KAJIAN KRIMINOLOGI TERHADAP PENCEGAHAN TINDAK PIDANA MANIPULASI DAN PERUBAHAN DATA PADA WEBSITE PERUSAHAAN

SKRIPSI

Diajukan Guna Memenuhi Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana Hukum
Program Studi Ilmu Hukum

Oleh :

LAILATUL FITRI TANJUNG
NPM. 1406200175

FAKULTAS HUKUM
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
MEDAN
2017

MAJELIS PENDIDIKAN TINGGI MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM
Jl. Kapten Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6624-567 Medan 20238 Fax. (061) 662
Website : http://www.umsuac.id E-mail : rektor@umsu.ac.id
Bankir. Bank Syariah Mandiri, Bank Mandiri, Bank BNI 1946, Bank Sumut

Unggul, Cerdas, Terpercaya

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

BERITA ACARA
UJIAN MEMPERTAHANKAN SKRIPSI SARJANA
BAGI MAHASISWA PROGRAM STRATA I

Panitia Ujian Sarjana Strata I Fakultas Hukum Universitas Muhammadiyah Sumatera Utara, dalam sidangnya yang diselenggarakan pada hari Senin, Tanggal 04 April 2018 Jam 08.30 WIB sampai dengan selesai, setelah mendengar, melihat, memperhatikan menimbang:

MENETAPKAN

NAMA	**: LAILATUL FITRI TANJUNG**
NPM	**: 1406200175**
PRODI/BAGIAN	**: ILMU HUKUM/HUKUM PIDANA**
JUDUL SKRIPSI	**: KAJIAN KRIMINOLOGI TERHADAP PENCEGAHAN TINDAK PIDANA MANIPULASI DAN PERUBAHAN DATA PADA WEBSITE PERUSAHAAN**
Dinyatakan	**: (B/A) Lulus Yudisium dengan Predikat Sangat Baik**
	( ) Lulus Bersyarat, Memperbaiki/Ujian Ulang
	( ) Tidak Lulus

Setelah lulus, dinyatakan berhak dan berwenang mendapatkan gelar Sarjana Hukum (SH) dalam Bagian Hukum Pidana

PANITIA UJIAN

Ketua

IDA HANIFAH, SH., M.H
NIDN: 0003036001

Sekretaris

FAISAL, SH., M.Hum
NIDN: 0122087502

ANGGOTA PENGUJI:

1. **NUR ALAMSYAH, S.H., M.H** 1. _____
2. **SYOFIATY LUBIS, S.H., M.H** 2. _____
3. **NURSARIANI SIMATUPANG, S.H., M.Hum** 3. _____
4. **ERWIN ASMADI, S.H., M.H** 4. _____

MAJELIS PENDIDIKAN TINGGI, PENELITIAN & PENGEMBANGAN
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM
Jalan Kapten Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6623301 Fax. (061) 6625474
Website : http://www.umsu.ac.id E-mail : rektor@umsu.ac.id
Bankir : Bank Syariah Mandiri, Bank Mandiri, Bank BNI 1946, Bank Sumut

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

PENDAFTARAN UJIAN SKRIPSI

Pendaftaran Skripsi Sarjana Fakultas Hukum Universitas Muhammadiyah Sumatera Utara Strata I bagi:

NAMA	:	**LAILATUL FITRI TANJUNG**
NPM	:	**1406200175**
PRODI/BAGIAN	:	**ILMU HUKUM/HUKUM PIDANA**
JUDUL SKRIPSI	:	**KAJIAN KRIMINOLOGI TERHADAP PENCEGAHAN TINDAK PIDANA MANIPULASI DAN PERUBAHAN DATA PADA WEBSITE PERUSAHAAN**
PENDAFTARAN	:	**Tanggal 29 Maret 2018**

Dengan diterimanya Skripsi ini, sesudah lulus dari Ujian Komprehensif, penulis berhak memakai gelar:

SARJANA HUKUM
BAGIAN HUKUM PIDANA

Diketahui
Dekan

IDA HANIFAH, S.H., M.H
NIDN: 0003036001

Pembimbing I	Pembimbing II
NURSARIANI SIMATUPANG, S.H., M.Hum	**ERWIN ASMADI, S.H., M.H**
NIDN: 0111117402	**NIDN: 0120028205**

MAJELIS PENDIDIKAN TINGGI, PENELITIAN & PENGEMBANGAN
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM
Jalan Kapten Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6623301 Fax. (061) 6625474
Website : http://www.umsu.ac.id E-mail : rektor@umsu.ac.id
Bankir : Bank Syariah Mandiri, Bank Mandiri, Bank BNI 1946, Bank Sumut

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

LEMBAR PERSETUJUAN PEMBIMBING

NAMA	:	LAILATUL FITRI TANJUNG
NPM	:	1406200175
PRODI/BAGIAN	:	ILMU HUKUM/HUKUM PIDANA
JUDUL SKRIPSI	:	KAJIAN KRIMINOLOGI TERHADAP PENCEGAHAN TINDAK PIDANA MANIPULASI DAN PERUBAHAN DATA PADA WEBSITE PERUSAHAAN

Disetujui Untuk Disampaikan Kepada
Panitia Ujian

Medan, 28 Maret 2018

Pembimbing I	Pembimbing II
NURSARIANI SIMATUPANG, S.H., M.Hum	ERWIN ASMADI, S.H., M.H
NIDN: 0111117402	NIDN: 0120028205

PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan di bawah ini:

Nama	:	LAILATUL FITRI TANJUNG
NPM	:	1406200175
Program	:	Strata – I
Fakultas	:	Hukum
Program Studi	:	Ilmu Hukum
Bagian	:	Hukum Pidana
Judul	:	KAJIAN KRIMINOLOGI TERHADAP PENCEGAHAN TINDAK PIDANA MANIPULASI DAN PERUBAHAN DATA PADA WEBSITE PERUSAHAAN

Dengan ini menyatakan dengan sesungguhnya bahwa skripsi yang saya tulis ini secara keseluruhan adalah hasil penelitian/karya saya sendiri, kecuali pada bagian-bagian yang dirujuk sumbernya.

Dan apabila ternyata di kemudian hari skripsi ini merupakan hasil plagiat atau merupakan karya orang lain, maka dengan ini saya menyatakan bersedia menerima sanksi akademik dari Fakultas Hukum Universitas Muhammadiyah Sumatera Utara.

Medan, Maret 2018

Saya yang menyatakan

LAILATUL FITRI TANJUNG

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM
Jalan Kapten Muchtar Basri No. 3 Medan 20238 Telp. (061) 6623301 Fax. (061) 6625474
Website: http://www.umsu.ac.id E-mail: rektor@umsu.ac.id

Unggul, Cerdas & Terpercaya

Mohon mengawab surat ini agar disebutkan nomor dan tanggalnya

SURAT KEPUTUSAN PROPOSAL SKRIPSI DAN PENGHUJUKAN DOSEN PEMBIMBING

Nomor: 09 /KEP/II.3-AU/UMSU-06/F/2018

Bismillahirrahmanirrahim

Dekan Fakultas Hukum Universitas Muhammadiyah Sumatera Utara, **Berdasarkan Surat Persetujuan Kepala Bagian Hukum Pidana, Menetapkan Proposal Skripsi dan Dosen Pembimbing Skripsi:**

Nama	:	**LAILATUL FITRI TANJUNG**
NPM	:	1406200175
Prodi/Bagian	:	Ilmu Hukum / Hukum Pidana
Jenjang Studi	:	Strata-1 (S-1)
Judul Skripsi	:	**KAJIAN KRIMINOLOGI TERHADAP PENCEGAHAN TINDAK PIDANA MANIPULASI DAN PERUBAHAN DATA PADA WEBSITE PERUSAHAAN**

Pembimbing I : NURSARIANI SIMATUPANG, SH., M. Hum
Pembimbing II : ERWIN ASMADI, SH., MH

Dengan demikian mahasiswa yang bersangkutan diizinkan untuk menyusun skripsi dengan ketentuan:

1. **Penulisan berpedoman** pada **buku panduan penulisan Skripsi,** Fakultas Hukum Universitas Muhammadiyah Sumatera Utara.
2. Tanggal Seminar: 16 Desember 2017
3. Surat penetapan proposal dan penghujukan dosen pembimbing ini **berlaku sampai tanggal: 16 Juni 2018.**

Ditetapkan di : Medan
Pada Tanggal : 18 Rabiul Akhir 1439 H
06 Januari. 2018 M

Wassalam
Dekan,

IDA HANIFAH, SH., MH

Tembusan :
1. Kepala Bagian
2. Pertinggal

MAJELIS PENDIDIKAN TINGGI MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM
Jl. Kapten Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6624-567 Medan 20238 Fax. (061) 662
Website : http://www.umsuac.id E-mail : rektor@umsu.ac.id
Bankir. Bank Syariah Mandiri, Bank Mandiri, Bank BNI 1946, Bank Sumut
Unggul, Cerdas, Terpercaya

KARTU BIMBINGAN
SKRIPSI MAHASISWA

NAMA : LAILATUL FITRI TANJUNG
NPM : 1406200175
PRODI/BAGIAN : ILMU HUKUM/HUKUM PIDANA
JUDUL SKRIPSI : KAJIAN KRIMINOLOGI TERHADAP PENCEGAHAN TINDAK PIDANA MANIPULASI DAN PERUBAHAN DATA PADA WEBSITE PERUSAHAAN
PEMBIMBING I : NURSARIANI SIMATUPANG, SH., M.Hum
PEMBIMBING II : ERWIN ASMADI, SH., M.H

TANGGAL	MATERI BIMBINGAN	KONSULTASI LANJUTAN	PARAF
02-02-2018	Seminar Proposal		
10-02-2018	Perbaikan Penulisan, tanda baca dan Metode penulisan		
28-02-2018	Perbaikan Penulisan sesuai petunjuk		
27-03-2018	Perbaikan Penulisan		
5-03-2018	Penulisan disempurnakan		
6-03-2018	Acc ke Pemb. I		
14/3.18	Bab III & IV Abstrak		PN
21-03-2018	Bedah Buku		
26/3.18	Abstrak.		PN
27/3.18	Acc dipertanggung jawabkan		PN

Diketahui Dekan

(Ida Hanifah, S.H., M.H)

Pembimbing I

PN

(Nursariani Simatupang, SH., M.Hum)

Pembimbing II

(Erwin Asmadi, SH., M.H)

ABSTRAK

KAJIAN KRIMINOLOGI TERHADAP PENCEGAHAN TINDAK PIDANA MANIPULASI DAN PERUBAHAN DATA PADA WEBSITE PERUSAHAAN

Lailatul Fitri Tanjung

Penggunaan website bagi perusahaan mempunyai manfaat yang positif seperti memudahkan urusan pemasaran, penjualan, serta pengelolaan informasi dan dokumen elektronik, namun juga mempunyai dampak negatif yaitu memunculkan perbuatan melawan hukum dan kejahatan, salah satunya adalah tindak pidana manipulasi dan perubahan data pada *website* perusahaan. Tindak pidana ini menimbulkan kerugian langsung secara materil bagi perusahaan dan membawa dampak buruk yang sangat fatal seperti hancurnya reputasi perusahaan sampai kepada perusahaan dapat mengalami kebangkrutan.

Masalah dalam penelitian ini adalah; Bagaimana bentuk tindak pidana manipulasi dan perubahan data pada website perusahaan, Bagaimana faktor-faktor penyebab tindak pidana manipulasi dan perubahan data pada website perusahaan, Bagaimana pencegahan tindak pidana manipulasi dan perubahan data pada website perusahaan. Penelitian ini adalah penelitian yuridis normatif, sumber data yang digunakan dalam penelitian ini adalah bersumber dari data sekunder yaitu studi kepustakaan (*library reseach*) yang terdiri dari bahan hukum primer, bahan hukum sekunder dan bahan hukum tersier.

Berdasarkan hasil penelitian maka diperoleh; Bentuk tindak pidana manipulasi dan perubahan data pada *website* perusahaan yaitu salah satu bentuk pemalsuan melalui komputer (*computer related forgery*) dan penipuan atau kecurangan melalui sistem komputer (*computer related fraud*) yang dilakukan dengan cara memanipulasi, menambah, mengubah data fiktif atau palsu dan membuatnya seolah-olah otentik. Faktor penyebabnya adalah faktor ekonomi, politik, balas dendam, pelampiasan kekecewaan, menguji ketangguhan pengamanan sistem komputer perusahaan dan menguji kemampuan diri sendiri dalam aplikasi teknologi informasi. Pencegahannya dengan cara upaya kebijakan penal yaitu melalui hukum pidana dan upaya kebijakan non-penal yaitu melakukan pelatihan bagi para hakim, pejabat, dan aparat penegak hukum mengenai *cybercrime*, melakukan pemantauan, pem-*back up*-an data perusahaan, memasang proteksi, pengecekan referensi atas pegawai baru/orang yang ingin bekerjasama dengan perusahaan sampai kepada pencegahan dengan menggunakan aplikasi (*software*) secara *personal computer*.

Kata kunci: kriminologi, manipulasi dan perubahaan data, website perusahaan.

KATA PENGANTAR

Assalamu'alaikum Wr. Wb

Alhamdulillahirabbil'alamin dengan mengucapkan puji syukur kehadirat Allah SWT yang Maha Pengasih lagi Maha Penyayang atas segala limpahan rahmat dan karuniaNya sehingga skripsi ini dapat diselesaikan. Skripsi merupakan salah satu syarat bagi setiap mahasiswa yang ingin menyelesaikan pendidikan strata satunya di Fakultas Hukum Universitas Muhammadiyah Sumatera Utara. Maka dari itu disusunlah skripsi yang berjudulkan: **Kajian Kriminologi Tehadap Pencegahan Tindak Pidana Manipulasi dan Perubahan Data Pada Website Perusahaan.**

Dengan selesainya skripsi ini, maka perkenankanlah diucapkan terima kasih yang sebesar-besarnya kepada:

1. Secara khusus dengan rasa hormat dan penghargaan yang setinggi-tingginya diberikan kepada Ayahanda yang tercinta, Ali Amran dan Ibunda tercinta Efdawita yang telah mengasuh serta mendidik dengan limpahan kasih sayang, juga kepada abangda Ichsan Aulia, Alfan Soni dan kakanda Lisa Safitri yang telah memberikan dukungan, semangat dan doa.
2. Rektor Universitas Muhammadiyah Sumatera Utara Bapak Dr. Agussani, M.AP atas kesempatan dan fasilitas yang diberikan kepada Penulis untuk mengikuti dan menyelesaikan pendidikan di program sarjana ini.

3. Dekan Fakultas Hukum Universitas Muhammadiyah Sumatera Utara Ibu Ida Hanifah, S.H., M.H., atas kesempatan menjadi mahasiswa Fakultas Hukum Universitas Muhammadiyah Sumatera Utara. Demikian juga halnya kepada Wakil Dekan I Bapak Faisal, S.H., M.Hum., dan Wakil Dekan III Bapak Zainuddin, S.H., M.H.
4. Terima kasih yang tak terhingga dan penghargaan yang setinggi-tingginya diucapkan kepada Ibu Nursariani Simatupang, S.H., M.Hum selaku Pembimbing I, dan Bapak Erwin Asmadi, S.H., M.H., selaku Pembimbing II yang dengan penuh perhatian telah memberikan arahan, dorongan, bimbingan dan saran sehingga skripsi ini selesai.
5. Terima kasih juga kepada seluruh Dosen Fakultas Hukum Universitas Muhammadiyah Sumatera Utara yang telah memberikan ilmunya kepada Penulis.
6. Terima kasih tidak lupa disampaikan juga kepada sahabat-sahabat yang telah banyak berperan dalam proses penyelesaian skripsi ini, memberikan semangat, motivasi serta doa terutama kepada Tri Satria, Bella Puspita Sari, Auliyani, Nur Ainun Aslam, Juti May Rena, Rini Sartika Barus, Azhari Kurniawan, Abdul Husein, Dapi Panjaitan, Penulis mengucapkan terimakasih dengan tulus semoga Allah SWT membalasnya.

Akhirnya, Mohon maaf atas segala kesalahan selama ini, begitu juga dengan skripsi ini jauh dari kata sempurna. Untuk itu, diharapkan ada masukan yang membangun untuk kesempurnaannya. Terima kasih kepada semuanya, tiada

lain yang diucapkan selain kata terima kasih, semoga kiranya mendapat balasan dari Allah SWT.

Medan, 01 Februari 2018

Hormat Penulis,

Lailatul Fitri Tanjung
NPM:1406200175

DAFTAR ISI

BAB I

PENDAHULUAN

A. Latar Belakang

Negara Indonesia merupakan negara hukum yang salah satu tujuan pembangunannya adalah mensejahterahkan kehidupan bangsa untuk terciptanya kemakmuran bagi rakyat Indonesia menjadi salah satu hal yang sangat penting. Pembangunan nasional merupakan rangkaian upaya pembangunan yang berkesinambungan yang meliputi seluruh kehidupan masyarakat, bangsa, dan negara untuk melaksanakan tugas mewujudkan tujuan nasional yang tertuang dalam Pembukaan Undang-Undang Dasar 1945 yaitu melindungi segenap bangsa dan seluruh tumpah darah Indonesia, memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa, serta ikut melaksanakan ketertiban dunia yang berdasarkan kemerdekaan, perdamaian abadi, dan keadilan sosial. Oleh karena itu, pembangunan nasional ini lebih dipusatkan pada pembangunan di bidang ilmu pengetahuan dan salah satunya dengan penerapan sistem teknologi dan informasi.

Teknologi informasi diyakini membawa keuntungan dan kepentingan yang besar bagi negara-negara di dunia terutama dalam hal memacu pertumbuhan ekonomi dunia seperti memudahkan transaksi bisnis terutama bisnis keuangan di samping bisnis-bisnis yang lainnya.[1] Dengan demikian, teknologi informasi telah memicu perubahan tatanan kebutuhan hidup masyarakat di bidang ekonomi yang notabane sebelumnya secara konvensional menjadi secara elektronik.

[1] Budi Suhariyanto. 2013. *Tindak Pidana Teknologi Informasi (Cybercrime)*. Jakarta: Rajawali Pers, halaman 1-2.

Teknologi informasi telah menciptakan jenis-jenis kegiatan dan peluang-peluang bisnis yang baru dan juga jenis-jenis pekerjaan bahkan karier baru dalam pekerjaan manusia. Dengan perkembangan teknologi informasi, transaksi-transaksi bisnis yang semula dilakukan dengan menggunakan dokumen-dokumen kertas atau *transaction based on papper* menjadi dilangsungkan dengan menggunakan dokumen-dokumen elektronik atau *electronic documents* sehingga disebut *paperless transactio*.[2]

Kemajuan teknologi informasi yang serba digital membawa orang ke dunia bisnis yang revolusioner(*digital revolution era)* dan menguntungkan pekerjaan, karena lebih mudah, murah, cepat, praktis dan dinamis. Kesempatan ini dipakai oleh para pengusaha dan dunia industri mencari pasar atas produk barang dan jasa ke seluruh dunia tanpa memerlukan modal besar dan tenaga kerja yang banyak sebagai *a bundle of rights.*[3]

Salah satu perkembangan teknologi informasi yang menarik perhatian bagi para pelaku bisnis ataupun perusahaan-perusahaan adalah aplikasi berbasis website yang berpaduan dengan teknologi internet. Aplikasi berbasis website ini dimanfaatkan oleh para pelaku bisnis atau perusahaan-perusahaan sebagai suatu sistem pemasaran dan penjualan produk-produk yang dihasilkannya, yang itu bertujuaan agar di dalam pemasarannya tidak memerlukan biaya promosi dan penjualannya cepat tinggi. Selain itu, penggunaan website juga bisa sekaligus

---

[2] Sutan Remy Syahdeini. 2009. *Kejahatan & Tindak Pidana Komputer*. Jakarta: PT Pustaka Utama Grafiti, halaman 4.

[3] Teguh Sulistia dan Aria Zurnetti. 2011. *Hukum Pidana Horizon Baru Pasca Reformasi*. Jakarta: Rajawali Pers, halaman 126.

dijadikan sebagai sistem pengelolaan informasi dan data-data elektronik atau dokumen elektronik perusahaan tersebut. Hal ini dinilai lebih efektif dan efisien.

Kenyataannya teknologi informasi kini menjadi pedang bermata dua, karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum dan kejahatan.[4] Semakin berkembang internet dalam kehidupan masyarakat ternyata menimbulkan pula sisi rawan yang gelap sampai tahap mencemaskan dengan kekhawatiran perkembangan tindak pidana baru, yakni bidang teknologi informasi berkaitan dengan *cybercrime.*[5] Seperti halnya penggunaan website yang mempunyai manfaat yang positif untuk perusahaan karena memudahkan urusan pemasaran, penjualan, serta pengelolaan informasi dan dokumen elektronik tetapi ternyata juga dapat mempunyai dampak negatif dan memunculkan perbuatan melawan hukum dan kejahatan di bidang ini.

Salah satu tindak pidana yang timbul dari penggunaan website oleh perusahaan adalah kejahatan manipulasi dan merubah data pada website perusahaan. Bentuk kejahatan manipulasi yang berhubungan dengan perusahaan sangat banyak, namun salah satunya adalah tindak pidana manipulasi dan merubah data pada website perusahaan seperti dalam perkara yang telah diputus oleh Mahkamah Agung Republik Indonesia, Putusan Nomor 116 K/Pid.Sus/2015 dan telah berkekuatan hukum tetap.

Perkara dalam putusan tersebut mengenai perusahaan perdagangan air minum kemasan dengan nama PT. Mulia Rejeki Waterindo, yang mana sistem

[4] Ahmad M Ramli. 2004. *Cyberlaw dan HAKI dalam Sistem Hukum Indonesia.* Bandung: PT Refika Editama, halaman 1.

[5] Teguh Sulistia dan Aria Zurnetti, *Loc. Cit.*

pemasaran dan penjualannya semula dilakukan secara konvensional dirubah menjadi sistem MLM (*multi level marketing*) secara *online* dengan menggunakan sarana internet dan website dengan nama www.myoxysuper.com. Dalam perkara ini dijelaskan tindak pidana dilakukan dengan cara melakukan manipulasi dan perubahan data terhadap website www.myoxysuper.com khususnya terhadap data informasi elektronik dan dokumen elektronik *member* perusahaan yaitu melakukan penambahan *member* dengan cara yang tidak sesuai dengan prosedur dan bukan informasi yang sebenarnya. Tindakan tersebut mempengaruhi struktur serta bonus *member* lain menjadi lebih sedikit sehingga menimbulkan kerugian sebesar kurang lebih Rp. 1.500.000.000,00 (satu miliar lima ratus juta rupiah) dan hilangnya kepercayaan para *member* terhadap PT. Mulia Rejeki Waterindo yang pada akhirnya akan menurunkan bahkan menghilangkan keuntungan PT. Mulia Rejeki Waterindo.

Berdasarkan contoh kasus tersebut dapat disimpulkan bahwa tindakan manipulasi dan merubah data pada website perusahaan adalah perbuatan yang dilakukan dengan kesengajaan yang bermaksud untuk mendapatkan keuntungan bagi pelakunya dan menimbulkan kerugian materil yang sangat besar bagi perusahaan tersebut, selain itu juga bisa membawa dampak buruk yang sangat fatal, seperti hancurnya reputasi perusahaan, kerugian bagi orang-orang yang berkaitan dengan perusahaan tersebut dan sampai kepada perusahaan dapat mengalami kebangkrutan. Karena itulah, agar tidak terjadi kasus-kasus lain seputar tindakan manipulasi dan merubah data pada website perusahaan maka diperlukan upaya pencegahannya agar teknologi informasi ini benar-benar dapat

dimanfaatkan sesuai dengan apa yang diharapkan, dan dapat mengurangi bahkan menghilangkan kejahatan manipulasi dan merubah data pada website perusahaan serta juga memberikan keamanan bagi perusahaan yang ingin mengembangkan usahanya melalui pemanfaatan tekonologi informasi khususnya dalam penggunaan website.

Upaya pencegahan yang berkenaan dengan kejahatan tersebut, seperti yang diatur dalam peraturan perundang-undangan salah satunya adalah Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 yang selanjutnya disingkat dengan UU ITE, belum dapat mencegah dan menanggulangi secara maksimal mengenai tindak pidana manipulasi dan perubahan data elektronik atau dokumen elektronik, karena dilihat dari berkembangnya bentuk-bentuk tindak pidana manipulasi dengan berbagai macam cara tindak pidana ini dilakukan. Hal ini menunjukkan bahwa sanksi terhadap tindak pidana ini belum cukup untuk membuat jera si pelaku, maka pencegahan dengan peraturan perundang-undangan saja tidak cukup untuk mencegah tindak pidana manipulasi data atau dokumen elektronik terkhusus tehadap tindakan manipulasi dan perubahan data pada website perusahaan, maka diperlukan upaya-upaya pencegahan lainnya. Untuk menemukan upaya-upaya pencegahan yang dapat menanggulangi tindak pidana manipulasi dan perubahan data terhadap website perusahaa harus diketahui terlebih dahulu apa saja bentuk-bentuk dan faktor penyebab terjadinya tindak pidana ini.

Berdasarkan uraian di atas, selanjutnya memunculkan ketertarikan untuk melakukan suatu penelitiaan untuk mengembangkan ilmu pengetahuan, penelitian

ini dituangkan dalam bentuk skripsi dengan judul: **Kajian Kriminologi Terhadap Pencegahan Tindak Pidana Manipulasi dan Perubahan Data pada Website Perusahaan.**

1. Rumusan Masalah

Berdasarkan uraian latar belakang di atas, maka dapat diambil suatu rumusan masalah yang menjadi permasalahan dalam penulisan ini. Adapun rumusan masalah dalam penelitian ini adalah sebagai berikut:

a. Bagaimana bentuk tindak pidana manipulasi dan perubahan data pada website perusahaan?
b. Bagaimana faktor-faktor penyebab tindak pidana manipulasi dan perubahan data pada website perusahaan?
c. Bagaimana pencegahan tindak pidana manipulasi dan perubahan data pada website perusahaan?

2. Faedah Penelitian

Berdasarkan permasalahan yang telah diuraikan, maka diharapkan penelitian ini memberikan faedah kepada banyak pihak. Adapun faedah penelitian diharapkan dapat memberikan manfaat baik secara teoritis maupun praktis yaitu:

a. Secara teoritis, dengan selesainya penulisan skripsi ini dapat memberikan faedah dari segi teoritis adalah faedah sebagai sumbangan kepada ilmu pengetahuan serta menambah wawasan dan khazanah ilmu hukum pada umumnya, khususnya dalam bidang hukum pidana terkhusus mengenai Kajian Kriminologi Terhadap Tindak Pidana Manipulasi dan Perubahan Data pada Website Perusahaan.

b. Secara Praktis, dengan selesainya penulisan skripsi ini dapat memberikan faedah dari segi praktisnya penelitian ini sebagai sumbangan pemikiran yang bermanfaat bagi kepentingan negara, bangsa, dan masyarakat, mahasiswa, serta khususnya bagi pihak-pihak yang terkait dengan permasalahan yang berkenaan dengan tindak pidana manipulasi dan perubahan data pada website perusahaan.

B. Tujuan Penelitian

Tujuan penelitian ini adalah sebagai berikut:

1. Untuk mengetahui bentuk tindak pidana manipulasi dan perubahan data terhadap website perusahaan.
2. Untuk mengetahui faktor-faktor penyebab tindak pidana manipulasi dan perubahan data pada website perusahaan.
3. Untuk mengetahui pencegahan tindak pidana manipulasi dan perubahan data pada website perusahaan.

C. Metode Penelitian

Penelitian merupakan suatu sarana pokok dalam pengembangan ilmu pengetahuan maupun teknologi. Guna mempermudah dan memperoleh hasil yang sesuai dengan standar penulisan skripsi sebagai suatu karya ilmiah, maka diperlukan suatu penelitian yang maksimal yang memerlukan ketelitian, kecermatan dan usaha yang gigih. Seiring dengan judul dan juga permasalahan yang diangkat, maka penulis akan menggunakan metode penelitian sebagai berikut:

1. Sifat Penelitian

Penelitian yang dilakukan merupakan penelitian yuridis normatif bersifat deskriptif analitis. Sifat penelitian tersebut dilakukan dengan menelaah teori-teori, konsep-konsep, asas-asas hukum, menelaah sistematika peraturan perundang-undangan, penelitian terhadap taraf sinkronisasi dari peraturan perundang-undangan, menelaah perbandingan hukum serta sejarah hukum.[6]

2. Sumber Data

Sumber data dalam penelitian ini berasal dari data sekunder. Data sekunder yakni data yang diperoleh dari bahan-bahan pustaka, bahan-bahan tersebut berkaitan dengan objek atau materi penelitian yang meliputi:

a. Bahan hukum primer, dalam penelitian ini dipakai adalah Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Putusan Nomor 116 K/Pid.Sus/2015.
b. Bahan hukum sekunder, yaitu bahan hukum yang memberikan penjelasan mengenai bahan hukum primer berupa karya-karya ilmiah, buku-buku dan lain yang berhubungan dengan permasalahan yang sesuai dengan judul skripsi.
c. Bahan hukum tersier, yaitu berupa bahan-bahan hukum yang memberikan petunjuk maupun penjelasan terhadap bahan hukum primer dan bahan hukum sekunder seperti kamus hukum, kamus besar bahasa indonesia, internet dan

[6] Soerjono Soekanto. 2014. *Pengantar Penelitian Hukum.* Jakarta: Universitas Indonesia (UI-Press), halaman 252.

sebagainya yang berhubugan dengan permasalahan yang sesuai dengan judul skripsi.

3. Alat Pengumpul Data

Alat pengumpul data dalam penelitian ini adalah penelusuran ke perpustakaan (*library research)* yaitu perpustakaan Universitas Muhammadiyah Sumatera Utara dan Perpustakaan Daerah Sumatera Utara.

4. Analisis Data

Data yang telah selesai dikumpulkan dengan lengkap, lalu kemudian di analisis secara kualitatif dan disajikan secara deskripsi yaitu menjelaskan, menguraikan, dan menggambarkan sesuai dengan permasalahan yang erat kaitannya dengan penelitian ini, kemudian menarik sebuah kesimpulan berdasarkan analisis yang telah dilakukan.

D. Definisi Operasional

Definisi operasional atau kerangka konsep adalah kerangka yang menggambarkan hubungan antara definisi-definisi konsep-konsep khususnya yang akan diteliti dalam penulisan ini. Konsep, merupakan salah satu unsur konkrit dari teori. Sesuai dengan judul penelitian yaitu **"Kajian Kriminologi Terhadap Pencegahan Tindak Pidana Manipulasi dan Perubahan Data pada Website Perusahaan"**, maka dapat diterangkan definisi operasional sebagai berikut:

1. Kriminologi adalah ilmu pengetahuan yang mempelajari tentang kejahatan, penjahat serta reaksi masyarakat terhadap kejahatan.[7] Terkhusus dalam

[7] Topo Santoso dan Eva Achjani Zulfa. 2013. *Kriminologi*. Jakarta: PT Rajagrafindo Persada, halaman 9.

penelitian ini mempelajari atau mengkaji tentang kejahatan manipulasi dan perubahan data pada website perusahaan.

2. Pencegahan tindak pidana adalah proses, cara, tindakan mencegah atau tindakan menahan agar tidak terjadi suatu tindak pidana. Dapat dikatakan suatu upaya yang dilakukan sebelum terjadinya pelanggaran atau tindak pidana. Upaya pencegahan kejahatan merupakan upaya awal dalam menanggulangi kejahatan.[8] Pencegahan tindak pidana yang dimaksud adalah pencegeahan tindak pidana manipulasi dan perubahan data pada website perusahaan.
3. Manipulasi dan merubah data adalah sebuah proses rekayasa dengan melakukan penambahan, pensembunyian, penghilangan atau pengkaburan terhadap bagian atau keseluruhan sebuah realitas, kenyataan dan fakta-fakta.[9]
4. *Website* Perusahaan adalah halaman yang merupakan satu alamat domain yang menyajikan informasi untuk publik mengenai profil perusahaan serta layanan yang dimilikinya yang lebih berfokus pada usaha dan merk produknya.[10]

[8] No Name, "Tinjauan Umum Pencegahan, Tindak Pidana dan Penipuan Jual Beli Online", melalui ***www.erepo.unud.ac.id***, diakses Senin, 19 Februari 2018, Pukul 10.02 wib.

[9] Wikipedia, "Pengertian Manipulasi", melalui ***www.wikipedia.com***, diakses Rabu, 6Desember 2017, Pukul 09.55 wib.

[10] Visigraphic, "Website Profil Perusahaan", melalui ***www.visigraphic.com***, diakses Rabu, 6 Desember 2017, Pukul 09.25 wib.

BAB II

TINJAUAN PUSTAKA

A. Kriminologi

Kriminologi merupakan ilmu pengetahuan yang mempelajari tentang kejahatan. Nama kriminologi yang ditemukan oleh P. Topinard seorang antropologi Perancis, secara harfiah berasal dari kata *crimen* yang berarti kejahatan atau penjahat dan "logos" yang berarti ilmu pengetahuan, maka kriminologi dapat berarti ilmu tentang kejahatan atau penjahat.[11]

Bonger memberikan definisi kriminologi sebagai ilmu pengetahuan yang bertujuan menyelidiki gejala kejahatan seluas-luasnya. Melalui definisi ini, Bonger membagi kriminologi ini menjadi kriminologi murni yang mencakup:[12]

1. Antropologi Kriminil ialah ilmu pengetahuan tentang manusia yang jahat (somatis)
2. Sosiologi Kriminil ialah ilmu pengetahuan tentang kejahatan sebagai suatu gejala masyarakat.
3. Psikologi Kriminologi ilmu pengetahuan tentang penjahat yang dilihat dari sudut jiwanya.
4. Psikopatologi dan Neuropatologi Kriminil ialah ilmu tentang penjahat yang sakit jiwa atau urat syaraf.
5. Penologi ialah ilmu tentang tumbuh dan berkembangnya hukuman.

Bonger juga membagi kriminologi terapan yang berupa:

1. Higiene kriminal yaitu usaha yang bertujuan untuk mencegah terjadinya kejahatan. Misalnya usaha-usaha yang dilakukan pemerintah untuk menerpkan undang-undang, sistem jaminan hidup dan kesejahteraan yang dilakukan semata-mata ntuk mencegah terjadinya kejahatan.
2. Politik kriminil yaitu usaha penanggulangan kejahatan di mana suatu kejahatan telah terjadi. Di sini dilihat sebab-sebab seorang melakukan kejahatan bila disebabkan oleh faktor ekonomi maka usaha yang dilakukan adalah meningkatkan keterampilan atau membuka lapangan kerja. Jadi tidak semata-mata dengan penjatuhan sanksi.

[11] Topo Santoso dan Eva Achjani, *Op. Cit.*, halaman 9.
[12] *Ibid.*, halaman 9-10.

Kriminologi dalam pengertian umum, merupakan kumpulan ilmu pengetahuan yang mempelajari gejala kejahatan. Dalam pengertian umum ini kriminologi merupakan kajian (*the study*) dengan pendekatan multidisiplin. Sebagai kajian dengan pendekatan multidisiplin, metode penelitiannya tergantung pada disiplin utamanya. Dalam kaitan ini penjelasan gejala kejahatan tersebut dapat berlandaskan pada berbagai ilmu dasar.[13]

Ahli biologi menjelaskan kejahatan sebagai gejala biologis, yaitu mencari adanya ciri-ciri biologis yang mempengaruhi tingkah laku manusia; ahli indokrinologi menduga adanya pengaruh kelenjar indokrin terhadap tingkah laku manusia; ahli psikologi menjelaskannya melalui aspek psikologis yang memengaruhi tingkah laku manusia; psikiater menjelaskan gejala kejahatan sebagai dipengaruhi adanya gangguan jiwa pada pelakunya; ahli hukum menjelaskannya sebagai tindakan melanggar hukum pidana; dan ahli sosiologi menjelaskannya sebagai gejala sosial yang merugikan masyarakat. Termasuk dalam pengertian kriminologi dalam arti luas ini adalah ilmu-ilmu forensik, misalnya kedokteran forensik, kimia forensik, daktiloskopi yang digunakan untuk mengungkap terjadinya peristiwa kejahatan.[14]

Menurut Wolfgang, Savitz dan Jhonston dalam *The Sociology of Crime and Delinquency* memberikan definisi kriminologi sebagai kumpulan ilmu pengetahuan tentang kejahatan yang bertujuan untuk memperoleh pengetahuan dan pengertian tentang gejala kejahatan dengan jalan mempelajari dan menganalisa secara ilmiah, keterangan-keterangan, keseragaman-keseragaman,

[13] Muhammad Mustofa. 2013. *Metodologi Penelitian Kriminologi*. Jakarta: Kencana, halaman 3.

[14] *Ibid.*, halaman 3-4.

pola-pola dan faktor-faktor kausal yang berhubungan dengan kejahatan, pelaku kejahatan serta reaksi masyarakat terhadap keduanya. Jadi objek studi kriminologi melingkupi:[15]

a. Perbuatan yang disebut sebagai kejahatan;
b. Pelaku kejahatan; dan
c. Reaksi masyarakat yang ditujukan baik terhadap perbuatan maupun terhadap pelakunya.

Banyak sekali perdebatan yang kontroversil dalam khasanah literatur kriminologi mengenai pengertian dari ketiga objek studi ini. Oleh Soerjono Soekanto dan kawan-kawan, pendapat para sarjana ini dibagi atas golongan-golongan sebagai berikut:[16]

1. Para Sarjana yang Menganut Aliran Hukum atau Yuridis

Sutherland menekankan bahwa ciri pokok dari kejahatan adalah perilaku yang dilarang oleh negara karena merupakan perbuatan yang merugikan negara dan terhadap perbuatan itu negara bereaksi dengan hukuman sebagai upaya pamungkas. Pengertian yuridis membatasi kejahatan sebagai perbuatan yang telah ditetapkan oleh negara sebagai kejahatan dalam hukum pidananya dan diancam dengan suatu sanksi. Sementara penjahat merupakan para pelaku pelanggar hukum pidana tersebut dan telah diputus oleh pengadilan atas perbuatannya tersebut. Penetapan aturan dalam hukum pidana itu merupakan gambaran dari

[15] Topo Santoso dan Eva Achjani Zulfa, *Op. Cit.*, halaman 12.
[16] *Ibid*., halaman 13.

reaksi negatif masyarakat atas suatu kejahatan yang diwakili oleh para pembentuk undang-undang pidana.[17]

2. Para Sarjana yang Menganut Aliran Non Yuridis atau Aliran Sosiologis.

Thorten Sellin mengutarakan bahwa pemberian batasan definisi kejahatan secara yuridis itu tidak memenuhi tuntutan-tuntutan keilmuan. Suatu dasar yang lebih baik bagi perkembangan kategori-kategori ilmiah menurutnya adalah dengan memberikan dasar yang lebih baik dengan mempelajari norma-norma kelakuan (*conduct norms*), karena konsep norma-norma perilaku yang mencakup setiap kelompok atau lembaga seperti negara serta merupakan ciptaan kelompok-kelompok normatif serta tidak terkurung oleh batasan-batasan politik dan tidak selalu harus terkandung dalam hukum.[18]

3. Pandangan Kriminologi baru tentang kejahatan, penjahat dan reaksi masyarakat

Rumusan kejahatan dalam kriminologi semakin diperluas. Sasaran perhatian terutama diarahkan kepada kejahatan-kejahatan yang secara politis, ekonomis dan sosial amat merugikan yang berakibat jatuhnya korban-korban bukan hanya korban individual melainkan juga golongan-golongan dalam masyarakat. Pengendalian sosial dalam arti luas dipahami sebagai usaha untuk memperbaiki atau mengubah struktur politik, ekonomi dan sosial sebagai keseluruhan.[19]

Pada umumnya, para sarjana kriminologi bersepakat bahwa yang merupakan objek penelitian kriminologi adalah kejahatan, penjahat, tingkah laku

[17] *Ibid.*, halaman 14.
[18] *Ibid.*, halaman 15.
[19] *Ibid.*, halaman 17.

menyimpang, pelaku penyimpangan, korban kejahatan, reaksi sosial terhadap tingkah laku jahat dan tingkah laku menyimpang, baik merupakan reaksi formal, yaitu bekerjanya pranata-pranata sistem peradilan pidana, maupun reaksi non formal dari sistem peradilan pidana, maupun reaksi non formal dari warga masyarakat terhadap pelaku kejahatan serta korban kejahatan dalam suatu peristiwa keseluruhan objek penelitian tersebut dianalisis dalam ruang lingkup sosiologi di bawah topik gejala sosial atau dengan kata lain objek penelitian kriminologi tersebut dipelajari sebagai gejala sosial.[20]

Fokus kajian kriminologi sebagai salah satu cabang ilmu sosial adalah kejahatan di dalam masyarakat, sehingga ruang lingkupnya sangat luas. Namun demikian, kriminologi selalu mengkaji pengertian, bentuk, modus, dan penyebab kejahatan serta reaksi masyarakat terhadap kejahatan. Salah satu reaksi masyarakat terhadap kejahatan adalah melakukan upaya memerangi kejahatan yang itu adalah upaya pencegahan atau penanggulangan kejahatan.[21]

B. Pencegahan Tindak Pidana

Definisi kata pencegahan menurut KBBI berarti menangkal sesuatu yang akan terjadi, sedangkan menurut ahli pencegahan merupakan salah satu upaya untuk menghindari kerugian, kerusakan yang terjadi pada seseorang atau masyarakat disekitarnya. Dengan demikan dapat di pahami bahwa pencegahan adalah suatu tindakan menahan, mencegah dengan sekumpulan cara-cara dan

[20] Muhammad Mustofa, *Op. Cit.*, halaman 8.
[21] Widodo. 2013. *Memerangi Cybercrime*. Yogyakarta: Aswaja Pressindo, halaman V.

melalui proses agar tidak terjadinya sesuatu yang buruk yang dapat merugikan seseorang dalam bentuk materil ataupun non materil.[22]

Berdasarkan pendapat Coffey bahwa pencegahan kejahatan dalam masyarakat dapat berarti ganda dan banyak orang berbeda pendapat dalam menjabarkan istilah tersebut. Menurut J. Edgar Hoover, pada saat menjabat Direktur *Federal Bureau of Investigation (FBI),* pencegahan kejahatan dimulai dari para pejabat tinggi, bukan hanya dengan kursi listrik yang digunakan untuk eksekusi terpidana mati di Amerika Serikat. Dapat dipahami bahwa pencegahan kejahatan sangat berkaitan dengan kebijakan-kebijakan ataupun peraturan-peraturan yang dibuat oleh pemerintah atau penguasa yang berwenang.[23]

Pencegahan kejahatan merupakan upaya awal dalam menanggulangi kejahatan. Artinya bahwa pencegahan kejahatan salah satu cara untuk menanggulangi kejahatan. Karena berkaitan dengan pengertian penanggulangan kejahatan, menurut Joseph E. Jacoby bahwa penanggulangan kejahatan meliputi aktivitas yang luas, yaitu penghapusan kondisi-kondisi sosial yang menjadi penyebab kejahatan, meningkatkan kemampuan sistem peradilan pidana untuk mendeteksi, mencegah, menilai dan mengintegrasikan kembali pelaku tindak pidana ke dalam masyarakat, yaitu mereka yang sudah melakukan kejahatan dan mengurangi situasi yang paling memungkinkan menyebabkan dilakukannya suatu kejahatan.[24] Maka dari itu membicarakan pencegahan tentu tidak jauh dari penanggulangan.

---

[22] KBBI Online, melalui ***www.kbbi.web.id,*** diakses Rabu, 6 Desember 2017, Pukul 08.00 wib.

[23] Widodo. 2013, *Op. Cit.,* halaman 33.

[24] *Ibid.*

Penanggulangan kejahatan dalam istilah kriminologi juga disebut dengan kebijakan kriminal (*criminal policy*) sebagaimana dikemukakan juga oleh G. Peter Hoefnagels. Lain halnya dengan Soedjono Dirdjosisworo, ia menyamakan pengertian penanggulangan kejahatan dengan istilah *crime prevention.* Perserikatan Bangsa-Bangsa (PBB) menggunakan istilah *prevention of crime* untuk menguraikan tentang langkah-langkah penanggulangan kejahatan. Istilah ini digunakan sejak dalam Kongres PBB ke-4 Tahun 1970 sampai dengan *The Millineum Congress* Tahun 2000.[25]

Ada dua metode yang dipakai untuk mengurangi frekuensi dari kejahatan dalam *crime prevention* yaitu:[26]

1. Metode untuk mengurangi pengulangan dari kejahatan. Cara yang ditujukan kepada pengurangan jumlah residivis (pengulangan kejahatan) dengan suatu pembinaan yang dilakukan secara konseptual.
2. Metode untuk mencegah kejahatan pertama kali (*the first crime*). Cara yang ditujukan untuk mencegah terjadinya kejahatan yang pertama kali (*the first time*) yang akan dilakukan oleh seseorang dan metode ini juga dikenal sebagai metode preventif (*prevention*).

Upaya preventif tersebut dapat beberapa cara untuk menanggulangi kejahatan yakni:[27]

1. Menyadari bahwa akan adanya kebutuhan-kebutuhan untuk mengembangkan dorongan-dorongan sosial atau tekanan sosial dan tekanan ekonomi yang dapat mempengaruhi tingkah laku seseorang ke arah perbuatan jahat.
2. Memusatkan perhatian kepada individu-individu yang menunjukkan potensialitas kriminal atau sosial, sekalipun potensial tersebut disebabkan gangguan psikologi dan biologi atau kurang mendapat kesempatan sosial ekonomis yang cukup baik sehingga dapat merupakan suatu kesatuan yang harmonis.

---

[25] *Ibid.,* halaman 33.

[26] No Name, "Tinjauan Umum Pencegahan, Tindak Pidana dan Penipuan Jual Beli Online", melalui *www.erepo.unud.ac.id*, diakses Senin, 19 Februari 2018, Pukul 17.02 wib.

[27] *Ibid.*

Penanggulangan kejahatan (kebijakan kriminal) dilakukan dengan cara mempengaruhi pandangan masyarakat terhadap kejahatan dan pemidanaan, menanggulangi kejahatan tanpa menggunakan hukum pidana dan menerapkan hukum pidana dalam masyarakat.[28]

Menurut Hoefnagels upaya penanggulangan kejahatan dapat ditempuh dengan:[29]

a. Penerapan hukum pidana (*criminal law application*);
b. Pencegahan tanpa pidana (*prevention without punishment*); dan
c. Memengaruhi pandangan masyarakat mengenai kejahatan dan pemidanaan lewat *mss media* (*influencing views of society on crime and punishment/mass media*).

Secara garis besar upaya penanggulangan kejahatan dapat dibagi dua, yaitu lewat jalur "penal" (hukum pidana) dan lewat jalur "nonpenal" (bukan/di luar hukum pidana). Dalam pembagian upaya penanggulangan kejahatan oleh Hoefnagels di atas, upaya-upaya yang disebut dalam butir (b) dan (c) dapat dimasukkan ke dalam upaya "nonpenal". Upaya penanggulangan kejahatan lewat jalur "penal" lebih menitik beratkan pada sifat *"repressive"* (penindasan/pemberantasan/penumpasan) sesudah kejahatan terjadi, sedangkan jalur "nonpenal" lebih menitik beratkan pada sifat *"preventive"* (pencegahan/penangkalan/pengendalian) sebelum kejahatan terjadi. Tindakan represif pada hakikatnya juga dapat dilihat sebagai tindakan preventif dalam arti luas. Maka dapat disimpulkan pencegahan kejahatan bukan hanya dilakukan sebelum kejahatan itu terjadi, tetapi dalam melakukan tindakan penumpasan

[28] Widodo. 2013, *Op.Cit.*, halaman 36.
[29] Barda Nawawi Arief. 2008. *Bunga Rampai Kebijakan Hukum Pidana.* Jakarta: Kencana, halaman 45.

kejahatan juga adalah suatu bentuk pencegahan agar kejahatan tersebut tidak terjadi lagi.[30]

Berdasarkan beberapa pendapat mengenai Penanggulangan kejahatan di atas, dapat dipahami bahwa penanggulangan kejahatan meliputi semua langkah yang ditempuh oleh semua pemangku kepentingan (***stake holders***) dalam rangka mencegah kejahatan agar tidak terjadi lagi atau menindak pelaku kejahatan agar tidak mengulangi kejahatannya atau kedua-duanya dilakukan secara bersama-sama. Langkah-langkah tersebut dapat meliputi semua kegiatan yang bersifat pre-emtif (mencegah dengan cara menghilangkan akar permasalahan kejahatan), preventif (misalnya pencegahan kejahatan dengan menggunakan hukum perdata, hukum administrasi) dan represif (penindakan dengan cara menggunakan hukum pidana). Upaya tersebut dilakukan secara terpadu (terintegrasi) melalui rencana aksi (***action plan***) yang ilmiah berdasarkan pertimbangan multidimensional, pelaksanaan aksi yang professional dan pengendalian yang andal.[31]

Tujuan utama dari kebijakan kriminal ialah "perlindungan masyarakat untuk mencapai kesejahteraan". Usaha-usaha yang rasional untuk mengendalikan atau menanggulangi kejahatan menggunakan dua sarana, yaitu:[32]

a. Kebijakan Pidana dengan Sarana Penal. Sarana penal adalah penanggulangan kejahatan dengan menggunakan hukum pidana yang di dalamnya terdapat dua masalah sentral yaitu:

---

[30] *Ibid.,* halaman 46.
[31] Widodo. 2013, *Op.Cit.,* halaman 34.
[32] NoName,"Tinjauan Umum Pencegahan, Tindak Pidana dan Penipuan Jual Beli Online", melalui *www.erepo.unud.ac.id*, diakses Senin, 19 Februari 2018, Pukul 17.22 wib.

1. Perbuatan apa yang seharusnya dijadikan tindak pidana;
2. Sanksi apa yang sebaiknya digunakan atau dikenakan pada pelanggar.

b. Kebijakan Pidana dengan Sarana Non Penal. Kebijakan penanggulangan kejahatan dengan sarana nonpenal hanya meliputi penggunaan sarana sosial untuk memperbaiki kondisi-kondisi sosial tertentu, namun secara tidak langsung memengaruhi upaya pencegahan terjadinya kejahatan.

C. Website Perusahaan

Perkembangan teknologi komputer seiring dengan perkembangan teknologi di bidang teknologi telekomunikasi, pada akhirnya mengakibatkan terjadinya perpaduan antar kedua bidang teknologi tersebut. Perpaduan keduanya membentuk piranti baru yang dikenal dengan nama internet.[33]

Internet (*inter-network*) didefinisikan sebagai jaringan komputer yang menghubungkan situs akademik, pemerintahan, komersil, organisasi maupun perorangan. Dalam definisi ini tampak bahwa internet mencakup juga terhadap jaringan yang biasa disebut dengan *LAN* (*local area network*) dan *WAN* (*wide area network*). Sementara *The US Supreme Court* mendefinisikan internet sebagai *international network of interconnected computers* yang artinya jaringan internasional dari komputer-komputer yang saling berhubungan. Berbeda dengan definisi di muka, dari definisi ini dilihat definisi internasionalnya, artinya bahwa jaringan antar komputer tersebut melewati batas-batas teritorial suatu negara. Agus Raharjo mendefinisikan internet sebagai jaringan komputer antar negara

[33] Abdul Wahid dan Mohammad Labib. 2010. *Kejahatan Mayantara (Cybercrime)*. Bandung: PT. Refika Aditama, halaman 33.

atau antar benua yang berbasis protokol *transmission control protocol/internet protocol* (TCP/IP).[34]

Terkait dengan koneksi internet, kata portal dan web merupakan kata yang menjadi penting untuk memahami cara kerja dan sekaligus melihat bagaimana pekembangan teknologi jejaring global ini. Sebab dalam keseharian penggunaan kata ini sering kali disalahartikan atau pengertiannya menjadi kabur karena adanya kesan penyamaan bahwa yang disebut internet itu yaitu *web* atau bisa disebut sebagai *portal*.[35]

Menurut Thurlow, *Portal* adalah pintu untuk memasuki ruang siber atau bisa juga bermakna sebagai gerbang yang mengantarkan pengguna untuk berselancar lebih jauh. *Portal* dalam bahasa Indonesia juga diartikan sebagai gerbang atau terowongan yang mengarahkan seseorang ke suatu tempat, artinya bahwa melalui *portal*-lah perjalanan *web* dimulai. Adapun kata *web* merupakan sistem dari *server* komputer yang terkoneksi melalui jaringan internet dan dengannya bisa dilakukan pertukaran data yang itu memuat halaman *web* (*webpages*) yang telah terformat, juga memuat tautan (*link*) yang bila diklik akan mengarahkan pengguna untuk menuju *web adresses* atau disebut juga *weblinks* dan bisa juga dengan kata yang banyak dikenal, yakni URLs (*Uniform Resource Locators*).[36]

Salah satu bentuk aplikasi internet yang relatif baru dan paling populer adalah *website* atau biasa dikenal dengan www (*world wide web*) atau sering

---

[34] *Ibid.*, halaman 31.

[35] Rulli Nasrullah. 2014. *Teori dan Riset Media Siber (Cyber Media). Jakarta: Kencana,* halaman 23.

[36] *Ibid.*, halaman 24-25

hanya disebut *web* saja. *Web* juga menyediakan pilihan yang banyak sekali untuk memudahkan memformat tampilan dokumen.[37] Situs (*website*) adalah halaman yang merupakan satu alamat domain yang berisi informasi, data, visual audio, memuat aplikasi hingga berisi tautan dari halaman *web* lainnya. Penggunaan website ataupun situs sebagai salah satu jenis media siber sepertinya bisa menjelaskan beragam bentuk media siber. Namun untuk lebih memberikan pembedaaan lebih tegas, maka yang dimaksud situs dalam pengertian umum. Artinya, situs yang disesuaikan dengan jenis informasi yang akan disampaikan, seperti www.kompas.com merupakan situs berita milik Kompas Gramedia Group.[38]

Pengertian perusahaan menurut Molengraff adalah keseluruhan perbuatan yang dilakukan secara terus menerus, bertindak keluar untuk mendapatkan pengahasilan dengan cara memperniagakan barang-barang, menyerahkan barang-barang atau mengadakan perjanjian-perjanjian perdagangan. Sedangkan menurut Polak, baru ada perusahaan bila diperlukan adanya perhitungan-perhitungan tentang laba-rugi yang dapat diperkirakan dan segala sesuatu itu dicatat dalam pembukuan.[39]

Pada era internet seperti sekarang ini, apapun bentuk usaha yang sedang digeluti, memiliki *website* merupakan suatu keharusan bagi perusahaan karena banyak sekali peluang yang bisa digarap di nternet, mulai dari pengembangan *brand* hingga meningkatkan penjualan, bahkan untuk melakukan *direct selling*.

---

[37] Maskun. 2013. *Kejahatan Siber (Cyber Crime) Suatu Pengantar.* Jakarta: Kencana, halaman 91.

[38] Rulli Nasrullah, *Op. Cit.*, halaman 25.

[39] Ida Nadirah. 2017. *Hukum Dagang dan Bisnis Indonesia*. Medan: Ratu Jaya, halaman 13.

Agar bisa memanfaatkan internet untuk kebutuhan usaha maka diperlukan *website* yaitu media yang akan mengantarkan suatu perusahaan merambah dan menjelajah di dunia maya, sehingga banyak orang di belahan dunia manapun bisa mengetahui keberadaan perusahaan serta usahanya melalui website bisnis atau perusahaan tersebut.[40]

Manfaat dari *website* biasanya sebagian orang memiliki suatu alasan untuk membuat *web* itu sendiri, di antaranya:[41]

a. Memperluas jangkauan promosi sesuatu, dengan memiliki *website* maka produk akan lebih bisa dikenal oleh masyarakat khususnya pengguna internet.
b. Bisa menjadi media tanpa batas, sebab internet adalah media informasi yang tanpa batas. Dengan memiliki *website* berarti sama saja memiliki banayak karyawan yang mempromosikan produk selama 24 jam. Yang artinya *website* akan memberikan suatu informasi kepada calon konsumen selama 24 jam.
c. Promosi yang luas, internet adalah suatu media promosi terluas di dunia jika dilihat dari jangkauan area.
d. Media pengenalan perusahaan, jika memiliki suatu perusahaan akan lebih mudah kita mengenalkan perusahaan lewat *website*, karana jangkauannya internet yang luas dan pemakainya yang banyak, sehingga perusahaan kita akan dikenal oleh masyarakat banyak sehingga dapat mendatangkan calon konsumen dengan cara promosi produk lewat *website*.

---

[40] Proweb Indonesia, "Manfaat Website Bagi Perusahaan", melalui *www.proweb.co.id*, diakses Rabu, 1 Maret 2018, Pukul 10.30 wib.

[41] Sora, "Mengetahui Pengertian Website dan Jenisnya", melalui *www.pengertianku.net*, diakses Rabu, 6 Desember 2017, Pukul 09.45 wib.

Website Profil Perusahaan atau dalam bahasa inggris umum disebut *Corporate Website* adalah *website* yang menyajikan informasi untuk publik mengenai profil perusahaan serta layanan yang dimilikinya. Hampir setiap perusahaan yang berinteraksi dengan publik, memiliki *website* atau setidaknya memasang profilnya melalui *website* direktori. Perusahaan besar biasanya memiliki satu induk *website* yang membawahi berbagai website lainnya yang lebih berfokus pada anak perusahaan atau merk produknya.[42]

Menyediakan sebuah *website*, maka harus tersedia unsur-unsur penunjangnya yaitu *Domain Name*. Apakah yang dimaksud dengan *domain name? Domain name* adalah nama dari suatu website di dalam jaringan Internet. *Domain name* merupakan kombinasi dari huruf-huruf dan angka-angka yang mengidentifikasikan *website* tertentu pada Internet.[43]

Domain name memiliki keterkaitan yang sangat erat dengan merek, tetapi perlu ditegaskan bahwa nama domain tidak identik dengan merek karena meskipun keduanya sama-sama merupakan jati diri suatu produk barang atau jasa, atau suatu nama perusahaan atau badan hukum lainnya, tetapi memiliki sistem dan syarat-syarat pendaftaran serta pengakuan eksistensinya secara berbeda.[44]

Domain name diperjualbelikan secara bebas di internet dengan status sewa tahunan. Setelah *Domain name* itu terbeli di salah satu penyedia jasa pendaftaran, maka pengguna disediakan sebuah kontrol panel untuk

---

[42] Visigraphic, "Website Profil Perusahaan", melalui *www.visigraphic.com*, diakses Rabu, 6 Desember 2017, Pukul 09.25 wib.
[43] Sutan Remy Syahdeini, *Op. Cit.*, halaman *50.*
[44] Ahmad M Ramli, *Op. Cit.*, halaman 9.

administrasinya. *Domain name* didaftarkan untuk jangka waktu tertentu, pada umumnya berjangka waktu untuk satu Tahun dan bisa diperpanjang. Jika pengguna lupa/tidak memperpanjang masa sewanya, maka nama domain itu akan di lepas lagi ketersediaannya untuk umum. Kebanyakan Perusahaan pendaftar untuk *domain name* menerima permohonan untuk registrasi berdasarkan asas "siapa cepat dia dapat" (*on first come, first served basis*).[45]

Nama domain sendiri mempunyai identifikasi ekstensi/akhiran sesuai dengan kepentingan dan lokasi keberadaan *website* tersebut. Contoh nama domain ber-ekstensi internasional adalah com, net, org, info, biz, name, ws. Contoh nama domain ber-ekstensi lokasi Negara Indonesia adalah :[46]

a. co.id, yaitu khusus untuk badan usaha yang berbadan hukum sah;
b. ac.id, yaitu khusus untuk lembaga pendidikan;
c. go.id, yaitu khusus lembaga pemerintahan Republik Indonesia;
d. mil.id, yaitu khusus lembaga Militer Republik Indonesia;
e. or.id, yaitu untuk segala macam organisasi;
f. warnet.id, yaitu untuk industri warung internet di Indonesia;
g. sch.id, yaitu khusus untuk lembaga pendidikan;
h. web.id, yaitu untuk siapapun yang melakukan kegiatannya di *World Wide Web*.

Unsur penunjang untuk mendapatkan sebuah *website* selain selain pembuatan *Domain Name*, ada unsur lainnya yaitu *Web Hosting*. *Web Hosting* dapat diartikan sebagai ruangan yang terdapat dalam hardisk tempat

[45] *Ibid.*, halaman 51.
[46] BOC Indonesia, "Pengertian Website, Webhosting, dan Domain Name", melalui *www.boc.web.id*, diakses Rabu, 6 Desember 2017, Pukul 09.06.

menyimpan berbagai data, berkas-berkas (*file*), gambar, video, data email, statistik, database dan lain sebagainya yang akan ditampilkan di *website*. Besarnya data yang bisa dimasukkan tergantung dari besarnya web hosting yang disewa/dipunyai, semakin besar web hosting semakin besar pula data yang dapat dimasukkan dan ditampilkan dalam *website*.[47]

Menteri Komunikasi dan Informatika secara resmi menyerahkan pengelolaan nama domain di Indonesia .id kepada PANDI (Pengelola Nama Domain Internet Indonesia). Penyerahan ini tertuang dalam Surat Keputusan Menteri Komunikasi dan Informatika Nomor 806 Tahun 2014 Tentang Penetapan Perkumpulan Pengelola Nama Domain Internet Indonesia Sebagai Registri Nama Domain Tingkat Tinggi Indonesia. Dalam Surat Keputusan tersebut menyebutkan bahwa PANDI ditetapkan sebagai Registri Nama Domain Tingkat Tinggi Indonesia.[48]

PANDI dibentuk untuk mengelola nama domain .id secara profesional, akuntabel, dan transparan sesuai dengan kaidah hukum Republik Indonesia. Pengelolaan Nama Domain di Indonesia diatur dalam UU ITE. Mengenai pendaftaran Nama Domain diatur dalam Pasal 23 UU ITE yang mana dalam Ayat (1) dikatakan bahwa yang berhak memiliki Nama Domain yang berdasarkan prinsip pendaftar pertama adalah setiap Penyelenggara Negara, Orang, Badan Hukum dan/atau masyarakat. Dalam Ayat (2) dijelaskan bahwa pemilikan Nama Domain tidak melanggar prinsip persaingan usaha secara sehat dan tidak melanggar hak orang lain. Berkenaan dengan penjelasan dalam Ayat (3) bahwa

---

[47] *Ibid.*

[48] Id.PANDI, "Tentang PANDI", melalui *www.pandi.id*, diakses Senin, 19 Februari 2018, Pukul 20.00 wib.

setiap Peyelenggara Negara, Orang, Badan Hukum atau masyarakat yang dirugikan karena penggunaan Nama Domain tanpa hak, berhak mengajukan gugatan pembatalan Nama Domain dimaksud.

Syarat dokumen pendaftaran Nama Domain Berlandaskan pada Pasal 23 UU ITE tersebut di atas, Pengelola Nama Domain Internet Indonesia menerapkan syarat dokumen dalam pendaftaran Nama Domain .id, yaitu:[49]

1. Dokumen status legalitas pelanggan sesuai nama domain peruntukkannya (SIUP/TDP/Akte Notaris/Surat Ijin Usaha Instansi lain untuk .co.id, SIUP Dirjen Postel untuk .net.id, Akte/SK Instansi terkait/SK Intern untuk .or.id, .ac.id dan .sch.id dsb).
2. Dokumen identitas pelanggan (KTP/SIM/Paspor).

Jika Pasal 23 ayat (1) UU ITE memberikan hak kepada pelanggan untuk memiliki nama domain dengan prinsip pendaftar pertama, Pasal 23 ayat (2) UU ITE memberikan amanah/kewajiban kepada Pengelola Nama Domain Internet Indonesia, agar menerapkan prinsip kehati-hatian dalam klarifikasi syarat dokumen untuk menjaga integritas dan reliabilitas/keterpercayaan nama domain .id. Sehubungan dengan itu, selain dua syarat pokok tersebut di atas, Pengelola Nama Domain Internet Indonesia memiliki kewajiban melakukan klarifikasi syarat dokumen tambahan, berupa surat pernyataan/keterangan/penjelasan jika dianggap perlu (dapat diisikan pada baris *description form template* pendaftaran).[50]

---

[49] *Ibid.*
[50] *Ibid.*

D. Manipulasi dan Mengubah Data dalam Cybercrime

Manipulasi adalah sebuah proses rekayasa dengan melakukan penambahan, persembunyian, penghilangan atau pengkaburan terhadap bagian atau keseluruhan sebuah realitas, kenyataan, fakta-fakta ataupun sejarah yang dilakukan berdasarkan sistem perancangan sebuah tata sistem nilai, manipulasi adalah bagian penting dari tindakan menanamkan gagasan, sikap, sistem berpikir, perilaku dan kepercayaan tertentu.[51]

Manipulasi menurut Kamus Besar Bahasa Indonesia (KBBI) adalah tindakan untuk mengerjakan sesuatu dengan tangan atau alat-alat mekanis secara terampil, upaya kelompok atau perseorangan untuk memengaruhi perilaku, sikap dan pendapat orang lain tanpa orang itu menyadarinya dan suatu penggelapan atau penyelewengan. Sedangkan pengertian mengubah atau perubahan menurut KBBI merupakan suatu pergantian, pertukaran atau suatu yang ditambahkan dan dikurangi, sesuatu yang berlainan dari yang semula.[52]

Data adalah kumpulan informasi yang diperoleh dari suatu pengamatan, dapat berupa angka, lambang atau sifat. Menurut *Webster New World Dictionary*, pengertian data adalah *things known or assumed*, yang berarti bahwa data itu sesuatu yang diketahui atau dianggap. Diketahui maksdunya sudah terjadi merupakan fakta (bukti). Data dapat memberikan suatu gambaran tentang suatu keadaan atau persoalan. Data juga dapat didefinisikan sebagai sekumpulan informasi atau nilai yang diperoleh dari pengamatan (observasi) suatu objek. Data

---

[51] Wikipedia, "Pengertian Manipulasi", melalui *www.wikipedia.com*, diakses Rabu, 6Desember 2017, Pukul 09.55 wib.

[52] KBBI Online, "Pengertian Manipulasi dan Data", melalui *www.kbbi.web.id*, diakses Rabu, 6 Desember 2017, Pukul 10.00 wib.

yang baik adalah data yang dapat dipercaya kebenarannya (*realible*), tepat waktu dan mencakup ruang lingkup yang luas atau bisa memberikan gambaran tentang suatu masalah secara menyeluruh merupakan data relevan.[53]

Cybercrime didefinisikan sebagai kejahatan komputer. Mengenai definisi kejahatan komputer sendiri, sampai sekarang para sarjana belum sependapat mengenai pengertian atau definisi dari kejahatan komputer. Bahkan pengguna istilah tindak pidana untuk kejahatan komputer dalam bahasa Inggris pun masih belum seragam. Beberapa sarjana menggunakan istilah *computer misuse*, *computer abuse*, *computer fraud*, *computer-related crime*, *computer crime*. Namun para sarjana pada waktu itu, pada umumnya lebih menerima pemakaian istilah *computer crime* oleh karena dianggap lebih luas dan biasa dipergunakan dalam hubungan internasional.[54]

Mandell membagi *computer crime* atas dua kegiatan, yaitu:[55]

1. Penggunaan komputer untuk melaksanakan perbuatan penipuan, pencurian atau penyembunyian yang dimaksud untuk memperoleh keuntungan keuangan, keuntungan bisnis, kekayaan atau pelayanan.
2. Ancaman terhadap komputer itu sendiri, seperti pencurian perangkat keras atau lunak, sabotase dan pemerasan.

Sistem teknologi informasi berupa internet telah dapat menggeser paradigma para ahli hukum terhadap definisi kejahatan komputer sebagaimana ditegaskan sebelumnya, bahwa pada awalnya para ahli hukum terfokus pada alat/perangkat keras yaitu komputer. Namun dengan adanya perkembangan teknologi informasi berupa jaringan internet, maka fokus dari indentifikasi

---

[53] Kumpulan Pengertian Menurut Para Ahli, "Pengertian Data dan Jenis Data", melalui *www.pengertianahli.com*, diakses Rabu, 06 Desember 2017, Pukul 10.15 wib.
[54] Budi Suhariyanto, *Op. Cit.*, halaman 9.
[55] *Ibid.*, halaman 10.

terhadap definisi *cybercrime* lebih diperluas lagi yaitu seluas aktivitas yang dapat dilakukan di dunia *cyber*. Oleh karena itu, pada dasarnya *cybercrime* meliputi semua tindak pidana yang berkenaan dengan sistem informasi, sistem informasi (*information system*) itu sendiri, serta sistem komunikasi yang merupakan sarana untuk penyampaian atau pertukaran informasi kepada pihak lainnya (*transmitter/originator to receptient*).[56]

Menurut NCIS (Naval Criminal Investigative Service) sebuah agensi federal yang bertujuan untuk menginvestigasi kejahatan di Inggris menguraikan bentuk-bentuk *cybercrime* sebagai berikut:[57]

1. *Recreational hackers.* Kejahatan ini dilakukan oleh *netter* tingkat pemula untuk sekedar mencoba kekuranghandalan sistem sekuritis suatu perusahaan.
2. *Crackers* atau *criminal minded hackers.* Pelaku kejahatan ini biasanya memiliki motivasi untuk mendapatkan keuntungan finansial, sabotase dan penghancuran data. Sebagai contoh, pada Tahun 1994, Citibank AS kebobolan senilai 400.000 dolar oleh *cracker* dari Rusia, yang akhirnya dijatuhi hukuman penjara selama tiga Tahun serta harus mengembalikan sejumlah uang tersebut. tipe kejahatan ini dapat terjadi dengan bantuan orang dalam, biasanya staf yang sakit hati atau datang dari kompetitor dalam bisnis sejenis.
3. *Political hackers.* Politis atau lebih populer dengan sebutan *hactivist* melakukan pengrusakan terhadap ratusan situs web untuk mengkampanyekan program-programnya, bahkan tidak jarang digunakan untuk menempelkan pesan untuk mendiskreditkan lawannya. Usaha tersebut pernah dilakukan secara aktif dan konsisten dalam usaha untuk kampanye anti-Indonesia dalam masalah Timor Timur yang dipelopori oleh Ramos Horta. Situs Deplu sempat mendapat serangan yang diduga keras dari kelompok anti-integrasi.
4. *Denial of service attack.* Serangan *Denial of service attack* atau oleh FBI dikenal dengan istilah "*unpressedented*", tujuannya adalah untuk memacetkan sistem dengan mengganggu akses dari pengguna yang *legitimate*. Taktik yang digunakan adalah dengan mengirim atau membanjiri situs web dengan data yang tidak perlu. Pemilik situs web

[56] *Ibid.*, halaman 11.

[57] Ade Maman Suherman. 2005. *Aspek Hukum dalam Ekonomi Global*. Bogor: Ghalia Indonesia, halaman 190-192.

menderita kerugian karena untuk mengendalikan atau mengontrol kembali situs web memakan waktu yang tidak sedikit.

5. *Insiders* atau *internal hackers. Insikder hacker* ini bisa dilakukan oleh orang dalam perusahaan sendiri. Modus operandinya dengan menggunakan karyawan yang kecewa atau bermasalah dengan perusahaan.
6. *Viruses.* Program pengganggu dengan penyebaran virus yang dapat menular ke aplikasi internet. Virus bisa bersembunyi dalam *file* dan terdownload oleh *user*, bahkan bisa menyebar melalui *e-mail.*
7. *Piracy*. Pembajakan *software*, pihak produsen *software* dapat kehilangan profit karena karyanya dapat dibajak melalu *download* dari internet dan dikopy ke dalam CD-ROM, yang selanjutnya diperbanyak secara ilegal atau tanpa seizin penciptanya.
8. *Fraud* adalah segala jenis manipulasi informasi keuangan dengan tujuan mengeruk keuntungan sebesar-besarnya, sebagai contoh adalah harga tukar saham yang menyesatkan melalui rumor. Situs lelang fiktif dengan mengeruk uang masuk daripada peserta lelang dan barangnya tidak dikirim.
9. *Gambling*. Perjudian di dunia *cyber* yang berskala global sulit sulit dijarat dengan hukum nasional suatu negara.
10. *Phornography* dan *paedophilia.* Melalui *news group*, *chat rooms* mengekploitasi *pornography* anak-anak di bawah umur.

Berdasarkan beberapa literatur serta praktiknya, *cybercrime* memiliki beberapa karakteristik, yaitu:[58]

1. Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis tersebut terjadi dalam ruang/wilayah siber/*cyber* (*cyberspace*), sehingga tidak dapat dipastikan yuridiksi negara mana yang berlaku terhadapnya.
2. Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang terhubung dengan internet.
3. Perbuatan tersebut mengakibatkan kerugian materiil maupun immateril (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan dengan kejahatan konvensional.

[58] Budi Suhariyanto, *Op. Cit.*, halaman 13.

4. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya.
5. Perbuatan tersebut sering dilakukan secara transnasional/melintasi batas negara.

Berdasarkan uraian mengenai pengertian manipulasi, data dan cybercrime di atas, maka dapat disimpulkan bahwa manipulasi dan mengubah data dalam cybercrime merupakan salah satu cara untuk melakukan kejahatan dengan menggunakan media komputer, ruang siber dan/atau media teknologi lainnya sebagai pendukung yang caranya itu adalah data tersebut berisi informasi yang tidak benar atau tidak sesuai dengan fakta yang sebenarnya dan data tersebut lain daripada yang semula sehingga menimbulkan kerugian secara materil/non materil.

BAB III

HASIL DAN PEMBAHASAN

A. Bentuk-bentuk Kejahatan Manipulasi dan Perubahan Data Pada Website Perusahaan

Tingkah laku jahat muncul sejak dahulu dan oleh masyarakat dianggap sebagai suatu realita dan fakta yang merugikan bagi masyarakat. Kerugian tersebut dapat berupa kerugian material maupun nonmaterial. Kerugian material adalah kerugian yang timbul atas suatu kejahatan berupa korban kejahatan dan harta benda serta biaya yang harus dikeluarkan untuk menanggulanginya. Sehingga kerugian nonmaterial adalah hilangnya kepercayaan masyarakat terhadap penegakan hukum yang dilakukan oleh aparat penegak hukum.[59]

Kejahatan dalam pengertian sosiologis mengandung konotasi tertentu dan merupakan penamaan yang bersifat relatif. Menurut J.E. Sahetapy dan B. Mardjono Reksodiputro, pengertian kejahatan sebenarnya hanya merupakan suatu nama atau cap (*label, stigma*) yang diberikan oleh orang-orang tertentu untuk menilai perbuatan-perbuatan dari seseorang atau sekelompok orang sebagai perbuatan jahat. Pengertian kejahatan sangat dipengaruhi oleh nilai-nilai yang dianut oleh suatu masyarakat.[60]

Kejahatan dalam pengertian yuridis adalah perbuatan yang dianggap melanggar atau bertentangan dengan apa yang ditentukan dalam kaidah peraturan perundang-undangan. Dalam perspektif hukum, kejahatan adalah segala perbuatan

[59] Widodo. 2013. *Aspek Hukum Pidana Kejahatan Mayantara.* Yogyakarta: Aswaja Pressindo, halaman 29.

[60] *Ibid*., halaman 30.

yang melanggar ketentuan hukum, sebagaimana diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP) maupun peraturan perundang-undangan.[61]

Secara terminologis, kejahatan yang berbasis teknologi informasi dengan menggunakan media komputer sebagaimana terjadi saat ini, dapat disebut dengan beberapa istilah yaitu *computer misuse, computer abuse, computer fraud, computer-related crime, computer-assited crime*, atau *computer crime*. Istilah kejahatan yang berhubungan dengan komputer (*computer-related crime*) seringkali digunakan perserikatan bangsa-bangsa (PBB). Namun, konvensi internasional Tahun 2001 menggunakan istilah *cybercrime*. Barda Nawawi Arief, Mengemukakan bahwa pengertian kejahatan yang berhubungan dengan komputer (*computer-related crime*) sama dengan *cybercrime*.[62]

Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Transaksi Elektronik merupakan *cyberlaw* pertama di Indonesia yang mengatur secara khusus tentang informasi dan transaksi elektronik. Materi UU ITE dapat dikelompokkan menjadi dua bagian besar: (i) pengaturan informasi dan transaksi elektronik, dan (ii) pengaturan mengenai perbuatan yang dilarang (*cybercrime*). Ketentuan *cybercrime* dalam UU ITE mengacu kepada *EU Conventionon cybercrime* yang merupakan instrumen internasional yang digunakan oleh banyak negara. Dalam

[61] *Ibid.*, halaman 32.
[62] Widodo. 2013. *Hukum Pidana di Bidang Teknologi Informasi Cyberlaw*. Yogyakarta: Aswaja Pressindo, halaman 12.

CoC (*Convention of Cybercrime*) diatur mengenai dua jenis *cybercrime*, yaitu *cybercrime* dalam arti *computer crime* dan dalam arti *computer-related crime.*[63]

Pengertian *cybercrime* dan *computer-related crime* adalah sama. Kalau dalam *cybercrime*, kejahatan dapat dilakukan baik menggunakan internet atau tidak dalam *cybercrime*, kejahatan dapat dilakukan dengan cara menggunakan komputer yang tidak terkoneksi dengan sistem internet (*offline*). *Computer crime* adalah tingkah laku manusia secara ilegal yang menjadikan komputer sebagai sasaran kejahatan, baik pada data maupun pengamannya. Sedangkan *cybercrime* adalah kejahatan dunia *cyber* dalam arti luas, baik menjadikan komputer sebagai sasaran maupun komputer dijadikan target kejahatan dan peristiwa tersebut terjadi baik dalam kondisi komputer tersambung melalui internet (*online*) atau hanya terkoneksi dengan komputer lain dalam lingkup terbatas (*intranet*), maupun komputer yang tidak terkoneksi (*offline*).[64]

Pengertian *cybercrime* adalah setiap aktivitas seseorang, sekelompok orang, badan hukum yang menggunakan komputer sebagai sarana melakukan kejahatan, dan komputer sebagai sasaran kejahatan. Kejahatan tersebut adalah bentuk-bentuk kejahatan yang bertentangan dengan peraturan perundang-undangan, baik melawan hukum secara materiel maupun melawan hukum secara formiel. Pengertian kejahatan *cybercrime* adalah tindak pidana yang diatur dalam perundang-undangan di Indonesia (sudah dikriminalisasi oleh legislator dalam

[63] Josua Sitompul. 2012. *Cyberspace, Cybercrimes, Cyberlaw Tinjauan Aspek Hukum Pidana*. Jakarta: PT. Tatanusa, halaman 44.
[64] Widodo. 2013, *Op. Cit*., halaman 8.

peraturan perundang-undangan), bukan kejahatan pada pengertian sosiologis atau pengertian lain.[65]

Apabila ketentuan substantif (*subtantive law*) dalam CoC (*Convention of Cybercrime*) dibandingkan dengan perbuatan yang dilarang dalam UU ITE diperoleh hasil dalam tabel sebagai berikut:[66]

Tabel I. Perbandingan *Cybercrime* dalam Coc dan UU ITE.

Convention on Cybercrime	KUHP	UU ITE
Article 2-*Illegal access*	Pasal 167 KUHP memaksa masuk ke dalam rumah, ruangan atau perkarangan tertutup.	Pasal 30
Article 3-*Illegal Interception*	Tidak diatur dalam KUHP	Pasal 31
Article 4-*Data Interference*	Pasal 406 KUHP tentang pengrusakan barang	Pasal 32
Article 5-*System interference*	Tidak diatur dalam KUHP	Pasal 33
Article 6-*Misuse of devices*	Tidak diatur dalam KUHP	Pasal 34
Article 7-*Computer-related Forgery*	Bab XII-Pemalsuan surat Pasal 263 KUHP:membuat surat palsu atau memalsukan surat	Pasal 35
Article 8-*Compter-related fraud*	Bab XXV perbuatan curang Pasal 378 dengan maksud untuk menguntungkan seseorang secara melawan hukum.	Tidak diatur secara spesifik
Article 9-*Offences related to child pornography*	Bab XIV-Kejahatan terhadap kesusilan	Pasal 27 ayat(1)
Article 10-*Offences*	UU Hak Cipta	Tidak diatur

[65] Widodo. 2013, *Op. Cit.*, halaman 13.
[66] Joshua Sitompul, *Op. Cit.*, halaman 44-46.

related to infringements of copyright and related rights		
Article 11-Attempt and aiding or abetting	Pasal 55 KUHP tentang penyertaan tindak pidana	Tidak diatur

Berdasarkan keterangan di atas, tindakan manipulasi dan perubahan data elektronik termasuk dalam bentuk kejahatan siber (*cybercrime*) yang diatur dalam CoC dan UU ITE yaitu bentuk kejahatan pemalsuan surat melalui komputer atau yang disebut dengan *computer related forgery* karena tindakan manipulasi dan perubahan data elektronik merupakan sebagian unsur-unsur yang termasuk dalam tindakan yang dilarang dan diatur dalam Pasal 35 Undang-Undang Nomor 19 Tahun 2016 atas perubahan Undang-Undang Nomor 11 Tahun 2008 yang berbunyi "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan informasi atau dokumen elektronik dengan tujuan agar informaasi atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik".

Tindakan yang dilarang dari pasal ini adalah dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan informasi atau dokumen elektronik dengan tujuan agar informasi atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik. Tujuan pengaturan Pasal 35 UU ITE ialah menjaga dapat dipercayanya informasi atau dokumen elektronik (*reability*) khususnya dalam transaksi elektronik. Sifat informasi atau dokumen elektronik yang mudah diubah dan dipindahtangankan merupakan salah satu pertimbangan urgensi ketentuan ini.[67]

[67] Josua Sitompul, *Op. Cit.*, halaman 247.

Pemalsuan data melalui komputer adalah perbuatan yang dilakukan oleh seseorang secara sengaja dan tanpa hak memasukkan, mengubah, menghapus data yang otentik (asli) menjadi tidak otentik dengan maksud untuk digunakan sebagai data otentik. Perbuatan ini juga dapat dilakukan untuk merubah isi perjanjian elektronik yang dibuat oleh pihak-pihak tertentu, baik dilakukan pada saat proses pembuatan perjanji (melakukan transmisi), maupun merubah data dipenyimpanan yang sudah ditandatangani secara elektronik (*digital signature*) oleh pihak-pihak. Selain itu, isi atau data suatu *website* juga dapat dipalsu.[68]

Keotentikan mengindikasikan bahwa informasi atau dokumen elektronik dapat dipercaya (*reliable*). Setidaknya ada dua hal yang diperhatikan dalam menentukan keotentikan suatu informasi atau dokumen elektronik, yaitu sumber dan konten. Suatu informasi atau dokumen elektronik dikategorikan otentik apabila sumbernya berasal dari orang atau pihak yang memiliki hak atau kewenangan untuk mengeluarkan informasi/dokumen elektronik yang dimaksud dan kontennya adalah konten yang dimaksudkan oleh sumber. "Otentik" di sini tidak hanya dimaksudkan pada data yang dibuat oleh atau di hadapan pejabat yang berwenang berdasarkan peraturan perundang-undangan tetapi juga mencakup data perusahaan atau pribadi yang dibuat oleh mereka. Sedangkan yang dimaksud konten yang otentik ialah bahwa informasi atau data yang terdapat dalam informasi atau dokumen elektronik ialah muatan yang dibuat, dikeluarkan, dipublikasikan, dikirimkan oleh sumber yang dimaksud.[69]

---

[68] Widodo. 2013, *Op. Cit.*, halaman 85.
[69] Josua Sitompul, *Op. Cit.*, halaman 248.

UU ITE mengatur beberapa kategori perbuatan yang termasuk dalam *computer-related forgery*, yaitu manipulasi, penciptaan, perubahan, penghilangan, dan pengrusakan. Semua perbuatan tersebut diatur secara alternatif, artinya cukup dibuktikan bahwa pelaku melakukan salah satu dari perbuatan yang dimaksud. Secara umum, yang dimaksud dengan manipulasi ialah upaya dengan kepandaian atau alat perangkat untuk memengaruhi orang lain untuk mencapai suatu tujuan yang merugikan orang lain, termasuk di dalamnya berbuat curang atau melakukan penipuan.[70]

Menurut Black's Law Dictionary, *fraud* didefinisikan sebagai kesengajaan atas salah pernyataan terhadap suatu kebenaran atau keadaan yang disembunyikan dari sebuah fakta material yang dapat mempengaruhi orang lain untuk melakukan perbuatan atau tindakan yang merugikannya, biasanya merupakan kesalahan namun dalam beberapa kasus (khususnya dilakukan secara sengaja) memungkinkan merupakan suatu kejahatan.[71]

The British Law mengartikan *computer fraud* sebagai manipulasi komputer dengan cara apapun yang dilakukan dengan itikad buruk untuk memperoleh uang, barang atau keuntungan lainnya atau dimaksudkan untuk menimbulkan kerugian kepada pihak lain.[72]

Berdasarkan definisi-definisi di atas dapat disimpulkan, *Fraud* adalah setiap perbuatan tidak jujur (penyalahgunaan kedudukan/jabatan atau penyimpangan) yang bertujuan mengambil uang (atau harta atau sumber daya

---

[70] *Ibid.*, halaman 250.

[71] Maskun dan Wiwik Meilarati. 2017. *Aspek Hukum Penipuan berbasis internet.* Bandung: CV Keni Media, halaman 43.

[72] Budi Suhariyanto, *Op. Cit.*, halaman 10.

orang lain/organisasi) melalui akal bulus, tipu muslihat, penipuan, kelicikan, penghilangan, kecurangan, saran yang salah, penyembunyian atau cara-cara lainnya yang dilakukan dengan sengaja oleh seseorang yang mengakibatkan kerugian organisasi atau orang lain dan/atau menguntungkan pelaku.[73]

Computer related fraud merupakan perkembangan *fraud* yang dipicu oleh kejahatan *fraud* yang awalnya dilakukan secara konvensional kini dapat dilakukan dengan sistem komputer dan internet. Selain istilah *computer related fraud,* dikenal juga istilah *internet fraud* yaitu penipuan berbasis internet. Bruce D. Mandelbit, mendefinisikan *internet fraud* dengan merujuk pada jenis penipuan yang menggunakan internet seperti *chat room, email, massege boards* atau *website*.[74]

Berdasarkan studi literatur di samping *internet fraud,* dikenal pula istilah *elektronik fraud offence* yang dipahami sebagai suatu tindakan yang menyerang seseorang atau perusahaan dengan cara melakukan pengenalan, modifikasi dan menghapus data elektronik yang dilakukan dengan cara melakukan akses yang tidak sah atau menghalangi penggunaan elektronik data terhadap seseorang atau perusahaan dengan maksud untuk memperoleh keuntungan dari orang atau perusahaan tersebut.[75]

Bentuk-bentuk kejahatan *fraud* begitu pesat jumlahnya karena dipicu oleh perkembangan ilmu, teknologi dan jenis usaha. Mengenai tindakan manipulasi dan perubahan data pada website perusahaan, maka kejahatan *fraud*

---

[73] Bona P. Purba. 2015. *Fraud dan Korupsi Pencegahan Pendeteksian dan Pemberantasannya.* Jakarta: Lestari Kiranatama, halaman 2

[74] Maskun dan Wiwik Meilarati, *Op. Cit.,* halaman 44.

[75] *Ibid.,* halaman 45.

yang dimaksud dan dianalisis adalah *fraud* yang dilakukan di ranah perusahaan, ada beberapa bentuk *fraud* di ranah perusahaan yang pertama adalah bentuk kejahatan *fraud* atas laporan. Bentuk *fraud* atas laporan dapat bersifat keuangan atau non keuangan. *Fraud* yang bersifat keuangan berbentuk lebih saji atau kurang saji atas laporan, sedangkan *fraud* bersifat non keuangan antara lain berbentuk penyalahgunaan kepercayaan pemberi kerja, manipulasi dan pemalsuan dokumen.[76]

Fraud atas laporan dapat dibagi menjadi 5 yaitu:[77]

a. Pendapatan fiktif, dilakukan dengan mencatat pendapatan yang berasal dari penjualan barang/jasa yang sebenarnya tidak terjadi (fiktif). Pelaku menciptakan perusahaan fiktif atau melakukan penjualan fiktif kepada perusahaan/organisasi tertentu.
b. Perbedaan waktu, berkaitan dengan pencatatan penjualan atau biaya pada periode yang salah.
c. Menyembunyikan kewajiban dan biaya, dilakukan dengan tidak mengungkap adanya kewajiban dan biaya dalam laporan keuangan.
d. Pengungkapan yang tidak tepat, dengan menyembunyikan data-data dan informasi penting yang berkaitan dengan perusahaan.
e. Penilaian aktiva yang tidak tepat, dilakukan dengan menilai aktiva yang dilaporkan secara salah dan tidak sesuai dengan standar akutansi yang berlaku umum.

[76] Bona P. Purba, *Op. Cit.,* halaman 12.
[77] *Ibid.*

Bentuk-bentuk kejahataan *fraud* di ranah perusahaan selain daripada *fraud* atas laporan yaitu penyalahgunaan aset dan korupsi. Berdasarkan penjelasan *Convention on Cybercrime*, pemalsuan dan penipuan melalui komputer tergolong dalam pelanggaran yang berhubungan dengan komputer. Pemalsuan dan penipuan dengan sarana komputer merupakan bentuk kejahatan yang dilakukan dengan cara memodifikasi data atau sistem komputer. Kriminalisasi terhadap perbuatan penipuan melalui komputer perlu dilakukan jika perbuatan tersebut menghasilkan suatu keuntungan ekonomi secara langsung, atau menyebabkan hilangnya hak milik orang lain. Keuntungan ekonomis tersebut diperoleh pelaku secara tidak sah, baik untuk kepentingan dirinya sendiri maupun orang lain. Istilah hilangnya hak milik mempunyai pengertian luas, meliputi hilangnya uang, barang berwujud atau tidak berwujud yang mempunyai nilai ekonomi. Agar dapat dikategorikan sebagai bentuk kejahatan ini, perbuatan tersebut harus dilakukan secara tidak sah.[78]

Berdasarkan penjelasan yang telah diuraikan di atas maka dapat di ambil suatu contoh kasus yang telah terjadi dan telah diputus dalam Putusan Mahkamah Agung Nomor 116 K/Pid.Sus/2015 mengenai perbuatan manipulasi dan mengubah data pada website milik perusahaan sistem *MLM online* yang bergerak dalam bidang produksi dan pemasaran air minum dalam kemasan dengan nama PT Mulia Rejeki Waterindo yang perbuatan itu dilakukan oleh

[78] Widodo. 2013*, Op. Cit.,* halaman 87.

terdakwa Handojo bin Achmadi Harsono selaku orang yang bekerjasama dengan Gabby Permata Starosa sebagai pemilik perusahaan tersebut.[79]

Berawal dari perjanjian kerjasama dan pembagian kerja yang dilakukan secara tertulis dan ditandatangani oleh saksi Gabby dan terdakwa di atas materai Rp.6000,00 (enam ribu rupiah) tertanggal 25 November 2011, hal ini yang menjelaskan bahwa terdakwa mempunyai tugas dan tanggung jawab pada bagian produksi, *system program online* bonus dan pengiriman produk. Lalu kemudian terdakwa bekerjasama dengan saksi Fajar Ahmad bin Maryono sekitar bulan Oktober 2011 dan terdakwa memerintahkan saksi Fajar untuk membuatkan sistem atau pemrograman serta *maintenance* website www.myoxysuper.com milik PT. Mulia Rejeki Waterindo dan membeli *Domain name* www.myoxysuper.com serta membeli server yang digunakan untuk menyimpan data system website www.mysuperoxy.com.[80]

Terdakwa menyuruh saksi Fajar untuk memanipulasi dan melakukan perubahan data terhadap website www.myoxysuper.com yang berkaitan dengan posisi *member* perusahaan 1, perusahaan 2, perusahaan 3 dengan cara melalui telpon selular dengan kata-kata "Mas Fajar, Ibu Gabby meminta untuk memasukkan posisi pada ID milik perusahaan" (yang setelah saksi Gabby dimintai keterangan di persidangan bahwa saksi Gabby tidak pernah menyuruh mengubah data).[81]

Saksi Fajar melakukan tindakan yang disuruh oleh terdakwa dengan cara membuka Admin Cpanel dengan mengunjungi website

[79] Putusan Mahkamah Agung Nomor 116 K/Pid. Sus/2015", halaman 2.
[80] *Ibid.*, halaman 3.
[81] *Ibid.*

www.myoxysuper.com/Cpanel, selanjutnya saksi Fajar membuka modul *database* pada Admin Cpanel tersebut dan setelah itu saksi Fajar melakukan manipulasi dan perubahan data terhadap perusahaan 1, perusahaan 2, perusahaan 3 dengan menambahkan posisi *member* dengan nama perusahaan 2 yang sebelumnya kosong menjadi Diamond, menambahkan posisi *member* dengan nama perusahaan 3 yang sebelumnya kosong menjadi Rubby, menambahkan posisi *member* dengan nama Perusahaan 1 yang sebelumnya kosong menjadi Sapphire. Nama-nama perusahaan ID member tersebut bersifat tidak jelas dan tidak dilengkapi dengan alamat yang jelas, hal tersebut menunjukkan adanya indikasi registrasi *member* yang tidak prosedural atau dalam artian bahwa nama-nama perusahaan ID *member* tersebut merupakan *member* fiktif yang sebenarnya tidak ada atau data-data palsu.[82]

Berdasarkan perubahan yang dilakukan terdakwa dengan menyuruh saksi Fajar untuk melakukan perubahan terhadap data pada website www.myoxysuper.com yang berkaitan dengan posisi *member*, maka mengakibatkan antara lain:[83]

1. Ketika kantor akan menginputkan nomor ID Produk atau ID Member untuk kota Makasar, ternyata nomor-nomor tersebut sudah pernah di-*input* dan bahkan sudah pernah dipakai di Pontianak.
2. Ketika *stokist* dan pontianak akan memposting ID *member* atau ID produk yang dibeli *member* di Pontianak, tiba-tiba sudah dipakai oleh *member* di

[82] *Ibid.*, halaman 4.
[83] *Ibid.*

Makasar yang menunjukkan bahwa kartu tersebut sudah dipakai oleh *member* lain.

3. Grafik network yang tidak sesuai dengan ketentuan dalam marketing plan di brosur maupun di website.
4. Banyak member yang merasa dirugikan karena berkurangnya bonus yang berupa nilai rupiah dikarenakan *member* fiktif tersebut.
5. Kerugian pada saksi korban Gabby sebagai pemilik perusahaan sebesar kurang lebih 1.500.000.000,00 (satu milyar lima ratus juta rupiah).
6. Hilangnya kepercayaan *member* terhadap MLM yang dirintis dan dikelola oleh saksi korban Gabby, yang mengakibatkan perusahaan berpotensi mengalami kebangkrutan.

Tindakan manipulasi dan perubahan data pada webite perusahaan yang terdapat dalam Putusan Nomor 116 K/Pid.Sus/2015 merupakan bentuk kejahatan *Computer related Forgery* atau pemalsuan data melalui komputer terhadap data-data website milik perusahaan. Karena dilihat dari pengertian *Computer related forgery* yaitu perbuatan yang dilakukan oleh seseorang secara sengaja dan tanpa hak memasukkan, mengubah, menghapus data yang otentik (asli) menjadi tidak otentik dengan maksud untuk digunakan sebagai data otentik. Hal tersebut sesuai dengan tindakan pelaku yang menambahkan *member* fiktif yang sebenarnya tidak ada (*ID member* palsu) dan membuatnya seolah-olah asli (otentik).[84]

[84] Widodo. 2013, *Op. Cit.*, halaman 85.

Perbuatan pemalsuan tersebut juga bertujuan untuk melakukan kejahatan *Computer related Fraud* di perusahaan dalam bentuk fraud atas laporan karena tindakan manipulasi dan perubahan data pada website perusahaan dalam Putusan Nomor 116 K/Pid.Sus/2015 tersebut sesuai dengan karakteristik atau unsur-unsur dari perbuatan yang tergolong ke dalam bentuk kejahatan *Computer related fraud* di perusahaan. Terdapat 5 unsur *Computer related fraud* yang terkandung dalam setiap tindakan *fraud* yang sesuai dengan perbuatan manipulasi dan perubahan data dalam perkara Putusan Nomor 116 K/Pid.Sus/2015 tersebut yaitu:

1. Merupakan perbuatan tidak jujur atau perbuatan penyalahgunaan kedudukan/jabatan atau perbuatan yang menyimpang.

   Terdakwa Handojo yang merupakan rekan kerjasama Gabby, menyalahgunakan kedudukannya dan berbuat tidak jujur dengan menyuruh saksi fajar untuk melakukan manipulasi dan perubahan data pada website PT. Mulia Rejeki Waterindo dengan mengatasnamakan saksi korban Gabby yang menyuruh padahal sebenarnya saksi korban Gabby tidak pernah menyuruh untuk melakukan perubahan data pada website perusahaannya.[85]

2. Perbuatan tersebut dilakukan dengan sengaja.

   Ada unsur kesengajaan karena sudah memiliki niat dengan membohongi Fajar untuk melakukan manipulasi dan mengubah data tersebut

[85] Bona P. Purba, *Op. Cit.,* Halaman 2-3.

yang menyebutkan atas perintah saksi Gabby agar keinginannya dapat terlaksana.[86]

3. Perbuatan tersebut dilakukan melalui akal bulus, tipu muslihat, penipuan, kelicikan, penghilangan, kecurangan, saran yang salah, penyembunyian, atau cara-cara curang lainnya.

Perbuatan manipulasi dan perubahan data website perusahaan yang dilakukan Handojo tersebut dilakukan melalui tipu muslihat dengan cara menambahkan *member* fiktif atau palsu agar terlihat seperti data yang otentik (asli).[87]

4. Perbuatan tersebut mengakibatkan kerugian bagi organisasi dan/atau oang lain.

Gabby selaku pemilik perusahaan dan juga *member* perusahaan yang sama-sama mengalami kerugian sebesar lebih kurang 1.500.000.000 (satu milyar lima ratus juta). Selain itu juga perusahaan kehilangan kepercayaan dari *member*-nya, kerusakan reputasi dan citra perusahaan yang itu membuat perusahaan sangat berpotensi mengalami kebangkrutan.[88]

5. Perbuatan tersebut menguntungkan pelaku dan/atau orang lain.

Perbuatan manipulasi dan perubahan data website yang dilakukan terdakwa Handojo tentu menguntungkan dirinya, karena dari pembuatan *member* fiktif maka aliran dana bonus yang seharusnya milik para *member*

[86] *Ibid.*
[87] *Ibid.*
[88] *Ibid.*

yang asli dapat digunakan terdakwa Handojo karena pengurangan bonus yang diakibatkan dari pembuatan *member* fiktif tersebut.[89]

Berdasarkan Putusan Nomor 116 K/Pid.Sus/2015 tersebut, terdakwa Handojo dinyatakan bersalah telah melakukan tindak pidana yang diatur dalam Pasal 35 UU ITE. Apakah Pasal 35 UU ITE yang mengatur adanya tindakan manipulasi untuk membuat informasi atau dokumen elektronik seolah-olah otentik merupakan pengaturan mengenai *computer related fraud* yang dimaksud? Jawabannya tidak. Manipulasi dan gangguan data (penciptaan, perubahan, penghilangan dan pengrusakan) yang diatur dalam Pasal ini memiliki tujuan agar informasi atau dokumen elektronik dianggap seolah-olah data yang otentik. Mengapa pelaku mau membuat informasi seolah-olah data yang otentik? Hal ini tidak dijelaskan oleh Pasal 35 UU ITE.[90]

Esensi penipuan (*computer-related fraud*) merupakan perbuatan menguntungkan diri sendiri atau orang lain dengan menggunakan Internet untuk melaksanakan muslihat atau rangkaian kebohongan kebohongan sehingga orang lain pada umumnya berdasarkan muslihat atau rangkaian kebohongan tersebut melakukan tindakan yang merugikan dirinya dan kehilangan suatu nilai material/ekonomis yang terkandung dalam informasi atau dokumen elektronik. Oleh karena itu yang menjadi tujuan utama penipuan adalah keuntungan yang diperoleh dengan cara yang tidak sah dengan menggunakan muslihat atau rangkaian kebohongan. Akan tetapi, jika dihubungkan dengan ketentuan Pasal 35 UU ITE, penipuan dapat dilakukan

[89] *Ibid.*
[90] Josua Sitompul, *Op. Cit.*, halaman 250.

dengan manipulasi informasi atau dokumen elektronik sehingga orang lain menganggap data yang di dalamnya adalah data yang otentik. Dengan perkataan lain, manipulasi merupakan bagian dari penipuan, manipulasi salah satu bentuk muslihat, sehingga tidak sama dengan penipuan.[91]

Berdasarkan teori-teori dan unsur-unsur yang berkaitan dengan bentuk-bentuk tindak pidana manipulasi dan perubahan data pada website perusahaan serta perkara dalam Putusan Nomor 116 K/Pid.Sus/2015 yang telah dianalisis dan telah diuraikan di atas maka dapat ditarik kesimpulan bahwa tindakan manipulasi dan perubahan data pada website perusahaan termasuk kejahatan *fraud* (penipuan/kecurangan) di perusahaan yang dilakukan dengan menggunakan sistem komputer dan internet. Data yang dimanipulasi dan diubah merupakan data elektronik yang tersimpan pada website dan untuk dapat mengakses data tersebut maka diperlukan sistem komputer dan internet. Istilah kejahatan ini adalah *computer related fraud, internet fraud* atau *electronic fraud offence*. Dengan demikian, bentuk-bentuk kejahatan manipulasi dan perubahan data pada website perusahaan yaitu kejahatan pemalsuan data melalui sistem komputer (*computer related forgery*) dan kejahatan penipuan atau perbuatan curang di perusahaan dalam bentuk *fraud* atas laporan yang dilakukan dengan menggunakan sistem komputer (*computer related fraud/internet fraud/electronic fraud offence*). Kedua bentuk kejahatan ini sangat berkaitan erat karena perbuatan pemalsuan data elektronik

[91] *Ibid.*

(*computer related forgery*) biasanya dilakukan untuk melakukan tindak pidana siber lainnya seperti *computer related fraud* atau *internet fraud.*[92]

B. Faktor-faktor Penyebab Tindak Pidana Manipulasi dan Perubahan Data pada Website Perusahaan.

Pengkajian tentang penyebab seseorang melakukan kejahatan dapat menggunakan teori-teori kriminologi. Dalam perspektif teori anomi sebagaimana dikemukakan Emile Durkheim, kejahatan disebabkan oleh ketiadaan norma (*normlessness*). Kondisi tersebut disebabkan oleh masyarakat yang berubah sangat cepat. Pengertian *normlessness* bukan hanya tidak adanya norma dalam masyarakat, melainkan juga anggapan anggota masyarakat yang tidak mengakui adanya norma.[93]

Selain Emile Durkheim, teori anomi juga dikemukakan oleh Robert Merton. Menurut Merton, kejahatan disebabkan oleh ketidaksesuaian antara tujuan dengan cara-cara yang melembaga untuk mencapai tujuan yang mampu ditempuh oleh seseorang, karena itu mereka melakukan segala cara untuk mencapai segala cara tersebut untuk mencapai tujuan tersebut meskipun melanggar hukum. Mayoritas *cybercrime* yang dilakukan karena motif ekonomi dan kadang kala ditunjang oleh kondisi anomi pelaku, yaitu ketiadaan sarana yang dimiliki pelaku untuk mencapai tujuan.[94]

Teori anomi dari Merton secara keseluruhan tidak dapat digunakan dalam memahami kejahatan yang beruhubungan dengan komputer, karena cenderung menganggap bahwa kejahatan tersebut dilakukan oleh orang-orang

---

[92] Sigit Suseno. 2012. *Yurisdiksi Tindak Pidana Siber*. Jakarta: PT. Refika Aditama, halaman 179.

[93] Widodo. 2013*, Op. Cit.,* halaman 113.

[94] *Ibid.,* halaman 114.

yang golongan ekonominya lemah, padahal pada beberapa kasus, para pelaku adalah pejabat atau orang-orang yang terhormat. Selain itu, khusus dalam kategori kejahatan yang menjadikan komputer sebagai sasaran, tidak ada motif mencari keuntungan ekonomi. Namun jika "keterbatasan sarana" mencapai tujuan termasuk "keserakahan" dari pelaku, maka teori Merton cukup rasional.[95]

Berdasarkan teori biologinya Lombrosso yang disempurnakan oleh Enrico Ferri, dengan menekankan bahwa kejahatan terjadi karena adanya hubungan yang erat antara faktor fisik, antropologis, dan sosial:[96]

1. Faktor-faktor fisik yaitu suku bangsa, iklim, letak geografis, pengaruh musim, temperatur, dan sebagainya.
2. Faktor-faktor antropologis yaitu umur, kelamin, kondisi-kondisi organis, kondisi-kondisi psikologi, dan sebagainya.
3. Faktor-faktor sosial yaitu rapatnya penduduk, kebiasaan, susunan pemerintahan, kondisi-kondisi ekonomis, kondisi-kondisi industri, dan sebagainya.

Secara kriminologis, kejahatan yang berhubungan dengan komputer pada hakikatnya merupakan kejahatan yang dihasilkan oleh masyarakat dan harus dianggap sebagai gejala sosial. Ini didasarkan pada pendapat Leon Radzinovicz yang menyatakan: "*crime is general phenomenon it occurred not marelly in all advanced societies whatever type at all stages in their development. There was no sign that it was on the decline. It must therefore be*

[95] *Ibid.*, halaman 115.
[96] Abdul Wahid dan Mohammad Labib, *Op. Cit.*, halaman 45.

accepted as a social fact a normal part of society, which could not be eradicated at will".[97]

Richard Quiney berpendapat bahwa[98]

> *"study of crimei involvesan investigation of such natural product and contradictions of capitalism as alienation, inequality, proverty, unemployment, spiritual melaise, and the economic crisis of the capitalist state. To understand crime we have to understand development of the political economy and capitalist society".*

Perspektif teori asosiasi diferensial yang mengutamakan proses pembelajaran tentang kejahatan bukan hanya terjadi pada orang-orang biasa, tetapi juga terjadi pada orang-orang terhormat sebagai pelaku *white collar crime*. Hal ini secara tegas dikemukakan oleh Sutherland, dalam teorinya Sutherland bertanya-tanya mengapa perhatian teori-teori kriminologi hanya terhadap kejahatan yang dilakukan oleh masyarakat yang kelas bawah. Ia merekomendasikan penggunaan teori asosiasi diferensisal untuk mengkaji "kejahatan kerah putih". Berdasarkan pendapat tersebut, *cybercrime* yang dilakukan oleh "orang-orang terhormat" juga dilatarbelakangi oleh konsep pembelajaran sebagaimana diuraikan oleh Sutherland dalam Teori Asosiasi Diferensial.[99]

John Hagan menegaskan bahwa teori kontrol sosial bertolak dari asumsi bahwa setiap individu di masyarakat mempunyai peluang sama untuk menjadi orang yang melanggar hukum atau orang yang taat hukum. Teori kontrol sosial mengajukan pertanyaan mendasar, mengapa tidak semua orang yang taat pada

---

[97] Widodo. 2017. *Perspektif Hukum Pidana dan Kebijakan Pemidanaan (Diversi dan Keadilan Restoratif, Terorisme, Cybercrime, Pidana Mati, dan Peradilan sesat).* Yogyakarta: Aswaja Pressindo, halaman 95.

[98] *Ibid.*

[99] Widodo. 2013, *Op. Cit.*, halaman 121.

hukum. Menurut teori kontrol sosial, manusia mempunyai kebebasan untuk bertindak dan penentu tingkah laku seseoang adalah ikatan-ikatan sosial yang sudah terbentuk. Larry J. Siegel menulis, *a person bont to society prevents him or her from violating social rules if his bond weakens, we person is free to commit crime"*. Sedangkan Travis Hirschi berpendapat, *"The social bond, comprises four elements, attachment, commitment, involevmen, and bilief"*. Berdasarkan pendapat ini bahwa ikatan sosial yang menjadi salah satu penyebab terjadinya tingkah laku jahat terdiri atas empat unsur, yaitu keterikatan, ketersangkutan yang terkait dengan kepentingan sendiri, keterlibatan, norma dan nilai. Keempat elemen di atas harus terbentuk dalam masyarakat karena apabila gagal dibentuk maka akan muncul tingkah laku menyimpang. Seseorang yang tidak dapat mengimplementasikan keempat komponen tersebut cenderung bertingkah laku jahat.[100]

Larry J. Siegel mengemukakan teori netralisasi, pendapat utama teori netralisasi adalah bahwa seseorang akan belajar untuk menetralkan moral yang mengendalikan tingkah laku manusia, kemudian melakukan prilaku menyimpang. Selain itu, teori ini juga menjelaskan bagaimana cara-cara pemuda melakukan penyimpangan dan cara-cara pemuda tersebut terlibat dalam tingkah laku menyimpang. Teori netralisasi mengasumsikan, bahwa tingkah laku manusia dikendalikan oleh pemikiran-pemikiran pelaku. Teori ini menanyakan, apakah yang ada dibalik pemikiran orang-orang yang baik sehingga kadang-kadang membuat mereka berubah menjadi orang yang

[100] Widodo. 2017, *Op. Cit.*, halaman 104.

berprilaku jahat atau buruk atau menyimpang dari norma masyarakat? Bedasarkan pertanyaan tersebut, teori ini menganggap bahwa kebanyakan orang, dalam sebagian besar waktunya, pada saat melakukan sesuatu pebuatan dikendalikan oleh pemikiran-pemikiran yang baik, tetapi mengapa pada umumnya memiliki pemikiran yang baik tersebut sampai melakukan perbuatan yang menyimpang atau melakukan kejahatan.[101]

Berkaitan dengan teori-teori kriminologis di atas tentang penyebab seseorang melakukan kejahatan komputer (*cybercrime*) dapat diketahui bahwa ada banyak faktor yang menyebabkan pelaku *cybercrime*, faktor penyebab sangat bervariasi. Antara satu bentuk kejahatan dengan kejahatan lainnya juga disebabkan oleh kombinasi dari beberapa penyebab yang berbeda. Dari banyaknya faktor penyebab dan bervariasinya beberapa faktor dalam suatu bentuk kejahatan, Sutherland menjelaskan uraian tentang *The Multiple Faktor*.[102]

Pendekatan multifaktor ini bukan merupakan suatu teori, teteapi dapat digunakan terutama dalam mendiskusikan kasus kejahatan individual. Pendekatan ini merupakan salah satu bentuk pendekatan yang dapat digunakan untuk menganalisis variasi tentang tingkat kejahatan. Perlu mempelajari kasus-kasus secara individual, sehingga mengetahui bahwa kadangkala seseorang dalam melakukan kejahatan disebabkan oleh kombinasi faktor tertentu dan

[101] *Ibid.*, halaman 105.
[102] Widodo. 2013, *Op. Cit.*, halaman 126.

orang lainnya dalam melakukan kejahatan juga disebabkan oleh kombinasi faktor lainnya lagi yang berbeda-beda.[103]

Pengertian motivasi dengan penyebab dibedakan. Motivasi adalah sesuatu yang menimbulkan motif yang berasal dari dalam diri seseorang (penyebab internal), sehingga seseorang melakukan kejahatan. Sedangkan pengertian penyebab lebih luas dari motivasi, yaitu termasuk faktor penyebab eksternal yang mendorong seseorang melakukan kejahatan. Berdasarkan konsepsi tersebut, pengertian motivasi merupakan bagian dari faktor penyebab. Dari perbedaan ini dapat digunakan legislator sebagai dasar perencanaan penanggulangan kejahatan (*criminal policy*) terhadap kejahatan yang tergolong dalam kejahatan berteknologi tinggi, khususnya kebijakan hukum pidana (*penal policy*) karena analisis kriminologi berkaitan erat dengan kriminalisasi, pertanggungjawaban pidana dan penalisasi. Secara praktis dapat digunakan oleh pemerintah sebagai dasar penentuan kebijakan kriminal, terutama kebijakan nonpenal.[104]

Berdasarkan analisis kriminologis terhadap *cybercrime* sebagai berikut:[105]

1. Teori anomi sebagaimana diajarkan Durkheim dapat digunakan sebagai alat analisis penyebab terjadinya *cybercrime*, yaitu adanya perasaan atau pemahaman pada pelaku kejahatan bahwa norma yang mengatur *cybercrime* di Indonesia belum ada, sehingga perbuatan tersebut dianggap bukan kejahatan.

[103] *Ibid.,* halaman 127-128.
[104] Widodo. 2017, *Op. Cit.,* halaman 97
[105] Widodo. 2013, *Op. Cit.,* Halaman 125-126.

2. Teori anomi sebagaimana diajarkan Robert Merton dapat digunakan untuk menganalisis penyebab seseorang melakukan *cybercrime* di Indonesia, karena kesenjangan antara "cita-cita" dengan "sarana yang tersedia" tidak selalu menjadi penyebab orang melakukan kejahatan.
3. Menurut analisis dari teori asosiasi diferensial, kejahatan tersebut dilakukan melalui proses pembelajaran yang terjadi pada komunitas "orang terhormat" maupun bukan.
4. Menurut analisis teori kontrol sosial, *cybercrime* terjadi karena melemahnya ikatan sosial pelaku kejahatan, karena itu cenderung dilakukan oleh para pemuda di kota-kota besar.
5. Perspektif teori netralisasi, pelaku kejahatan melakukan aktivitasnya didasari oleh rasa ingin balas dendam, merasa tidak berdaya menghadapi masyarakat dan hukum, bahaya yang ditimbulkan tidak serius bagi masyarakat dan ingin memperoleh kebebasan bertingkah laku dengan cara menganggap UU sebagai penghalang aktivitas di internet.

Teori-teori kriminologi tersebut belum dapat mengulas secara detail tentang peranan korban dan objek *cybercrime* dalam perkara *cybercrime*.[106] Kejahatan Komputer dapat dilakukan secara internal dan eksternal. Kejahatan komputer secara internal adalah kejahatan yang dilakukan oleh atau bantuan dari "orang dalam". Yang dimaksud dengan "orang dalam" di sini adalah para pekerja di dalam suatu instansi dimana komputer pusat tersebut berada, atau

[106] *Ibid.*

dari seorang *programmer* yang memprogram komputer tersebut. Dengan demikian, para pelaku kejahatan tidak perlu mengetahui bagaimana cara mendapatkan akses ke dalam komputer perusahaan. Kejahatan komputer jenis ini sangat tergantung pada mekanisme kerja sistem komputer perusahaan yang bersangkutan. Lubang-lubang kelemahan dari sistem komputer atau prosedur-prosedur dalam pengelolaan data adalah sasaran utama dari kejahatan komputer. Pada dasarnya kejahatan komputer ini dapat dilakukan dengan cara manipulasi transaksi input dan mengubah data.[107]

Perkara dalam Putusan Nomor 116 K/Pid.Sus/2015 setelah dianalisis dengan mengkaitkan teori di atas maka dapat dikatakan sebagai kejahatan komputer yang dilakukan secara internal karena dapat dilihat dari Handojo sebagai rekan kerja sama perusahaan mempunyai kedudukan serta kewenangan untuk menjalankan tugas-tugas dan tanggung jawabnya dalam menjalani perusahaan. Handojo melakukan tindak pidana manipulasi dan perubahan data pada website perusahaan dengan menyuruh saksi Fajar selaku orang yang bekerja atau sebagai pegawai perusahan yang membuat system dan pemrograman serta melakukan pemeliharaan (*maintenance*) website www.myoxysuper.com milik PT. Mulia Rejeki Waterindo. Singkatnya, saksi Fajar merupakan pegawai yang dapat menjalankan system website perusahaan dengan melakukan pengelolaan data terhadap nama-nama *ID member*

[107] Suheimi. 1991. *Kejahatan Komputer*. Yogyakarta: Andi Offset, halaman 74-75.

perusahaan sistem *MLM* tersebut. maka dapat dikatakan bahwa Handojo dan Fajar adalah "orang dalam" yang dimaksud.[108]

Tindak pidana manipulasi dan perubahan data pada website perusahaan untuk mengetahui faktor-faktor penyebabnya perlu dengan pendekatan multifaktor, pendekatan ini merupakan salah satu bentuk pendekatan yang dapat digunakan untuk menganalisis variasi tentang kejahatan dengan mempelajari suatu kasus secara individual, sehingga mengetahui bahwa kadangkala seseorang melakukan kejahatan disebabkan oleh kombinasi faktor tertentu dan orang lainnya melakukan kejahatan juga disebabkan oleh kombinasi faktor lainnya yang berbeda-beda.[109]

Mengenai perkara dalam Putusan Nomor 116 K/Pid.Sus/2015 dengan pendekatan multifaktor yaitu mempelajari, menganalisis dan juga mengaitkannya dengan teori-teori di atas maka terlihat sangat jelas bahwa faktor perbuatan itu dikarenakan adanya kesempatan yang paling besar pada area di mana pengendalian internalnya lemah atau tidak ada pengendalian internalnya. Dilihat dari pelakunya yang merupakan orang yang menjalin kerjasama dengan pemilik perusahaan dengan adanya perjanjian pembagian kerja secara tertulis yang mana dalam perjanjian tersebut Handojo mempunyai tugas dan tanggung jawab dalam pengelolaan teknologi informasi *system online*, dan saksi Fajar sebagai orang yang membuat dan yang menjalankan *system website* artinya perbuatannya termasuk ke dalam pengawasannya sendiri dan pelakunya ialah dirinya sendiri. Menurut penelitian yang dilakukan

---

[108] *Ibid.*
[109] Widodo. 2013, *Op. Cit.*, halaman 127.

oleh Hollinger dan Clark, sebab yang paling umum karyawan melaksanakan *fraud* di perusahaan adalah adanya kesempatan (yang umumnya timbul dari lemahnya pengendalian).[110]

Berdasarkan uraian di atas bahwa faktor-faktor tindakan *fraud* karena adanya kesempatan dan lemahnya pengendalian internal, selain kedua faktor tersebut, Hollinger dan Clark juga mengatakan bahwa faktor penyebab seseorang melakukan *fraud* adalah ketidakpuasan terhadap upah kerja atau karena faktor ekonomi, ini sesuai dengan tindak pidana manipulasi dan merubah data pada website perusahaan dalam perkara Putusan Nomor 116 K/Pid.Sus/2015 yaitu pelaku melakukan perbuatan tersebut dengan cara sengaja menambahkan *member* fiktif secara melawan hukum yang mengakibatkan kerugian bagi *member* perusahaan yang asli.[111]

Berdasarkan dari perbuatannya itu mengakibatkan struktur dan jumlah bonus masing-masing *member* menjadi berkurang, tujuannya agar pelaku dapat meraup keuntungan. Hal tersebut dapat dilihat dari kerugian yang dialami oleh perusahaan yaitu sebesar kurang lebih 1.500.000.000 (satu milyar lima ratus juta rupiah) dalam sistem telah terprogram ada penyisihan dana sebesar 8%, dan bonus-bonus member yang tidak ada dananya, serta laba perusahaan yang selama 6 (enam bulan) tidak ada uangnya dan tidak diketahui oleh Gabby selaku pemilik perusahaan. Berdasarkan akibat dari tindakan pelaku, mak faktor penyebab tindak pidana manipulasi dan perubahan data pada website

[110] Bona P. Purba, *Op. Cit.*, halaman 8.
[111] *Ibid.*

perusahaan dalam perkara Putusan Nomor 116 K/Pid.Sus/2015 adalah karena ketidakpuasan upah kerja atau faktor ekonomi.[112]

Penjelasan lain tentang faktor-faktor dan penyebab terjadinya *fraud* diberikan oleh Donald R. Cressey yang meneliti 200 pelaku *fraud* pada Tahun 1940-an. Penelitiannya menyimpulkan bahwa mayoritas orang melaksanakan *fraud* adalah untuk memenuhi kewajiban keuangannya. Cressey menyimpulkan, untuk menjalankan paraktik *fraud*, pelaku harus memiliki kesempatan (*Oppurtinity*) untuk melaksanakan dan menyembunyikan kejahatannya (*concealment*) dan pembenaran (*rationalization*) bahwa tindakannya bukan perbuatan jahat (*criminal activity*).[113]

Faktor-faktor penyebab kejahatan komputer (*cybercrime*) sangat banyak dan bervariasi, dilihat dari bentuk-bentuk kejahatan yang satu dan kejahatan yang lainnya, selaras dengan "*multi-faktor theory*". Maka untuk mengetahui faktor-faktor penyebab dari suatu bentuk *cybercrime*, diperlukan pendekatan multifaktor dengan menganalisis suatu kasus. Faktor-faktor penyebab kejahatan komputer dalam bentuk tindakan manipulasi dan perubahan data pada website perusahan dengan menggunakan teori-teori kriminologi dan pendekatan multifaktor dengan cara menganalisis suatu kasus yaitu menganalisis perkara dalam Putusan Nomor 116 K/Pid.Sus/2015. Maka faktor-faktornya adalah sebagai berikut:[114]

1. Faktor lemahnya pengendalian internal perusahaan, yaitu tidak adanya elemen pengendalian internal yang seharusnya dimiliki oleh perusahaan

[112] *Ibid.*
[113] *Ibid.*
[114] Widodo. 2013, *Op. Cit.,* halaman 128.

seperti aktivitas pengendalian dan pemantauan, karena tidak adanya elemen tersebut maka menimbulkan kesempatan yang besar bagi orang-orang yang melakukan tindakan *fraud* di ranah perusahaan.

2. Faktor ekonomi, yaitu ketidakpuasan terhadap upah kerja, maka yang menjadi tujuan pelaku adalah untuk mendapatkan uang dengan cara menguntungkan diri sendiri dan menimbulkan kerugian perusahaan serta *member* perusahaan yang asli.
3. Politik, Faktor ini merupakan salah satu faktor yang sangat mempengaruhi dikarenakan terjadinya persaingan usaha yang semakin tinggi dan ketat antara perusahaan satu dan yang lainnya dan hal ini seringkali memunculkan konflik yang berkaitan dengan politik seperti menjatuhkan pihak-pihak tertentu.
4. Balas dendam, faktor ini muncul karena alasan emosional pelaku yang ingin membalaskan dendamnya, biasanya karena alasan-alasan pribadi.
5. Pelampiasan kekecewaan, faktor ini muncul karena rasa kekecewaan pelaku terhadap suatu produk milik perusahaan.
6. Menguji ketangguhan pengamanan sistem komputer perusahaan dalam mengelola dan mengamankan situs/website, faktor ini muncul karena rasa ingin tahu pelaku terhadap sistem pengamanan situs web milik perusahaan.
7. Menguji kemampuan diri sendiri dalam aplikasi teknologi informasi, faktor ini muncul karena pelaku ingin menguji kemampuannya dan

ingin mendapatkan pengakuan orang lain atas kemampuannya dalam menguasai teknologi informasi.

C. Pencegahan Tindak Pidana Manipulasi dan Perubahan Data pada Website Perusahaan.

Pengertian memerangi kejahatan sama dengan pengertian menanggulangi kejahatan. Dalam istilah kriminologi, penanggulangan kejahatan sering juga disebut dengan kebijakan kriminal (*criminal policy*) sebagaimana dikemukakan juga oleh Hoefnagels dalam beberapa literatur, penggulangan kejahatan disebut juga dengan istilah "perang terhadap kejahatan" atau memerangi kejahatan.[115]

Kebijakan kriminal adalah ilmu pengetahuan yang memberi tanggapan. Kebijakan tersebut merupakan ilmu pengetahuan dalam menanggulangi kejahatan. Kebijakan kriminal juga penjelmaan dari ilmu pengetahuan dan bersifat terapan. Pembuatan Undang-undang dan kebijakan penegakanna merupakan bagian dari politik sosial. Selanjutnya, Hoefnagels mengutip pendapat Marc Ancel bahwa *criminal policy is part of longer policy; the law enforcement policy; the legislative and enforcement policy is in the turn part of social policy.* Kebijakan kriminal tersebut merupakan bagian dari kebijakan yang sangat luas yaitu kebijakan penegakan hukum.[116]

Banyak cara yang dapat dilakukan untuk menanggulangi kejahatan, baik menggunakan cara persuasif maupun represif. Pengertian pencegahan kejahatan mengacu kepada strategi dan tindakan untuk mereduksi resiko

---

[115] *Ibid.*, halaman 31.
[116] Widodo. 2013, *Op. Cit.*, halaman 179-180.

kejahatan, dan efek dari berbahayanya kejahatan bagi individu dan masyarakat, sambil melakukan intervensi terhadap pengaruh-pengaruh kejahatan dengan menekan berbagai faktor penyebab kejahatan. Prinsip utama pencegahan kejahatan kepemimpinan, kerjasama, dan penegakan hukum di negara hukum, sambil membuat rencana aksi pencegahan kejahatan, kemudian melaksanakan program tersebut dengan selalu berbasis keilmiahan, termasuk melakukan pendekatan-pendekatan untuk meminimalisasi peluang terjadinya kejahatan.[117]

Menanggulangi kejahatan diperlukan strategi yang mantap dari negara dan masyarakat, dan harus dilakukan secara bersama-sama secara simultan. Allan R. Coffey berpendapat sebagai berikut:[118]

> *"Strategies to prevent crime and delinquency can take two basics focuses: effort to prevent first offense or effort to prevent to repetition of criminal anddelinquent acts; these are the preventivention of contact with the justice system n the first instance and the prevention of the penetration of the justice system after contact has been made."succesful efforts of law enforcment with community aid in preventing crime generally include both type of strategies".*

Strategi pencegahan kejahatan dan kenakalan dapat dilakukan melalui dua fokus utama, yaitu: (a) usaha mencegah pelanggaran yang pertama, dan (b) mencegah pengulangan pelanggaran dengan cara melakukan pencegahan, yaitu melakukan tindakan pencegahan sebelum melakukan penindakan dengan cara menggunakan sistem peradilan pidana. Sedangkan usaha yang kedua, dilakukan dengan cara penetrasi melalui penerapan sistem peradilan pidana.

---

[117] Widodo. 2013, *Loc., Cit*.
[118] *Ibid.*, halaman 34.

Usaha penegakan hukum yang sukses perlu ditopang oleh masyarakat, baik pencegahan kejahatan preventif maupun penindakan secara represif.[119]

Hoefnagels berpendapat bahwa penanggulangan kejahatan (*criminal policy*) dapat dilakukan dengan cara *"influencing views of society on crime and punishment/mass media, prevention without punishment, and criminal law application."* Penanggulangan kejahatan (kebijakan kriminal) dilakukan dengan cara mempengaruhi pandangan masyarakat terhadap kejahatan dan pemidanaan, menanggulangi kejahatan dengan tanpa menggunakan hukum pidana, dan menerapkan hukum pidana dalam masyarakat.[120] Selanjutnya Hoefnagels, mengemukakan bahwa penerapan hukum pidana untuk menanggulangi kejahatan meliputi ruang lingkup berikut:[121]

1. Administrasi peradilan pidana dalam arti sempit, yaitu pembuatan hukum pidana dan yurisprudensi, proses peradilan pidana dalam arti luas (meliputi kehakiman, ilmu kejiwaan, ilmu sosial), dan pemidanaan
2. Psikiatri dan psikologi forensik.
3. Forensik kerja sosial.
4. Kejahatan, pelaksanaan pemidanaan dan kebijakan statistik.

Muladi dan Barda Nawawi Arief menyebutkan upaya penanggulangan kejahatan dengan tanpa menggunakan hukum pidana dengan istilah *nonpenal policy.* Sedangkan upaya penanggulangan kejahatan dengan menerapkan hukum pidana disebut dengan *penal policy.*[122]

Salah satu penanggulangan kejahatan *cyber* adalah melalui sarana hukum pidana. Hukum pidana dipanggil untuk menyelamatkan kerugian yang

---

[119] *Ibid.,* halaman 35.
[120] *Ibid.,* halaman 36.
[121] Widodo. 2013, *Op. Cit.,* halaman 188-189.
[122] Widodo. 2013, *Loc., Cit.*

diderita masyarakat, karena kejahatan tersebut dapat menghalangi aktivitas kehidupan sosio-ekonomi masyarakat. Demikian pula aspek-aspek lain yang mendukung pembangunan kesejahteraan masyarakat. Sehingga sebagai bentuk perlindungan terhadap kepentingan masyarakat (*social defence*) tersebut, maka keberadaan hukum pidana sangat diperlukan agar dapat teratasinya kejahatan di dunia *cyber* yang notabenenya telah menjadi penghambat pembangunan kesejahteraan masyarakat (*social welfare*). Upaya melalui kebijakan hukum pidana yang integral harus dimaksimalkan. Mulai dari substansi hukum, struktur hukum bahkan kultur hukumnya harus berjalan dengan maksimal. Hanya melalui penegakan hukum pidana dalam penanggulangan *cybercrime* dapat terealisasi.[123]

Perserikatan Bangsa-Bangsa (PBB), pernah mengadakan kongres mengenai *The Prevention Of Crime and The Treatment Of Offenders* yang telah membahas masalah mengenai *cybercrime*. Masalah *cybercrime* diagendakan pada Kongres VIII/1990 di Havana dan pada Kongres X/2000 di Wina. Resolusi Kongres mengenai *computer related crimes* tindakan penanggulangan terhadap *cybercrime* tidak hanya melalui kebijakan antara lain:[124]

a. Mengimbau negara anggota untuk mengintensifkan upaya-upaya penanggulangan penyalahgunaan komputer yang lebih efektif dengan mempertimbangkan langkah-langkah diantaranya:

[123] Budi Suhariyanto, *Op. Cit.,* halaman 44-45.
[124] Maskun dan Wiwik Meilarati, *Op. Cit.,* halaman 42.

1) Melakukan modernisasi hukum pidana materiil dan hukum acara pidana;
2) Mengembangkan tindakan-tindakan pencegahan dan pengamanan komputer;
3) Melakukan langkah-langkah untuk membuat peka (sensitif) warga masyarakat, aparat pengadilan dan penegak hukum, terhadap pentingnya pencegahan kejahatan yang berhubungan dengan komputer;
4) Melakukan upaya-upaya pelatihan (*training*) bagi para hakim, pejabat, dan aparat penegak hukum mengenai kejahatan ekonomi dan *cybercrime*;
5) Memperluas *rules of ethics* dalam penggunaan komputer dan mengajarkannya melalui kurikulum informatika;
6) Mengadopsi perlindungan korban *cybercrime* sesuai dengan Deklarasi PBB mengenai korban dan mengambil langkah-langkah untuk mendorong korban melaporkannya adalah *cybercrime*.

b. Mengimbau negara anggota meningkatkan kegiatan internasional dala upaya penanggulangan *cybercrime*.
c. Merekomendasikan kepada Komite pengendalian dan pencegahan kejahatan (*Committee on Crime Prevention Control/CCPC*) PBB untuk:
    1) Menyebarluaskan pedoman dan standar untuk membantu negara anggota menghadapi *cybercrime* di tingkat nasional, regional, dan internasional;

2) Mengembangkan penelitian dan analisis lebih lanjut guna menggunakan cara-cara baru menghadapi *problem of cybercrime* di masa yang akan datang;
3) Mempertimbangkan *cybercrime* sewaktu meninjau mengimplementasikan perjanjian ekstradisi dan bantuan kerja sama di bidang penanggulangan kejahatan.

Menindaki resolusi tersebut, pada Tahun 1994, PBB mengeluarkan *International Review of Criminal Policy-United Nation Manual on the Preention and Control of Computer-Related Crime* yang memberikan pedoman mengenai substansi hukum pidana yang perlu diatur dalam hukum nasional negara anggota, termasuk kriminalisasi terhadap pelanggaran privasi. Menurut pedoman ini, kejahatan komputer yang umum terdiri dari:[125]

1. Penipuan melalui manipulasi dengan menggunakan sarana komputer (*fraud by computer manipulation*);
2. Pemalsuan dengan menggunakan komputer (*computer forgery*);
3. Perusakan atau modifikasi terhadap data atau program komputer (*damage to or midifications of computer data or programs*);
4. Pengaksesan sistem atau layanan komputer secara tanpa hak terhadap program komputer yang dilindungi secara hukum (*unauthorized reproduction of legally protected computer programs*).

Berdasarkan pedoman di atas, maka mengenai kejahatan manipulasi dan perubahan data pada website perusahaan yang termasuk ke dalam bentuk

[125] *Ibid.,* halaman 78.

kejahatan pemalsuan data elektronik (*computer related forgery)* dan juga kejahatan penipuan/kecurangan di perusahaan dengan menggunakan sistem komputer (*computer related fraud*) maka kejahatan ini merupakan salah satu *cybercrime* yang sering terjadi. Pengaturan penipuan dengan menggunakan sarana komputer (*computer related fraud*) perlu di atur dalam hukum positif Indonesia karena pengaturan penipuan di dalam KUHP dan UU ITE belum mencukupi dalam mencakup jenis kejahatan penipuan dengan menggunakan teknologi canggih dan kompleks. Untuk itu diperlukan aturan hukum pidana yang baik dalam hukum nasional masing-masing negara sehingga tindak pidana ini dapat dicegah dengan membuat pelakunya jera.[126]

Negara-negara anggota *Council of Europe* telah menghasilkan suatu draf tentang *cybercrime*, dari draf tersebut mengenai *computer related forgery* dan *computer related fraud* di atur dalam Pasal 8 titel 2. Aturan tersebut menyebutkan bahwa setiap negara peserta harus memiliki aturan nasional yang diperlukan dalam menangani tindakan pelanggaran atau tindak kriminal, yang dilakukan dengan sengaja dan tanpa hak dan mnyebabkan hilangnya harta orang lain, dengan cara; memasukkan, mengubah, mengurangi, merusak data komputer, dengan menggunakan tindakan yang curang/tipu muslihat dan tidak jujur untuk memperoleh keuntungan ekonomis bagi dirinya atau untuk orang lain.[127]

Aturan mengenai *internet fraud* pada Pasal 8 dalam konvensi ini (*computer-related fraud*) bertujuan untuk mengkriminalisasikan segala jenis

[126] Joshua Sitompul, *Op. Cit.*, halaman 59.
[127] Maskun dan Wiwik Meilarati, *Op. Cit.*, halaman 85-86.

manipulasi dalam pemrosesan data dengan tujuan untuk mentransfer properti secara ilegal. *Computer related fraud* dikriminalisasi jika manipulasi menimbulkan kerugian langsung terhadap kehilangan kepemilikan atau kerugian secara ekonomi bagi orang lain, dan pelaku melakukan tindakannya dengan melakukan tujuan mengambil keuntungan secara ekonomis bagi dirinya atau untuk orang lain dengan cara yang tidak sah. Pengertian kehilangan properti disini diartikan secara luas, termasuk di dalamnya kehilangan uang, benda berwujud dan tidak berwujud yang memiliki nilai ekonomis.[128]

Kebijakan non-penal untuk mencegah terjadinya kejahatan sistem komputer. Agus Rahardjo mengemukakan bahwa dalam rangka menerapkan kebijakan non-penal perlu adanya beberapa langkah preventif dari pemilik jaringan komputer. Langkah tersebut yaitu:[129]

a. Mengatur akses, melalui *authetication* dan *access control*;
b. Menutup *service* yang tidak digunakan;
c. Memasang proteksi;
d. *Firewall*;
e. Pemantauan adanya serangan;
f. Pemantauan integritas sistem;
g. Mengamati berkas *log*;
h. Melakukan *back up* secara rutin;
i. Penggunaan *encription* untuk meningkatkan keamanan;
j. Menggunakan *shell* yang aman.

Berdasarkan uraian di atas, maka mengenai kejahatan manipulasi dan perubahan data pada website perusahaan juga dapat di cegah dengan kebijakan non-penal tersebut karena kejatan ini termasuk dalam salah satu kejahatan

[128] *Ibid.*
[129] Widodo. 2013, *Op. Cit*., halaman 150.

komputer (*cybercrime*). Karena kejahatan manipulasi dan perubahan data pada website perusahaan merupakan bentuk *computer related fraud* yang dilakukan di ranah perusahaan, pengembangan dan implementasi pencegahan *fraud* dan pendeteksisan *fraud* harus merupakan upaya yang dikoordinasikan oleh top manajemen dengan seluruh pejabat dan pegawai organisasi/perusahaan. Secara kolektif, pembersihan *fraud* harus ditujukan pada risiko-risiko *fraud* pada suatu organisasi/perusahaan.[130]

Ada banyak teknik pencegahan yang lazim diterapkan dalam perusahaan/organisasi/lembaga-lembaga publik. Masing-masing teknik mempunyai kelebihan dan kekurangan. Perusahaan dapat menerapkan teknik yang paling sesuai dengan kultur, etika kerja dan juga jenis perusahaan yang bersangkutan. Berdasarkan survey yang dilakukan Asosiasi Akuntan Publik Amerika AICPA, yang mengindentifikasi teknik-teknik pencegahan yang paling banyak digunakan dan efektif yaitu:[131]

1. Perbaikan pengendalian atas teknologi informasi (98%);
2. Pengecekan referensi atas pegawai baru (97%);
3. Penegakan aturan prilaku (81%);
4. Peningkatan penggunaan analisis risiko (80%);
5. Pengawasan atas korepondensi elektronik (75%).

Apabila dikaitkan dengan perkara dalam Putusan Nomor 116 K/Pid.Sus/2015 mengenai tindak pidana manipulasi dan perubahan data pada website perusahaan, maka pencegahannya dapat dilakukan dengan teknik

---

[130] Bona P. Purba, *Op. Cit.*, Halaman 42.
[131] *Ibid.*

pencegahan seperti di atas. Survei tersebut juga menyimpulkan bahwa teknik pencegahan *fraud* di perusahaan yang paling efektif adalah teknik no. 2 yakni "pengecekan referensi atas pegawai baru". Maka terhadap kasus dalam putusan tersebut karena pelakunya adalah orang yang bekerja sama dengan perusahaan, maka pencegahan yang paling efektif adalah melakukan pengecekan referensi orang-orang yang ingin bekerjasama dengan perusahaan.[132]

Upaya pencegahan lainnya juga dapat dilakukan dengan menggunakan aplikasi (*software*) apabila kejahatan manipulasi dan perubahan data pada website perusahaan dilakukan secara eksternal, artinya yang melakukannya adalah orang lain diluar dari orang-orang yang ada dalam perusahaan dengan menggunakan komputer dan jaringan internet (*internet fraud*) maka perusahaan dapat melakukan pencegahan melalui aplikasi (*software*) yang dapat digunakan pada *personal computer, handphone* dan media lain yang digunakan dalam mengakses internet. Contoh aplikasi tersebut seperti aplikasi yang bernama *Dr. Safety*, aplikasi ini merupakan produk perusahaan Taiwan yang *trend micro* yang sangat *concern* terhadap keamanan data.[133]

Berdasarkan uraian di atas maka dapat diambil suatu kesimpulan bahwa pencegahan tindak pidana manipulasi dan perubahan data pada website perusahaan dapat dilakukan dengan upaya-upaya kebijakan penal dan non penal. Kebijakan penal yaitu melalui hukum pidana, walaupun kejahatan ini sudah diatur dengan UU ITE, tetapi aturan tersebut belum mencukupi untuk membuat pelaku jera, maka diperlukan pengaturan secara khusus mengenai

---

[132] *Ibid.*
[133] Maskun danWiwik Meilarati, *Op. Cit.*, halaman 99.

kejahatan *computer related forgery* dan *computer related fraud* di ranah perusahaan. Kebijakan non-penal yaitu melakukan upaya-upaya pelatihan (*training*) bagi para hakim, pejabat, dan aparat penegak hukum mengenai kejahatan ekonomi dan *cybercrime*, melakukan pengendalian teknologi informasi, melakukan pemantauan dan pem-*back up*-an data perusahaan, memasang proteksi, pengecekan referensi atas pegawai baru/orang yang ingin bekerjasama dengan perusahaan sampai kepada pencegahan menggunakan aplikasi (*software*) secara *personal computer*.

BAB IV

KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan uraian pada pembahasan dan hasil penelitian, maka dapat diambil suatu kesimpulan sebagai berikut:

1. Tindakan manipulasi dan perubahan data pada website perusahaan yaitu kejahatan komputer (*cybercrime*) dalam bentuk-bentuk kejahatan *computer related forgery* (pemalsuan data/dokumen elektronik) dan kejahatan *computer related fraud* (penipuan/kecurangan) di ranah perusahaan, yang mana bentuk-bentuk tindakan tersebut apabila dikaitkan dengan Putusan Nomor 116 K/Pid. Sus/2015 adalah membuat *member* fiktif yang seolah-olah otentik sehingga menguntungkan pelaku dan menyebabkan kerugian terhadap *member* perusahaan yang asli serta perusahaan kehilangan kepercayaan dan berpotensi mengalami kebangkrutan.
2. Faktor-faktor tindak pidana manipulasi dan perubahan data pada website ditinjau dari teori kriminologi dengan cara menganalisis suatu contoh kasus bahwa faktor-faktornya yaitu:
   a. Ekonomi, memperoleh uang secara tidak sah.
   b. Politik.
   c. Balas dendam.
   d. Pelampiasan kekecewaan.
   e. Menguji ketangguhan pengamanan sitem komputer perusahaan dalam mengelola dan mengamankan situs/website.

f. Menguji kemampuan diri sendiri dalam aplikasi teknologi informasi.

3. Pencegahan tindak pidana manipulasi dan perubahan data pada website perusahaan dapat dilakukan dengan cara upaya kebijakan penal dan non-penal. Kebijakan penal yaitu melalui hukum pidana, walaupun kejahatan ini sudah di atur dengan UU ITE tetapi belum mencukupi untuk membuat pelakunya jera maka diperlukan pengaturan secara khusus mengenai kejahatan *computer related forgery* dan *computer related fraud* di ranah perusahaan. Kebijakan non-penal yaitu melakukan upaya-upaya pelatihan (*training*) bagi para hakim, pejabat, dan aparat penegak hukum mengenai kejahatan ekonomi dan *cybercrime*, melakukan pengendalian teknologi informasi, melakukan pemantauan dan pem-*back up*-an data perusahaan, memasang proteksi, pengecekan referensi atas pegawai baru/orang yang ingin bekerjasama dengan perusahaan sampai kepada pencegahan menggunakan aplikasi (*software*) secara *personal computer*.

B. Saran

Berdasarkan uraian kesimpulan di atas, maka dalam penelitian ini disarankan:

1. Agar berkurangnya kejahatan manipulasi dan perubahan data pada website perusahaan maka diharapkan kepada pemerintah untuk memberikan perhatian khususnya dengan membentuk suatu aturan yang mengatur secara khusus mengenai kejahatan ini. Karena dari kejahatan ini sangat berpotensi menyebabkan kebangkrutan bagi perusahaan dan menyangkut kepada

orang-orang banyak karena sangat merugikan secara materil maupun non-materil.

2. Perlu ditingkatkannya kesadaran masyarakat terhadap suatu aturan hukum terkhusus pada aturan *cybercrime*, dan berperan dalam mencegah *cybercrime* terkhusus pada kejahatan pemalsuan dan penipuan melalui komputer dan internet.
3. Perusahaan haruslah lebih teliti dalam menentukan orang-orang yang akan melakukan kerjasama, haruslah melakukan penelitian terhadap latar belakang seseorang tersebut, selain itu perusahaan harus melakukan perbaikan mengenai pengendalian teknologi informasi serta pengawasan yang canggih baik secara internal maupun eksternal.

DAFTAR PUSTAKA

A. Buku

Abdul Wahid. 2010. *Kejahatan Mayantara (Cybercrime).* Bandung: PT. Refika Aditama.

Ade Maman Suherman. 2005. *Aspek Hukum dalam Ekonomi Global*. Bogor: Ghali

Ahmad M Ramli. 2010. *Cyber Law & HAKI dalam Sistem Hukum Indonesia.* Bandung: PT. Refika Aditama.

Barda Nawawi Arief. 2008. *Bunga Rampai Kebijakan Hukum Pidana*. Jakarta: Kencana.

Bona P. Purba. 2015. *Fraud dan Korupsi*. Jakarta: Lestari Kiranatama.

Budi Suhariyanto. 2013. *Tindak Pidana Teknologi Informasi (Cybercrime)*. Jakarta: Rajawali Pers.

Josua Sitompul. 2012. *Cyberspace,* C*ybercrimes, Cyberlaw Tinjauan Aspek Hukum Pidana*. Jakarta: PT. Tatanusa.

Maskun. 2010. *Kejahatan Siber (Cyber Crime) Suatu Pengantar.* Jakarta: Kencana

Maskun dan Wiwik Meilarati. 2017. *Aspek Hukum Penipuan Berbasis Internet*. Bandung: CV. Keni Media.

Muhammad Mustofa. 2013. *Metodologi Penelitian Kriminologi*. Jakarta: Kencana.

Rulli Nasrullah. 2014. *Teori dan Riset Media Siber (Cybermedia).* Jakarta: Kencana.

Sigid Suseno. 2012. *Yuridiksi Tindak Pidana Siber*. Bandung: PT. Refika Aditama.

Soerjono Soekanto. 2014. *Pengantar Penelitian Hukum.* Jakarta: Universitas Indonesia (UI-Press).

Suheimi. 1991. *Kejahatan Komputer*. Yogyakarta: Andi Offset.

Sutan Remy Syahdeini. 2009. *Kejahatan & Tindak Pidana Komputer*. Jakarta: PT. Pustaka Utama Grafiti.

Teguh Sulistia dan Aria Zurnetti. 2011. *Hukum Pidana Horizon Baru Pasca Reformasi.* Jakarta: Rajawali Pers.

Topo Santoso dan Eva Achjani Zulfa. 2013. *Kriminologi*. Jakarta: PT. Raja Grafindo.

Widodo. 2013. *Hukum Pidana di Bidang Teknologi Informasi (Cybercrime Law) Telaah Teoritik dan Bedah Kasus.* Yogyakarta: Aswaja Pressindo.

_____. 2013. *Aspek Hukum Pidana Kejahatan Mayantara*. Yogyakarta: Aswaja Pressindo.

_____. 2013. *Memerangi Cybercrime (Karakteristik, Motivasi dan Strategi Penanganannya dalam Perspektif Kriminologi)*. Yogyakarta: Aswaja Pressindo.

_____. 2017. *Perspektif Hukum Pidana dan Kebijakan Pemidanaan (Diversi dan Keadilan Restoratif, Terorisme, Cybercrime, Pidana Mati dan Peradilan Sesat.* Yogyakarta: Aswaja Pressindo.

B. Peraturan Perundang-undangan

Republik Indonesia, Undang-Undang Dasar Tahun 1945.

Republik Indonesia, Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

C. Internet

BOC Indonesia, "Pengertian Website, Webhosting dan Domain Name" *www.boc.web.id*, diakses Rabu, 6 Desember 2017.

Id.PANDI, "Tentang PANDI", melalui *www.pandi.id*, diakses Senin, 19 Februari 2018.

KBBI Online, "Pengertian Manipulasi dan Data", *www.kbbi.web.id*, diakses Rabu, 6 Desember 2017.

Kumpulan Pengertian Menurut Para Ahli, "Pengertian Data dan Jenis Data", *www.pengertianahli.com*, diakses Rabu, 06 Desember 2017.

NoName, "Tinjauan Umum Pencegahan, Tindak Pidana dan Penipuan Jual Beli Online", *www.erepo.unud.ac.id*, diakses Senin, 19 Februari 2018.

Sora N, “Mengetahui Pengertian Website dan Jenisnya”, *www.pengertianku.net*, diakses Rabu, 6 Desember 2017.

Visigraphic, “Website Profil Perusahaan”, *www.visigraphic.com*, diakses Rabu, 6 Desember 2017.

Wikipedia, “Pengertian Perusahaan”, *www.wikipedia.com*, diakses Sabtu, 2 Desember 2017.

Wikipedia, “Pengertian Manipulasi”, *www.wikipedia.com*, diakses Rabu, 6 Desember 2017.