didahului oleh tindakan penyelidikan oleh penyidik.

Penindakan kasus *cyber crime* sering mengalami hambatan terutama dalam penangkapan tersangka dan penyitaan barang bukti. Dalam penangkapan tersangka sering kali tidak dapat menentukan secara pasti siapa pelakunya karena mereka melakukannya cukup melalui komputer yang dapat dilakukan dimana saja tanpa ada yang mengetahuinya sehingga tidak ada saksi yang mengetahui secara langsung. Hasil pelacakan paling jauh hanya dapat menemukan IP Address dari pelaku dan komputer yang digunakan. Hal itu akan semakin sulit apabila menggunakan warnet sebab saat ini masih jarang sekali warnet yang melakukan registrasi terhadap pengguna jasa mereka sehingga kita tidak dapat mengetahui siapa yang menggunakan komputer tersebut pada saat terjadi tindak pidana.[7]

Perkembangan *hacking* diluar negeri berkembang sangat pesat demikian juga halnya di Indonesia. Tentunya ini sangat berbeda dibandingkan dengan kejahatan-kejahatan biasa oleh karena itu tindak pidana *hacking* termasuk kedalam tindak pidana khusus. Salah satu contoh kejahatan *cyber crime hacking* yang pernah terjadi di Indonesia yaitu kasus yang terjadi di Sleman, dengan tersangka peretas alias *hacker* dengan inisial BBA. BBA ditangkap karena diduga meretas *server* sebuah perusahan di San Antonio Texas Amerika Serikat dan meraup uang senial Rp. 31,5 Miliar.

Dari hasil penyelidikan polisi, peretasan dilakukan BBA dengan modus serangan program jahat (virus komputer) jenis *Ramsomeware*. BBA membeli *Ramsomeware* atau *malware* yang mampu mengambil alih kendali yang berisi *Cryptolocker* di pasar gelap internet atau *dark ware*. *Ramsomeware* tersebut dikirimkan secara luas ke lebih dari 500 alamat email di luar negeri. Salah satu korban yang menerima dan membuka email tersebut, maka *software* perusahaan akan terenkripsi. Hal inilah yang

[6] Wawancara dengan Asep priyanto selaku Jaksa Negeri Bantul Pada 2 Juli Pukul 10.00
[7] Wawancara dengan Kurniawan selaku polisi reserse unit cibercrime Bantul Pada 2 Juni Pukul 14.00

IJCLC
Indonesian Journal of Criminal Law and Criminology (IJCLC)
Vol. 1, No. 2, November 2020, 162-169.
E-ISSN: 2745-7184
P-ISSN: 2745-7192
Pusat Kajian Hukum Pidana dan Kriminologi
Fakultas Hukum, Universitas Muhammadiyah Yogyakarta
E-mail: ijclc@umy.university

menjadi kesempatan bagi BBA untuk meminta uang tebusan kepada korban. Sebab, jika tidak diberi uang tebusan dalam waktu tertentu, sistem perusahaan itu akan lumpuh. BBA ditangkap pada 18 Oktober 2019 oleh direktorat tindak pidana Siber Bareskrim Polri di kediamannya Sleman. BBA disidangkan di Pengadilan Negeri Bantul dengan nomor perkara 41/Pid.Sus/2020/PN Btl (ITE). BBA terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana *cyber yang* mengakibatkan terganggunya sistem elektronik sehingga Pengadilan Negeri Bantul menjatuhkan pidana kepada terdakwa BBA berupa pidana penjara selam 7 bulan.

Pertanggungjawaban pidana peretasan (*hacking*) di dasarkan pada ketentuan pasal 30 UU ITE. Di dalam pasal 30 UU ITE, seseorang dapat dipidana apabila orang tersebut mengakses sistem elektronik atau komputer korban dan juga dalam pasal ini menentukan bahwa cara yang dilakukan adalah dengan cara apapun (termasuk peretasan) selama hal tersebut dilakukan dengan cara tanpa haknya. Apabila suatu *website* di retas oleh *hacker,* maka si penyedia layanan *web hosting* tidak dapat dimintai pertanggungjawaban pidana. Penyedia layanan *web hosting* hanya sebagai media penyedia saja, tetapi pemilik penyedia layanan *web hosting* tidak dapat mengelak untuk dimintai pertanggungjawaban pidana apabila pemilik membuat layanan-nya semata-mata untuk memfasilitasi tindak pidana. Sama halnya dengan seorang penyedia bangunan apartemen tidak dapat dimintakan pertanggungjawaban apabila pemilik apartemen dimasuki oleh kawanan pencuri.

Pemidanaan di Indonesia seharusnya merujuk pada pendekatan norma yang bersifat menghukum penjahat sehingga dapat membuat efek jera. Eksistensi penegakan hukum dalam hal visi dan misi penegakan hukumnya, baik di tingkat penyidik, penuntut sampai tingkat pengadilan, harusnya memiliki presensi yang sama sesuai tuntutan hukum dan keadilan masyarakat.[8] Analisis yang didapat dari kasus tersebut mengenai *cyber crime hacker*, merupakan salah satu perbuatan melanggar hukum, sebagaimana sudah diatur dalam Pasal 32 ayat (1) jo Pasal 48 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana diubah dengan Undang-undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Karena perbuatan kejahatan menggunakan media elektronik yang sudah diatur secara khusus di Undang-Undang ITE sehingga pasal yang terdapat didalam KUHP dikesampingkan sesuai dengan asas pidana *lex specialis derogate legi generali* yang berbunyi "Jika suatu tindakan masuk dalam suatu ketentuan pidana umum, tetapi termasuk juga dalam ketentuan pidana khusus, maka hanya yang khusus itu yang diterapkan".

Mengenai alat bukti yang terdapat dalam Pasal 184 KUHAP yang terdiri dari, keterangan ahli, saksi, bukti, surat petunjuk, dan keterangan terdakwa. Langkah selanjutnya dalam menentukan seseorang dapat dikatakan bersalah atau tidaknya ialah dengan adanya minimal 2 alat bukti yang dianggap sah. Adapun alat bukti yang terdapat dalam kasus tersebut antara lain, keterangan saksi atau tambahan alat bukti lainnya yaitu barang bukti berupa: - 1) 1 (satu) bendel percakapan email antara korban dengan hacker (pelaku), 2) 1 (satu) bendel Log Akses Ip Address 179.170.139.23 tanggal 26-08- 2020; 3) 1 (satu) bundle Shipping Order #200037315 eml; 4) 1 (satu) bundle Shipping Order # 200037315 Source 5) 1 (satu) Whois Website Http://ddiam.com; 6) 1 (satu) Whois IP Address 136.243 70.231, 7) 1 (satu) percakapan email antara Matt Meredith kepada sales Website ddiam.com; 8) 1 (satu) bendel Takedown Immediately : Mallware Hosted om ddiam.com; 9) 1 (satu) Ewhite Demand Email. Eml; 10)1 (satu) bundel Ewhite Response.Eml; 11)1 (satu) bundel Bitcoin Confirmation Purchasing Bitcoin; 12)1 (satu) bundel Bitcoin Confirmation Purchasing Bitcoin to Bad Actor, 13)1 (satu) bundel Email With Dinstruments As Jowl Springer 14)1 (satu) bundel Raw Email From Dinstrument, percakapan 15)1 (satu) bundel email antara korban (joel.springer1977@gmail.com) dengan hacker (drinstrumentspayment@gmail.com).

Atas perbuatan tersebut pelaku di jerat dengan ketentuan Pasal 49 Jo Pasal 33 dan Pasal 48 ayat (1) Jo Pasal 32 ayat (1) dan Pasal 45 ayat (4) Jo Pasal 27 ayat (4) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang ITE. Pasal tersebut yang dijadikan sebagai dasar bagi Jaksa untuk merumuskan dakwaan dan tuntutan terhadap pelaku. Proses penuntutan terhadap pelaku *cyber crime* adalah setelah berkas di kirim oleh penyidik kepada jaksa dan

[8] Laksana, A. (2016). Tinjauan Hukum Pemidanaan Terhadap Pelaku Penyalahguna Narkotika Dengan Sistem Rehabilitasi. *Jurnal Pembaharuan Hukum*, 2(1). h.75.

IJCLC
Indonesian Journal of Criminal Law and Criminology (IJCLC)
Vol. 1, No. 2, November 2020, 162-169.
E-ISSN: 2745-7184
P-ISSN: 2745-7192
Pusat Kajian Hukum Pidana dan Kriminologi
Fakultas Hukum, Universitas Muhammadiyah Yogyakarta
E-mail: ijclc@umy.university

dinyatakan lengkap maka kejaksaan mengeluarkan surat P21. Penuntutan dimulai setelah tersangka dan barang bukti di serahkan ke kejaksaan. Kemudian dari kejaksaan melimpahkan ke pengadilan berupa barang bukti dan surat dakwaan untuk menentukan hari persidangan.

Proses persidangan kemudian di pimpin oleh Hakim. Hakim menjadi penentu apakah pelaku terbukti bersalah atau tidak. Dalam menjatuhkan putusan, Hakim akan merujuk pada ketentuan pasal tersebut dengan di dasarkan beberapa pertimbangan termasuk dalam proses pembuktian dan pemeriksaan saksi dalam persidangan. Saksi harus lah memberikan keterangan yang sesuai dengan fakta tanpa mengurangi atau melebihkan pernyataanya. Terlebih saksi sudah disumpah untuk memberikan keterangan yang sebenar-benarnya.

Adapun analisa terkait pertimbangan hakim dalam memutus perkara dibedakan menjadi, hal-hal yang dapat memberatkan dan hal-hal yang dapat meringankan. Hal-hal yang dapat memberatkan tuntutan terhadap pelaku *hacker* adalah adanya akibat yang ditimbulkan dari perbuatan yang dilakukan oleh pelaku. Akibat tersebut misalnya terganggunya fungsi situs yang di retas misalnya situs pemerintahan atau situs pendidikan. Hal tersebut tentu akan berdampak pada korban, sehingga tidak hanya berdampak pada situs itu saja tetapi juga berdampak untuk masyarakat luas. Hal yang dapat meringankan tuntutan terhadap pelaku *hacker* antara lain, kejahatan tersebut merupakan kejahatan yang pertama kali dilakukan, dan tidak ada catatan kriminal sebelumnya. Pelaku memberikan keterangan jujur, tidak berbelit-belit, tidak menutupi fakta yang sebenarnya, dan pelaku mengakui dan menyesali perbuatan yang dilakukannya.

Banyak kendala yang di hadapi oleh aparat penegak hukum dalam memberantas *cyber crime.* Kendala tersebut tentu akan mempengaruhi penegakan hukum terhadap *cyber crime* sehingga tidak dapat di atasi dengan maksimal. Kepolisian sebagai salah satu penegak hukum tidak luput dari kendala tersebut. Beberapa kendala yang menghambat upaya penanggulangan *cyber crime* dari pihak kepolisian, dapat dilihat dari empat aspek berdasarkan hasil wawancara dan penelusuran referensi, yaitu:

1. Aspek Penyidik

Penyidik kepolisian memiliki peran penting dalam upaya penanggulangan *cyber crime*, dimana kemampuan penyidik sangat dibutuhkan untuk mengungkap kasus-kasus *cyber crime*. Adanya unit *cyber crime* di lingkungan kepolisian membuktikan bahwa dibutuhkannya penyidik khusus yang memiliki kemampuan di bidang informasi dan transaksi elektronik guna menangani kejahatan-kejahatan di dunia maya. Pendidikan khusus untuk memberikan pengetahuan terkait *cyber* kepada para penyidik yang khusus menangani masalah *cyber crime* sangat penting untuk dilakukan agar dapat mengakomodir kebutuhan penyidik dalam mengungkap kasus *cyber crime*.

2. Aspek Alat Bukti

Dalam proses penyidikan kasus *cyber crime*, alat bukti elektronik memiliki peran penting dalam penanganan kasus. Alat bukti dalam kasus *cyber crime* berbeda dengan alat bukti kejahatan lainnya dimana sasaran atau media *cyber crime* merupakan data-data atau sistem komputer / internet yang sifatnya mudah diubah, dihapus, atau disembunyikan oleh pelaku kejahatan. Terutama jika melihat dalam pengaturan alat bukti dalam Pasal 184 KUHAP yang tidak mengenal istilah bukti elektronik/digital *(digital evidence)* sebagai bukti yang sah menurut undang-undang. Sering kali juga di dapati alat bukti elektronik sudah dilakukan modifikasi, di ubah bahkan di hapus, meski hal tersebut tidak berlaku bagi pelaku yang tertangkap tangan dalam melakukan aksi nya karena alat bukti dapat langsung diamankan oleh pihak kepolisian.

3. Aspek Fasilitas

Dalam mengungkap kasus-kasus *cyber crime* dibutuhkan fasilitas yang mampu menunjang kinerja aparat kepolisian. Salah satunya adalah dengan memaksimalkan kemampuan digital forensik. Digital forensik ini dapat bekerja dalam laboratorium komputer forensik. Laboratorium komputer forensik di gunakan untuk mengamankan dan menganalisis bukti digital sehingga diperoleh fakta atas suatu kasus yang terjadi. Digital forensik ini dapat bekerja dengan mengungkap data-data yang bersifat digital serta merekam dan menyimpan bukti-bukti yang berupa *soft copy* (gambar, program, html, suara, dan lain sebagainya). Sayangnya belum semua kantor polisi memiliki laboratorium komputer forensik tersebut, padahal laboratorium tersebut sangat penting digunakan dalam mengungkap kasus *cyber crime.*

IJCLC
Indonesian Journal of Criminal Law and Criminology (IJCLC)
Vol. 1, No. 2, November 2020, 162-169.
E-ISSN: 2745-7184
P-ISSN: 2745-7192
Pusat Kajian Hukum Pidana dan Kriminologi
Fakultas Hukum, Universitas Muhammadiyah Yogyakarta
E-mail: ijclc@umy.university

4. Aspek jurisdiksi

Asas-asas berlakunya hukum pidana menurut tempat yang konvensional / tradisional (jurisdiksi fisik) tentunya menghadapi tantangan sehubungan dengan masalah pertanggungjawaban *cyber crime*. Penanganan *cyber crime* tidak akan berhasil jika aspek jurisdiksi diabaikan. Karena pemetaan yang menyangkut kejahatan dunia maya menyangkut juga hubungan antar kawasan, antar wilayah, dan antar negara. Penetapan jurisdiksi diperlukan dan diatur dalam Pasal 2 undang-undang informasi dan transaksi elektronik nomor 11 tahun 2008, yaitu: "Undang-undang ini berlaku untuk setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam undang-undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau diluar wilayah hukum indonesia dan merugikan kepentingan Indonesia".

V. Simpulan

Berdasarkan hasil penelitian yang dilakukan oleh penulis dapat disimpulkan bahwa penegakan hukum pidana terhadap *cyber crime hacker* berdasarkan Undang-Undang Nomor 19 tahun 2016 tentang Informasi dan Transaksi Elektronik yaitu atas perubahan undang-undang nomor 11 tahun 2008 dengan berfokus pada peran dari aparat penegak hukum yang terdiri dari pihak kepolisian, kejaksaan, dan pengadilan. Kasus peretasan yang dilakukan oleh BBA merujuk pada ketentuan pasal Pasal 49 Jo Pasal 33 dan Pasal 48 ayat (1) Jo Pasal 32 ayat (1) dan Pasal 45 ayat (4) Jo Pasal 27 ayat (4) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang ITE. Pasal tersebut yang dijadikan sebagai dasar bagi Jaksa untuk merumuskan dakwaan dan tuntutan terhadap pelaku. Sedangkan hakim akan memimpin proses persidangan dan memberikan putusan sesuai dengan pembuktian dan pemeriksaan dalam persidangan. Pertimbangan hakim dalam memutus perkara dapat bersifat memberatkan dan meringankan terdakwa. Sehingga dalam kasus tersebut, terdakwa dijatuhi hukuman selama tujuh bulan. Adapun pihak kepolisian dalam menjalankan fungsinya memiliki beberapa kendala, yang didasarkan pada aspek kemampuan penyidik, terbatasnya alat bukti, terbatasnya sarana dan prasarana yang ada, dan luasnya yurisdiksi yang ada.

Daftar Pustaka

Buku

Suhariyanto, B. (2014). *Tindak Pidana Teknologi Informasi (Cyber Crime) Urgensi Pengaturan Dan Celah Hukumnya*. Jakarta:Rajawali Pers.

Fajar, M & Achmad, Y. (2010). *Dualisme Penelitian Hukum Normatif Dan Empiris*. Yogyakarta:Pustaka Pelajar.

Soekanto, S. (1990). *Polisi Dan Lalu Lintas (Analisis Menurut Sosiologi Hukum)*. Bandung:Mandar Maju.

Jurnal

Laksana, A. (2016). Tinjauan Hukum Pemidanaan Terhadap Pelaku Penyalahguna Narkotika Dengan Sistem Rehabilitasi. *Jurnal Pembaharuan Hukum*, 2(1).

Regulasi

R.I., Kitab Undang-Undang Hukum Pidana.

R.I., Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Wawancara

Wawancara dengan Khairumam selaku Hakim Pengadilan Bantul. Pada 28 Juli Pukul 13.00.

Wawancara dengan Asep priyanto selaku Jaksa Negeri Bantul. Pada 2 Juli Pukul 10.00.

IJCLC

Indonesian Journal of Criminal Law and Criminology (IJCLC)
Vol. 1, No. 2, November 2020, 162-169.

E-ISSN: 2745-7184
P-ISSN: 2745-7192

Pusat Kajian Hukum Pidana dan Kriminologi
Fakultas Hukum, Universitas Muhammadiyah Yogyakarta
E-mail: ijclc@umy.university

Wawancara dengan Kurniawan selaku Polisi Reserse Unit Cyber Crime Bantul. Pada 2 Juni Pukul 14.00.

Webiste

Hadtriyadi, Y. (2014). Kasus.Hacking.Paling.Heboh.Di.2014. Diakses pada tanggal 4 Agustus 2016, http://Tekno.kompas.com.

Kusuma, W. (2019). Hacker Asal Sleman Yang Retas Perusahaan As Dikenal Pribadi Tertutup. Diakses Pada Tanggal 27 November 2019, http://Kompas.com.