KEJAHATAN ELEKTRONIK DALAM TRANSASKSI (FRAUD CYBER CRIME) BURSA EFEK INDONESIA PT DSFI

Syah Rani Azura
syahraniazura9@gmail.com
Izari
Izariizari98@gmail.com
Sauh Galia Maharani
sauhgaliamaharani@gmail.com
Fakultas Ekonomi dan Bisnis Universitas Maritim Raja Ali Haji

ABSTRACT

Indonesia is one of the countries that is not immune from technological developments. The influence of globalization and free trade, supported by advances in telecommunications and information technology, has expanded the space for the flow of goods transactions entering Indonesia, both legally and illegally. This study aims to analyze the case of Fraud Cyber Crime as a detection tool in the disclosure of electronic transaction crimes in a company listed on the Indonesia Stock Exchange. This research uses a qualitative research approach with the dependent variable and the independent variable. Sources of data obtained from this research are through documentation from the internet and literature study from books and journals. The results of this study are in the form of scope of cyber fraud stim. The legal basis underlying the crime of electronic transactions. detection of PT DSFI cases and prevention of electronic transaction crimes. This study focuses on cases with a type of securities market manipulation that is detrimental to customers. So it can be concluded that the importance of legal protection for victims of Cyber Crime fraud and tight security in a transaction.

Keywords: *Fraud Cyber Crime, Cyber Crime, PT DSFI, securities market, securities, technology*

1. PENDAHULUAN

1.1 Latar Belakang

Indonesia adalah salah satu negara yang tidak luput dari perkembangan teknologi. Pengaruh arus globalisasi dan perdagangan bebas yang didukung oleh kemajuan teknologi telekomunikasi dan informatika telah memperluas ruang gerak arus transaksi barang yang masuk ke Indonesia, baik secara legal maupun ilegal. Saat ini, teknologi telah berkembang dengan sedemikian pesat, sehingga proses komunikasi menjadi lebih mudah dan berkembang dengan sangat cepat. Salah satu yang diuntungkan dengan perkembangan ini adalah proses bisnis baru yang seluruhnya bergantung pada jaringan internet. Hadirnya masyarakat modern pun ditandai dengan pemanfaatan internet yang semakin luas dalam berbagai aktivitas kehidupan manusia, bukan saja di negara-negara maju, tapi juga di negara-negara berkembang termasuk Indonesia.

Perkembangan teknologi informasi di era globalisasi saat ini memiliki implikasi terhadap munculnya jenis peluang bisnis yang baru dengan berbagai transaksi yang dilakukan menggunakan alat elektronik. Meskipun perkembangan internet memberi pengaruh yang signifikan terhadap segala aspek kehidupan di seluruh penjuru dunia dengan mudah dan cepat, namun tidak menutup kemungkinan bahwa internet juga membuka peluang bagi kejatahan terutama dalam sebuah transaksi. Sehubungan dengan hal tersebut, tidak jarang juga setiap orang mudah bermain dengan hukum seperti melakukan jual beli.

Kejahatan dalam sebuah transaksi sering sekali terjadi ketika penjual dan pembeli tidak saling bertemu secara fisik untuk. Tentu hal tersebut merugikan para pihak yang bertransaksi atau korban penipuan karena kejahatan yang telah dilakukan sepihak demi keuntungan pribadi. Hal tersebut sering sekali terjadi dalam dunia bisnis di perusahaan sekuritas khususnya Bursa Efek Indonesia. Dengan beragam perkembangan teknologi pun, kerap ada berbagai bentuk kejahatan yang terjadi di pasar sekuritas karena para pelaku pasar modal baik analisis saham maupun investor merupakan faktor penting dalam pengaruh harga saham. Tentunya, dalam sebuah lembaga efek tidak pernah lepas dari segala kekeliruan dan keamanan yang terancam sehingga menjadi peluang timbulnya *Fraud Cyber Crime*.

Menurut Kamus Besar Bahasa Indonesia (KBBI) Fraud adalah tidak jujur; tidak lurus hati;tidak adil; mencurangi dan berbuat curang terhadap seseorang; menipu;mengakali; kecurangan; perbuatan yang curang; ketidak jujuran dan keculasan. Standar Kompetensi Kerja Nasional Indonesia Bidang - Audit Forensik (SKKNI AF) mendefinisikan Fraud sebagai perbuatan yang disengaja atau diniatkan untuk menghilangkan uang atau harta seseorang dengan cara akal bulus, penipuan atau cara lain yang tidak fair. Menurut Jones dan Bates (1990) Fraud terjadi dimana seseorang memperoleh kekayaan atau keuntungan keuangan melalui kecurangan atau penipuan. Kecurangan semacam ini menunjukkan adanya keinginan yang disengaja.

Cyber crime adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan termasuk ke dalam kejahatan dunia maya antara lain adalah penipuan lelang secara online, pemalsuan cek, penipuan kartu kredit/*carding*, *confidence fraud*, penipuan identitas, pornografi anak, dll. Menurut brenda nawawi (2001) kejahatan cyber merupakan bentuk fenomena baru dalam tindak kejahatan sebagai dampak langsung dari perkembangan teknologi informasi beberapa sebutan diberikan pada jenis kejahatan baru ini di dalam berbagai tulisan, antara lain: sebagai ‒kejahatan dunia maya‖ (*cyberspace/virtual-space offence*), dimensi baru dari ‒*hi-tech crime*‖, dimensi baru dari ‒*transnational crime*‖, dan dimensi baru dari ‒white collar crime.

Judul ini dipilih karena maraknya penggunaan internet di era globalisasi yang menyebabkan segala transaksi beralih penggunaannya dengan alat elektronik. Dengan sistem demikian pula, masih banyak juga terjadi penipuan dan kurangnya keamanan dalam sebuah transaksi. Oleh sebab itu, *Fraud Cyber Crime* menjadi titik fokus suatu tindak kejahatan yang fokus incarannya mencakup sektor jasa keuangan. Dalam hal ini pula, titik fokus permasalahan ada pada entitas yang bertahan lama di sector perikanan Indonesia yaitu PT Dharma Samudera Fishing Industries.

PT. Dharma Samudera Fishing Industries, Tbk adalah perseroan terbatas yang didirikan di Jakarta di bawah peraturan perundang-undangan di Indonesia, sesuai dengan akta notaris No. 3 tanggal 2 Oktober 1973 yang dibuat dihadapan Tan Thong Kie, Notaris di Jakarta dan disetujui oleh Menteri Kehakiman Republik Indonesia dengan Surat Keputusan No. YA5 / 41/9 tanggal 6 Februari 1974. Juga tercatat di Pengadilan Negeri Jakarta tanpa . 441 tanggal 13 Februari 1974 dan diumumkan dalam surat kabar resmi Republik Indonesia no. 18 tertanggal 1 Maret 1974, Addendum no.93. Operasi perusahaan mengandalkan tangkapan cakalang dan ikan kakap merah dengan fokus penjualan di pasar ekspor. Dalam perkembangannya, ruang lingkup bisnis perusahaan berkembang menjadi pengolahan industri ikan terpadu, termasuk aktivitas pengolahan sehingga menghasilkan produk yang memiliki nilai tambah seperti fillet ikan, tuna, gurita, sotong dan produk bernilai tambah lainnya. Namun, dari informasi yang didapatkan, PT Dharma Samudera Fishing Industries Tbk pernah melakukan manipulasi pasar dalam sebuah transaksi efek.

1.2 Identifikasi Masalah

Dari beberapa uraian yang telah dikemukakan pada latar belakang, maka dapat diidentifikasi masalah-masalah sebagai berikut :

1. Apa saja ruang lingkup *Fraud Cyber Crime* dan landasan hukum terhadap perlindungan korbannya?
2. Bagaimana analisis deteksi kasus manipulasi pasar pada PT DSFI?
3. Apa saja kerugian yang akan dialami oleh korban Fraud Cyber Crime?
4. Bagaimana cara memperkuat keamanan dalam transaksi elektronik dan mencegah terjadinya *Fraud Cyber Crime*?

1.3 Tujuan Penelitian

Berdasarkan identfikasi masalah tersebut, maka dapat diketahui tujuan penelitian ini adalah sebagai berikut:

1) Untuk mengetahui pengaruh *cyber crime* terhadap penipuan keuagan sehingga dapat menganalisis dan mendeteksi terjadinya *Fraud Cyber Crime* pada PT DSFI.
2) Untuk menemukan solusi pencegahan *Fraud Cyber Crime* berdasarkan landasan hukum yang berlaku serta menemukan cara memperkuat keamanan dalam sebuah transaksi di pasar Sekuritas.

2. Tinjauan Pustaka

2.1 Fraud Triangle

Cressey (1953) menemukan ada 3 (tiga) elemen yang dapat mendorong seseorang melakukan kecurangan, yaitu tekanan yang dirasakan (pressure), peluang atau kesempatan yang dimiliki (opportunity) dan pembenaran atas tindakannya (rationalization). Ketiga faktor ini dikenal sebagai *Fraud Triangle* atau segitiga kecurangan, yang ditunjukkan pada Gambar 2.1. Model *Fraud Triangle* dapat menjelaskan kenapa seseorang melakukan fraud (Free dan Murphy, 2014; Morales et. al., 2014; Murphy, 2012; Murphy dan Dacin, 2011).

Sumber: Google

Gambar 2.1

Semakin besar peluang yang dimiliki atau semakin kuat tekanan yang dirasakan, maka semakin sedikit rasionalisasi yang dibutuhkan untuk memotivasi seseorang melakukan kecurangan. Sebaliknya, semakin tidak jujur seorang pelaku, semakin sedikit kesempatan atau tekanan yang diperlukan untuk melakukan kecurangan (Zimbelman, 2014).

Cressey (1953) menyatakan ada 2 (dua) elemen mendasar dari peluang untuk melakukan kecurangan. Pertama adalah general information yang dimiliki setiap pegawai. Setiap orang dalam organisasi memiliki pengetahuan atas organisasi tempatnya bekerja,

sehingga mampu untuk mengambil keuntungan atas jabatannya dalam organisasi. Elemen yang kedua adalah technical skill, yaitu keterampilan dan kemampuan teknis seseorang yang dapat memperbesar peluangnya melakukan kecurangan. Pegawai dengan keterampilan dan kemampuan di bidang akuntansi berpeluang lebih besar untuk melakukan kecurangan dan menyembunyikannya dibanding orang dengan kemampuan non-akuntansi.

Tekanan adalah elemen kedua dari segitiga kecurangan. Tekanan yang dimaksud Cressey (1953) lebih spesifik kepada tekanan keuangan. Gaya hidup mewah dan upaya meningkatkan status di masyarakat dapat memotivasi seseorang melakukan kecurangan. Tekanan keuangan biasanya terkait langsung dengan pelaku, seperti sifat serakah, gaya hidup mewah, tagihan dan utang yang tinggi, kerugian keuangan pribadi serta kebutuhan keuangan yang tak terduga (Zimbelman, 2014).

Rasionalisasi adalah elemen ketiga dari segitiga kecurangan. Cohen et al. (2010) menyatakan rasionalisasi terkait dengan attitude, yaitu bagaimana seorang fraudster menyikapi perbuatannya. Rasionalisasi terkait dengan perilaku, karakter, atau seperangkat nilai etis yang mengijinkan pegawai untuk melakukan tindakan tidak jujur, atau mereka berada dalam lingkungan yang membenarkan tindakan tidak jujur tersebut (Jusup, 2014). Pelaku kecurangan berusaha mencari pembenaran untuk menjustifikasi bahwa kecurangan yang dilakukannya adalah benar (Cressey, 1953).

2.2 Cyber Crime

Secara hukum di Indonesia pun telah memiliki undang- undang khusus menyangkut kejahatan dunia maya, yaitu undang ITE tahun 2008, yang membahas tentang tata cara, batasan penggunaan computer dan sangsi yang akan diberikan jika terdapat pelanggaran. Misalnya perbuatan *illegal access* atau melakukan akses secara tidak sah perbuatan ini sudah diatur dalam pasal 30 undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik disebutkan, bahwa: –setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain ayat (1)) dengan cara apapun, (ayat (2)) dengan cara apa pun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik, (ayat (3)) dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol system pengaman.

Cybercrime pada dasarnya tindak pidana yang berkenaan dengan informasi, sistem informasi (*information system*) itu sendiri, serta sistem komunikasi yang merupakan sarana untuk penyampaian/pertukaran informasi itu kepada pihak lainnya (*transmitter/originator to recipient*) menurut (Sutanto) dalam bukunya tentang cybercrime- motif dan penindakan cybercrime terdiri dari dua jenis, yaitu:

1) Kejahatan yang menggunakan teknologi informasi (TI) sebagai fasilitas. Contoh-contoh dari aktivitas cybercrime jenis pertama ini adalah pembajakan (copyright atau hak cipta intelektual, dan lain-lain); pornografi; pemalsuan dan pencurian kartu kredit (*carding*); penipuan lewat e-mail; penipuan dan pembobolan rekening bank; perjudian on line; terorisme; situs sesat; materi-materi internet yang berkaitan dengan sara (seperti penyebaran kebencian etnik dan ras atau agama); transaksi dan penyebaran obat terlarang; transaksi seks; dan lain-lain.
2) Kejahatan yang menjadikan sistem dan fasilitas teknologi informasi (TI) sebagai sasaran. *Cybercrime* jenis ini bukan memanfaatkan komputer dan internet sebagai media atau sarana tindak pidana, melainkan menjadikannya sebagai sasaran. Contoh dari jenis-jenis tindak kejahatannya antara lain pengaksesan ke suatu sistem secara ilegal (*hacking*), perusakan situs internet dan server data (*cracking*), serta *defecting*.

Menurut Freddy Haris, *cyber crime* merupakan suatu tindak pidana dengan karakteristik-karakteristik sebagai berikut:

1) *Unauthorized access* (dengan maksud untuk memfasilitasi kejahatan);
2) *Unauthorized alteration or destruction of data*;
3) Mengganggu/merusak operasi computer.

3. Metodologi Penelitian

3.1 Jenis Penelitian

Penelitian ini menggunakan pendekatan penelitian kualitatif. Penelitian kualitatif berfokus pada berbagai metode yang melibatkan pendekatan naturalistik dan interpretatif terhadap pokok bahasannya. Penelitian kualitatif ini memiliki tujuan yang berbeda dengan penelitian kuantitatif. Tujuan penelitian kualitatif itu sendiri, berguna untuk memahami fenomena yang terjadi pada individu ataupun masyarakat yang disajikan dalam penuturan deskriptif yang terperinci.

Menurut Moleong, penelitian kualitatif adalah penelitian yang bermaksud untuk memahami fenomena tentang apa yang dipahami oleh subyek penelitian, misalnya perilaku, persepsi, motivasi, tindakan, secara holistik dan dengan cara deskripsi dalam bentuk kata-kata dan bahasa, pada suatu konteks khusus yang alamiah dan dengan memamfaatkan berbagai metode ilmiah. Menurut Kirl dan Miller, penelitian kualitatif adalah tradisi tertentu dalam ilmu pengetahuan sosial yang secara fundamental bergantung dari pengamatan pada manusia, baik dalam kawasannya maupun dalam peristilahannya.

3.2 Variabel Data

Sugiyono menyatakan bahwa variabel penelitian adalah atribut dari sekelompok objek yang diteliti yang memiliki variasi antara satu dengan yang lain dalam kelompok tersebut (Husein, 2001). Dalam penelitian ini, peneliti menggunakan 2 macam variabel, yaitu :

1. Variabel yang tergantung pada variabel lain disebut variabel terikat (dependent variable). Variabel terikat merupakan variabel yang mendapatkan pengaruh dari data karena adanya variabel bebas (Sugiyono, 2004: 33). Variabel terikat yang digunakan dalam penelitian ini yaitu Pengungkapan *Fraud Cyber Crime*.
2. Variabel yang tidak tergantung dengan variabel lainnya disebut variabel bebas (independent variable). Variabel bebas adalah variabel yang memberikan perubahan pada variabel terikat (Sugiyono, 2004: 33). Variabel bebas dalam penelitian ini yaitu Peran BAPEPAM dalam pemeriksaan sekuritas.

3.3 Teknik Pengumpulan Data

1) Dokument
   asi
   Dokumen adalah merupakan catatan peristiwa yang telah lalu.Dokumen dapat berbentuk tulisan, gambar, atau karya menumental dari seseorang lainnya.Dokumen yang berbentuk tulisan, misalnya catatan harian, sejarah kehidupan (*life histories*), cerita, biografi, peraturan, kebijakan.Dokumen yang berbentuk gambar, misalnya foto, gambar hidup, sketsa, film, video, CD, DVD, cassete, dan lain-lain.Dokumen yang berbentuk karya misalnya karya seni, karya lukis, patung naskah, tulisan, prasasti dan lain sebagainya. Secara interpretatif dapat diartikan bahwa dokumen merupakan rekaman kejadian masa lalu yang ditulis atau dicetak, dapat merupakan catatan anekdotal, surat, buku harian dan dokumen-dokumen.
2) Studi Pustaka
   Studi kepustakaan merupakan teknik pengumpulan data dengan tinjauan pustaka ke perpustakaan dan pengumpulan buku-buku, bahan-bahan tertulis serta referensi-referensi yang relevan dengan penelitian yang sedang dilakukan

4. Hasil dan Pembahasan

4.1 Ruang Lingkup *Fraud Cyber Crime* dan Landasan Hukum

Fraud Cyber Crime merupakan suatu tindak kejahatan yang fokus incarannya mencakup sektor jasa keuangan. Ada dua identifikasi terkait *Fraud Cyber Crime*, yaitu:

Social Engineerin. Tindakan manipulasi psikologis untuk mencapai suatu tujuan atau memperoleh informasi tertentu melalui tipuan secara halus hingga sang korban tidak menyadarinya. Para pelaku biasanya menggunakan media tertentu untuk memengaruhi pikiran korbannya. Misalnya dengan menyebarkannya di suatu forum online, atau dengan memasang gambar erotis, hingga membuat tulisan persuasif untuk memancing para korban agar mengklik suatu tautan yang sudah dirancang untuk menipu. Tindakan jenis ini memakai metode berbasis interaksi komputer dan biasa juga disebut sebagai *Phising*. Bagi orang-orang yang tidak terlalu melek teknologi, gegabah dan memiliki tuntutan nafsu yang tinggi, mereka lebih rentan untuk menjadi korban. Selain itu, Social Engineering juga bisa terjadi melalui interaksi sosial. Misalnya, lewat komunikasi antar individu yang dilakukan di telepon. Di sini, pelaku akan melakukan pendekatan terhadap korban untuk mendapatkan informasi yang diperlukan atau memengaruhi sang korban agar melakukan suatu tindakan. *Social Engineering* jenis ini disebut sebagai *Vishing*. Penipuan penawaran pinjaman dengan bunga yang murah, pemalsuan *Contact Center Bank*, hingga SMS penipuan merupakan beberapa contoh dari modus *Social Engineering* yang biasa terjadi.

Skimming. *Skimming* ialah suatu tindakan pencurian informasi dengan cara menggandakan informasi yang terdapat pada pita magnetik atau kartu debit secara ilegal yang bertujuan untuk memiliki kendali atas rekening korban. Tindakan ini pertamakali teridentifikasi pada tahun 2019 di California, Amerika Serikat. Saat itu pelaku menggunakan suatu alat yang ditempelkan pada slot mesin ATM. Alat ini kemudian dikenal dengan nama skimmer. Bahkan, sekarang teknologi yang digunakan oleh para pelaku skimming semakin canggih. Seperti yang tertulis pada laman *How Stuff Works*, jika kini telah beredar jenis skimmer yang dilengkapi kemampuan membaca kode PIN kartu ATM. Hebatnya lagi, alat ini dapat langsung mengirimkan data- data yang telah diperoleh melalui SMS kepada pelaku. Para pelaku tindak kejahatan memang tidak pandang bulu dan bulan. Siapa saja atau kapan saja, mungkin anda bisa menjadi salah satu korbannya. Untuk itu, perlu ketelitian dan kehati-hatian ketika berselancar di dunia maya, mendapat SMS dengan iming-iming hadiah, atau ketika ditelepon oleh nomor dan orang yang tidak dikenal.

Penyalahgunaan teknologi informasi ini yang dapat merugikan orang lain, bangsa dan negara yang menggunakan sarana komputer yang memiliki fasilitas internet yang dilakukan oleh hacker atau sekelompok cracker dari rumah atau tempat tertentu tanpa diketahui oleh pihak korban yang dapat menimbulkan kerugian moril, materil maupun waktu akibat dari perusakan data yang dilakukan oleh hacker. Untuk mengatasi kejahatan cybercrime dibutuhkan aparat penegak hukum yang memahami dan menguasai teknologi, kendala yang dihadapi oleh korban adalah dikarnakan ketidaktahuan, pengetahuan komputer dan internet sehingga apabila dirugikan tidak dapat melaporkaan segala peristiwa pidana yang dialami tentunya ini menjadi permaslahan kita bersama.

Asas dan tujuan undang-undang ini adalah pemanfaatan Teknologi Informasi dan Transaksi Elektronik dilaksanakan berdasarkan asas kepastian hukum, manfaat, kehati- hatian, iktikad baik, dan kebebasan memilih teknologi atau netral teknologi. Jadi dapat diartikan bahwa pengunaan teknologi informasi dan Transaksi elektronik diharapkan dijamin dengan kepastian hukum, memiliki manfaat, penuh kehati-hatian, beritikad baik, dan adanya kebebasan memilih teknologi dan netral.

Terdapat beberapa hukum positif lain yang berlaku umum dan dapat dikenakan bagi para pelaku *cybercrime* terutama untuk kasus-kasus yang menggunakan komputer sebagai sarana, antara lain:

1) KUHP
2) Undang-Undang Nomor 11 tahun 2008 tentang ITE
3) Undang-Undang Nomor 44 tahun 2008 tentang Pornografi
4) Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi
5) Undang-Undang Nomor 5 tahun 1999 tentang Larangan Praktek Monopoli dan Persaingan Usaha Tidak Sehat
6) Undang-Undang Nomor 8 tahun 1999 tentang Perlindungan Konsumen
7) Undang-Undang Nomor 19 tahun 2002 tentang Hak Cipta
8) Undang-Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan
9) Undang-Undang Nomor 25 Tahun 2003 tentang Perubahan atas UndangUndang Nomor 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang
10) Undang-Undang Nomor 15 Tahun 2003 tentang Pemberantasan Terorisme

Undang-undang informasi dan transaksi elektronik (UU ITE) atau yang disebut dengan *cyberlaw*, digunakan untuk mengatur berbagai perlindungan hukum atas kegiatan yang memanfaatkan internet sebagai medianya,baik transaksi maupun pemanfaatan informasinya. Pada UU ITE ini juga diatur berbagai macam hukuman bagi kejahatan melalui internet. UU ITE mengakomodir kebutuhan pelaku bisnis di internet dan masyarakat pada umumnya untuk mendapat kepastian hukum dengan diakuinya bukti elektronik dan tanda tangan elektronik digital sebagai bukti yang sah dipengadilan.UU ITE sendiri baru ada di Indonesia dan telah disahkan oleh DPR pada tanggal 25 Maret 2008. UU ITE terdiri dari 13 Bab dan 54 Pasal yang mengupas secara mendetail bagaimana aturan hidup di dunia maya dan transaksi yang terjadi di dalamnya.

4.2 Analisis Deteksi Kasus PT DSFI

Kasus manipulasi pasar yang dilakukan oleh PT Dharma Samudera Fishing Industries Tbk (DSFI) adalah sebagai berikut:

1. Pihak yang melakukan manipulasi pasar adalah PT Dharma Samudera Fishing Industries Tbk (DSFI) dan beberapa perusahaan yang turut serta bersama – sama membantu PT DSFI.
2. Melakukan transaksi perdagangan efek.
3. Tidak menyebabkan perubahan nama kepemilikan efek tersebut. Hal ini merupakan salah satu gambaran semu yang dimaksud dalam UUPM karena mereka melakukan transaksi efek namun tidak berahli kepemilikan nama atas efek tersebut. Sama saja hal nya seolah – olah tidak ada transaksi. Serta direktur dan pegawai Perusahaan Efek telah melakukan penjaminan saham milik nasabah tanpa sepengetahuan dan izin dari nasabah, yang digunakan untuk kepentingan Perusahaan Efek.

Pada kasus PT DSFI ini telah jelas terjadi praktek manipulasi pasar karena telah memenuhi unsur – unsur di dalam Pasal 92 UUPM. Seharusnya PT DSFI harus mengantikan nama kepemilikan atas saham yang sudah dijual. Dan harus meminta izin terlebih dahulu apabila akan menjaminkan efek nasabahnya. Bukan secara sembunyi – sembunyi mengambil keuntungan dari perbuatan PT DSFI tersebut. Atas perbuatan yang dilakukan oleh PT DSFI tersebut Bapepam telah memberikan sanksi administrasi kepada PT DSFI dan perusahaan – perusahaan yang turut serta membantu melakukan kejahatan PT DSFI dan anggota – anggota yang terlibat.

Berikut pola transaksi aneh saham PT DSFI:

Gambar 4.1
Sumber: Google

4.3 Kerugian Korban *Fraud Cyber Crime*

Setiap tindak kejahatan di dunia maya tentu saja mengakibatkan kerugian yang dirasakan oleh korbannya. Inilah beberapa kerugiannya:

1. Reputasi Online Bisa Terancam
   Kerugian yang ditimbulkan dari *cyber crime* adalah reputasi online bisa terancam. Apalagi jika menggunakan aktivitas online untuk berbisnis. Jika menjadi korban, bisa jadi bisnis online akan kehilangan kepercayaan pelanggan. Katakanlah, toko online terkena hacking. Pengunjung akan merasa tidak aman untuk mengunjungi situs tersebut, sehingga bisa jadi ia memutuskan untuk tidak lagi berbelanja dari toko.
2. Kehilangan Data Penting
   Kejahatan internet dapat menyebabkan kehilangan data penting. Salah satu kerugian terbesar *cyber crime* adalah kehilangan data. Hal ini bisa terjadi baik pada akun pribadi maupun website yang menyimpan data pribadi pelanggan. *Cyber crime* selalu mencari celah agar dapat mencuri data penting dan menggunakannya untuk berbagai kepentingan. Salah satunya untuk tujuan pemerasan atau menjualnya di pasar gelap. Sebagai contoh, Blackbaud, salah satu pembuat perangkat lunak manajemen keuangan pernah menjadi korban pencurian data rahasia. Perusahaan ini melaporkan bahwa situs mereka telah diretas. Peretas berhasil mencuri data tentang siswa dan alumni dari 10 Universitas di Inggris, AS, dan Kanada. Dampaknya, pelaku dapat menyebarluaskan data pribadi siswa dan alumni. Mulai nama, hingga nomor jaminan sosial.
3. Kerusakan Software dan Sistem Komputer
   Kerusakan software dan program juga bisa terjadi akibat ulah *cyber crime*. Salah satu yang membuat heboh adalah serangan *Ransomware WannaCry* yang menyerang berbagai website pemerintah. Saat itu, serangan yang terjadi menyebabkan banyak perangkat yang tidak bisa diakses. Aksi ini terutama terjadi pada sistem operasi yang rentan, baik yang sudah lawas maupun yang versi bajakan.
4. Kehilangan Sejumlah Uang
   Kerugian finansial juga menjadi dampak terbesar dari kegiatan *cyber crime*. Bentuk aksinya bisa bermacam-macam, mulai dari phishing hingga *extortion*. Tak hanya dialami oleh individu, maupun perusahaan, kehilangan sejumlah uang akibat tindak *cyber crime* juga dialami oleh negara. Negara merugi hingga ratusan miliar akibat kasus cyber crime. Berdasarkan penelitian Frost & Sullivan yang diprakarsai

Microsoft pada 2018, kejahatan siber di Indonesia bisa menyebabkan kerugian mencapai Rp 478,8 triliun atau 34,2 miliar dollar AS. Jumlah itu tergolong sangat fantastis.

4.4 Pencegahan *Fraud Cyber Crime*

1. Gunakan *Security Software* yang *Up to Date*
   Penting untuk menjaga *Security Software* kita tetap terbarukan atau up to date. Perlakuan ini akan memberikan pendefinisian kembali atas ancaman *cyber crime* maupun virus yang belum didefinisikan pada versi sebelumnya. Pembaruan ini sangat berguna bagi pengguna yang cukup sering menggunakan koneksi internet. Disarankan bagi para pemilik gadget menggunakan *Security Software* untuk membuka akses ke internet. Hal ini harus dilakukan minimal dua atau tiga kali dalam seminggu. Saat pengguna online, secara otomatis *Security Software* akan meng-*up to date* versi terbarunya.
2. Antivirus menjaga perangkat komputer dari virus Melindungi Komputer dan menjaga keamanan, paling tidak kita harus mengaplikasikan tiga program, yaitu:
   a. Antivirus, menjaga perangkat komputer dari virus
   b. Antispyware, melindungi data pemakai agar tidak ada yang melacak kebiasaan kita saat online
   c. Firewall, sistem atau perangkat yang mengijinkan lalu lintas jaringan yang dianggap aman untuk melaluinya dan mencegah lalu lintas jaringan yang tidak aman.
3. Buat Password yang sangat sulit
   Ganti password akun-akun kita untuk mencegah terjadinya cybercrime terhadap kita. Bila bisa masukan campuran huruf kecil, besar dan angka pada setiap akun kita agar memperkuat kata sandi kita. Contoh kata sandi dengan di campur dengan angka C0ntohny4. Kata sandi ini cukup kuat untuk sandi akun kita karnya di campur dengan huruf kecil, besar dan angka.
   Back up data Sebaiknya para pengguna komputer memiliki salinan dari dokumen pribadinya, entah itu berupa foto, musik, atau yang lainnya. Ini bertujuan agar data kita masih tetap bisa terselamatkan bila sewaktu-waktu terjadi pencurian data atau ada kesalahan pada sistim komputer kita.
   Jangan Sembarangan Mengklik Link yang Muncul di Social Network entah melalui Facebook, Twitter, atau Blog, sering kita temui link yang menarik perhatian. Walaupun tidak mengetahui jelas soal apa link tersebut, sajian yang menarik berupa iklan atau sekedar kuesioner dan angket membuat kita membukanya. Tidak sedikit hal ini dijadikan peluang cybercrime atau penyebaran virus komputer. Tidak jarang pula link seperti ini dikirimkan oleh teman atau saudara kita sendiri. Maka dari itu, lebih baik hanya membuka iklan yang kita butuhkan saja. Jangan tergiur akan sesuatu yang malah akan membuat kita terjebak dalam cybercrime atau virus computer.
   Ganti Password Secara Berkala Melihat banyak dan mudahnya cybercrime dilakukan sampai 15 kasus perdetik, tidak menutup kemungkinan password terpanjang pun dapat dibajak apabila digunakan bertahun-tahun. Maka, disarankan untuk mengganti password tersebut, baik secara berkala atau acak.
4. Penanggulangan Pengamanan Sistem
   Tujuan yang paling nyata dari suatu sistem keamanan adalah meminimasi dan mencegah adanya perusakan bagian dalam sistem, karena dimasuki oleh pemakai yang tidak diinginkan. Pengamanan sitem ini harus terintegrasi pada keseluruhan subsistem untuk mempersempit atau bahkan menutup adanya celah-celah unauthorized actions yang merugikan. Pengamanan secara personal dapat dilakukan mulai dari tahap instalasi sistem sampai akhirnya tahap pengamanan fisik dan

pengamanan data. Pengamanan sistem melalui jaringan dapat juga dilakukan dengan melakukan pengamanan terhadap FTP, SMTP, Telnet. dan Pengamanan Web Server.

5. Penanggulangan Global
   OECD (*The Organization for Economic Cooperation and Development*) telah merekomendasikan beberapa langkah penting yang harus dilakukan setiap negara dalam penanggulangan *Cybercrime*, yaitu :
   a. Melakukan modernisasi hukum pidana nasional dengan hukum acaranya yang diselaraskan dengan konvensi internasional.
   b. Meningkatkan sistem pengamanan jaringan komputer nasional sesuai standar internasional.
   c. Meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi dan penuntutan perkara- perkara yang berhubungan *cybercrime*.
   d. Meningkatkan kesadaran warga negara mengenai masalah cybercrime serta pentingnya mencegah kejahatan tersebut terjadi.
   e. Meningkatkan kerjasama antar negara, baik bilateral, regional maupun multilateral, dalam upaya penanganan *cybercrime*, antara lain melalui perjanjian ekstradisi dan mutual *assistance treaties*.
6. Perlunya Cyberlaw
   Cyberlaw merupakan istilah hukum yang terkait dengan pemanfaatan TI. Istilah lain adalah hukum TI (*Low of IT*), Hukum Dunia Maya (*Virtual World Law)* danhukum Mayantara. Perkembangan teknologi yang sangat pesat membutuhkan pengaturan hukum yang berkaitan dengan pemanfaatan teknologi tersebut. Hanya saja, hingga saat ini banyak negara yang belum memiliki perundang-undangan khusus di bidang teknologi informasi, baik dalam aspek pidana maupun perdata-nya. Kekhawatiran akan kejahatan mayantara di dunia sebetulnya sudah dibahas secara khusus dalam suatu lokakarya (‒*Workshop On Crimes To Computer Networks*‖) yang diorganisir oleh UNAFEI selama kongres PBB X/2000 berlangsung, dengan kesimpulan:
   a. CRC (*conputer-related crime*) harus dikriminalisasikan.
   b. Diperlukan hukum acara yang tepat untuk melakukanb penyidikan dan penuntutan terhadap penjahat cyber.
   c. Harus ada kerjasama pemerintah dan industri terhadap tujuan umum pencegahan dan penanggulangan kejahatan komputer agar internet menjadi tempat yang aman.
   d. Diperlukan kerja sama internasional untuk menelusuri para penjahat di internet.
   e. PBB harus mengambil langkah / tindak lanjut yang berhubungan dengan bantuan dan kerjasama teknis dalam penganggulangan CRC.
7. Perlunya Dukungan Lembaga Khusus
   Lembaga khusus yang dimaksud adalah milik pemerintah dan NGO (*Non Government Organization*) diperlukan sebagai upaya penanggulangan kejahatan di internet. Lembaga ini diperlukan untuk memberikan informasi tentang cybercrime, melakukan sosialisasi secara intensif kepada masyarakat, serta melakukan riset-riset khusus dalam penanggulangan cybercrime. Indonesia sendiri sudah memiliki IDCERT (*Indonesia Computer Emergency Response Team*) yang diperlukan bagi orang-orang untuk melaporkan masalah-masalah keamanan komputer.
8. Strategi Penanggulangan Cybercrime di Indonesia
   a. Strategi Jangka Pendek
      1) Penegakan hukum pidana: salah satu manivestasi untuk mebuat hukum tidak hanya sebagai barang hukum tidak hanya senagai barang rongsokan yang tidak berguna.

2) Mengoptimalkan UU khusus lainnya. Sector cyber space banyak bersentuhan dengan sektor- sektor laun yang telah memiliki aturan khusus dalam pelaksanaannya. Ada beberapa aturan yang bersentuhan dengan dunia cyber yang dapat digunakan untuk menjerat pelaku cybercrime, sehingga sepak terjangnya semakin sempit.
3) Rekruitment aparat penegak hukum. Diutamakan dari masyarakat yang menguasai dunia komputer dan internet di samping kemampuan lain yang dipersyaratkan. Strategi Jangka Menengah.
4) *Cyber police*: orang-orang khusus yang dilatih dan dididik untuk melakukan penyidikan cybercrime. Pola pembentukannya merupakan bagian dari upaya reformasi kepolisian.
5) Kerjasama internasional. Hal ini dikarenakan kejahatan modern sudah melintasi batas-batas negara yang dilakukan berkat dukungan teknologi, sistgem komunikasi, dan trasnportasi. Hal ini dapat menunjukkan adanya sistem kepolisian yang terbuka, dan mendapatkan keuntungan dalam kerjasama mengatasi penjahat- penjahat internasional yang masuk melintasi wilayah hukum Indonesia.

b. Strategi Jangka Panjang
1) Membuat UU *cybercrime*. Tujuannya adalah untuk pemberatan atas tindakan pelaku agar dapat menimbulkan efek jera dan mengatur sifat khusus dari sistem pembuktian.
2) Membuat perjanjian bilateral. Media internet adalah media global, yang tidak memiliki batasan waktu dan tempat. *Cybercrime* dapat melibatkan beberapa negara, sehingga perlu hubungan di jalur bilateral untuk menaggulanginya.

9. *Cip* sebagai anti *skimming*
Mengganti kartu debit dari teknologi pita magnetik ke kartu yang dilengkapi cip. Sebab, data nasabah yang bisa diambil oleh pelaku kejahatan adalah yang tersimpan di kartu yang dilengkapi pita magnetik.

5. Kesimpulan dan Saran

Berdasarkan pembahasan pada bab-bab sebelumnya, terdapat kesimpulan yang dapat diambil dari penelitian ini, yaitu:

4. *Fraud Cyber Crime* merupakan suatu tindak kejahatan yang fokus incarannya mencakup sektor jasa keuangan. Di samping keunggulan dan kemajuan teknologi pada transaksi efek, penting disadari bahwa ada potensi kejahatan yang bisa terjadi. Beberapa tindakan ilegal bisa dilakukan oleh pihak yang memanfaatkan teknologi untuk meraup keuntungan, ini disebut kejahatan elektronik (*Fraud Cyber Crime*). Kejahatan elektronik inilah yang berdampak merugikan nasabah maupun perusahaan sekuritas di dalam sirkulasi transaksi efek.
5. Ruang lingkup yang dikatakan kejahatan pasar modal adalah sebagai berikut: pertama, penipuan (*fraud*), sebagaimana didasarkan pada Pasal 90 UUPM. Kedua, manipulasi pasar, sebagaimana didasarkan pada Pasal 91 dan 92 UUPM. Ketiga, perdagangan orang dalam (*insider trading*), yang dasar hukumnya dapat dilihat pada Pasal 95 sampai Pasal 99 UUPM. Keempat, informasi yang menyesatkan (*misleading information*), yang dasar hukumnya dapat dilihat pada Pasal 80,81,93 UUPM. Semua pelaku kejahatan pasar modal adalah orang–orang yang melakukan aktifitas di pasar modal.
6. Pada kasus PT DSFI sudah terbukti jelas melakukan manipulasi pasar efek dengan maksud untuk menciptakan gambaran semu atau menyesatkan mengenai perdagangan, keadaan pasar, atau harga efek di bursa efek. Sehingga, penerapan

sanksi yang ada dalam UUPM berupa sanksi pidana dan sanksi administratif dalam kasus – kasus pelanggaran pasar modal yang merupakan kategori kejahatan pasar modal agar dapat menimbulkan efek jera dan memberikan kepastian hukum.

Berdasarkan uraian-uraian pada bab-bab terdahulu dan kesimpulan-kesimpulan tersebut di atas, dapat dirumuskan saran-saran sebagai berikut:

1. Sebaiknya, dalam rangka penegakkan hukum, maka segala bentuk kejahatan yang terjadi di pasar modal perlu diatur secara rinci dalam suatu peraturan yang khusus. Sehingga orang dapat langsung mengetahui dan memahami setiap perbuatan yang terjadi yang menyimpang dalam Undang-Undang yang berlaku. Sehingga tidak terjadi multitafsir mengenai kategori kejahatan pasar modal itu sendiri.
2. Hendaknya sebagai lembaga baru yang menggantikan kedudukan OJK (Otoritas Jasa Keuangan) lebih cermat dan berhati – hati dalam melakukan fungsi pengawasan di bidang pasar modal karena menginggat banyaknya kasus kejahatan pasar modal yang terjadi oleh pihak yang berusaha untuk mengambil keuntungan. Dan sebaiknya wewenang OJK ditambah untuk dapat memberikan sanksi pidana.
3. Seharusnya kasus – kasus kejahatan pasar modal yang terjadi di BEI masih belum banyak yang dapat diakses publik dan vonis yang di jatuhkan oleh Bapepam saat itu juga masih tergolong lemah. Sehingga diperlukan ketegasan kembali oleh pihak Bapepam yang memiliki tanggung jawab terhadap hal tersebut.

DAFTAR PUSTAKA

Buku:

Nasution, Bismar. *Keterbukaan Dalam Pasar Modal*. Jakarta: Universitas Indonesia Fakultas Hukum

Program Pasca Sarjana, 2001.

Agus, Rahardjo. *Cybercrime : Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*. PT Citra

Aditya Bakti: Bandung, 2002.

Peraturan Perundang-Undangan:

Republik Indonesia. Undang–Undang No. 8 Tahun 1995 Tentang Pasar Modal.
Republik Indonesia. Undang–Undang No. 21 Tahun 2011 Tentang Otoritas Jasa Keuangan. PP No. 46 Tahun 1995 Tentang Tata Cara Pemeriksaan di Bidang Pasar Modal.

Artikel Jurnal:

Witya. Bismar Nasution, dan T. Keizerina Devi. 2014. Kajian Yuridis Atas Kejahatan Pasar Modal Di
Bursa Efek Indonesia Menurut UU No. 8 Tahun 1995 Tentang Pasar Modal. Hukum Ekonomi, 3(2), 1-12.