Jurnal Hukum Progresif

Vol 7 No 2, Feb 2024
EISSN : 24490120

PENEGAKAN HUKUM KEJAHATAN TEKNOLOGI INFORMASI (CYBER CRIME) MENGENAI TINDAK PIDANA PERETASAN BERDASARKAN UNDANG-UNDANG NOMOR 19 TAHUN 2016 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK (ITE)

Ahmad Sadriansyah Yusuf
a.sadriansyahyusuf@gmail.com
Universitas Bandar Lampung

Abstrak: Sejalan dengan teknologi dan informasi yang kian bertumbuh dengan pesat, ada banyak sekali fasilitas yang tersedia di dunia maya. Pertumbuhan teknologi ini juga memberikan peluang untuk para pelaku kejahatan khususnya kejahatan di dunia maya. Kejahatan dunia maya merupakan bentuk atau dimensi baru kejahatan yang saat ini telah banyak mendapatkan perhatian dari dunia internasional. Salah satu kejahatan dunia maya yang dimaksud ini adalah kejahatan peretasan. Berdasarkan latar belakang tersebut, penelitian ini dilakukan dengan tujuan mendeskripsikan bagaimana penegakan hukum terhadap tindak pidana peretasan (hacking) dan bagaimana upaya menanggulangi kejahatan cyber crime. Penelitian ini dilakukan dengan menggunakan metode penelitian hukum normatif dan pendekatan perundang-undangan. Hasil dari penelitian ini me-nunjukkan bahwa penegakan hukum terhadap tindak pidana peretasan diatur dalam Undang-Undang Nomor 19 Tahun 2016 perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pelaku akan diberikan sanksi pidana berupa kurungan penjara dan denda atas pelanggaran di bidang peretasan. Selain itu, upaya pemberantasan kejahatan cyber crime ini mengacu kepada Undang-Undang Informasi dan Transaksi Elektronik yang dilakukan dngan tindakan preventif dan represif. Oleh karena itu, tindak pidana peretasan yang termasuk dalam ranah kejahatan cyber telah diatur dalam pasal 30 ayat (1), (2), dan (3) Undang-Undang Informasi dan Transaksi Elektronik, sedangkan hukumannya diatur dalam pasal 46 ayat (1), (2), dan (3) dari Undang-Undang Informasi dan Transaksi Elektronik.
Kata Kunci: cyber crime, hacking, Penegakan Hukum, Undang-Undang.

Abstract*: Along with technological developments, there are a lot of facilities available in cyberspace. The development of this technology can also provide opportunities for criminals, especially crimes in cyberspace. Cybercrime is a new form or dimension of a crime that is currently receiving a lot of attention from the international community. One type of cybercrime is hacking. Based on this background, this research was conducted with the aim of describing law enforcement against criminal acts of hacking and the efforts to deal with cybercrime. This research was conducted using normative legal research methods and statutory approaches. The results of this study showed that law enforcement against criminal acts of hacking is regulated in Law Number 19 of 2016 amending Law Number 11 of 2008 concerning Electronic Information and Transactions. The perpetrator will be given criminal sanctions in the form of imprisonment and fines for violations in the field of hacking. In addition, efforts to eradicate cybercrime refers to the Law on Information and Electronic Transactions which is carried out with preventive and repressive measures. Therefore, the criminal act of hacking which is included in the realm of cybercrime has been regulated in Article 30 paragraph (1), (2) and (3) of the ITE Law, while the punishment is regulated in Article 46 paragraph (1), (2), and (3) of the ITE Law. In this regard, the government has taken various countermeasures in the form of preventive and repressive measures.*
Keywords*: cyber crime, hacking, Law Enforcement, Law Regulated*

PENDAHULUAN

Perkembangan teknologi informasi yang semakin pesat dan tanpa batas selalu memiliki nilai penggunaan yang dapat dilihat dari sisi positif maupun sisi negatif. Efek tambahan dari globalisasi adalah ekspansi yang cepat dari dunia maya, yang membawa data dalam jumlah besar dengan kecepatan tinggi. Sebagian kecil orang percaya bahwa globalisasi pada akhirnya akan meruntuhkan batasan-batasan antar negara dan budaya. Hingga semua hal menyatu dalam keluarga global, pasar global, dan budaya global. Melalui internet, segala jenis informasi dapat diakses melalui dunia maya.

Dampak dari adanya globalisasi menjadi salah satu penyebab perkembangan teknologi berkembang pesat dan tanpa batas dan didukung dengan daya fikir manusia yang menimbulkan sebuah pengetahuan baru. Pengetahuan yang baru tersebut, tidak semua manusia dapat menggunakannya dengan bijak dan benar, sehingga hal tersebut dapat merugikan orang lain. Salah satu contohnya adalah tindak pidana peretasan atau hacking yang timbul akibat dampak negatif kemajuan teknologi.

Kejahatan teknologi informasi (cyber crime) dibagi menjadi 2 (dua) kategori, yakni cyber crime dalam arti sempit dan dalam arti luas. Cyber crime dalam pengertian sempit adalah kejahatan terhadap sistem komputer, sedangkan cyber crime dalam arti luas mencakup kejahatan terhadap sistem atau jaringan komputer dan kejahatan yang menggunakan sarana komputer.

Tindak pidana peretasan sudah diatur dalam sistem hukum di Indonesia. Aksi peretasan sendiri telah bertentangan dengan ketentuan perlindungan hak kebebasan berpendapat dan menyampaikan informasi baik dalam instrumen nasional maupun inter-nasional yang telah diatur dalam Undang-Undang No.19 Tahun 2016 perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang selanjutnya disebut dengan UUITE.

Tindakan peretasan yang semakin marak inilah yang kemudian menimbulkan banyak kerugian berupa materiil dan non materiil yang kerugian nya tersebut ditanggung oleh korban sendiri. Peretasan tidak hanya dilakukan pada situs web tetapi juga pada akun sosial media milik perorangan.

Berdasarkan latar belakang yang telah diuraikan di atas, penelitian ini dilakukan dengan tujuan mendeskripsikan bagaimana penegakan hukum terhadap tindak pidana peretasan (hacking) dan bagaimana upaya menanggulangi kejahatan cyber crime..

METODE PENELITIAN

Metode pendekatan yang dilakukan dalam penelitian hukum ini adalah dengan menggunakan metode pendekatan yuridis normatif. Penelitian hukum normatif merupakan penelitian yang mengutamakan data kepustakaan yaitu penelitian terhadap data sekunder. Data sekunder tersebut dapat berupa bahan hukum primer, sekunder, maupun tersier.

Sumber bahan hukum yang digunakan bersumber dari sumber kepustakaan berupa sumber bahan hukum primer berdasarkan atas peraturan Perundang-Undangan mengenai Informasi dan Transaksi Elektronik. Bahan hukum sekunder diperoleh dari berbagai macam bacaan atau literatur dan peraturan Perundang-Undangan dan pendapat ahli hukum yang berkaitan dengan tulisan ini. Teknik pengumpulan bahan hukum dilakukan dengan mengumpulkan berbagai buku, literatur-literatur, serta bahan hukum lainnya yang berkaitan dengan tulisan ini. Data yang sudah terkumpul dianalisis menggunakan metode kualitatif. Hasil analisis data kemudian disajikan secara deskripti.[1]

PEMBAHASAN

Penegakan Hukum Terhadap Tindak Pidana Peretasan (hacking)

Cyber crime timbul akibat adanya kemajuan teknologi yang berkembang pesat dan menimbulkan dampak positif dan negatif. Dampak positif dari teknologi adalah adanya e-mail, internet, banking, dan

[1] Soejono dan H Abdurahman, "*Metode Penelitian Hukum",* Rineka Cipta, Jakarta, Tahun 2003, Halaman 40-54

lain sebagainya. Tetapi, perkembangan ini juga membawa pengaruh negatif seperti adanya tindak pidana peretasan (hacking) yang dilakukan dengan tujuan untuk memperoleh informasi atau data-data penting milik seseorang atau sekelompok orang.

Kejahatan cyber crime ini dapat dikategorikan sebagai kejahatan yang relatif baru jika dibandingkan dengan lainnya. Meskipun kejahatan ini telah muncul pada awal tahun 1961, namun masyarakat masih belum begitu banyak yang mengetahui kejahatan ini.

Kemampuan membuat suatu program yang disalahgunakan oleh seseorang yang tidak bertanggungjawab menyebabkan terjadinya sebuah pelanggaran norma atau hukum yang berlaku. Salah satu contohnya adalah tindakan meretas situs web atau akun sosial media yang bersifat pribadi milik orang lain.

Ketentuan khusus yang mengatur tindak pidana peretasan telah termuat dalam pasal 30 ayat (1),(2), dan (3) UU ITE. Pasal ini menjelaskan bahwa setiap orang yang mencobaa masuk atau mengakses sistem elektronik milik orang lain dengan cara apapun dengan sengaja dan tanpa hak melawan hukum. Pasal ini berkaitan dengan pasal 46 ayat (1), (2), dan (3) UU ITE yang mengatur mengenai sanksi pidana atas pelanggaran yang tercantum dalam pasal 30 tersebut.

Dalam melakukan penegakan hukum khususnya bidang kejahatan cyber crime, memiliki jangkauan yang sangat luas tanpa mengenal batas wilayah teritorial suatu negara karena kejahatan ini bersifat transnasional. Setiap negara harus memiliki yurisdiksi yang dapat terlibat langsung di dalamnya. Jika melakukannya tanpa adanya kerjasama antar negara dalam upaya pemberantasan serta penegakan hukum yang sebagaimana diatur, maka kejahatan transnasional ini akan menimbul-kan masalah yang berkelanjutan.

Penegakan hukum pada dasarnya adalah bagian dari kebijakan kriminal yang tidak terpisahkan dari kebijakan sosial. Kebijakan-kebijakan tersebut kemudian di-terapkan dalam sistem peradilan pidana yang memiliki beberapa dimensi fungsional. Di sisi lain, sistem peradilan pidana berfungsi sebagai alat sosial untuk mengatur dan mengendalikan kejahatan pada tingkat tertentu (sistem pencegahan kejahatan) dan mengurangi kejahatan yang dilakukan oleh mereka.

Seringkali masalah ini menjadi rumit karena kendala teritorial batas negara. Yurisdiksi dalam hal ini telah mencakup dan bertanggungjawab atas orang, benda, atau peristiwa hukum yang terjadi di dalamnya. Hukum Internasional telah membagi beberapa prinsip yang dapat menjadi acuan dalam masalah yurisdiksi yakni prinsip teritorial, prinsip nasionalitas, prinsip perlindungan, serta prinsip universal:

1. Prinsip teritorial: suatu negara memilki kewenangan untuk membuat per-aturan perundang-undangan yang terkait dengan perbuatan pidana dan memberlakukannya dalam wilayahnya.
2. Prinsip nasionalitas: negara dianggap berhak untuk mengadili setiap warga-negaranya terhadap segala kejahatan yang dilakukannya diamanapun warga negara tersebut berada.
3. Prinsip perlindungan: prinsip ini lebih bersifat melindungi kepentingan vital negara.
4. Prinsip universal:prinsip ini bersifat umum dimana dalam yurisdiksi setiap ne-gara dianggap berhak atau dapat mengadili suatu kejahatan tertentu yang dianggap membahayakan masyarakat dalam lingkup internasional.

Salah satu cara yang dapat dilakukan oleh negara yang memilki yurisdiksi ter-hadap pelaku kejahatan yang berada di negara lain adalah dengan meminta kepada ne-gara di tempat pelaku berada agar dapat lebih leluasa untuk menangkap pelaku tersebut. Yurisdiksi terhadap cyber crime khususnya dalam tindak pidana peretasan (hacking) dapat dilaksanakan melalui kerjasama internasional berupa ekstradisi, bantuan hukum timbal balik, dan kerjasama antar penegak hukum.

Ruang lingkup berlakunya hukum pidana dalam kejahatan cyber crime telah di-atur dalam Kitab Undang-Undang Hukum Pidana Indonesia (KUHP) dalam BAB I Buku Kesatu mengenai batas-batas berlakunya suatu aturan dalam hukum pidana, yang mana termuat sembilan pasal dimulai dari pasal 1 sampai pasal 9. Pasal 1 diatur mengenai batas berlakunya suatu hukum pidana berdasarkan waktu,

sedangkan untuk pasal 2 sampai dengan pasal 9 memuat mengenai batas berlakunya hukum pidana berdasarkan atas tempat terjadinya.

Berdasarkan uraian di atas, penegakan hukum mengenai tindak pidana pereta-san yang masuk dalam ranah kejahatan cyber crime dapat dimulai dan dibangun melalui kesadaran masing-masing masyarakat dan penanganan untuk menyelesaikan kasus cyber crime ini diharuskan menggunakan teknologi.

Upaya Menanggulangi Kejahatan Cyber Crime

Undang-Undang No 19 Tahun 2016 perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik merupakan piranti hukum terbesar yang diharapkan mampu mengakomodir segala jenis pelanggaran dalam bidang teknologi dan infromatika. Disamping terdapat perlindungan hukum, disana juga terdapat ancaman sanksi pidana atas pelanggaran yang dilakukan.

Tindak pidana peretasan yang diatur dalam pasal 30 ayat (1),(2), dan (3) mengan-dung unsur sebagai berikut:

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". Dalam pasal ini sudah jelas tertera unsur setiap orang, unsur dengan sengaja dan tanpa hak melawan hukum, unsur mngakses komputer dan/atau sistem elektronik milik orang lain, serta unsur dengan cara apapun.

1. Unsur setiap orang

Dalam unsur ini setiap orang yang dimaksud adalah orang sebagai subjek hukum yang dapat bertanggungjawab dan cakap hukum berdasarkan atas perundang- undangan.

2. Unsur dengan sengaja dan tanpa hak melawan hukum

Unsur ini merujuk pada niat atau kesengjaan dan penuh dengan kesadaran dari orang tersebut dalam melakukan suatu tindakan yang melawan hukum.

3. Unsur mengakses komputer dan/atau sistem elektronik untuk orang lain

Unsur ini memberi gambaran bahwa sistem elektronik milik orang lain berarti hal yang bersifat pribadi milik orang lain, dan bukan bersifat umum.

4. Unsur dengan cara apapun

Dengan cara apapun yang dimaksud adalah baik peretas tersebut masuk menggunakan perangkat milik korban yang diretas atau melalui perangkat atau jaringan internet.

Dalam pasal 30 ayat (1) ini setiap orang dilarang secara tegas masuk kedalam sistem elektronik milik orang lain yang bersifat pribadi atau privat. Sanksi pidana yang dapat menjerat pelaku peretasan tersebut telah diatur dengan jelas pada pasal 46 ayat (1) yang berbunyi: "setiap orang yang memenuhi unsur sebagaimana dimaksud pada pasal 30 ayat (1), dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 600.000.000 (enam ratus juta rupiah).

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". Dalam pasal 30 ayat (2) ini memiliki unsur yang sama pada pasal 30 ayat (1), namun ayat (2) terdapat unsur memperoleh informasi elektronik dan/atau dokumen elektronik. Hal tersebut berarti orang yang mencoba masuk kedalam sistem tersebut memiliki tujuan untuk mencuri suatu data atau informasi elektronik yang terdapat dalam sistem milik korban. Pasal 30 ayat (2) ini berkaitan langsung dengan pasal 46 ayat (2) mengenai ancaman pidana jika melanggar ketentuan pasal 30 ayat (2).

Pasal 46 ayat (2): "setiap orang yang memenuhi unsur sebagaimana dimaksud pada pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp. 700.000.000 (tujuh ratus juta rupiah)".

Pada pasal 30 ayat (3) terdapat unsur dengan melanggar, menerobos, melampaui, atau menjebol sistem keamanan. Unsur ini memberi indikasi bahwa pelaku peretasan atau hacker melakukan tindakan tersebut dengan cara menerobos sistem keamanan kompu-ter tersebut. Untuk sanksi pidananya sendiri

telah diatur dalam pasal 46 ayat (3) dimana untuk pelanggaran tersebut dikenakan hukuman kurungan penjara sebert-beratnya 8 (delapan) tahun dan/atau membayar denda sebanyak-banyaknya Rp. 800.000.000 (dela-pan ratus juta rupiah).

Pemberatan penajtuhan pidana bagi pelau peretasan berdasarkan atas objek dan subjek dari tindak pidana yang bersangkutan yaitu:

1. Berdasarkan objek tindak pidana peretasan atau hacking

a. Pasal 52 ayat (2) UU ITE

Dalam pasal ini pemberatan penjatuhan hukuman pidana bagi pelaku tindak pidana peretasan apabila objek dari pelanggaran ini adalah sistem elekronik yang dimiliki oleh pemerintah atau sistem yang dipergunakan untuk pelaya-nan publik.

b. Pasal 52 ayat (3) UU ITE

Pemberatan dalam pasal ini dapat dijatuhkan apabila pelaku peretasan me-nyerang situs web milik pemerintah yang berhubungan langsung dengan ke-amanan atau stabilitas negara.

2. Berdasarkan atas subjek tindak pidana peretasan atau hacking

Pasal 52 ayat (4) UU ITE yaitu pemberatan dapat dijatuhkan apabila terbukti bahwa peretasan tersebut dilakukan oleh korporasi.

Pemerintah dalam melakukan upaya menanggulangi kejahatan cyber crime dengan skala nasional telah menerapkan peraturan perundang-undangan yang mengatur secara khusus mengenai IT pada Undang-Undang No. 19 Tahun 2016 perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Keja-hatan yang tanpa mengenal batas ini bisa saja sangat membahayakan jika tidak ditang-gulangi dan tidak memiliki payung hukum yang kuat untuk mengakomodasinya.

Selain itu, upaya yang dapat dilakukan negara untuk mencegah tindakan pereta-san ini adalah dengan menghadirkan suatu lembaga khusus yang bernama Badan Siber dan Sandi Negara (BSSN) yang mempunya tugas melaksanakan keamanan siber secara efekif dan efisien dengan memanfaatkan, mengembangkan, dan mengkonsolidasikan semua unsur yang terkait dengan keamanan siber.

Tugas legislasi nasional pemerintah juga memiliki peran penting dalam melin-dungi kekuatan hukum peraturan perundang-undangan, khususnya Undang-Undang No. 19 Tahun 2016 perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Oleh sebab itu, berbagai perubahan atau pembentukan hukum Indonesia harus menyesuaikan kebutuhan hukum sesuai dengan tingkat perkembangan di segala bidang.

KESIMPULAN

Berdasarkan hasil dan pembahasan di atas, ada beberapa simpulan yang dapat dibuat, yaitu:

Pertama, penegakan hukum yang dilakukan terhadap tindak pidana peretasan atau hacking yang tergolong ke dalam ranah kejahatan cyber crime dilakukan dengan menerapkan Undang-Undang No. 19 Tahun 2016 yang merupakan perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-undang ini akan memberikan sanksi berupa membayar denda serta hukuman kurungan penjara sebagaimana telah dicantumkan dalam pasal 30 ayat (1), (2), dan (3). Sanski pidananya telah diatur dalam pasal 46 ayat (1),(2), dan (3).

Kedua, upaya dalam melakukan penanggulangan kejahatan mayantara atau cyber crime telah mengacu pada Undang-Udang Informasi dan Transaksi Elektronik, dan berbagai upaya lain seperti dengan menghadirkan suatu lembaga khusus yang bernama Badan Siber dan Sandi Negara (BSSN) yang mempunya tugas melaksanakan keamanan siber secara efekif dan efisien dengan memanfaatkan, mengembangkan, dan mengkonsoli-dasikan semua unsur yang terkait dengan keamanan siber.

DAFTAR PUSTAKA

A. Buku

Johanes Irawan E. (2021). Pelaksanaan Yurisdiksi Universal dalam Kedaulatan Nasional Negara-Negara. RajaGrafindo Persada, Depok. hlm. 11-17

Yosua Putra Iskandar, dkk. (2021). Hak Asasi Manusia & Pandemi Covid-19. Zifatama Jawara, Sidoarjo. hlm.66

B. Jurnal

Hasan, Z., Apriano, I., Simatupang, Y., & Muntari, A. (2023). Penegakan Hukum Terhadap Pelaku Tindak Pidana Perjudian Online. Jurnal Multidisiplin Dehasen (MUDE), 2(3), 375-380. https://doi.org/10.37676/mude.v2i3.4153

Hasan, Z., Cantika, A. B., H. L., & Indiana, P. N. K. (2023). Harmonisasi Sumber Hukum: Jurisprudensi Dan Konstitusi Tertulis Dalam Filsafat Dan Penerapan Hukum. Innovative: Journal Of Social Science Research, 3(2), 7959-7964. https://doi.org/10.31004/innovative.v3i2.1334

Indri S,M., Sabrina, A., Putri, B.M., Gistaloka, A., & Hasan, Z. (2024). Kejahatan Mayantara Berupa Tindak Pidana Perjudian Melalui Media Elektronik. Innovative: Journal of Social Science Research, 4 (1).4409-4418. https://doi.org/10.31004/ innovative.v4i1.7851

Nugroho, I. Y. (2015). Sanksi Hukum Kejahatan Peretasan Website Presiden Republik Indonesia. AL-DAULAH: JURNAL HUKUM DAN PERUNDANGAN ISLAM, 5(1),171-203