UPAYA PENEGAKAN HUKUM TERHADAP TINDAK PIDANA AKSES TANPA HAK DIHUBUNGKAN DENGAN UNDANG-UNDANG UNDANG NOMOR 19 TAHUN 2016 ATAS PERUBAHAN UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

LEGAL ENFORCEMENT EFFORTS ON CRIMINAL ACCESS ACTION WITHOUT RELATIONSHIP RELATED TO LAW NUMBER 19 OF 2016 FOR AMENDMENT TO LAW NUMBER 11 OF 2008 CONCERNING ELECTRONIC INFORMATION AND TRANSACTIONS

Bambang Meiryawan, Hernawati
Program Pascasarjana Universitas Langlangbuana
jurnalpascaunla@gmail.com

ABSTRAK

Kejahatan berkembang seiring dengan kemajuan peradaban manusia, kejahatan teknologi informasi telah berkembang seiring dengan semakin berkembangnya Teknologi Informasi, salah satunya adalah tindak pidana akses tanpa hak yang sangat merugikan pihak lain, akibat akses tanpa hak ini dapat menimbulkan kerugian yang sangat besar baik secara finansial maupun non finansial, dalam kasus pembobolan tiket.com pemilik server dirugikan senilai 5 (lima) milyar rupiah, dan banyak kasus tindak pidana akses tanpa hak yang sangat merugikan, antara lain pembobolan situs KPU, pembobolan server milik institusi pemerintah lainnya, berdasarkan latar belakang tersebut penulis menemukan beberapa permasalahan untuk diangkat dalam penelitian ini, yaitu Bagaimana pengaturan akses tanpa hak di Indonesia yang diatur dalam Undang-undang Nomor 19 tahun 2018 Tentang Perubahan Undang-undang nomor 11 Tahun 2008 Tentang Informasi dan transaksi Elektronik?. Tindakan Hukum Yang Dapat Dilakukan Polri dalam Mengantisipasi Kejahatan Akses tanpa hak Yang Terjadi Di Indonesia? Penulis melakukan penelitian menggunakan metode pendekatan yuridis Normatif yaitu dengan menganalisa terhadap pasal-pasal dalam peraturan perundang-undangan dengan permasalahan yang diteliti. Sifat penelitian adalah deskriptif analisis, yaitu untuk memberikan data yang seteliti mungkin tentang keadaan atau gejala yang menjadi objek penelitian. Tahapan penelitian dilakukan melalui penelitian kepustakaan untuk mendapatkan data-data sekunder yang berasal dari bahan hukum primer, bahan hukum sekunder, bahan hukum tersier dan melalui penelitian lapangan, yaitu analisis data tanpa menggunakan rumus dan angka. Dari hasil penelitian yang didapat kesimpulan pengaturan mengenai akses tanpa hak diatur dalam Pasal 30 Undang-Undang ITE, Kemudian Pasal 32 Undang-Undang ITE. Pasal 33 Undang-Undang ITE. Kelemahan dalam pengelolaan server menjadi salah satu penyebab dari bobolnya sistem informasi dari serangan akses tanpa hak, jaksa penuntut dalam kasus tiket.com harusnya lebih teliti karena unsur tindak pidana pencucian uang telah terpenuhi unsurnya disertai alat bukti yang ada. Pelunya evaluasi terhadap kebijakan dalam cybercrimes tetap diperlukan sekiranya ada kelemahan kebijakan formulasi dalam perundang-undangan tersebut. Evaluasi atau kajian ulang ini perlu dilakukan, karena ada keterkaitan erat antara kebijakan formulasi perundang-undangan (*legaslative policy*) dengan kebijakan penegakan hukum (*law enforcement policy*) dan kebijakan pemberantasan/penanggulangan kejahatan (*criminal polic*y).

Kata kunci: Penegakan Hukum, Tindak Pidana, Informasi dan Elektronik

ABSTRACT

Crime develops along with the advancement of human civilization, information technology crime has developed along with the development of Information Technology, one of which is the criminal act of illegal access which is very detrimental to others, due to illegal access this can cause enormous losses both financially and non-financially. in the case of ticket.com burglary, the owner of the server was harmed worth 5 (five) billion rupiah, and many criminal cases of illegal access were very detrimental, including burglary on the KPU website, burglary of servers belonging to other government institutions, based on this background the authors found several problems for appointed in this study, namely How is the regulation of illegal access in Indonesia regulated in Law Number 19 of 2016 concerning Amendments to Law number 11 of 2008 concerning Information and Electronic transactions? Legal Measures That Police Can Do In Anticipating Crimes of Illegal Access That Occur In Indonesia? The author conducted a study using the Normative juridical approach method by analyzing the articles in the legislation with the problems studied. The nature of the research is descriptive analysis, which is to provide data as thoroughly as possible about the situation or symptoms that are the object of research. The stages of research are carried out through library research to obtain secondary data derived from primary legal materials, secondary legal materials, tertiary legal materials and through field research, namely data analysis without using formulas and numbers. From the results of the research, it was concluded that the regulation regarding illegal access is regulated in Article 30 of the ITE Law, then Article 32 of the ITE Law. Article 33 of the ITE Law. Weaknesses in server management are one of the causes of the collapse of the information system from attacks on illegal access, prosecutors in the case of Tiket.com should be more careful because the elements of money laundering have been fulfilled with the elements accompanied by available evidence. The need for evaluation of policies in cybercrimes is still needed if there are weaknesses in the formulation policy in the legislation. This evaluation or review needs to be done, because there is a close relationship between the policy formulation of legislation (legislative policy) with law enforcement policies (law enforcement policy) and policies on crime/crime (criminal policy).

***Keywords**: Law Enforcement, Criminal Acts, Information and Electronics*

PENDAHULUAN

Tujuan nasional Negara Indonesia adalah mewujudkan keadilan sosial bagi seluruh rakyat Indonesia baik materiil maupun spiritual, yaitu menerapkan hukum sebagai sarana pengendalian sosial. Pasal 27 ayat (1) Undang-Undang Dasar 1945 menegaskan bahwa : "segala warga negara bersamaan kedudukannya di dalam hukum dan pemerintahan dan wajib menjunjung hukum dan pemerintahan itu dengan tidak ada kecualinya."

Hukum merupakan bagian integral dari kehidupan masyarakat. Setiap masyarakat selalu ada sistem hukum. Hukum berupaya menjaga dan mengatur keseimbangan antara kepentingan atau hasrat individu yang egoistis dan kepentingan bersama agar tidak terjadi konflik. Kehadiran hukum adalah untuk menegakan keseimbangan perlakuan antara hak perorangan dengan hak bersama.

Hukum mempunyai fungsi yang sangat penting dalam pelaksanaan pembangunan di Indonesia yang menitikberatkan pada pembangunan di segala bidang, hampir setiap bidang kehidupan diatur oleh peraturan-peraturan hukum. Melalui penormaan terhadap tingkah laku manusia ini hukum

menelusuri hampir semua bidang kehidupan manusia. Campur tangan hukum yang semakin meluas kedalam bidang kehidupan masyarakat menyebabkan masalah efektivitas penerapan hukum menjadi semakin penting untuk diperhitungkan.

> "Banyak faktor yang terkait dengan upaya mewujudkan hukum yang efektif, antara lain substansi hukum itu sendiri, aparatur penegak hukum dan budaya hukum masyarakat, merupakan faktor yang paling dominan dalam upaya mewujudkan hukum yang efektif, mengingat budaya hukum merupakan keseluruhan nilai, sikap, perasaan, perilaku dan kesadaran hukum."

Eksistensi Indonesia sebagai negara hukum secara tegas disebutkan dalam Penjelasan UUD 1945 (setelah amandemen) yaitu Pasal 1 ayat (3); "Indonesia ialah negara yang berdasar atas hukum *(rechtsstaat)*". Indikasi bahwa Indonesia menganut konsepsi *welfare state* terdapat pada kewajiban pemerintah untuk mewujudkan tujuan-tujuan negara, sebagaimana yang termuat dalam alinea keempat Pembukaan UUD 1945, yaitu; "Melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia, memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan melaksanakan ketertiban dunia". Tujuan-tujuan ini diupayakan perwujudannya melalui pembangunan yang dilakukan secara bertahap dan berkesinambungan dalam program jangka pendek, menengah, dan panjang.

Penggabungan komputer dengan telekomunikasi melahirkan suatu fenomena yang mengubah konfigurasi model komunikasi konvensional, dengan melahirkan kenyataan dalam dimensi ketiga. Jika dimensi pertama adalah kenyataan keras dalam kehidupan empiris (*hard reality*), dimensi kedua merupakan kenyataan dalam kehidupan simbolik dan nilai-nilai yang dibentuk (dipadankan dengan sebutan *soft reality*), maka dengan dimensi ketiga dikenal kenyataan maya (*virtual reality*) yang melahirkan suatu masyarakat lainnya.

Kemajuan dan perkembangan teknologi, khususnya telekomunikasi, multimedia dan teknologi informasi (telematika) pada akhirnya dapat merubah tatanan organisasi dan hubungan sosial kemasyarakatan. Hal ini tidak dapat dihindari, karena fleksibilitas dan kemampuan telematika dengan cepat memasuki berbagai aspek kehidupan manusia.

> "Kemajuan di bidang teknologi akan berjalan bersamaan dengan munculnya perubahan-perubahan di bidang kemasyarakatan. Perubahan-perubahan di dalam masyarakat dapat mengenai nilai sosial, kaidah-kaidah sosial, pola-pola perikelakuan, organisasi dan susunan lembaga kemasyarakatan".

Kejahatan merupakan masalah sosial yang tidak hanya dihadapi oleh Negara Indonesia atau masyarakat dan negara tertentu, tetapi merupakan masalah yang dihadapi oleh seluruh masyarakat di dunia, tidak hanya jumlahnya saja yang meningkat tetapi juga kualitasnya dipandang serius dibanding masa lalu. Masalah kejahatan dan cara penanggulangannya selalu saja dihadapi oleh setiap negara apapun bentuk dan sistem hukumnya. Mulai dari *street crime* seperti pembunuhan, perampokan, penganiayaan dan sebagainya sampai pada apa yang disebut sebagai *white collar crime* atau yang dikenal dengan istilah kejahatan kerah putih seperti kejahatan teknologi informasi, korupsi, kejahatan perbankan dan sebagainya.

Revolusi yang dihasilkan oleh teknologi informasi dan komunikasi dilihat dari sudut pandang perkembangan teknologi informasi yang demikian pesatnya haruslah diantisipasi dengan

hukum yang mengaturnya. Dampak negatif dari penggunaan teknologi informasi harus diantisipasi dan ditanggulangi dengan hukum yang terkait dengan pemanfaatan teknologi informasi dan komunikasi.

Hukum yang terkait kejahatan teknologi informasi digunakan scara internasional digunakan istilah hukum siber atau *cyber law*. Istilah lain yang juga digunakan adalah hukum teknologi informasi *(law of information technology)*, hukum dunia maya *(virtual world law)*, dan hukum mayantara. Dewasa ini telah lahir suatu rezim hukum baru yang dikenal dengan hukum *cyber* atau hukum telematika. Hukum *cyber* atau *cyber law*, secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan teknologi informasi dan komunikasi. Demikian pula, hukum telematika yang merupakan perwujudan dari konvergensi hukum telekomunikasi, hukum media, dan hukum informatika.

Cyber Law adalah aspek hukum yang artinya berasal dari *Cyberspace Law* yang ruang lingkupnya meliputi aspek-aspek yang berhubungan dengan orang perorangan atau subyek hukum yang menggunakan dan memanfaatkan teknologi internet yang dimulai pada saat mulai *online* dan memasuki dunia *cyber* atau maya. Pemberlakuan *cyber law* dikarenakan saat ini mulai muncul kejahatan-kejahatan yang ada di dunia maya yang sering di sebut sebagai *Cybercrime*.

Pemerintah Indonesia telah melakukan kebijakan di bidang Teknologi Informasi dengan terbitnya Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disingkat Undang-Undang ITE) yang diundangkan pada tanggal 21 April 2008. Undang-Undang ITE merupakan payung hukum pertama yang mengatur khusus terhadap duniamaya (*cyber law*) di Indonesia.

Substansi/materi yang diatur dalam Undang-Undang ITE ialah menyangkut masalah yurisdiksi, perlindungan hak pribadi, azas perdagangan secara *e-comerce*, azas persaingan usaha-usaha tidak sehat dan perlindungan konsumen, azas-azas hak atas kekayaan intelektual (HaKI) dan hukum Internasional serta azas *Cybercrime*.

Undang-undang tersebut mengkaji *cyber case* dalam beberapa sudut pandang, fokusnya adalah semua aktivitas yang dilakukan dalam *cyberspace* seperti perjudian, pornografi, pengancaman, penghinaan dan pencemaran nama baik melalui media *internet* serta akses komputer tanpa ijin oleh pihak lain (*cracking)* dan menjadikan seolah dokumen otentik *(phising)* .

Transaksi bisnis *online* saat ini berkembang dengan sangat pesat sehingga orang dapat melakukan transaksi perbankan melalui Komputer, Laptop, *Handphone*, PDA atau perangkat lainnya dengan aman.

Beberapa kasus cybercrime yang banyak menarik perhatian masyarakat antara lain Kasus Pembobolan Situs KPU, Aparat Satuan *Cyber Crime* Direktorat Reserse Khusus Kepolisian Daerah Metro Jaya telah menangkap Dani Firmansyah, yang diduga kuat sebagai pelaku yang membobol situs *(hacker)* di Pusat Tabulasi Nasional Pemilu Komisi Pemilihan Umum (TNP KPU). Tersangka mengaku meng-hack situs tersebut hanya karena ingin mengetes keamanan sistem keamanan server tnp.kpu.go.id, yang disebut-sebut mempunyai sistem pengamanan berlapis-lapis.

Kasus Pembobolan Situs Mabes Polri, situs resmi Polri di alamat www.polri.go.id tidak bisa diakses. Bila laman ini diakses, secara otomatis diarahkan (*forward*) ke alamat http://www.polri.go.id/backend/ index.html, lalu muncul dua buah gambar mujahidin sedang mengangkat bendera di

atas sebuah bukit. Di bawah gambar tersebut terpampang video bertitel "Doa Hamba Allah yang Prihatin dengan Kondisi Umat Islam" yang berisi doa dari Syaikh Muhammad Al-Muhaisiny, Imam Masjidil Haram, Mekkah dengan link ke Youtube. Menurut dugaan sementara situs resmi Polri tersebut diretas oleh kelompok terorisme.

Kasus Pembobolan Situs Depkominfo, Situs Depkominfo diserang dengan menggunakan *Fake IP Address* ketika undang-undang tentang Informasi dan Transaksi Elektronik (UU ITE) baru diberlakukan yaitu pada bulan Maret 2009. Hacker mengacak-acak situs atau laman Depkominfo selama sepuluh setengah jam sejak Rabu 26 Maret 2009 malam, pukul 23.00 WIB, hingga Kamis pagi 27 Maret 2009, pukul 09.30 WIB. Di situs milik departemen tersebut, terpampang tulisan "Buktikan UU ini dibuat bukan untuk menutupi kebodohan pemerintah"

Kasus Pembobolan Situs Partai Golkar, Unit *Cyber Crime* Badan Reserse dan Kriminal (Bareskrim) Mabes Polri menangkap pembobol *website* (situs) Partai Golkar, tersangka diduga kuat membobol *website* Partai Golkar hingga menyebabkan tampilan halaman berubah. Tersangka mengganti tokoh Partai Golkar yang termuat dalam situs dengan gambar gorilla putih tersenyum dan di bagian bawah halaman dipasang gambar artis Holywood yang seronok.

Kriminalisasi terhadap perbuatan dunia maya muncul ketika dihadapkan pada suatu perbuatan yang merugikan orang lain atau masyarakat yang sebelumnya belum/kurang diatur baik oleh hukum pidana maupun oleh undang-undang khusus di bidang Teknologi Informasi. Hukum selalu berkembang dan semakin diperluas untuk mencakup situasi atau perubahan teknologi informasi yang terus berkembang dalam kehidupan masyarakat, perubahan hukum akan menuntut masyarakat dunia maya untuk menyesuaikan dengan hukum yang baru tersebut. Akan tetapi pada kenyataannya hukum sendiri belum dapat mengatasi secara riil terhadap permasalahan-permasalahan yang ditimbulkan oleh teknologi khususnya teknologi informasi. Salah satu bukti konkretnya adalah timbulnya berbagai kejahatan di dunia virtual yang ternyata belum bisa diatasi sepenuhnya oleh hukum.

Membahas yang mendalam mengenai masalah ini maka perlu dilakukan penelitian yang mendalam agar memberi gambaran yang jelas dalam menentukan kebijakan dalam menanggulangi tindak pidana teknologi informasi melalui hukum pidana. Kebijakan penanggulangan hukum pidana (*penal policy*) tersebut pada hakekatnya bertujuan sebagai upaya perlindungan masyarakat untuk mencapai keadilan dan kesejahteraan masyarakat (*social welfare*).

Kasus kejahatan di dunia maya atau cyber crime menjadi kasus paling banyak yang ditangani Ditreskrimsus Polda Metro Jaya di sepanjang 2016. Dari 1.627 kasus yang ditangani polisi, 1.207 kasus merupakan kasus cyber crime. Dari 1.207 laporan kasus tersebut, sebanyak 699 kasus telah diselesaikan. "Dari lima direktorat, cyber crime tertinggi," ungkap Dir Krimsus Polda Metro Jaya, Kombes Pol Wahyu Hadiningrat. Adapun lima direktori yang dimaksud yakni Subdit 1 Indag atau Industri dan Perdagangan, Subdit 2 Fismondev atau Fiskal, Moneter dan Devisa, Subdit 3 Sumdaling atau Sumber Daya Lingkungan, Subdit 4 Cyber Crime dan Subdit 5 Korupsi.

Indonesia berada di urutan kedua dalam daftar lima besar negara asal serangan kejahatan siber atau cyber crime, berdasar laporan State of The Internet 2013. Wakil Direktur Tindak Pidana Ekonomi Khusus Bareskrim Polri Kombespol Agung Setya mengatakan, dalam kurun waktu tiga tahun terakhir,

tercatat 36,6 juta serangan cyber crime terjadi di Indonesia.

Data Security Threat 2013 yang menyebutkan Indonesia adalah negara paling berisiko mengalami serangan cyber crime. Sejak 2012 sampai dengan April 2015, Subdit IT/ Cyber Crime telah menangkap 497 orang tersangka kasus kejahatan di dunia maya, dari jumlah tersebut, sebanyak 389 orang di antaranya merupakan warga negara asing, dan 108 orang merupakan warga negara Indonesia.

Total kerugian cyber crime di Indonesia mencapai Rp33,29 miliar. "Angka ini jauh lebih besar dibandingkan perampokan nasabah bank secara konvensional.

Isu kemanan siber yang kini memang menjadi pehatian banyak pihak, termasuk pemerintah. ID-SIRTII (Indonesia Security Incident Response Team On Internet Infrastructure) mengatakan bahwa sepanjang tahun 2014, setidaknya terjadi 48,4 juta serangan keamanan siber dalam berbagai bentuk, termasuk serangan ke situs tertentu atau penyebaran malware melalui berbagai teknik. Informasi ini disampaikan langsung oleh

Ketua ID-SIRTII Rudi Lumanto saat menjadi salah satu pembicara utama dalam Virtus Security Day 2015 Dia menjelaskan, puluhan juta serangan yang muncul tahun lalu ini ternyata bukan berasal dari hacker atau oknum lain di luar negeri. “60 persen serangan ternyata berasal dari Indonesia sendiri, bukan dari luar negeri,” pada 2014, Indonesia memiliki sekitar 12 juta aktivitas malware, dengan 12 ribu merupakan insiden website. Jumlah 12 ribu ini, setidaknya ada 3 ribu serangan siber terhadap situs pemerintah alias yang menggunakan domain .go.id. “Secara index, Indonesia memiliki kekuatan siber cukup tinggi, yaitu peringkat 13 di dunia, dan peringkat 5 di Asia Pasifik.

Kasus lainnya yaitu yang akan penulis teliti yaitu kasus tiket.com, dimana otak pelaku sindikat peretas adalah seorang hacker remaja, bernilai Rp 4,1 miliar, Haikal alias SH (19 th), berhasil dibekuk petugas Siber Bareskrim Polri di perumahan Pesona Gintung Residen, Tangerang Selatan, Banten. Tiga anak buahnya lebih dulu dibekuk di Balikpapan, Kalimantan Timur, dua hari lalu.

Haikal terbilang hacker hebat. Sebab, usianya baru 19 tahun dan hanya lulusan SMP, tapi sudah berhasil meretas lebih 4.600 situs. Situs pemerintah pusat dan daerah hingga institusi Polri pernah dijebolnya.

Pemeriksaan terhadap ketiga tersangka, telah berhasil membobol lebih dari 4.600 situs. Di antaranya situs milik polri juga ada, situs milik pemerintah pusat dan daerah, beberapa situs luar negeri dan bahkan situs ojek online juga dibobol," ungkap Rikwanto.

Haikal tidak semata bertujuan mencari keuntungan saat ingin menjebol suatu situs. Tapi, ia juga sering meretas suatu situs, seperti situs lembaga tertentu, demi "unjuk gigi". "Untuk menunjukan kelasnya, bahwa dia bisa membobol situs tertentu dengan mudahnya," kata Rikwanto.

Penelitian tentang hal ini belum pernah dilakukan karena ini kasus yang baru belum pernah dilakukan penelitan dan analisis sebelumnya.

Berdasarkan deskripsi permasalahan sebagaimana diuraikan di atas, maka penulis tertarik untuk mengadakan penelitian yang dituangkan dalam bentuk Tesis dengan judul : ”UPAYA PENEGAKAN HUKUM TERHADAP TINDAK PIDANA AKSES TANPA HAK DIHUBUNGKAN DENGAN UNDANG-UNDANG UNDANG NOMOR 19 TAHUN 2016 ATAS PERUBAHAN UNDANG-UNDANG NOMOR 11 TAHUN 2008

TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK"

Identifikasi Masalah

1. Bagaimana pengaturan akses tanpa hak di Indonesia yang diatur dalam Undang-undang Nomor 19 tahun 2018 Tentang Perubahan Undang-undang nomor 11 Tahun 2008 Tentang Informasi dan transaksi Elektronik?
2. Tindakan Hukum Yang Dapat Dilakukan Polri Dalam Mengantisipasi Kejahatan Akses tanpa hak Yang Terjadi Di Indonesia?

Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian ini adalah sebagai berikut:

1. Untuk teridentifikasi dan teranalisis pengaturan Akses Terlarang di Indonesia sebgaimana diatur dalam Undang-undang Nomor 19 Tahun 2016 Tentang perubahan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.
2. untuk teridentifikasi dan teranalisis penyebab tingginya angka kejahatan Akses Terlarang di Indonesia dan menganalisis untuk menemukan solusi untuk menurunkan angka kejahatan cybercrime di Indonesia.

Kegunaan Penelitian

Penekanan yang dilakukan dalam penelitian ini diharapkan mampu memberikan kegunaan yang positif yaitu dari segi :

1. Teoritis
   Kegunaan teoritis dari hasil penelitian ini diharapkan dapat digunakan bagi pendalaman kajian sehubungan dengan fungsi hukum sebagai alat pembaharuan masyarakat dan memberikan sumbangan pemikiran bagi pengembangan Ilmu Hukum pada umumnya dan Hukum Pidana pada khususnya terutama yang berkaitan dengan Hukum Teknologi Informasi. Hasil penelitian ini juga diharapkan dapat memberikan referensi bagi dilakukannya penelitian lanjutan dengan obyek yang sama.
2. Praktis
   Agar dapat memberikan informasi, pemikiran dan pertimbangan bagi para penegak hukum dalam menangani kasus kejahatan yang terjadi di internet (*cybercrime*), bagi pemerintah agar dapat lebih inten dalam mengeluarkan kebijakan yang berhubungan dengan *cybercrime,* dan bagi masyarakat agar lebih waspada terhadap terjadinya penyalahgunaan dan/atau kejahatan *cybercrime.*

Metode Penelitian

Sebelum melakukan suatu penelitian ilmiah, seorang peneliti dituntut untuk terlebih dahulu memahami tentang dasar-dasar berpikir secara sistematis dan metodologis. Hal ini sangat penting agar dapat memperoleh hasil penelitian yang baik dan bermutu dalam bentuk karya ilmiah. Tanpa metode yang benar, maka sebuah karya ilmiah tidak akan mempunyai nilai ilmiah yang kebenarannya diragukan atau dipertanyakan.

Penelitian pada umumnya bertujuan untuk menemukan, mengembangkan atau menguji kebenaran suatu pengetahuan. Agar penelitian ini memenuhi syarat keilmuan maka tidak akan terlepas dari suatu penelitian ilmiah, yang bertujuan:

1. Menemukan berarti berusaha memperoleh sesuatu untuk mengisi kekosongan atau kekurangan.
2. Mengembangkan berarti memperluas dan menggali lebih dalam sesuatu yang sudah ada.
3. Menguji berarti menguji kebenaran dilakukan jika apa yang sudah ada masih atau menjadi diragu-ragukan kebenarannya

Metode penelitian mempunyai peranan yang sangat penting dalam penulisan karya ilmiah. Metode penelitian

adalah "Sebagian pengetahuan mengenai berbagai macam cara kerja yang sangat diperlukan didalam suatu penelitian, sebab metodologi memberikan atau menunjukan cara-cara untuk memahami obyek yang menjadi sasaran penelitian, adapun tahap penelitian sebagai berikut:

1. Metode pedekatan yang digunakan dalam penelitian ini adalah Metode Yuridis Normatif, yaitu suatu penelitian yang menekankan pada peraturan perundang-undangan untuk mengkaji permasalahan dengan menemukan peraturan hukumnya yang bertujuan untuk menemukan asas dan teori hukum yang kemudian ditetapkan dalam praktek yaitu mencari, menemukan dan mengumpulkan dasar-dasar yuridis berupa aturan-aturan yang berasal dari hukum-hukum yang kemudian dihubungkan dan diterapkan dalam masalah yang timbul di masyarakat.
2. Spesifikasi Penelitian yang digunakan adalah bersifat deskriptif analitis yaitu menggambarkan realitas sosial dari fakta-fakta yang diketemukan, untuk selanjutnya dilakukan upaya analisis dengan mendasarkan pada teori-teori yang terdapat dalam disiplin ilmu hukum, khususnya Hukum Pidana berkenaan dengan persoalan Teknologi Informasi.
3. Penulis dalam penelitian ini menggunakan metode pengumpulan data kepustakaan. yaitu terdiri dari :
   a. Bahan hukum primer, yaitu bahan-bahan hukum yang mempunyai kekuatan hukum mengikat, misalnya perundang-undangan, diantaranya Kitab Undang-Undang Hukum Pidana dan Undang-Undang ITE.
   b. Bahan hukum sekunder, yaitu bahan-bahan yang erat hubungannya dengan bahan-bahan hukum primer dan dapat membantu menganalisis dan memahami bahan hukum primer, misalnya hasil-hasil penelitian, tulisan para sarjana, terutama yang membahas mengenai Teknologi Informasi khususnya kejahatan cybercrime
   c. Bahan hukum tersier, yaitu bahan-bahan yang memberikan informasi tentang bahan hukum primer dan bahan hukum sekunder, misalnya majalah hukum, kliping, koran, kamus hukum, dan situs-situs internet *(website)*.
4. Analisis Data yang dipergunakan dalam penelitian adalah suatu tahapan yang sangat penting dalam suatu penelitian sehingga akan mendapatkan hasil yang akan mendekati kebenaran yang ada. Dalam penelitian ini digunakan teknik analisis yuridis kualitatif, yaitu data yang terkumpul dituangkan dalam bentuk uraian logis dan sistematis tanpa menggunakan rumus-rumus atau angka-angka statistik, selanjutnya dianalisis untuk memperoleh kejelasan penyelesaian masalah, kemudian ditarik kesimpulan secara Induktif.

PEMBAHASAN

Pengaturan Akses Tanpa Hak Di Indonesia Yang Diatur dalam Undang-undang Nomor 19 tahun 2016 Tentang Perubahan Undang-undang nomor 11 Tahun 2008 Tentang Informasi dan transaksi Elektronik

Meningkatnya angka penetrasi pengguna internet di Indonesia telah memunculkan berbagai bentuk aktivitas di Internet, dan juga mendorong tindak pidana antara lain akses tanpa hak yang telah diatur dalam Pasal 30 Undang-Undang ITE, unsur tindak pidana yang pertama adalah (1) Setiap orang dengan

sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apapun, namun apabila pelaku menggunakan alamat internet yang palsu (Fake IP address) ini akan mengelabui atas keberadaan dipelaku. (2) setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses computer dan/atau system elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik, (3) setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses computer dan/atau system elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol system pengamanan.

Pasal 32 Undang-Undang ITE mengatur bahwa setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik orang lain atau milik publik.

Unsur tindak pidana yang diatur dalam Pasal 32, yaitu (1) setiap orang dengan sengaja dan tanpa hak atau melawan hokum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu informasi elektronik dan/atau dokumen elektronik milik orang lain

Pasal 33 Undang-Undang ITE mengatur bahwa setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apapun yang berakibat terganggunya sistem elektronik dan/atau mengakibatkan sistem elektronik menjadi tidak bekerja sebagaimana mestinya.

Pelanggaran terhadap ketentuan Pasal 33 tersebut dapat diancam dengan sanksi pidana berdasarkan Pasal 49 yang berbunyi sebagai berikut :

"Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 33 dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp. 10.000.000.000,00 (sepuluh miliar rupiah).

Actus reus dari tindak pidana tersebut adalah "tindakan apapun". Mens rea dari tindak pidana tersebut adalah "dengan sengaja". Yang penting berkenaan dengan berlakunya Pasal 33 tersebut adalah sasaran dari actus reus yang ditentukan dalam Pasal tersebut harus berupa sistem elektronik.

Selain yang menjadi sasaran adalah sistem elektronik juga harus diperhatikan bahwa akibat tindakan tersebut berupa terganggunya sistem elektronik yang menjadi sasarannya.. Konsekuensi yang demikian itu adalah karena tindak pidana dalam pasal ini dirumuskan sebagai tindak pidana materiil. Artinya pelaku hanya dapat dipidana apabila akibat perbuatan pelaku telah terjadi. Di dalam praktik, gangguan yang terjadi terhadap sistem elektronik itu adalah berupa tidak bekerjanya atau berfungsinya sistem elektronik tersebut sebagaimana mestinya.

Pada kasus tiket.com Kasus ini bermula ketika PT Global Tiket Network sebagai pengelola Tiket.com melaporkan ke Bareskrim polri bahwa mereka mengetahui adanya peretasan terhadap sistem aplikasi jual beli tiket.com yang berlangsung dari tanggal 11 November sampai dengan tanggal 27 November 2016. Otak dibalik kasus pembobolan ini adalah SH (19). Menurut hasil penyelidikan sementara, Pemuda tamatan SMP tersebut dan ketiga rekannya MKU (19), NTM (27) dan AI (19) telah berhasil membobol 4.600 situs. Total kerugian diperkirakan mencapai mencapai 4,1 miliar Rupiah.

SH meretas situs Tiket.com untuk mendapatkan username dan password untuk bisa masuk ke server Citilink dengan menggunakan ID tersebut. tujuannya untuk mendapatkan kode booking tiket pesawat Citilink lalu dijual ke pembeli. Akan tetapi, haikal tidak bekerja sendiri, dia memiliki tim yang terdiri dari MKU, NTM, AI yang direkrut lewat komunikasi di media sosial dan game online.

MKU berperan menawarkan penjualan tiket pesawat melalui akun Hairul Joe pada jejaring sosial Facebook MKU juga ikut membantu SH meretas situs Tiket.com. NTM berkewajiban mencari calon pembeli melalui akun Facebook bernama Nokeyz Dhosite Kashir. Setelah mendapatkan calon pembeli, data calon pembeli diberikan kepada AI untuk diprosess lebih lanjut. AI bertugas memasukkan data pesanan tiket pesawat Citilink dari pembeli yang selanjutnya data tersebut dimasukkan ke aplikasi penjualan maskapai Citilink dengan menggunakan username dan password milik travel agen Tiket.com dan setelah kode booking pesawat didapat, selanjutnya kode booking tersebut dikirim ke pihak pembeli.

Terungkapnya kasus ini berawal dari pengaduan PT Global Network kepada polisi tentang adanya peretasan pada sistem aplikasi jual beli tiket daring Tiket.com yang tersambung dengan sistem penjualan tiket pada maskapai penerbangan PT Citilink Indonesia (*www.citilink.co.id*) pada 11-27 Oktober 2016.

Berdasarkan hasil penelusuran tim dari direktorat Tindak Pidana Siber, kasus pembobolan ini dilakukan oleh tim yang terdiri dari SH (19) sebagai otak pembobolan, MKU (19), NTM (27) dan AI (19). Ketiga pelaku MKU, NTM dan AI berhasil dibekuk pada tanggal 28 Maret 2017. Dan SH ditangkap pada tanggal 30 Maret 2017.

Modus dan tujuan kejahatan dalam teknologi informasi ini makin kompleks seiring berkembangnya kemjuan teknologi informasi ini, bentuk tindakan akses tanpa hak pun semakin kompleks, dari yang mengakses untuk mendapatkan keuntungan secara finansial maupun yang sekedar iseng dalam melakukan tindakan akses tanpa hak ini, pengaturan tindakan akses tanpa hak ini sudah cukup yang tertuang dalam UU ITE namun seiring perkembangan kemajuan teknologi sebaiknya pengaturan mengenai akses tanpa hak ini dilengkapi, seperti yang pernah diajukan dalam RUU cybercrime.

Terdakwa Haikal dalam kasus pembobolan tiket.com dipidana atas Tindak Pidana Akses Tanpa hak sebagaimana diatur dalam Pasal 30 UU ITE dan dipidana selama 2 (dua) tahun 4 (empat) bulan, sedangkan dakwaan atas pasal pencucian uang tidak terbukti dalam putusan tersebut, seharusnya jaksa penuntut lebih jeli dalam mengajukan dakwaannya, kerna unsur money laundry dalam kasus tersebut karena unsur pencucian uangnya telah terbukti berdasarkan pengumpulan alat bukti dan kesaksian dalam proses penyidikan.

Tindakan Hukum yang Dapat Dilakukan Polri dalam Mengantisipasi Kejahatan Akses Tanpa Hak Yang Terjadi di Indonesia

Ketentuan mengenai Akses Tanpa Hak ini dapat pula dimasukan dalam KUHPidana Nasional mendatang, yang merupakan pembaharuan hukum pidana, dimana hukum yang hidup dimasyarakat dan kesadaran hukum masyarakat, harus diadopsi menjadi hukum nasional, karena kejahatan-kejahatan yang terkait dengan teknologi informasi saat ini sudah sangat memprihatinkan dan masyarakat sadar akan bahaya atau kerugian yang ditimbulkan dari cybercrime ini.

Penulis menganalisis mengenai kebijakan kriminalisasi berkaitan dengan

Akses Tanpa Hak ini dengan berdasarkan pada pendapat Barda Nawawi Arif yang mengatakan suatu upaya kriminalisiasi terhadap tindak pidana mayantara perlu memperhatikan hal-hal fundamental, di antaranya:

Pertama, untuk terwujudnya tujuan pembangunan nasional, yaitu mewujudkan masyarakat adil makmur secara material dan spiritual berdasarkan Pancasila;

Penulis berpendapat bahwa kejahatan di internet bermula dari kejahatan komputer berupa peningkatan kualitas kecanggihan teknologi komputer. Berbagai hasil pengamatan baik dari media masa (cetak dan elektronik), penelitian lapangan, menunjukan bahwa kejahatan penyalahgunaan Akses Tanpa Hak ini memiliki dampak yang sangat serius terhadap perkembangan sosial masyarakat itu sendiri. Sehingga upaya kriminalisasi adalah cara yang paling tepat, dimana kebijakan kriminalisasi ini pada hakikatnya merupakan penanggulangan kejahatan sekaligus satu kesatuan dengan upaya perlindungan masyarakat (*social defence*) dan upaya mencapai kesejahteraan rakyat (*social welfare*). Dengan kata lain tujuan final dari kebijakan kriminal adalah perlindungan masyarakat untuk mencapai kesejahteraan masyarakat. Hal ini sejalan dengan Tujuan pembangunan Nasional.

Kedua, perbuatan yang diusahakan untuk dicegah atau ditanggulangi dengan hukum pidana harus merupakan perbuatan yang tidak dikehendaki, tidak disukai atau dibenci oleh warga masyarakat yaitu perbuatan yang merugikan atau dapat merugikan, mendatangkan korban atau dapat mendatangkan korban. Selain itu harus pula dipertimbangkan sejauh mana perbuatan tersebut bertentangan dengan nilai-nilai fundamental yang berlaku dalam masyarakat.

Terhadap hal yang kedua ini penulis berpendapat bahwa kejahatan akses tanpa hak adalah khas yaitu ekses negatif dari masyarakat informasi. Kejahatan penyalahgunaan akses tanpa hak berbeda dan lain dari kejahatan yang telah ada dan dikenal sebelumnya sebagaimana aksioma kejahatan tiada lain adalah produk masyarakat itu sendiri (*crime is a product of society its self*). Dampak negatif kejahatan ini menyedot perhatian masyarakat baik nasional, regional bahkan internasional. Ini pertanda bahwa kejahatan ini serius dan berbahaya bagi masyarakat. Jika di kaji lebih jauh berbagai kekhawatiran, kecemasan dan warning untuk segera membuat klep pengaman terhadap kejahatan akses tanpa hak ini kepada masyarakat luas.

Bentuk Kejahatan yang ditimbulkan dari Akses Tanpa Hak yang kemudian menyerang korban saat ini dapat dikategorikan sebagai cyber teroris, karena akibat yang ditimbulkan dari Akses Tanpa Hak ini, begitu besarnya kerusakan yang terjadi atau ditimbulkan apabila pelaku berhasil melumpuhkan jaringan listrik dari satu ibukota suatu negara, melumpuhkan sistem jaringan komputer suatu markas biro intelejen nasional, melumpuhkan jaringan komputer suatu bank sentral suatu negara, jaringan penerbangan, mengacaukan situs-situs pemerintah khususnya yang berkaitan dengan kepemilikan data-data rahasia Negara, dan lain sebagainya.

Ketiga, Perhitungan prinsip biaya dan hasil (cost benefit principle) dari penggunaan hukum pidana tersebut, yaitu apakah biaya mengkriminalisasi seimbang dengan hasilnya yang akan dicapai, artinya cost pembuatan undang-undang, pengawasan dan penegak hukum, serta beban yang dipikul oleh korban dan pelaku kejahatan itu sendiri harus seimbang dengan situasi tertib hukum yang akan dicapai.

Bekerjanya/berfungsinya hukum pidana memerlukan sarana pendukung yang lebih bervariasi dan Sumber Daya Manusia yang lebih berkualitas, sedangkan untuk mencapai hal tersebut membutuhkan

sumber biaya yang cukup besar. Sebaiknya Anggaran sekalipun dirasakan kurang mencukupi untuk kebutuhan seluruh proses pidana, namun hendaknya diusahakan memanfaatkan anggaran yang tersedia secara berhasil dan berdaya guna.

Keempat, kapasitas atau kemampuan daya kerja dari badan-badan penegak hukum, yaitu jangan sampai ada kelampauan beban tugas dan keseimbangan sarana-sarana yang digunakan dalam hubungannya dengan hasil-hasil yang ingin dicapai.

Untuk hal ini menurut pendapat penulis yang dapat dilakukan yaitu membentuk kerjasama yang baik antara pihak kepolisian dengan Departemen komunikasi dan informasi yang berkepentingan dalam pengaturan/regulasi di bidang teknologi Informasi serta pengelola jaringan internet, sehingga terjalin sinergi untuk melakukan penegakan hukum di bidang teknologi informasi yang terpadu, hal ini dapat dibentuk dalam suatu cyber task force. Cyber task force ini nantinya akan berperan dalam proses upaya penegakan hukum, baik yang yang bersifat preventif maupun represif.

Penanganan kejahatan teknologi informasi diperlukan adanya kerjasama Internasional dalam proses penegakan hukumnya, karakteristik kejahatan teknologi informasi (cybercrime) yaitu *transnasional* dan *borderless*, sehingga akan sulit mengungkap kejahatan-kejahatan cybercrime yang melibatkan jaringan-jaringan Internasional, seperti dalam beberapa kasus Akses Tanpa Hak ini melibatkan jaringan serta lokasi negara yang berbeda, sehingga membutuhkan kerjasama antara aparatur penegakan hukum di Negara kita dengan aparatur penegakan hukum di Negara lain.

Selain pembaharuan hukum, hal lain yang perlu diperhatikan adalah sarana dan prasarana serta fasilitas di bidang teknologi informasi, fasilitas ini diperlukan untuk mengungkap data-data digital serta merekam dan menyimpan bukti-bukti berupa soft copy (image, program, dsb). Polri masih perlu meningkatkan fasilitas forensic computing yang memadai. Fasilitas forensic computing Polri diharapkan akan dapat melayani tiga hal penting yaitu *evidence collection, forensic analysis, expert witness*.

Dalam Kasus Tiket.com dapat tergambar ancaman yang Dapat Terjadi untuk Situs Online

Terdapat beberapa Risko dalam menjalankan E-Commerce, antara lain : Kehilangan segi financial secara langsung karena kecurangan, Pencurian informasi rahasia yang berharga, Kehilangan kesempatan bisnis karena gangguan pelayanan, Penggunaan akses ke sumber oleh pihak yang tidak berhak, Kehilangan kepercayaan dari para konsumen, Kerugian-kerugian yang tidak terduga, ancaman-ancaman yang dapat terjadi saat menjalankan E-Commerce: System Penetration : orang-orang yang tidak berhak, mendapatkan akses ke sistem computer dan diperbolehkan melakukan segalanya. Authorization Violation: Ancaman berupa pelanggaran atau penayalahgunaan wewenang legal yang dimiliki oleh seseoarang yang berhak. Planting: Ancaman yang terencana misalnya Trojan horse yang masuk secara diam-diam yang akan melakukan penyerangan pada waktu yang telah ditentukan. Communications Monitoring: penyerang dapat melakukan monitoring semua informasi rahasia. Communications Tampering: penyerang mengubah informasi transaksi di tengah jalan pada sebuah jaringan komunikasi dan dapat mengganti sistem server dengan yang palsu. Denial of Service (DoS): Penolakan service terhadap client yang berhak. Repudiation: Penolakan terhadap sebuah aktivitas transaksi atau sebuah komunikasi yang terjadi dikarenakan sesuatu yang

bersifat sengaja, kecelakaan ataupun kesalahan teknis lainnya.

Kelemahan pengendalian internal pada tiket.com terdapat pada risk identification, risk assessment dan monitoring yang ada pada perusahaan tiket.com. Dimana Tiket.com gagal mengidentifikasi risiko eksternal pada situs website mereka sehingga gagal untuk mendeteksi adanya koneksi yang terkena hack. Hal ini sejalan dengan yang dikatakan ahli digital forensic

Tindakan peretasan oleh Haikal ini masih dalam level yang ringan. Hal ini memungkinkan bisa dikarenakan pengamanan server jual-beli tiket online tersebut memang rendah. Mereka cuma memanfaatkan informasi pengetahuan serta tools yang ada. Kebetulan situs-situs tersebut memang tidak aware terhadap sekuriti yang cukup tinggi, akhirnya gampang dibobol. Selain itu juga, menurut ahli keamanan cyber, Taufik Yahya, ada banyak kemungkinan cara yang digunakan Haikal untuk membobol situs www.tiket.com. Ada kemungkinan dari sisi tiket.com sendiri yang rentan seperti belum membatasi penyaringan terhadap special character yang memungkinkan seorang penyerang untuk menarik konten di database dari halaman front end aplikasi (dikenal SQL Injection).

Umumnya dari hasil ini, seseorang dapat mempergunakan data untuk login ke halaman yang lebih tertentu (seperti halaman admin) atau dapat juga untuk mengambil data sensitif pengguna lain. Bila ditarik dari kesimpulan tersebut, masih terlalu banyak hal yang dapat dijadikan dugaan karena tidak hanya SQL Injection yang dapat membuat seseorang berhasil memperoleh akses masuk. Yang kemudian dilanjutkan dengan melakukan pencurian data setelah penyerang berhasil mengambil akun untuk mengambil alih komputer yang dipakai individu terkait atau sistem yang dikelola Dan berdasarkan akan hal itu dapat diketahui bahwa risk assessment tiket.com tidak dilaksanakan dengan baik. Dimana tiket.com tidak merespon risiko dengan baik. hal tersebut dapat dikatakan demikian karena tiket.com seharusnya mengetahui adanya risiko – risiko baik itu bawaan maupun residual dari website mereka dan mempersiapkan atau melakukan cara untuk merespon risiko-risiko tersebut. Hal ini sesuai dengan COSO Risk Assessment bahwa cara untuk merespon risiko dapat dilakukan oleh perusahaan dengan menerapkan: a) Mengurangi. Mengurangi kemungkinan dan dampak dari risiko dengan menerapkan sistem pengendalian internal yang efektif. b) Menerima. Menerima kemungkinan dan dampak dari risiko tersebut. c) Membagi. Membagi risiko atau mentransfernya ke pihak lain dengan membeli asuransi, outsourcing suatu aktivitas atau melakukan transaksi hedging. d) Menghindar. Menghindari risiko dengan tidak terlibat dalam aktivitas yang menghasilkan risiko.

Dari cara tersebut yang mungkin dapat dilakukan oleh tiket.com adalah mengurangi kemungkinan dan dampak risiko sistem pengendalian internal yang efektif. Selain hal tersebut diatas, pengendalian preventif dan detektif pada tiket.com masih kurang. Karena mereka tidak mampu mencegah terjadinya hal tersebut dan deteksi yang digunakan juga tidak dapat mendeteksi dengan segera apabila ada akses dari luar yang bukan pengelola dari tiket.com. Yang paling disayangkan adalah masalah ini telah terjadi agak lama sebelum akhirnya diketahui oleh pihak tiket.com. Pihak IT tiket.com seharusnya secara berkala memonitoring dan melakukan modifikasi yang diperlukan serta melaporkan kekurangan-kekurangan yang ada pada pihak manajemen atau lini diatas mereka. Sehingga tiket.com dapat mempersiapkan diri guna terhindar dari risiko-risiko negative yang ada.

Pengendalian atas Ancaman, pengendalian yang dapat dilakukan untuk mengatasi ancaman-ancaman dalam kegiatan E-commerce Security service safe guards: 1. Authentication Service: Memberikan kepastian identitas pengguna. Entity authentication: contohnya password. Data origin authentication: membuktikan sah tidaknya identitas dalam bentuk pesna tertulis. 2. Access Control Services: Melindungi semua fasilitas dan sumber-sumber yang ada dari akses-akses yang tidak berhak. 3. Confidentiality Service: Memberikan perlindungan terhadap informasi yang berusaha disingkap oleh orang lain yang tidak berhak. 4. Data Integrity Srevice: Perlindungan terhadap ancaman yang dapat mengubah data item seandainya ini terjadi di dalam lingkungan security policy. 5. Non-Repudiation Service: Melindungi user melawan ancaman yang berasal dari user berhak lainnya. Ancaman tersebut dapat berupa kesalahan penolakan ketika transaksi atau komunikasi sedang terjadi.

Pengendalian Internal yang harus dilakukan untuk meminimalisir kejadian seperti yang dialami oleh Tiket.com adalah dengan melakukan pengendalian preventif yaitu dengan cara melakukan kendali atas akses jaringan. Dimana perusahaan dapat menggunakan batasan-batasan pengamanan seperti router, firewall, dan instrusion prevention system lainnya untuk melindungi atau mengendalikan informasi apa saja yang boleh dimasuki dan diambil dari sistem informasi perusahaan. Perusahaan juga dapat melakukan perlindungan terhadap akses nirkabel dengan mengaktifkan fitur-fitur pengaman yang ada, otentifikasi semua peralatan yang akan digunakan untuk mengakses data nirkabel ke jaringan sebelum memberikan IP address ke setiap peralatan tersebut, konfigurasi semua piranti nirkabel agar hanya beroperasi dalam mode infrastruktur, yang mengharuskan piranti tersebut terhubung hanya dengan titik nirkabel, penggunaan nama yang tidak informative untuk alamat titik akses service net identifier (SSID) agar tidak mudah menjadi target serangan, mengurangi kekuatan broadcast titik akses nirkabel, menempatkan di dalam interior ruangan dan menggunakan antenna pengarah agar data yang tidak terotorisasi tidak mudah masuk, dan menggunakan penggunaan enkripsi atas semua trafik nirkabel.

Selain melakukan pengendalian preventif tiket.com juga dapat memperbaiki pengendalian detektifnya untuk meningkatkan keamanan dengan cara memonitor keefektifan pengendalian preventif. Pengendalian yang dapat dilakukan yaitu, melakukan analisis log, intrusion detection system, dan pengujian keamanan. Analisis log merupakan proses untuk memeriksa catatan atas siapa saja yang mengakses sistem dan secara spesifik apa saja yang dilakukan oleh setiap pengguna ketika mengakses sistem untuk mengidentifikasi potensi kemungkinan serangan yang dapat terjadi.Instrusion Detection System (IDS) yang berisi seperangkat sensor dan unit monitoring pusat yang menghasilkan catatan trafik jaringan yang telah diizinkan untuk melewati firewall dan kemudian menganalisis catatan tersebut untu mendeteksi adanya tanda-tanda usaha untuk melakukan instruksi gangguan atau gangguan yang sudah terjadi. Pengujian keamanan dilakukan dengan cara melakukan pengujian secara berkala atas efektivitas prosedur pengaman yang saat ini sudah ada. Salah satunya dengan menggunakan vulnerability scanner untuk mengidentifikasi potensi kelemahan dalam konfigurasi sistem.

Selain itu juga melakukan penetration test yang merupakan usaha yang disahkan yang dilakukan oleh tim audit intern dan konsultan TI eksternal untuk menerobos masuk ke dalam sistem informasi organisasi. Hal ini dilakukan

guna mengidentifikasi dimana saja perlindungan khusus harus diberikan untuk mencegah adanya akses tidak sah terhadap sistem perusahaan. Salah satu cara untuk mengetahui kelemahan sistem informasi juga dapat dilakukan dengan menyerang diri sendiri dengan paket-paket program penyerang (attack) yang dapat diperoleh di Internet. Dengan menggunakan program ini anda dapat mengetahui apakah sistem anda rentan dan dapat dieksploitasi oleh orang lain. Selain program penyerang yang sifatnya agresif melumpuhkan sistem yang dituju, ada juga program penyerang yang sifatnya melakukan pencurian atau penyadapan data. Untuk penyadapan data, biasanya dikenal dengan istilah "sniffer".

Meskipun data tidak dicuri secara fisik (dalam artian menjadi hilang), sniffer ini sangat berbahaya karena dia dapat digunakan untuk menyadap password dan informasi yang sensitif. Ini merupakan serangan terhadap aspek privacy.Tiket.com juga dapat menggunakan Sistem pemantau jaringan (network monitoring) untuk mengetahui adanya lubang keamaman. Misalnya apabila anda memiliki sebuah server yang semetinya hanya dapat diakses oleh orang dari dalam, akan tetapi dari pemantau jaringan dapat terlihat bahwa ada yang mencoba mengakses melalui tempat lain. Selain itu dengan pemantau jaringan dapat juga dilihat usaha-usaha untuk melumpuhkan sistem dengan melalui denial of service attack (DoS) dengan mengirimkan packet yang jumlahnya berlebihan. Oleh karena dari apa yang telah jabarkan diatas, tiket.com mungkin dapat melakukan hal tersebut agar kejadian tersebut tidak dapat terjadi lagi dan dapat mengurangi risiko akan terkena hal tersebut lagi. Seperti yang diketahui bahwa hal ini kemungkinan besar terjadi karena kurang aware nya tiket.com terhadap hal tersebut sehingga dapat diterobos oleh hacker dengan mudah.

Kesimpulan

1. Pengaturan mengenai akses tanpa hak diatur dalam Pasal 30 Undang-Undang ITE, unsur tindak pidana yang pertama adalah (1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apapun, namun apabila pelaku menggunakan alamat internet yang palsu (Fake IP address) ini akan mengelabui atas keberadaan sipelaku. (2) setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses computer dan/atau system elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik, (3) setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses computer dan/atau system elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol system pengamanan. Kemudian Pasal 32 Undang-Undang ITE mengatur bahwa setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik orang lain atau milik publik. Pasal 33 Undang-Undang ITE mengatur bahwa setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apapun yang berakibat terganggunya sistem elektronik dan/atau mengakibatkan sistem elektronik menjadi tidak bekerja sebagaimana mestinya. Kelemahan dalam pengelolaan server menjadi salah satu penyebab dari bobolnya sistem informasi dari serangan akses tanpa hak, jaksa penuntut dalam kasus tiket.com harusnya lebih teliti karena unsur tindak pidana pencucian uang

telah terpenuhi unsurnya disertai alat bukti yang ada.

2. Tindakan hukum yang dapat dilakukan Kepolisian Negara Republik Indonesia dalam mengantisipasi kejahatan. yaitu membentuk kerjasama yang baik antara pihak kepolisian dengan Departemen komunikasi dan informasi yang berkepentingan dalam pengaturan/regulasi di bidang teknologi Informasi serta pengelola jaringan internet, sehingga terjalin sinergi untuk melakukan penegakan hukum di bidang teknologi informasi yang terpadu, hal ini dapat dibentuk dalam suatu *cyber task force. Cyber task force* ini nantinya akan berperan dalam proses upaya penegakan hukum, baik yang yang bersifat preventif maupun represif.

   Akses tanpa hak juga harus ditempuh dengan pendekatan teknologi (techno prevention). Disamping itu diperlukan pula pendekatan budaya/kultural, pendekatan edukatif dan bahkan pendekatan global (kerja sama internasional) karena kejahatan ini melampaui batas-batas negara atau bersifat transnational/ transborder, sehingga perlu dilakukan juga kerjasama internasional untuk mengantisipasi kejahatan lintas teritorial, karena banyak kasus yang melibatkan beberapa negara, sehingga akan sulit dalam prosesnya tanpa bantuan kerjasama internasional.

Saran

1. Pengaturan mengenai tindak pidana akses tanpa hak masih kurang lengkap yang termuat dalam UU ITE, sebaiknya dilakukan kebijakan hukum pidana, mengikuti perkembangan pesatnya teknologi informasi, sehingga dapat menjangkau bentuk kejahatan yang cybercrime yang makin kompleks, bukan hanya itu pengaturan money laundry melalui sarana teknologi informasi harus diatur, supaya pelaku money laundry melalui sarana teknologi informasi dapat dijerat pidana.
2. Polri perlu meningkatkan sarana, prasarana, dan sumberdaya manusia dan membangun puslabfor forensic yang lebih baik, serta dibentuknya kerjasama dengan kementrian Kominfo maupun APJII dalam mengantisipasi meningkatnya tindak pidana akses tanpa hak, baik dari segi kuantitas maupun kualitas, ini merupakan salah satu faktor penegakan hukum, juga tingkat kesadaran masyarakat dalam mematuhi hukum.

DAFTAR PUSTAKA

A. BUKU

Abdul Kadir Muhammad dan Rilda Murniati, *Segi Hukum Lembaga Keuangan dan Pembiayaan*, (Bandung: PT. Citra Aditya Bakti, 2000).

Adami Chazawi, *Pelajaran Hukum Pidana Bagian 2.,* Jakarta: Rajawali Pers, 2005

Adami Chazawi, *Pelajaran Hukum Pidana I.*, Jakarta : PT. Raja Grafindo, 2010.

Adami Chazawi, *Pelajaran Hukum Pidana*, Jakarta; Raja Grafindo Persada, 2002

Aloysius Wisnusubroto, *Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer,* Universitas Atmajaya, Yogyakarta, 1999

Andi Hamzah dalam Lilik Mulyadi, *Hukum Acara Pidana Normatif, Teoritis, Praktik, dan Permasalahannya*, Bandung: PT. Alumni. 2007.

Andi Hamzah dan Boedi D. Marsita, *Aspek-aspek Pidana Dibidang Komputer*, Sinar Grafika, Jakarta, 1989..

Andi Hamzah, *Hukum Acara Pidana Indonesia*, Edisi Kedua Sinar Grafika, Jakarta, 2013.

Andi Hamzah, *Sistem Pidana dan Pemidanaan Indonesia,dari Retribusi ke Reformasi*, (Jakarta: Pradnya Paramita, 1986).

Ashadi Siregar, *"Negara, Masyarakat dan Teknologi Informasi"*, Makalah pada Seminar Teknologi Informasi, Pemberdayaan Masyarakat, dan Demokrasi, Yogyakarta, 2001.

B. Arief Sidharta, *Refleksi tentang Struktur Ilmu Hukum : Sebuah Penelitian tentang Fondasi Kefilsafatan dan Sifat Keilmuan Ilmu Hukum sebagai Landasan Pengembangan Ilmu Hukum Nasional Indonesia*, Bandung, Mandar Maju, 1999.

B. Simandjuntak, *Pengantar Kriminologi dan Patologi Sosial*., Bandung : Tarsito, 1981.

B.E. Morrison, *The School System : Developing its capacity in the regulation of a civil society*, in J. Braithwaite & H. Strang (Eds.), *Restorative Justice and Civil Society*, (Cambridge University Press, 2001).

Bambang Poemomo, *Asas-asas Hukum Pidana.,* Jakarta : Graha Indonesia, 1994.

Barda Nawawi Arief, *Beberapa Aspek Kebijakan Penegakan dan Pengembangan Hukum Pidana,* (Bandung: PT. Citra Aditya Bakti, 2005).

Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, (Jakarta: PT. Kencana Prenada Media Group, 2008).

Barda Nawawi Arief, *Kapita Selekta Hukum Pidana*, PT.Citra Aditya Bakti, Bandung, 2003.

Barda Nawawi Arief, *Mediasi Penal Penyelesaian Perkara Diluar Pengadilan*, (Semarang: Pustaka Magister, 2010).

Barda Nawawi Arif, *Kebijakan Penanggulangan Kejahatan dengan Pidana Penjara*., Semarang : CV. Ananta, 1994.

Black Law Dictionary

C.S.T. Kansil dan Christine S.T. Kansil, *Latihan Ujian Hukum Pidana*., Jakarta : Sinar Grafika, 2007.

David S. Wall, *Cybercrimes and the Internet,* Routledge Publisher, London, 2001.

Didik J.Rachbini, *"Mitos dan Implikasi Globalisasi" : Catatan Untuk Bidang Ekonomi dan Keuangan*, Pengantar edisi Indonesia dalam Hirst, Paul dan Grahame Thompson, Globalisasi adalah Mitos, Jakarta, Yayasan Obor, 2001.

Didik M. Arief Mansyur, Elisatris Gultom, *Cyber law Aspek Hukum Teknologi Informasi*, Bandung, Reflika Aditama, 2005.

Djoko Sarwoko, *Computer Crime : sebagai dimensi Baru Tindak Pidana Ekonomi*, Varia Peradilan Nomor 21 Tahun II Juni 1987.

Donn B. Parker, *Fighting Computer Crime*, Charles Scrbner's Sons, New York.

Edmond Makarim, *Kompilasi Hukum Telematika*, PT. Raja Grafindo Persada, Jakarta, 2003.

Abdul Wahid, *Kejahatan Mayantara (Cyber Crime)*, Refika Aditama, Bandung, 2005.

Erman Rajagukguk, *Tindak Pidana Pencucian Uang (Money Laundering) Peraturan Perundang-undangan*, (Jakarta: Fakultas Hukum Universitas Indonesia Lembaga Studi Hukum dan Ekonomi, 2004.

Erna Dewi, Firganefi, *Sistem Peradilan Pidana Indonesia (Dinamika dan*

Perkembangan), PKKPUU FH UNILA, 2013.

Nyoman Serikat Putra Jaya, *Beberapa Pemikiran ke Arah Pengembangan Hukum Pidana*, PT.Citra Aditya Bakti, Bandung, 2008.

Finacial Action Task Force On Money Laundering, FATF-VII Report on Money Laundering Typologies, Annex 3. 28 June 1996:5.

Financial Intelligence Unit /FIU's in Action: 100 Cases from the Egmont Group.

H.T. Siahaan , *Money Laundering Pencucian Uang dan Kejahatan Perbankan*, cet. 1, Jakarta: Pustaka Sinar Harapan, 2002.

Harkristuti Harkrisnowo, *Kriminalisasi Pemutihan Uang: Tinjauan Terhadap UU No. 15 tahun 2002*, Proceedings-Kerjasama Pusat kajian Huum dan Mahkamah Agung RI, cet. I. (Jakarta: Mahkamah Agung RI, 2003)

I Dewa Made Suartha, *Hukum Pidana Korporasi : pertanggungjawaban pidana dalam kebijakan hukum pidana Indonesia.*, Malang : Setara Press, 2015.

Jan Remmelink, *Hukum Pidana: Komentar atas Pasal-Pasal Terpenting Dari KUHP Belanda dan Padanannya Dalam KUHP Indonesia*, Terjemahan T. P. Moeliono, (Jakarta: Gramedia Pustaka Utama, 2003).

Abdul Wahid, *Kriminologi*. Raja grafindo Persada, Jakarta, Jakarta, 1996.

JE.Sahetapy, *Hukum Pidana*, Liberty, Yogyakata.

Josua Sitompul. *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana*, Tatanusa, Jakarta, 2012.

Kadri Husin, Budi Rizki H, *Sistem Peradilan Pidana di Indonesia*, Lembaga Penelitian Universitas Lampung.

Koentjaraningrat, *Kebudayaan Mentalitet dan Pembangunan*, Jakarta, Gramedia, 1992.

Leden Marpaung, *Proses Penanganan Perkara Pidana*, Jakarta: Sinar Grafika, 1992.

Marc Ancel, *Social Defence (terjemahan dari La Nouvelle Defence Sociale*),London,1965, hlm. 209. Lihat dalam Sudarto, Hukum dan Hukum Pidana.

Mas Wigrantoro Roes Setiyadi, *"Implikasi Multi dimensional dari Kebijakan Telematika Indonesia",* makalah pada seminar Dies Natalis Fisipol UGM Yogyakarta ke-46, 19 September 2001.

Mochtar Kusumaatmadja, *Pengantar Ilmu Hukum: Suatu Pengenalan Pertama*, Ruang Lingkup Berlakunya Hukum (Buku 1), Bandung, Alumni, 2000

Moeljatno, *Asas-Asas Hukum Pidana*, Rineka Cipta, Jakarta, 2008.

Muladi dan Barda Nawawi Arief, *Teori-Teori dan Kebijakan Pidana*, Alumni, Bandung, 1984.

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

Peter J. Quirk, *Money Laundering: Muddying the Macro Economic,* March 1997.

Petrus Reinhard Golose, *Perkembangan Cybercrime Dan Upaya Penangananya Di Indonesia Oleh Polri*, Buletin Hukum Perbankan dan Kebanksentralan 29 Volume 4 Nomor 2, Agustus 2006

Prodjohamidjoyo, *Memahami Dasar-Dasar Hukum Pidana*, Pradnya Paramita, Jakara, 1997.

Romli Atmasasmita, *Sistem Peradilan Pidana: Perspektif Eksistensialisme dan*

Abolisionisme, (Bandung: Bina Cipta, 1996).

Ronny Hanitijo Soemitro, *Metodologi Penelitian Hukum*, Jakarta, Ghalia Indonesia, 1982.

Soerjono Soekanto, *Kegunaan Sosiologi Hukum Bagi kalangan Hukum*, Alumni, Bandung, 1986.

Soerjono Soekanto, *Pengantar Penelitian Hukum*, UI Press, Jakarta, 1986.

Soerjono Soekanto, *Pokok-pokok Sosiologi Hukum*, Rajawali Pers, Jakarta, 1980.

Sudarto, *Hukum dan Hukum Pidana*, Alumni, ,Bandung , 1977.

Sudarto, *Hukum pidana I*, Semarang; Yayasan Sudarto, 1990.

Sudikno Mertokusumo, *Mengenal Hukum Sebab Pengantar*, Liberti, Yogyakarta, 1999.

Summary Report, Resource Material Series No.7,UNAFEI,1974,hlm.95, lihat dalam Barda Nawawi Arief, Bunga Rampai Kebijakan Hukum Pidana.

Sutan Remy Sjahdeini, *Seluk Beluk Tindak Pidana Pencucian Uang dan Pembiayaan Terorisme,* (Jakarta: Pustaka Utama Grafiti), 2007.

Tangled Web: *Tales of Digital Crime from the shadoows of cyberspace, richard Power*, QUE Division of Macmillan USA, 2000.

Tri Andrisman, *Delik Tertentu Dalam KUHP,* Universitas Lampung, Bandar Lampung, 2011.

Wolfgang, Marvin E., Leonard Savizt, Norman Johnson. *The Sociology of Crime and Delinquency*. Second Edition. New York/London/Sydney/Toronto: John Wiley & Sons In., 1962, 1970.

Yenti Ganarsih, *Kriminalisasi Pencucian Uang (Money laundering),* cet. 1, (Jakarta: Program Pascasarjana Fakultas Hukum Universitas Indonesia, 2003).

Yunus Husein (c), *Bunga Rampai Anti Pencucian Uang*. (Bandung: Books Terrace&Library), 2007.

Yunus Husein (d), *"Upaya Memberantas Pencucian Uang (Money Laundering) dan Penerapan Ketentuan Know Your Customer," (Makalah Disampaikan dalam Rangka Sosialisasi UU No. 15 tahun 2002 tentang Tindak Pidana Pencucian Uang*, Jakarta 5 September 2002).

Yunus Husein (d), *Negeri Sang Pencuci Uang*, (Jakarta: Pustaka Juanda Tigalima, 2005).

Yunus Husein, *Bunga Rampai Anti Pencucian Uang*, (Jakarta: Books Terrace & Library, 2007).

B. PERUDANG-UNDANGAN

UUD 1945 Amandemen ke I sampai dengan ke IV.

Undang-Undang Nomor 8 Tahun 1981 Tentang Kitab Undang-Undang Hukum Acara Pidana

Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Undang-Undang tentang Tindak Pidana Pencucian Uang

C. WEBSITE

Susan W Brenner dalam The Computer Fraud and Abuse Act, di unduh dari http://www.panix.com/ ~eck/computer- fraud-act.html

Sara L. Marler, The Convention on Cybercrime : Should the United States Ratifiy, www.nesl.edu/lawrev/vol37/1/ marler.pdf, didownload pada 6 Mei 2018

Penal Code of Japan, diunduh dari http://www.isc.meiji.ac.jp/~sumwel_h/Arc-Laws/Penal%20Code%20Japan.htm

M.E. Kabay, Crime, Use Of Computers in, www2.norwich.edu/mkabay/ overviews/ crime_ use_of_computers_in.pdf, di download pada 6 Mei 2018.

http:// typinggugungunawan.blogspot. com/2012/ 03/ pengertian- dan-sistemhukum acara. htm, Diakses hari Kamis, 22 Juni 2018 Pukul 04.00.

http://en.wikipedia.org/wiki/Computer_ crime

http://nasional.kompas.com/read/2015/0 5/12/06551741/ Indonesia. Urutan. Kedua. Terbesar. Negara.Asal.Cyber.Crime.di.Du nia

https://www.cnnindonesia.com/nasional / 20161230232449-12-183255/cyber-crime-kasus-kejahatan-terbanyak-di-2016

Budi Raharjo, Pernak-pernik Pengaturan Cyber Space di Indonesia, 2001, http/www budi_insan.web.id