BAB III
CONTOH KASUS WEBSITE ATAU SITUS PERUSAHAAN YANG DI RETAS ATAU *HACKING*

A. Kasus *hacking* atau peretasan terhadap Telkomsel

Pertama, situs telkomsel yang diretas *hacker*, kejadian tersebut terjadi pada tanggal 28 april 2017, ramai dengan pembahasan soal situs resmi telkomsel yang tampak beda dari biasanya. Dalam laman tersebut peretas (hacker) memprotes harga paket data telkomsel yang dianggap terlalu mahal. Deskripsinya berisi kata-kata kasar. Direktur Utama Telkomsel, Ririek Adriansah menceritakan kronologi dan motif pelaku yaitu dengan menjebol sistem dari telkomsel. Kejadian tersebut terjadi karena diketahui pelaku kecewa dengan tarif mahal dari telkomsel sehingga pelaku menjebol sistem dari telkomsel. Dengan kejadian tersebut tentunya menimbulkan kerugian dan membuat malu provaider tersebut. karena notaben nya telkomsel adalah perusahan telekomunikasi tetapi faktanya masih dapat diretas oleh hacker.

Kejadian tersebut telah dilaporkan oleh pihak dari telkomsel dan penyidik pun mulai bekerja, akan tetapi hingga saat ini kasus tersebut masih belum terungkap dan belum diketahui siapa pelakunya. Modus pelaku dalam menjalankan aksi nya yaitu dengan menggunakan server luar lalu secara masuk ke jaringan atau web milik telkomsel. Hal tersebut biasa digunakan oleh pelaku hacking, karena dapat menghilangkan jejak dan/atau tidak dapat terditeksi keberadaanya. Setelah pelaku masuk ke jaringan atau website dari telkomsel lalu pelaku menliskan kalimat-kalimat

yang berisi sindiran kepada telkomsel terkait tarif mahal dan tidak sebanding dengan kwalitasnya.

Kejadian tersebut berdampak kerugian bagi perusahaan telkomsel karena diketahui pada saat diretas oleh pelaku, secara langsung website dari telkomsel tidak dapat diakses dan digunakan selama beberapa saat. Tndakan tersebut merupakan tindak pidana yang harus segera di usut “ujar direktur utama telkomsel”.

B. Kasus *hacking* atau peretasan terhadap indosat

Kedua, situs milik Indosat yang diretas hacker. Pada tanggal 29 april 2017 giliran situs indosat yang diretas oleh hacker. Selang sehari dari peretasan telkomsel. Untuk kasus peretasan situs indosat, peretas menjahili subdomain. Si *hacker* menganti tampilan situs web atau dikenal dengan istilah deface. Hacker pun meninggalkan pesan di situs web tersebut yang isinya berupa rasa kesal setelah melihat oprator lain menyindir diretasnya situs telkomsel oleh *hacker* tersebut. berbeda dengan kasus telkomsel, *hacker* tersebut meningglkan nama tim di subdomain yang ditulis indoxploit-Sanjungan jiwa- J1oVal. Setelah itu situs arena indosat sudah tidak bisa di akses selama satu hari. Tentunya tindakan tersebut membawa rugi bagi perusaahan provaider tersebut.

Modus yang digunakan pelaku dalam menjalankan aksi nya masih sama dengan kasus peretasan terhadap telkomsel. Pelaku menggunakan server luar untuk menjebol website indosat yang pada akhirnya situs tersebut tidak dapat diakses selama satu hari, sehingga jejak dari pelaku

pun tidak dapat ditemukan. Dari beberapa kegiatan hacking tersebut pelaku dapat masuk secara bebas kedalam situs perusahaan yang mana pelaku pun dapat mengakses data-data rahasia dari perusahaan.

BAB IV
PENERAPAN SANKSI PIDANA TERHADAP PELAKU *HACKING* ATAU PERETASAN TERHADAP SITUS ATAU *WEBSITE* PERUSAHAAN BERDASARKAN PASAL 30 UNDANG-UNDANG NOMOR 19 TAHUN 2016 TENTANG PERUBAHAN ATAS UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

1. Penerapan sanksi pidana terhadap pelaku hacking atau peretasan terhadap situs atau website perusahaan

Penerapan sanksi pidana terhadap pelaku hacking atau peretasan terhadap situs atau website perusahaan dapat dikenakan dengan Pasal 30 ayat (3) Undang-Undang nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, yang menyatakan bahwa ‘ setiap orang dengan sengaja dan tanpa hak melawan hukum mengakses computer dan/atau system elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol system pengamanan di penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp. 800.000.000,- (delapan ratus juta rupiah). akan tetapi yang menjadi permasalahan adalah ketika pelaku hacking tersebut hingga saat ini tidak dapat ditemukan atau diketahui keberadaanya. Inilah yang menjadi permasalahan serius bagi pemerintah, karena akibat tidak diketahuinya pelaku peretasan maka norma hukum tersebut tidak dapat diterapkan secara langsung.

TindakanHacking merupakan bagian dari cyber crime, dimana tindakan tersebut merupakan perbuatan pidana dan dapat dikenai dan/atau dijatuhkan sanksi pidana.Sebagai Negara hukum pemerintah harus

melindungi dan memberikan rasa aman kepada masyarakat termasuk diantaranya terhadap korban dari tindakan peretasan, dimana hal tersebut merupakan domain dari tujuan hukum pidana.

Mengacu kepada kasus peretasan website indosat, pelaku menggunakan server luar sehingga perbuatan hacking tersebut tidak dapat terditeksi oleh server lokal.Prilaku tersebut memudahkan perbuatan pidana yang dilakukan oleh pelaku sehingga sulit terditeksi oleh penegak hukum. Inilah yang menjadi kelemahan dalam proses penegakan hukum dimana sarana atau fasilitas yang digunakan oleh penegak hukum tidiak terakomodir oleh pemerintah sehingga menjadi celah bagi para hacker untukmelangsungkan perbuatannya.

Sulitnya menditeksi keberadaan pelaku hacking merupakan suatu bentuk tidak berjalannya proses penegakan hukum, sehingga penerapan sanksi pidananya pun tidak dapat diterapkan,Sementara perbuatan yang dilakukan oleh pelaku tersebut telah terjadi dan merupakan suatu tindak pidana yang diatur di dalam Pasal 30 Undang-Undang nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Inilah yang sebenarnya menjadi permasalahan. Ketika suatu norma hukum nya telah diatur akan tetapi prosesnya tidak berjalan dengan baik. Jika melihat kepada contoh kasus yang penulis teliti, dapat dilihat bahwa tindakan cyber dapat menimpa siapapun termasuk diantaranya provider sekalipun.Lemahnya upaya preventif dan represif dari pemerintah menjadikan tindakan tersebut terus berulang.

Tindakan cyber atau cyber crime adalah permasalah yang terjadi karena perkembanan zaman yang begitu cepat. Dalam hal ini upaya penanggulannya secara nyata yaitu dengan hukum pidana.Hukum pidana sebagai alat untuk mengatur tindakan-tindakan atau perbuatan yang hidup di masyarakat seharusnya dapat meredam arus perkembangan teknologi informasi yang begitu cepat, sehingga tujuan dari hukum pidana tersebut dapat tercapai.Mengacu kepada contoh kasus peretasan website milik indosat dan telkomsel yang diretas dan hingga saat ini pelaku nya tidak dapat ditemukan, merupakan contoh kongkrit bahwa tujuan dari hukum pidana tidak tercapai. Sebagaimana diketahui bahwa tujuan dari hukum pidana modern yaitu pencegahan dan penanggulangan kejahatan, akan tetapi hal tersebut belum dilakukan secara maksimal sehingga kaidah hukumnya pun tidak dapat diterapkan secara benar.

Meskipun dunia siber adalah dunia virtual, hukum tetap diperlukan untuk mengatur sikap tindak masyarakat setidaknya karena dua hal.Pertama masyarakat yang ada di dunia virtual ialah masyarakat yang berasal dari dunia nyata, masyarakat memiliki nilai dan kepentingan baik secara sendiri-sendiri maupun bersama-sama yang harus dilindungi.Kedua, walaupun terjadi di dunia virtual, transaksi yang dilakukan olehmasyarakat memiliki pengaruh dalam dunia nyata, baik secara ekonomis maupun non ekonomis, dari sisi tersebut hukum harus hadir untuk mengakomodir kebutuhan hukum di tengah masyarakat untuk menghadapi perkembangan teknologi yang begitu cepat saat ini. Secara

teoritis dalam rangka penanggulangan kejahatan dapat meggunakan upaya-upaya hukum yang diantaranya adalah upaya penanggulangan secara preventif dan penanggulangan secara revresif. Upaya penanggulangan tersebut dapat dijalankan sebelum dan sesudah terjadinya tindakan kejahatan dalam hal ini adalah kejahatan cyber. Secara kongkrit pemerintah dapat menanggulangi perbuatan hacking yaitu dengan menggunakan upaya preventif terlebih dahulu dengan cara melakukan pengawasan secara serius terhadap perkembangan teknologi sehingga secara tidak langsung dapat membatasi tindakan hacking di indonesia. Selain itu upaya revresif nya yaitu dengan menerapkan sanksi pidana yang maksimal terhadap pelaku.

Pemanfaatan teknologi informasi dan transaksi elektronik dilaksanakan berdasarkan asas kepastian hukum, manfaat, kehati-hatian, itikad baik, dan kebebasan memilih teknologi atau netral teknologi.Hal-hal tersebut seharusnya digunakan oleh para penggunan teknologi untuk senantiasa memanfaatkan perkembangan teknologi secara bijak, bukan untuk dijadikan sebagai sarana perbuatan melawan hukum.Dalam hal ini perlu kesadaran hukum yang dilakukan oleh semua masyarakat untuk mengunakan dan memanfaatkan teknologi secara baik dan bijak.

2. Penegakan hukum terhadap tindakan hacking atau peretasan di Indonesia

Penegakan hukum terhadap tindakan hacking atau peretasan di indonesia masih lemah dan/atau belum ditegakan secara nyata dimana

pada kedua contoh kasus yang penulis teliti yaitu kasus peretasan situs atau website telkomsel dan kasus peretasan situs indosat hingga saat ini pelaku nya belum ditemukan. Ini lah yang menjadi permasalahan dimana ketika suatu aturan hukum nya telah ada tetapi tidak di imbangi oleh profesionalisme dari apratur penegak hukum nya itu sendiri yang dalam hal ini adalah kepolisian. Meskipun telah dibentuk unit cyber pada tingkatan kepolisian tetapi tidak dapat mengakomodir permasalahan peretasan/cyber crime di indonesia. Seolah-olah pelaku lebih mahir dari pada penegak hukum nya.Penegakan hukum dapat diartikan sebagai tindakan menerapkan perangkat sarana hukum untuk memaksa sanksi hukum guna menjamin penataan terhadap ketentuan yang ditetapkan di dalam suatu peraturan. Esensi penegakan hukum dipengaruhi oleh beberapa faktor diantaranya yaitu hukum nya itu sendiri, penegak hukum (pihak-pihak penegak hukum), sarana atau fasilitas yang mendukung penegak hukum, masyarakat dan faktor kebudayaan yang hidup dimasyarakat. Faktor-faktor tersebut sangat mempengaruhi penegakan hukum khususnya penegakan hukum perkara cyber crime seperti contoh kasus yang penulis teliti.

Permasalahan tersebut perlu di evaluasi oleh pemerintah, dimana untuk dapat mengungkap kasus-kasus cyber tidak hanya dibebankan kepada kepolisian yang pada prinsipnya sebagai pintu gerbang sistem peradilan pidana, tetapi perlu melibatkan elemen-elemen lain seperti kominfo, kejaksaan dan kementrian lainya yang terkait dengan kemananan dan pertahanan.

Penegakan hukum terhadap pelaku cyber dinilai sulit karena terkadang pelaku lebih mahir dari apratur penegak hukum itu sendiri. Merujuk pada kedua kasus yang penulis teliti, yang mana hingga saat ini pelaku tidak dapat ditemukan merupakan gambaran nyata terkait dengan proses penegakan hukum terhadap kasus-kasus cyber crime di indonesia.

Kepolisian sebagai sub sistem awal dari proses penegakan hukum seharusnya dapat meningkatkan kualitas dan profesionalisme nya terkait untuk mengungkap kasus-kasus cyber crime, sehingga proses penegakan hukum nya pun akan berjalan.

Faktanya kedua kasus yang penulis teliti yaitu peretasan website indosat dan peretasan website telkomsel hingga saat ini tidak dapat terungkap siapa pelakunya. Tentunya ketika suatu kasus tidak terungkap dan/atau tidak dapat ditegakan maka dikhawatirkan perbuatan tersebut akan terus berulang. Kasus tersebut merupakan bagian kecil dari kejahatan cyber yang tidak terungkap oleh pihak kepolisian.Ditengah masyarakat terdapat kasus-kasus serupa yang dianggap hal biasa, sementara terdapat aturan hukum yang mengatur terkait perbuatan tersebut.

Dari fakta yang hidup tengah masyarakat seharusnya aparat penegak hukum meningkatkan kualitas untuk senantiasa memberikan rasa aman bagi masyarakat terkait tindakan hacking. Membahas penegakan hukum tidak terlepas dari kinerja apratur penegak hukum tersebut dimana seharusnya perbuatan hacking atau peretasan dapat ditegakan setegak-tegaknya. Secara konsepsional inti dan arti penegakan hukum terletak pada kegiatan menyerasikan hubungan nilai-nilai yang

terjabarkan di dalam kaidah atau norma hukum yang terdapat di dalam suatu peraturan untuk menciptakan, memelihara dan mempertahankan kedamaian pergaulan hidup.

Kejahatan siber atau cybercrime merupakan kejahatan *exstraordinary crime* yang mengancam keamanan bahkan kedaulatan suatu bangsa. Oleh karena hal tersebut maka penindakan dan penegakan hukum nya pun perlu dilakukan secara luar biasa.Maka untuk mengimbangi hal tersebut perlu aparat penegak hukum yang professional dan memiliki kapasitas untuk menegakan kasus-kasus *cyber* sehingga diharapkan para penegak hukum dapat selangkah lebih maju dari pada pelaku dan dapat mengungkap perkara-perkara *cyber.* Jika hal tersebut dapat berjalan maka diharapkan perbuatan *hacking* dapat diminimalisir atau bahkan setidak-tidaknya dapat diredam dan/atau ditegak proses hukumnya tersebut.Kesadaran hukum masyarakat mempengaruhi pelaksanaan penegakan hukum. Tanpa adanya kesadaran hukum masyarakat maka mustahil pula penegakan hukum dapat berjalan dengan baik .sebelum ada kesadaran hukum di masyarakat, maka harus ada kepatuhan hukum itu sendiri salah satunya timbul karena adanya pengtahuan tentang hukum, sehingga dalam hal ini sosialisasi hukum menjadi sesuatu yang penting untuk dilakukan oleh pemerintah. Hukum diciptakan untuk manusia, untuk itu hukum harus memberikan manfaat bagi seluruh manusia sehingga kepastian hukum, keadilan dan kemanfaatan hukum dapat terwujud dan diaplikasikan kedalam kehidupan bermasyarakat dan bernegara. Di dalam suatu negara yang sedang berkembang sepertihal nya perkembangan teknologi, fungsi hukum tidak

hanya sebagai alat kontrol sosial atau sarana untuk menjaga stabilitas semata, akan tetapi juga sebagai alat untuk melakukan pembaharuan atau perubahan di dalam suatu masyarakat.