Jurnal Preferensi Hukum | ISSN: 2746-5039
Vol. 5, No. 1 – Maret 2024, Hal. 1 – 7 | Available online at
https://www.ejournal.warmadewa.ac.id/index.php/juprehum
DOI: 10.55637/jph.5.1.8636.1-7

ANALISIS YURIDIS ATAS KEABSAHAN PERTANGGUNGJAWABAN PIDANA TERHADAP PELAKU TINDAK PIDANA PEMBOBOLAN SISTEM DATA KEAMANAN KOMPUTER (CRACKING)

Cok Rai Kesuma Putra[1], I Nyoman Gede Sugiartha[2], I Made Minggu Widyantara[3]
Fakultas Hukum, Universitas Warmadewa, Denpasar, Indonesia
cokrai00@gmail.com[1], nyomansugiartha14@gmail.com[2], mademinggu21@gmail.com[3]

Abstrak

Kejahatan digital merupakan salah satu dampak negatif dari perkembangan teknologi saat ini. Berbagai kejahatan digital seperti pembobolan dan peretasan data komputer yang dilakukan oleh seseorang akan dapat mengacu pada tindakan kriminal hingga dapat menimbulkan korban. Anak dari itu perlu adanya penegakan hukum agar tidak adanya tindakan kriminal melalui digital ini. Tujuan penelitian ini adalah untuk mengetahui pengaturan hukum tindak pidana pembobolan sistem keamanan data computer dan pertanggungjawaban hukum pelaku tindak pidana pembobolan sistem keamanan data komputer. Penelitian ini menggunakan tipe penelitian normatif dan pendekatan undang-undang dan konseptual. Hasil dari penelitian ini bahwa pengaturan tindak pidana pembobolan sistem keamanan data komputer diatur dalam undang-undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, Pasal 46 ayat (3) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp 800.000.000 (delapan ratus juta rupiah).

Kata Kunci: Kejahatan Digital, Pembobolan, Tindak Pidana

Abstract

Digital crime is one of the negative impacts of current technological developments. Various digital crimes such as breaking and hacking computer data committed by someone will be able to refer to criminal acts that can cause victims. Therefore, it is necessary to enforce the law so that there are no criminal acts through this digital. Therefore, this problem is interesting regarding the legal regulation of criminal acts of breaking into computer data security systems? And the legal liability of perpetrators of criminal acts of breaking into computer data security systems. This research uses normative research type and statutory and conceptual approach. The result of this study is that the regulation of criminal acts of breaking into computer data security systems is regulated in Law Number 19 of 2016 concerning Electronic Information and Transactions, Article 46 paragraph (3) Every person who fulfills the elements as referred to in Article 30 paragraph (3) shall be punished with a maximum imprisonment of 8 (eight) years and / or a maximum fine of Rp 800,000,000 (eight hundred million rupiah).

Keywords: Cybercrime, Breach, Criminal Act

I. PENDAHULUAN

Hukum Pidana di NRI berdasarkan analisis sejarah memperoleh transformasi yang sangat tinggi, sebab sesuai pada perkembangan kebudayaan warga di mana hukum tersebut ditetapkan. Pada hubungan tersebut, hukum pasti berganti sebab kekejaman yang terlaksana juga berganti dan berkehendak memperoleh perkembangan jaman dan khususnya bidang unit teknologi "media sosial". Buat menanggapi problem tersebut diperlukan fitur hukum yang mencukupi, membuat penegakkan hukum "law enforcement" tidak hadapi kesusahan saat melaksanakan cara penegakannya. Sepanjang ini petugas penegak hukum hadapi kesusahan disebabkan terjalin kekosongan hukum yang diakibatkan terdapatnya berbagai kejahatan baru yang belum diatur pada

UU. Sesuai pada perihal tersebut, kejahatan yang bertabiat tradisional semakin tumbuh bersamaan pada pergantian era semakin meningkat.

Peradaban warga hadapi pergantian ekstrem pada dekade di abad sembilan belas. Pergantian tersebut paling utama terkait interaksi serta hubungan yang tidak terhingga dalam memakai alat telekomunikasi. Dari tata hubungan dunia yang baru tersebut, bukan nampak lagi penghalang ataupun batasan sesuatu negeri. Tidak lagi dipermasalahkan warna kulit, ras serta kalangan. Sebab bukan lagi menuruti jarak serta waktu, ikatan bisa dicoba kapan saja, dimana saja saja serta dari mana saja. Perihal tersebut yang diketahui selaku ikatan mendunia (Sutarman 2007). UUD 1945 memiliki peran penting saat memberikan hak-hak warga di setiap lapisan. Itulah menyebabkan penting bagi warga NRI mengetahui dengan baik. UUD 1945 diresmikan dari sidang yang dilaksanakan oleh Panitia Persiapan Kemerdekaan Indonesia "PPKI" pada 18 Agustus 1945. Ada arti yang terkandung pada UUD 1945, utamanya pada pembukaan yang isinya empat alinea penting. Pembukaan UUD 1945 adalah pokok dari tujuan kaidah negara yang sifatnya "fundamental", di mana memiliki prinsip negara seperti bentuk negara, dasar negara, dan tujuan NRI.

Meningkatnya "iptek" yang cukup cepat saat ini telah sebagai realita tiap hari dan sebagai permintaan warga yang tidak bisa di nego lagi. Tujuan pertama meningkatnya iptek adalah perubahan energi masa mendatang makhluk hidup yang semakin bagus, sederhana, ekonomis, gesit dan damai. Meningkatnya iptek, utamanya teknologi informasi "information technology" misalnya internet sangat membantu tiap orang memperoleh niat hidupnya pada tempo cepat, mau resmi atau tidak resmi dalam melakukan segala langkah agar ingin mendapatkan profit sesuai "potong kompas" (Arief 2011).

Peningkatan teknologi ialah hasil budaya manusia disamping memperoleh akibat yang baik, yang artinya bisa dipakai agar keperluan umat manusia juga memperoleh akibat negatif terhadap perkembangan manusia dan peradabannya. Akibat negatif yang dituju ialah berhubungan pada dunia kejahatan. Diantara kejahatan yang diakibatkan oleh kemajuan dan peningkatan teknologi informasi dan telekomunikasi ialah yang berhubungan pada pemakaian internet. Perbuatan itu pada Bahasa asing dikatakan juga sebagai "Cyber Crime" (Labib 2005). Cyber Crime yang selanjutnya disingkat "CC" ialah kejahatan yang berkaitan pada komputer, jaringan komputer dan para penggunanya, serta bentuk-bentuk kejahatan konvensional yang memakai atau dibantunya dengan alat-alat computer.

Warga modern yang mengglobal semacam dikala ini, kejahatan yang bisa dicoba dimanapun, baik dari dunia nyata maupun dunia maya "Cyber Space". Perihal itu terjalin sebab masa keuniversalan membuat sebagian kesempatan terbentuknya kejahatan, sehingga dibutuhkan penanganan secara menyeluruh lewat kerjasama antar pihak yang berkeperluan. "CC" ialah diantara satu sisi hitam oleh peningkatan teknologi yang memiliki akibat tidak baik yang sangat jauh untuk segala bentuk kehidupan yang maju dikala ini. Seperti biasanya, "CC" dibagi atas dua tipe, ialah kejahatan yang memakai "Teknologi Data" "TI" selaku sarana serta kejahatan yang memakai sistem serta "TI" selaku target. Cracking serta Hacking termasuk pada kejahatan yang memakai "TI" selaku target. Inti dari "CC" tipe ini merupakan penyerbuan pada "Content (Isi/Substansi), Computer System (Sistem Pembedahan), serta Communication System (Sistem Komunikasi) kepunyaan orang lain ataupun universal di dalam Cyberspace" (Mursito 2005).

Kejahatan pada media sosial beragam wujudnya, mulai dari "kejahatan carding, hijacking, spamming serta cracking". Dari ulasan tersebut, peneliti terfokus mengulas menimpa tindakan Cracking. Wujud kejahatan yang diartikan merupakan kejahatan Cracking. Cracking adalah aktivitas menerobos sistem komputer disebut "PC" yang tujuannya mendapatkan keuntungan dengan cara mengusili serta menghancurkan dalam motivasi terbatas. Cracker merupakan sebutan merengkah yang dikemukakan dari Richard Stallman buat terpacu terhadap peretas yang hanya melaksanakan aktivitas "Black Hat Hacker". Hacker serta Cracker mempunyai kesamaan serta perbandingan. Bersama melaksanakan aktivitas hacking, namun berbeda pada perihal motivasi serta tujuan hacking. Cracker hanya melaksanakan Hacking yang mengganggu, sebaliknya Hacker aslinya ialah spirit para handal buat menolong menuntaskan permasalahan pada sistem PC (Mundzir 2014).

Tindakan seorang cracker tentunya tidak dapat dibiarkan begitu saja yang akan terus-menerus merugikan dan membuat resah masyarakat pengguna internet maupun masyarakat yang tidak mengerti tentang "Cyberspace" dunia maya. Adanya satu peraturan dibentuk tentunya sebagai mengatur tingkah laku warga agar mereka memahami Batasan saat melaksanakan suatu aktivitas di dunia maya atau dunia nyata. Kembali pada hukum positif di Indonesia yang secara umum sudah mempunyai "teori dasar hukum" tentang cracking. Islam mengetahui tentang aturan pidana Islam, yang pastinya tidak sama dari aturan pidana yang berlaku. Tujuan penelitian ini adalah untuk mengetahui pengaturan Hukum tindak pidana dalam pembobolan sistem data keamanan komputer (cracking) dan Bagaimana pertanggungjawaban hukum yang dilakukan oleh pelaku tindak pidana pembobolan sistem data keamanan komputer (cracking).

II. METODE PENELITIAN

Tipe penelitian yang dipakai pada penelitian ini adalah tipe penelitian hukum normatif yakni menganalisis kepustakaan sesuai bahan hukum yang dipakai, baik primer, sekunder dan tersier. Sedangkan pendekatan masalah yang dipakai pada penelitian ini adalah pendekatan Perundang-undangan dan pendekatan Konseptual. (Jonaedi Efendi 2018). Pendekatan Perundang-undangan adalah, pendekatan yang dilakukan dengan menelaah semua peraturan perundang-undangan yang berhubungan dalam permasalahan "isu hukum" yang sedang diteliti. Sedangkan Pendekatan konseptual adalah pendekatan yang beranjak dari pandangan dan doktrin-doktrin yang berkembang di dalam ilmu hukum. Pendekatan ini menjadi penting sebab pemahaman terhadap pandangan atau doktrin yang berkembang dalam ilmu hukum dapat menjadi pijakan untuk membangun argumentasi hukum ketika menyelesaikan isu hukum yang dihadapi. Sumber bahan hukum terdiri dari bahan hukum primer, sekunder dan tersier, bahan hukum primer termasuk "UUD NRI Tahun 1945, KUHP, UU No. 36 Tahun 1999, UU No. 19 Tahun 2016."

Bahan hukum sekunder ialah bahan-bahan hukum yang bisa didapatkan oleh pengkajian kepustakaan yakni dalam membaca buku-buku, jurnal-jurnal hukum, dan artikel yang berkaitan terhadap pertanggungjawaban pidana terhadap pelaku tindak pidana pembobolan sistem data keamanan komputer "cracking". Bahan hukum tersier yang merupakan pendukung dari bahan hukum primer dan bahan hukum sekunder yang mana bahan hukum tersier adalah bahan hukum yang seperti Kamus-Kamus baik itu KBBI maupun Kamus bahasa latin dan bahasa Inggris. Teknik pengumpulan bahan hukum agar mendapatkan bahan-bahan hukum primer, sekunder dan tersier memakai teknik inventarisasi atau penelusuran bahan hukum yang berkaitan lalu diklasifikasi atau dikelompokan dan didokumentasikan, dicatat, dikutip, diringkas, diulas berdasarkan kebutuhan dengan pendekatan kualitatif. Setelah semua bahan hukum terkumpul, selanjutnya dianalisis memakai teknik bersifat sistematis yang diajukan secara deskriptif-analitis, yakni dengan mendeskripsikan bahan hukum terlebih dahulu sesuai sistematis selanjutnya dianalisis berdasarkan dari teknik analisis dan teknik tafsiran serta memakai pendapat yang tertuju pada logika hukum dengan deduktif-induktif.

III. HASIL DAN PEMBAHASAN

1. *Pengaturan Hukum Tindak Pidana Pembobolan Sistem Data Keamanan Komputer (Cracking)*

Cracking merupakan aktivitas membobol sesuatu sistem komputer selanjutnya disebut PC dengan tujuan memperoleh. Sebaliknya orang yang melaksanakan Cracking diucap Cracker. Crack merupakan sesuatu kegiatan pembobolan sesuatu aplikasi berbayar supaya pada saat pendaftarannya bisa dijalani tidak wajib membeli dan juga pembayaran lisensi formal dari sang pembentuk aplikasi tersebut. Perihal ini memiliki itikad kalau kita dapat mendapatkan sebagian persyaratan supaya aplikasi yang berbayar tersebut bisa bekerja secara maksimal. Umumnya pula wajib didaftarkan ataupun sangat tidak memasukkan no pendaftaran untuk dalam aplikasi tersebut. Crack Aplikasi merupakan settingan fitur lunak buat menghapus ataupun menonaktifkan fitur yang dikira tidak diidamkan oleh orang. Cracking Aplikasi, umumnya berkaitan pada tata cara proteksi yaitu terhadap "manipulasi aplikasi, trial atau demo version, no seri, hardware kunci, bertepatan pada pengecekan, CD cek ataupun fitur lunak kendala semacam layar serta adware."

Distribusi serta pemakaian kopian Crack merupakan melanggar hukum di sebagian banyak negeri. Terdapat gugatan hukum atas empat puluh empat fitur lunak Crack, jadi sangat pasti kegiatan Crack merupakan suatu yang melanggar hukum. Cracker umumnya berupaya datang di dalam sesuatu sistem PC tanpa kewenangan "otorisasi". Orang ini umumnya bersifat jahat atau kurang baik, selaku kebalikan dari "hacker", serta umumnya menambah penghasilan saat merambah sesuatu sistem. Cracker ataupun perlengkapan buat Crack aplikasi untuk kebanyakan antivirus umumnya dikira virus maupun trojan. Trojan Horse ialah sebagai program yang seakan menempuh kewajiban sebagaimana seharusnya tetapi tanpa dikenal dia pula melaksanakan kegiatan lain yang umumnya merugikan. Trojan horse umumnya diperlukan untuk membuat suatu "backdoor yang nantinya sanggup dimanfaatkan oleh penyerang buat sanggup masuk ke dalam sistem PC sehingga mempermudah dalam melaksanakan penyerangan. Selain itu pada umumnya dimanfaatkan buat jadi spyware yang sanggup mengenali kegiatan korban dalam memakai PC. Virus PC ialah program yang sanggup menduplikasi diri sehingga nantinya hendak menyebar serta menyisipkan dirinya ke dalam program executable serta jenis file yang lain. Filosofi virus dalam pc sama pengertiannya dengan virus dalam kehidupan. Virus dikategorikan selaku program yang mengusik, malicious aplikasi malware".

Telah diuraikan di awal bahwa jika tetap berpatokan pada asas legalitas, maka akan sulit bagi kita untuk menerapkan peraturan yang ada dalam KUHP terhadap kasus Cracking. Berkaitan dengan itu, perlu suatu penafsiran terhadap undang-undang sehingga suatu perbuatan yang tidak diatur dalam undang-undang tidak begitu saja dikesampingkan karena alasan tidak ada peraturan atau ketentuannya. Keberanian hakim untuk menafsirkan undang-undang merupakan bentuk antisipasi terhadap "CC", khususnya mengenai Cracking. Penerapan KUHP terhadap tindak pidana cracking memerlukan pemilah-milahan, perbuatan mana yang substansinya hampir sama dengan rumusan tindak pidana biasa dalam KUHP. Dalam KUHP terdapat aturan yang mengatur perihal perusakan atau penghancuran tersebut, yaitu pada Pasal 406 ayat (1) KUHP, yang rumusannya sebagai berikut: "Barangsiapa dengan sengaja dan melawan hukum, menghancurkan merusakkan, membuat tidak dapat dipakai atau menghilangkan barang sesuatu baik seluruhnya atau sebagian adalah kepunyaan orang lain, diancam dengan pidana penjara dua tahun delapan bulan penjara atau denda paling banyak empat ribu lima ratus rupiah." Tanggal 23 April 2008 telah diundangkan UU ITE, UU ini bukanlah UU tindak pidana khusus, selain itu juga terkait mengenai pengaturan tentang pengelolaan ITE dalam tujuan pembangunan, namun UU ini juga menjaga dari pengaruh negatif oleh manfaat peningkatan teknologi ITE. Yakni dalam ditetapkannya hukum pidana khususnya mengenai perbuatan pidana yang menyerang keperluan hukum individu, warga, maupun keperluan hukum negara dalam memakai majunya teknologi ITE, atau biasa dikatakan dengan perbuatan pidana Cracking.

UU ITE sudah menetapkan berbagai perbuatan mana yang tercantum perbuatan pidana di bidang ITE "Cracking" dan sudah ditetapkan berbagai unsur perbuatan pidana dan penyerangan kepada bermacam keperluan hukum dalam bentuk berbagai rumusan perbuatan pidana tertentu. Perbuatan pidana Cracking pada UU ITE diatur dalam 9 Pasal, dari Pasal 27 sampai pada Pasal 35. Dari 9 Pasal tersebut dirumuskan 20 bentuk atau jenis perbuatan pidana ITE. Pasal 36 tidak mencantumkan jenis perbuatan pidana ITE tertentu, akan tetapi mencantumkan mengenai dasar pemberatan pidana yang ditempatkan pada akibat membuat rugi orang lain terhadap perbuatan pidana yang ditetapkan pada Pasal 27 hingga Pasal 35 UU ITE.

2. *Pertanggungjawaban yang Dilakukan oleh Pelaku Tindak Pidana Pembobolan Sistem Data Keamanan Komputer (Cracking)*

Dalam hal melaksanakan penegakan hukum khususnya pada bidang kejahatan dunia maya, kejahatan tersebut mempunyai jarak yang amat luas tanpa mengetahui perbatasan wilayah teritorial suatu negara sebab kejahatan ini sifatnya "transnasional". Bentuk kejahatan yang tidak mengetahui perbatasan ini mengwajibkan yurisdiksi suatu negara terhubung langsung di dalamnya sebab sangat jauh dari capaian suatu negara. Jika tidak melakukan hubungan antar negara saat melaksanakan penindakan serta menegakkan hukum yang seharusnya, kejahatan yang

sifatnya transnasional tersebut bisa berakibat permasalahan individu terkait pada kekuasaan (Ayu Suanti Karnadi Singgi I Gusti, Bagus Suryawan I Gusti 2020).

Pembobolan mewujudkan suatu langkah maupun aktivitas menjebolkan sesuatu. Membobol yang artinya "menjebol, mengacaukan, mendobrak, dan mengacaukan dengan kekejaman, atau mendobrak dengan suatu paksaan. Pertanggungjawaban pidana yang dasarnya menyimpan arti timbal balik atas tindakan si pembuat pidana atas kejahatan yang dilakukan. Maka, tanggung jawab kejahatan isinya unsur objek dan unsur subjek. Maksudnya, menurut faktual pembuat kejahatan sudah berbuat delik kejahatan kriminalitas dimana secara individu yang membuat kejahatan pantas disalahkan atas delik yang dilakukan itu maka bisa dihukum" (Purwadi Sastra Komang Saeramessatya 2020).

Kejahatan atau perbuatan kriminal ialah sebagai bentuk sebagai "perilaku menyimpang yang selalu ada dan melekat pada tiap bentuk masyarakat. Perilaku menyimpang itu merupakan suatu ancaman yang nyata atau ancaman terhadap norma-norma sosial yang mendasari kehidupan atau keteraturan sosial, dapat menimbulkan ketegangan individual maupun ketegangan-ketegangan sosial, dan merupakan ancaman riil atau potensi bagi berlangsungnya keteraturan sosial".

Cracking adalah aktivitas membobol sistem komputer yang bertujuan "mengambil keuntungan dengan cara merusak dan menghancurkan dengan motivasi tertentu. Cracker ialah istilah perengkah yang diajukan oleh Richard Stallman untuk mengacu kepada peretas yang cenderung melakukan kegiatan Black Hat Hacker. Cracker merupakan seseorang yang masuk tanpa izin atau illegal ke dalam sebuah sistem komputer" (Christiara Febriliani, Ismunarno 2019). Istilah Cracker memiliki kecenderungan hacker pada penjelasan "white hat Hacker". Hacker mempunyai kesamaan dan ketidaksamaan. Sama-sama melaksanakan aktivitas Hacking, tetapi tidak sama dari hal motivasi dan tujuan Hackingnya. Cracker cenderung melaksanakan hacking yang merusak, selain itu Hacker sejatinya merupakan spirit para profesional untuk membantu menyelesaikan masalah pada sistem komputer. Dalam UU ITE tindak pidana Cracking telah diatur dan dirumuskan dalam pasal-pasal yang dapat menjerat pelaku tindak pidana Cracking. Pada dasarnya tindak pidana Cracking diatur secara umum pada Pasal 30 UU ITE yang berbunyi sebagai berikut: "Pertama, Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun. Kedua, Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik. Ketiga, Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan." Pasal 30 ayat (1) UU ITE "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau Sistem Elektronik milik orang lain dengan cara apapun." Pasal 30 Ayat (2) UU ITE "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apapun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik". Pasal 30 ayat (3) UU ITE: "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan. Sanksi pidana yang ada pada ketentuan pidana Pasal 46 ayat (1) UU ITE: Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama enam tahun dan/atau denda paling banyak enam ratus juta rupiah. Sanksi pidana Pasal 30 ayat (3) terdapat pada Pasal 46 ayat (3) UU ITE: hukuman pidana penjara paling lama delapan tahun dan/atau denda paling banyak delapan ratus juta rupiah. Yang dapat dijerat oleh ketentuan pasal 46 ayat (3) ialah pihak yang melakukan tindakan yang dilarang sebagaimana dimaksud pada pasal tersebut seperti menjebol sistem keamanan yang membatasi dengan berdasarkan kategorisasi atau klasifikasi pengguna beserta tingkat kewenangan yang ditentukan" (Hakim 2007).

Sebagai salah satu bentuk pertanggungjawaban pidana dalam pelaku tindak pidana pembobolan sistem data keamanan komputer (Cracking) khususnya di Indonesia dapat digambarkan dalam contoh kasus sebagai berikut: "Pada tahun 2013 sudah terlaksana

pembobolan website individu milik Presiden Republik Indonesia Susilo Bambang Yudhoyono yaitu http://presidensby.info yang dilakukan oleh pemuda asal Jember bernama WYA. Terdakwa WYA ditangkap di warnet tempat dia bekerja yaitu Warnet Surya Com, Wildan melakukan peretasan terhadap website http://presidensby.info dengan cara terlebih dahulu melakukan akses ilegal ke dalam web hosting http://techspace.co.id yang kemudian dalam pengaksesan hal tersebut ditemukan DNS Server dari domain http://presidensby.info sehingga terdakwa dapat mengakses website milik Presiden Susilo Bambang Yudhoyono tersebut. Website http://presidensby.info kemudian setelah diretas oleh terdakwa berubah tampilan websitenya menjadi hitam dengan lambang tengkorak bertuliskan Jember Hacker Team." Oleh sebab itu tersangka digugat pada Pasal 46 ayat (1) Jo. Pasal 30 ayat (1) UU ITE, "bahwa tindakan terdakwa W Y A dalam melakukan peretasan website pribadi milik Presiden S B Y telah memenuhi unsur-unsur didalam Pasal 30 ayat (1) Jo Pasal 40 ayat (1) yang dimana unsur-unsurnya yaitu: Setiap Orang dan "dengan sengaja dan tanpa hak melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun" yang dilakukan Terdakwa W Y A telah terpenuhi".

Majelis Hakim memberikan vonis pidana kepada tersangka dengan "pidana penjara selama enam bulan dan denda sebesar dua ratus lima puluh ribu subsidair lima belas hari kurungan, Majelis Hakim menjatuhkan pidana sesuai dengan tuntutan Jaksa Penuntut Umum yang menyatakan bahwa terdakwa Wildan Yani Ashari Alias Yayan Alias MJL 007 bersalah melakukan tindak pidana dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun, sebagaimana diatur dalam Pasal 46 ayat (1) Jo. Pasal 30 ayat (1) UU ITE dalam dakwaan alternatif ke dua."

IV. KESIMPULAN DAN SARAN

1. *Kesimpulan*

Berdasarkan adanya penelitian serta pembahasan pada uraian diatas, maka bisa disimpulkan menjadi: Pengaturan hukum tindak pidana dalam pembobolan sistem data keamanan komputer cracking ialah suatu aturan yang menjelaskan apa itu aktivitas membobol sistem PC yang tujuannya memperoleh keuntungan yang caranya merusak dan menghancurkan dengan motivasi. Mengenai tindakan perusakan atau penghancuran diatur pada KUHP Pasal 406 ayat (1). Pengaturan tindak pidana Cracking diatur pada UU ITE yang terdapat dalam 9 pasal, yakni "dari Pasal 27 sampai dengan Pasal 35. UU ITE telah menetapkan perbuatan-perbuatan mana yang termasuk tindak pidana di bidang Informasi dan Transaksi Elektronik terutama tindak pidana cracking dan telah ditentukan unsur-unsur tindak pidana dan penyerangan terhadap berbagai kepentingan hukum dalam bentuk rumusan-rumusan tindak pidana tertentu."

Pertanggungjawaban hukum yang dilakukan oleh pelaku tindak pidana pembobolan sistem data keamanan komputer (Cracking) sudah diatur pada UU ITE perbuatan pidana Cracking dan dirumuskan pada berbagai pasal yang bisa mengenai pelaku perbuatan pidana Cracking. Perumusan cracking sebagai perbuatan pidana dalam UU ITE sesuai dengan Pasal 30 diancam dengan "sanksi pidana yang terdapat dalam ketentuan pidana Pasal 46. Pemberian sanksi pidana tersebut merupakan sebagai bentuk pertanggungjawaban yang sah dalam putusan hakim yang diberikan kepada pelaku tindak pidana Cracking sesuai dengan unsur-unsur serta alat bukti persidangan sebagai acuan dalam pemberian hukuman."

2. *Saran*

Simpulan yang sudah diuraikan diatas mencetuskan beberapa saran yang bisa diberikan, yaitu Bagi Pemerintah, pemerintah diharapkan untuk lebih responsive dalam menerima dan memproses laporan masyarakat terkait keluhan transaksi elektronik seperti kejahatan Cracking ini dan pemerintah diharapkan untuk lebih memahami kecanggihan teknologi masa kini serta memberikan sosialisasi mengenai penggunaan teknologi yang baik dan benar serta menekankan mengenai pengaturan penggunaan teknologi agar tidak ada masyarakat yang menyalahgunakan kecanggihan teknologi ini sebagai alat untuk melakukan tindakan melawan hukum (kejahatan). Karena tindakan Cracking ini selain dapat merugikan individu dapat pula merugikan negara,

maka dari itu pemerintah harus lebih waspada dalam mengawasi masyarakat dalam penggunaan teknologi.

Bagi Masyarakat, diharapkan dengan adanya kemajuan dan kecanggihan teknologi dapat membantu dan meringankan pekerjaan di masyarakat namun tetap dalam penggunaan yang lazim agar masyarakat tidak menyalahgunakan teknologi tersebut untuk mencari keuntungan dengan cara merugikan pihak lain dan melakukan tindakan yang dilanggar oleh hukum. Bagi Pelaku, diharapkan dengan apa yang sudah diperbuat dengan unsur-unsur perbuatannya yang tentu saja sudah melanggar hukum tentu pelaku harus mempertanggungjawabkan apa yang telah diperbuat sesuai dengan hukuman yang diberikan dan diharapkan menimbulkan efek jera kepada pelaku untuk tidak terjadi kembali sehingga baik itu perbuatan yang sama maupun perbuatan melawan hukum lainnya.

DAFTAR PUSTAKA

Arief, Barda Nawawi. 2011. *Pornografi, Cyberporn dan Porno Aksi*. Semarang: Badan Penerbit Universitas Diponegoro.

Ayu Suanti Karnadi Singgi I Gusti, Bagus Suryawan I Gusti, Gede Sugiartha I. Nyoman. 2020. "Penegakan Hukum terhadap Tindak Pidana Peretasan sebagai Bentuk Kejahatan Mayantara (Cyber Crime)." *Jurnal Konstruksi Hukum* 1(2).

Christiara Febriliani, Ismunarno, Diana Lukitasari. 2019. "Kajian Etiologi Kriminal Tindak Pidana Cracking Sistem Operasi Windows di Provinsi Daerah Istimewa Yogyakarta." *Jurnal Hukum Pidana dan Penanggulangan Kejahatan* 8(3).

Hakim, Abdul. 2007. *Pengantar Hukum Ketenagakerjaan Indonesia*. Bandung: PT. Citra Aditya Bakti.

Jonaedi Efendi, Johnny Ibrahim. 2018. *Metode Penelitian Hukum Normatif dan Empiris*. Depok: Prenadamedia.

Labib, Abdul Wahid dan Moh. 2005. *Kejahatan Mayantara Cyber Crime*. Bandung: Refika Aditama.

Mundzir, MF. 2014. *Tips & Trik Belajar Hacker*. Yogyakarta: Notebook.

Mursito, Danan. 2005. *Pendekatan Hukum untuk Keamanan Dunia Cyber serta Urgensi Cyberlaw bagi Indonesia*. Jakarta: Tesis Fakultas Ilmu Komputer Universitas Indonesia.

Purwadi Sastra Komang Saeramessatya, Putu Budiartha I. Nyoman dan Gede Sugiartha I. Nyoman. 2020. "Jurnal Analogi Hukum, Sanksi Pidana terhadap Tindak Pidana Pembobolan Rekening melalui Anjungan Tunai Mandiri (ATM)." *Fakultas Hukum Universitas Warmadewa, Bali* 2(2).

Sutarman. 2007. *Cyber Crime, Modus Operandi dan Penanggulangannya*. Yogyakarta: LaksBang Pressindo.