KEBIJAKAN PIDANA PEMBAJAKAN AKUN MEDIA SOSIAL YANG MENIMBULKAN KERUGIAN MATERIL BAGI PEMILIK AKUN DI INDONESIA

SKRIPSI

Diajukan Untuk Memenuhi Tugas Akhir
Guna Memperoleh Gelar Sarjana Hukum

Oleh:

DONNA RIZKY RAGILLIA
NPM: 1906200590

FAKULTAS HUKUM
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
MEDAN
2023

بسم الله الرحمن الرحيم

PENETAPAN
HASIL UJIAN SKRIPSI MAHASISWA FAKULTAS HUKUM
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA

Berdasarkan Berita Acara Ujian Skripsi yang dilaksanakan pada hari Rabu tanggal 08 Mei 2024. Panitia Ujian skripsi Fakultas Hukum Universitas Muhammadiyah Sumatera Utara, dengan ini menetapkan bahwa :

Nama	: Donna Rizky Ragillia	
Npm	: 1906200590	
Prodi/Bagian	: Hukum / Hukum Pidana	
Judul Skripsi	: **Kebijakan Pidana Pembajakan Akun Media Sosial Yang Menimbulkan Kerugian Materil Bagi Pemilk Akun di Indonesia**	
Penguji	: 1. Dr. Nursariani Simatupang, S.H., M.Hum	NIDN. 0111117402
	2. Harisman, S.H., M.H	NIDN. 0103047302
	3. Dr. Tengku Erwinsyahbana, S.H., M.Hum	NIDN. 0006076814

Lulus, dengan nilai **B-** Predikat **Cukup**

Oleh karenya dinyatakan berhak menggunakan gelar Sarjana Hukum (SH)

Ditetapkan di Medan
Tanggal, 15 Mei 2024

PANITIA UJIAN

Ketua	**Sekretaris**
Dr. FAISAL, S.H., M. Hum.	**Dr. ZAINUDDIN, S.H., M.H**
NIDN: 0122087502	**NIDN: 0118047901**

PENGESAHAN SKRIPSI

Judul Skripsi	: Kebijakan Pidana Pembajakan Akun Media Sosial Yang Menimbulkan Kerugian Materil Bagi Pemilik Akun di Indonesia
Nama	: Donna Rizky Ragillia
Npm	: 1906200590
Prodi/Bagian	: Hukum / Hukum Pidana

Skripsi tersebut diatas telah diujikan oleh Dosen Penguji Fakultas Hukum Universitas Muhammadiyah Sumatera Utara pada tanggal 08 Mei 2024

Dosen Penguji

Dr. Nursariani Simatupang, S.H., M.Hum	**Harisman, S.H., M.H**	**Dr. Tengku Erwinsyahbana, S.H., M.Hum**
NIDN.0111117402	**NIDN. 0103047302**	**NIDN. 0006076814**

Dishkan Oleh :
Dekan Fakultas Hukum UMSU

Dr. Faisal, S.H., M.Hum
NIDN. 0122087502

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM
UMSU Akreditasi Unggul Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 1913/SK/BAN-PT/Ak.KP/PT/XI/2022
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003
https://fahum.umsu.ac.id fahum@umsu.ac.id umsumedan umsumedan umsumedan umsumedan

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

BUKTI PENDAFTARAN UJIAN SKRIPSI

Panitia Ujian Skripsi Fakultas Hukum Universitas Muhammadiyah Sumatera Utara telah menerima Pendaftaran Ujian Skripsi :

NAMA	**: Donna Rizky Ragillia**
NPM	**: 1906200590**
PRODI/BAGIAN	**: HUKUM / HUKUM PIDANA**
JUDUL SKRIPSI	**: KEBIJAKAN HUKUM PIDANA PEMBAJAKAN AKUN MEDIA SOSIAL YANG MENIMBULKAN KERUGIAN MATERIL BAGI PEMILIK AKUN DI INDONESIA**
PEMBIMBING	**: Dr.TENGKU ERWINSYAHBANA, S.H.,M.HUM NIDN. 0006076814**

Selanjutnya layak untuk diujikan.

Medan, 8 Mei 2024

PANITIA UJIAN

Ketua	**Sekretaris**
Dr. Faisal, S.H., M.Hum	**Dr. Zainuddin, S.H., M.H**
NIDN : 0122087502	**NIDN : 0118047901**

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM
UMSU Terakreditasi A Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 89/SK/BAN-PT/Akred/PT/III/2019
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003
http://fahum.umsu.ac.id fahum@umsu.ac.id umsumedan umsumedan umsumedan umsumedan

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan dibawah ini :

Nama	: DONNA RIZKY RAGILLIA
NPM	: 1906200590
Program	: Strata -1 (S-1)
Fakultas	: Hukum
Program Studi	: Ilmu Hukum
Bagian	: Hukum Pidana
Judul Skripsi	: Kebijakan Pidana Pembajakan Akun Media Sosial yang Menimbulkan Kerugian Materil Bagi Pemilik Akun Di Indonesia

Dengan ini menyatakan dengan sesungguhnya bahwa skripsi yang saya tulis ini secara keseluruhan adalah hasil peneltian / karya saya sendiri. Kecuali bagian-bagian yang dirujuk sumbernya.

Dan apabila ternyata dikemudian 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, 28 Maret 2024
Saya yang menyatakan

Donna Rizky Ragillia

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM
Akreditasi Unggul Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 1913/SK/BAN-PT/Ak.KP/PT/XI/2022
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003
https://umsu.ac.id rektor@umsu.ac.id umsumedan umsumedan umsumedan umsumedan

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

KARTU BIMBINGAN SKRIPSI MAHASISWA

NAMA : **DONNA RIZKY RAGILLIA**
NPM : **1906200590**
PRODI/BAGIAN : **HUKUM/ HUKUM PIDANA**
JUDUL SKRIPSI : **KEBIJAKAN PIDANA PEMBAJAKAN AKUN MEDIA SOSIAL YANG MENIMBULKAN KERUGIAN MATERIL BAGI PEMILIK AKUN DI INDONESIA**
PEMBIMBING : **Dr. Tengku Erwinsyahbana, S.H., M.Hum**

TANGGAL	MATERI BIMBINGAN	TANDA TANGAN
29-12-2024	PERBAIKAN UKURAN LOGO	
03-01-2024	PERBAIKAN BAB I	
22-01-2024	PERBAIKAN BAB II	
23-01-2024	PERBAIKAN AYAT SUCI AL QURAN	
26-01-2024	PERBAIKAN PENULISAN ISI BAB II	
13-02-2024	REVISI BAB III	
18-02-2024	PERBAIKAN DAFTAR PUSTAKA	
20-02-2024	REVISI BAB III	
23-02-2024	SKRIPSI di acc	

Diketahui,
DEKAN FAKULTAS HUKUM

(Dr. FAISAL, S.H., M.Hum)

DOSEN PEMBIMBING

(Dr. Tengku Erwinsyahbana, S.H., M.Hum)

ABSTRAK

KEBIJAKAN PIDANA PEMBAJAKAN AKUN MEDIA SOSIAL YANG MENIMBULKAN KERUGIAN MATERIL BAGI PEMILIK AKUN DI INDONESIA

DONNA RIZKY RAGILLIA

Globalisasi teknologi informasi yang telah mengubah dunia ke era cyber dengan sarana internet yang menghadirkan cyberspace dengan realitas virtualnya menawarkan kepada manusia berbagai harapan dan kemudahan menggunakan Media Sosial. Akan tetapi di balik itu, timbul persoalan berupa kejahatan yang dinamakan cyber crime, kejahatan ini tidak mengenal batas wilayah (borderless) serta waktu kejadian karena korban dan pelaku sering berada di negara yang berbeda. Pembajakan akun media sosial dapat dilakukan melalui sistem jaringan komputernya itu sendiri yang menjadi sasaran dan komputer itu sendiri yang menjadi sarana untuk melakukan kejahatan. Perkembangan teknologi informasi yang demikian pesatnya haruslah diantisipasi dengan hukum yang mengaturnya. Dampak negatif tersebut harus diantisipasi dan ditanggulangi dengan hukum yang terkait dengan pemanfaatan teknologi informasi dan komunikasi.

Berdasarkan latar belakang permasalahan tersebut untuk melakukan penelitian terhadap Kebijakan Hukum Pidana Pembajakan Akun Media Sosial di Indonesia. Tujuan Penelitian ini untuk mengetahui kebijakan hukum pidana melalui pendekatan KUHP untuk menanggulangi tindak pidana Pembajakan akun media sosial di Indonesia dan mengetahui kebijakan hukum pidana melalui UU ITE untuk menanggulangi pembajakan akun media sosial di Indonesia serta mengetahui penegakan hukum cyber crime di Indonesia. Penelitian ini bersifat yuridis normatif sebagai pendekatan utama, mengingat pembahasan didasarkan pada peraturan perundangundangan dan prinsip hukum yang berlaku dalam masalah kejahatan cyber crime. Pendekatan yuridis dimasudkan untuk melakukan pengkajian terhadap bidang hukum, khususnya hukum pidana.

Upaya penegakan hukum tidak hanya terbatas terhadap peningkatan kemampuan, sarana dan prasarana aparat penegak hukum tetapi juga diiringi kesadaran hukum masyarakat yang didukung dengan kerjasama dengan penyedia layanan internet.

Kata Kunci : Kebijakan Hukum Pidana , Pembajakan, Media Sosial.

BAB I

PENDAHULUAN

A. Latar Belakang

Seseorang dengan sengaja hack akun Facebook orang lain. Bahkan pelaku juga *ngehack* akun *Facebook* teman dekat dari pemilik akun dan melakukan tindakan penipuan dengan berpura-pura menjadi pemilik akun. Bagaimana hukum dari orang yang membajak media sosial milik orang lain[1]

Identitas seseorang ialah jati dirinya baik yang ia peroleh secara natur berdasarkan karakteristik yang ada padanya yang secara umum tidak dimiliki oleh orang lain (seperti tanda lahir dan ciri tubuh), secara pemberian (seperti nama dan agama), maupun yang ia peroleh melalui proses (pekerjaan dan pendidikan).

Adapun identitas berupa nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan, termasuk nomor telepon merupakan bagian data pribadi yang bersifat umum yang dilindungi dalam UU Perlindungan Data Pribadi.

Perbuatan meretas (*hack*) akun Media Sosial orang lain dengan cara apapun untuk mengakses akun Media Sosial, misalnya dengan mencari tahu password orang lain atau menerobos sistem keamanan tanpa hak merupakan tindak pidana dan dapat diancam pidana berdasarkan Pasal 30 UU ITE, yaitu dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik orang lain.

[1] https://www.hukumonline.com/klinik/a/jerat-hukum-bagi-hacker-akun-medsos-yang-lakukan-penipuan-lt525aa19bc487b/ diakses 22 Juli 2023

Adapun ancaman pidana perbuatan tersebut di atas adalah sebagai berikut.

1. Dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun dipidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp. 600 juta.
2. Dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik dipidana penjara paling lama 7 tahun dan/atau denda paling banyak Rp. 700 juta.
3. Dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan dipidana penjara paling lama 8 tahun dan/atau denda paling banyak Rp. 800 juta.

Peretas atau menbajak akun orang lain dapat dijerat menggunakan Pasal 30 ayat (1), (2), atau (3) UU ITE sebagaimana disebutkan sebelumnya.

Orang yang melakukan penipuan dapat pula dijerat menggunakan Pasal 378 KUHP yaitu barangsiapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum dengan menggunakan nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi utang maupun menghapuskan piutang, diancam pidana penjara paling lama 4 tahun.

Tidak hanya Pasal 378 KUHP, hacker yang menggunakan data pribadi yaitu identitas orang lain untuk melakukan penipuan melalui akun yang *dihack*nya dapat

dijerat pasal pelanggaran data pribadi yang tercantum dalam ketentuan Pasal 65 ayat (1) dan (3) jo. Pasal 67 ayat (1) dan (3) UU PDP yang berbunyi sebagai berikut.

Setiap orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian subjek data pribadi dipidana penjara paling lama 5 tahun dan/atau pidana denda paling banyak Rp. 5 miliar.

Setiap orang yang dengan sengaja dan melawan hukum menggunakan data pribadi yang bukan miliknya dipidana penjara paling lama 5 tahun dan/atau pidana denda paling banyak Rp5 miliar.

Perkembangan teknologi dan ilmu pengetahuan sejatinya telah tertuang dalam Kitab Suci Al-Quran Q.S. Al Naml : 40 tepatnya pada surat:

قَالَ ٱلَّذِى عِندَهُۥ عِلْمٌ مِّنَ ٱلْكِتَٰبِ أَنَا۠ ءَاتِيكَ بِهِۦ قَبْلَ أَن يَرْتَدَّ إِلَيْكَ طَرْفُكَ ۚ
فَلَمَّا رَءَاهُ مُسْتَقِرًّا عِندَهُۥ قَالَ هَٰذَا مِن فَضْلِ رَبِّى لِيَبْلُوَنِىٓ ءَأَشْكُرُ أَمْ
أَكْفُرُ ۖ وَمَن شَكَرَ فَإِنَّمَا يَشْكُرُ لِنَفْسِهِۦ ۖ وَمَن كَفَرَ فَإِنَّ رَبِّى غَنِىٌّ كَرِيمٌ ﴿٤٠﴾

Artinya : "Aku akan membawa singgasana itu kepadamu sebelummatamu berkedip". Maka tatkala Sulaiman melihat singgasana itu terletak di hadapannya, iapun berkata: "Ini Termasuk kurnia Tuhanku untuk mencoba aku Apakah aku bersyukur atau mengingkari (akan nikmat-Nya). dan Barangsiapa yang bersyukur Maka Sesungguhnya Dia bersyukur untuk (kebaikan) dirinya sendiri dan Barangsiapa yang ingkar, MakaSesungguhnya Tuhanku Maha Kaya lagi Maha Mulia".[2]

[2] Departemen Agama RI. (2019). Al Quran dan Terjemahanya. Bandung: Syamil Cipta Media

Teknologi terus dikembangkan dalam rangka mempermudah manusia melakukan aktifitasnya sehari-hari. Salah satu produk teknologi informasi dan komunikasi yang kecanggihannya berkembang pesat dan menguasai hampir seluruh aspek kehidupan manusia adalah Internet.[3]

Teknologi informasi dan komunikasi terbagi menjadi beberapa macam, salah satu nya yaitu internet. Internet merupakan singkatan dari Interconnected Networking yang apabila di artikan dalam Bahasa Indonesia yaitu serangkaian komputer yang terhubung dalam beberapa jaringan. Internet merupakan salah satu sarana informasi telekomunikasi yang dapat digunakan oleh hampir seluruh masyarakat di dunia, hal tersebut dikarenakan internet menjadi salah satu sarana media yang sangat mudah di gunakan untuk membantu setiap pekerjaan yang akan di lakukan. Internet sebagai salah satu teknologi telekomunikasi memiliki sebuah layanan yang memungkinkan penggunanya melakukan percakapan jarak jauh, mengunggah foto dan video, bertukar informasi, hingga sebagai ajang promosi produk yang telah diciptakan oleh seseorang, hal ini dapat kita sebut sebagai Media Sosial (Medsos). Teknologi internet merupakan teknologi yang tidak asing lagi di dengar dikalangan masyarakat modern, hal tersebut di karenakan manfatnya yang sangat besar bagi kehidupan zaman sekarang. Tujuan dibentuknya internet berawal dari keperluan militer Amerika Serikat dalam menghadapi serangan nuklir pada tahun 1969, hingga pada saat sekarang kegunaan dibentuknya internet mulai terasa untuk membantu keperluan kehidupan sehari-hari. Berbagai penemuan di bidang

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

teknologi informasi dan komunikasi saat ini memungkinkan orang menggunakan internet melalui computer pribadi (Personal Computer/ PC) atau media elektronik lainnya dimanapun. Kemajuan-kemajuan yang dicapai menusia tersebut telah banyak memberikan kemudahan-kemudahan dan manfaat bagi manusia dalam upayanya untuk memungkinkan kesejahteraan umat manusia. Teknologi informasi dan komunikasi saat ini di manfaatkan oleh pribadi (Individu), korporasi, pemerintah dan kelompok-kelompok masyarakat untuk berbagai aktivitas manusia, seperti pendidikan, kesehatan, bisnis, pemerintahan, komunikasi, hiburan dan lain-lain.[4] Penemuan-penemuan yang telah di ciptakan oleh manusia menempuh waktu yang cukup lama untuk menciptakan penemuan yang berguna dan bisa di manfaatkan oleh semua orang, sehingga penemuan tersebut menjadi salah satu alternative untuk membantu setiap pekerjaan yang sulit. Teknologi informasi dan komunikasi telah mengubah prilaku masyarakat dan peradaban manusia secara global.

Pembangunan teknologi informasi telah menyebabkan dunia menjadi tanpa batas (borderless) dan menyebabkan perubahan social yang secara signifikan berlangsung demikian cepat. Teknologi informasi saat ini menjadi pedang bermata dua, karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum.[5] Saat ini teknologi internet banyak digemari oleh semua kalangan. Bukan hanya orang dewasa bahkan anak-anak sudah mulai menggunakan internet

[4] Sigid Susesno, *Yurisdiksi Tindak Pidana Siber*, Reflika Aditama, Bandung, cet.ke-1 2012,hlm.1.

[5] Ahmad M.Ramli, *Cyber Law dan HAKI*, Reflika Aditama, Bandung ,2010, hlm 1.

untuk beberapa kegiatan sehari-harinya, mulai dari mengerjakan tugas sekolah hingga bermain. Untuk dunia usaha pun internet menjadi suatu hal yang sangat dibutuhkan saat ini. Komunikasi antar karyawan dalam perusahaan dan berbagai kegiatan perusahaan sudah banyak yang menggunakan teknologi internet. Faktor pembawa perubahan terbesar dalam bidang teknologi dan informasi di seluruh dunia maupun Indonesia adalah internet. Internet memiliki karakteristik yang berbeda dengan media lainnya karena internet bersifat global dan tidak mengenal batas Negara. Ilmu pengetahuan telah memberikan banyak melahirkan karya-karya yang sangat bermanfaat bagi setiap orang, dari karyakarya tersebut terdapat banyak manfaat kemudahan dalam membantu setiap kegiatan yang akan dilakukan didalam kehidupan suatu Negara. Kemudahan yang dihasilkan dari karya ilmu pengetahuan berasal dari banyak cabangcabang karya intelektual yang diciptakan oleh manusia salah satunya teknologi internet yang telah hadir didalam kehidupan manusia.

Perkembangan internet sebagai media informasi tanpa batas telah menyentuh berbegai aspek kehidupan masyarakat. Dengan berkembangnya media internet dan semakin terbukanya pola pikir masyarakat mengenai hak untuk berbicara atau berpendapat mengakibatkan fenomena baru di masyarakat. Media internet yang dapat diakses dimana saja, oleh siapa saja dan kapan saja menjadi suatu wadah baru bagi masyarakat untuk berbicara atau mengeluarkan pendapat. Perkembangan teknologi internet yang begitu pesat ini, kini banyak melahirkan berbagai jenis media sosial. Hal ini didukung pula dengan perkembangan teknologi telefon seluler yang menyediakan fasilitas bagi pengguna media sosial. Media sosial ini menjadi sangat popular karena memberikan kemudahan-kemudahan

dalam melakukan komunikasi. Media social yang paling popular digunakan baik anak-anak maupun dewasa antara lain, *Facebook*, *Twitter*, *Instagram*, *Whatsapp*, *Youtube*, dan Masih banyak lagi.[6] Hingga saat ini telah ditemukan banyak penemuan dalam bidang teknologi yang membawa keuntungan serta kemudahan. Berbanding lurus dengan itu banyak pula lahir masalah dan kasus seiring dengan perkembangan teknologi tersebut. Munculnya teknologi internet dan fitur-fitur yang ada didalamnya, tentunya menimbulkan tantangan baru bagi rezim hukum hak kekayaan intelektual. Saat ini beberapa persoalan yang muncul adalah menyangkut perlindungan terhadap objek media sosial melalui saran internet dan media komunikasi lainnya. Kejahatan yang berbasis teknologi sering kali sulit dipecahkan hal tersebut di karenakan jangkaunnya yang sangat luas dan terkadang pelaku kejahatan tersebut berada diluar Negara Indonesia.[7]

Media sosial yang sejatinya berfungsi sebagai penghubung persaudaraan antar manusia pada kenyataanya berbelok menjadi pemantik konflik, banyak masalah yang timbul akibat penyalahgunaan media sosial, masalah-masalah ini bahkan sudah mengarah kepada perkara kriminal seperti penipuan, stalking, penculikan dan juga kasus pencemaran nama baik. Media sosial adalah sebuah media online, yang mendukung interaksi sosial di mana para pengguna dapat dengan mudah beradaptasi, berbagi, dan menciptakan isi. Media sosial sangat

---

[6] Ladya Diana Warpindiastuti dan Meiva eka sri sulistyawati, *Pemanfaatan Teknologi Internet Menggunakan Media Sosial Sebagai Sarana Penyebaran Informasi dan Promosi pada MIN* 18 Jakarta, Vol. II No.1 Maret 2018, hlm 91.

[7] Ahmad Ramli, *Cyber Law dan HAKI Dalam Sistem Hukum Indonesia*, Bandung, Refika Aditama, 2004, hlm. 5.

beragam, sehingga masyarakatdapat mengakses dengan mudah dan memanfaatkannya untuk interaksi sosial.[8]

Berdasarkan permasalahan di atas dan banyaknya kasus penyalahgunaan atau Pembajakan yang terjadi terhadap data pribadi milik seseorang, penulis tertarik untuk membuat penelitian dan menulis skripsi dengan judul "Kebijakan Pidana Pembajakan Akun Media Sosial Yang Menimbulkan Kerugian Materil Bagi Pemilik Akun Menurut Hukum di Indonesia".

1. Rumusan Masalah

Berdasarkan uraian diatas, dapat ditarik permasalahan yang akan menjadi batasan pembahasan dari penelitian ini. Adapun permasalahan yang dirumuskan pada penelitian ini adalah:

a. Bagaimana kebijakan hukum pidana terhadap tindak pidana yang ditimbulkan akibat pembajakan akun media sosial di Indonesia?
b. Bagaimana penegakan hukum dalam kejahatan pembajakan akun media sosial di Indonesia?
c. Bagaimana faktor-faktor yang mempengaruhi dalam penanggulangan pembajakan akun media sosial di Indonesia ?

2. Faedah Penelitian

a. Secara teoritis, penelitian ini diharapkan dapat bermanfaat bagi akademis maupun masyarakat dan dapat memberikan suatu pemikiran baru guna

[8] Budi Suhariyanto, Tindak Pidana Teknologi Informasi (CYBERCRIME) Jakarta: PT Raja Grafindo Persada, 2014 .hlm. 2

perkembangan ilmu pengetahuan mengenai nafkah madliyah dalamperceraian Aparatur Sipil Negara.

b. Secara praktis, penulisan skripsi ini diharapkan dapat menjadi masukan bagi pihak-pihak yang terkait termasuk bagi kepentingan negara, bangsa, masyarakat, dan praktisi hukum dalam penetapan dan penerapan mengenai pembajakan Akun Media Sosial

B. Tujuan Penelitian

a. Untuk mengetahui Kebijakan Hukum Pidana Dalam Menangani Tindak Pidana yang ditimbulkan akibat pembajakan akun media sosial
b. Untuk mengetahui langkah penegakan hukum yang tepat dalam Kejahatan pembajakan akun media sosial ?
c. Untuk mengetahui faktor faktor yang mempengaruhi dalam penanggulangan tindak pidana pembajakan akun media sosial di Indonesia?

C. Defenisi Operasional.

Definisi Operasional atau kerangka konsep adalah kerangka yang berhubungan dengan antara definisi-definisi atau konsep khusus yang akan diteliti.[9] Sesuai judul penelitian yang akan diajukan yaitu: **"Kebijakan Pidana Pembajakan Akun Media Sosial Yang Menimbulkan Kerugian Materil Bagi Pemilik Akun Menurut Hukum di Indonesia.** yang selanjutnya penulis menguraikan definisi operasional penelitian sebagai berikut:

[9] Fakultas Hukum Universitas Muhammadiyah Sumatera Utara, 2018, *Pedoman Penulisan Tugas Akhir Mahasiswa*, Medan: CV. Pustaka Prima, halaman. 17

1. Kebijakan hukum pidana pada dasarnya ialah keseluruhan dari peraturan yang menetukan perbuatan apa yang dilarang dan termasuk kedalam tindak pidana, serta bagaimana sanksi yang dijatuhkan terhahadap pelakunya dengan tujuan untuk penanggulangan kejahatan. Secara teori, banyak doktrin yang dikemukan oleh para ahli terkait dengan pengertian kebijakan hukum pidana
2. Kebijakan penanggulangan Pembajakan Akun Media Sosial, merupakan bagian dari criminal policy. Dilihat dari sudut criminal policy, upaya penanggulangan kejahatan (termasuk penanggulangan cyber crime) tidak dapat dilakukan sematamata secara parsial dengan hukum pidana (sarana penal), tetapi harus pula ditempuh dengan pendekatan integral. Operasionalisasi kebijakan penal meliputi kriminalisasi, dekriminalisasi, penalisasi dan depenalisasi. Penegakan hukum pidana tersebut sangat tergantung pada perkembangan politik hukum, politik kriminal, dan politik sosial. Oleh karena itu, penegakan hukum tidak hanya memperhatikan hukum yang otonom, melainkan memperhatikan juga masalah kemasyarakatan dan ilmu perilaku sosial. Sebagai salah satu bentuk high tech crime yang dapat melampaui batas-batas negara (bersifat transnational/transborder), merupakan hal yang wajar jika upaya penanggulangan cyber crime juga harus ditempuh dengan pendekatan teknologi (techno prevention). Di samping itu, diperlukan pula pendekatan budaya/kultural, pendekatan moral/edukatif, dan bahkan pendekatan global melalui kerjasama internasional.

3. Media sosial merupakan sebuah media online, di mana para penggunanya bisa berpartisipasi, berbagi, menciptakan isi seperti blog, jejaring sosial, wiki, forum, hingga dunia virtual dengan mudah.

D. Keaslian Penelitian

Berdasarkan permasalahan dan cara yang terdapat dalam penelitian ini. Penulisan ini merupakan hasil karya asli penulis dan bukan merupakan bahan duplikasi ataupun plagiat dari hasil karya penulis lain. Walaupun ada beberapa penelitian lain yang hampir sejenis dengan penelitian yang peneliti lakukan, yaitu:

1. Ratu Indra Kasih Pratiwi, Fakultas Hukum Universitas Hasanuddin tahun 2020, skripsi dengan judul penelitian "Tinjauan Kriminologis Terhadap Tindak Pidana Penipuan *Online* Berbasis kejahatan Penyalahgunaan Kartu Kredit (*Carding*) Di Kota Makassar". Pada penelitian yang dilakukan Ratu Indra Kasih Pratiwi mempunyai dua rumusan masalah yaitu:
   a. Apakah penyebab terjadinya tindak pidana penipuan *online* berbasis kejahatan penyalahgunaan kartu kredit (*carding*) di kota Makassar?
   b. Bagaimanakah upaya penanggulangan oleh aparat penegak hukum terhadap tindak pidana penipuan *online* berbasis kejahatan penyalahgunaan kartu kredit (*carding*) di kota Makassar?
2. Asa Intan Primanta, Fakultas Hukum Universitas Airlangga tahun 2019, skripi dengan judul penelitian "Penyalahgunaan Data Pribadi Yang Berindikasi Tindak Pidana". Dalam penelitian yang dilakukan oleh Asa Intan Primanta terdapat dua rumusan masalahnya yaitu:

a. Apakah penggunaan data pribadi tanpa izin dapat dikualifikasikan sebagai tindak pidana?
b. Bagaimana pertanggungjawaban pidana bagi pelaku penggunaan data pribadi tanpa izin?

3. Dalle Ambotang, NPM B11110190, Mahasiswa Fakultas Hukum Universitas Hasanudin Makasar 2016, dengan judul "Skripsi analisis yuridis Tindak Pidana pornografi Dalam Media Elektronik (Studi Kasus Putusan No. 01/Pid.B/2015/Pn.Mks)" Adapun rumusan masalah penelitian tersebut adalah sebagai berikut:
   a. Bagaimanakah penerapan hukum pidana materiltindak pidana pornografi dalamputusan No. 01/Pid.B/2015/PN.Mks?
   b. Bagaimanakah pertimbangan hukum hakim tentang alasan-alasan pemberat dan peringanan pidana dalam putusan No. 01/Pid.B/2015/PN.Mks?

E. Metode Penelitian

Metode penelitian adalah salah satu faktor dari masalah yang diangkat, dimana metode penelitian adalah cara melakukan penelitian pendekatan kualitatif yang sesuai dengan rumusan masalah dan tujuan penelitian.

Metodologi merupakan suatu unsur yang mutlak yang harus ada di dalam penelitian dan pengembangan ilmu pengetahuan. Istilah "metodelogi" berasal dari kata "metode" yang berarti "jalan ke". Terhadap pengertian metodelogi, biasanya diberikan arti - arti sebagai logika dari penelitian ilmiah, studi terhadap prosedur

dan teknik penelitian.[10] Maka metode penelitian ini yang dipergunakan dalam penelitian ini terdiri dari :

1. Jenis dan Pendekatan Penelitian

Jenis Penelitian ini yuridis normatif yang merupakan penelitian yang memiliki objek hukum, baik hukum dalam suatu ilmu atau norma-norma yang sifatnya dogmatif atau hukum yang bersangkutan dengan tingkahlaku dan kehidupan masyarakat. Menurut Soerjono Soekanto, sifat normatif adalah kegiatan ilmiah, yang berdasar pada metode sistematika dan pemikiran tertentu yang ditujukan untuk mempelajari satu atau beberapa gejala hukum tertentu dengan cara menganalisisnya[11]

Pendekatan Penelitian yang dilakukan adalah pendekatan perundang-undangan dan pendekatan Kasus.

1. Pendekatan Perundang-undangan (Statute Approach) Pendekatan perundang-undangan adalah pendekatan yang dilakukan dengan menelaah semua peraturan perundang-undangan dan regulasi yang bersangkut paut dengan isu hukum yang ditangani

Dalam metode pendekatan perundang-undangan peneliti perlu memahami hirarkhi, dan asas-asas dalam peraturan perundang-undangan. Telah didefinisikan dalam Pasal 1 angka 2 Undang-undang RI Nomor 10 tahun 2004, peraturan perundang-undangan adalah peraturan yang tertulis yang dibentuk oleh lembaga negara atau pejabat yang berwenang dan mengikat secara umum. Dari pengertian

[10] Soerjono Soekanto.2014. *Pengantar Penelitian Hukum*.Jakarta: UI-press, halaman. 5.
[11] Soerjono Soekanto, 2004, *Penelitian Hukum Normatif*, Rajawali Pers, Jakarta, hlm.1.

tersebut, secara singkat dapat dikatakan bahwa yang dimaksud dengan statute berupa legislasi dan regulasi. Dengan demikian pendekatan perundang-undangan adalah pendekatan yang menggunakan legislasi dan regulasi.

2. Sifat Penelitian

Sifat penelitian yang digunakan dalam menyelesaikan penelitian ini adalah deskriptif yaitu penelitian yang hanya semata-mata melukiskan keadaan objek atau peristiwanya tanpa suatu maksud untuk mengambil kesimpulan-kesimpulan yang berlaku umum dengan menggunakan pendekatan yuridis normatif, dimana cara dalam penggunaan metode ini yaitu dengan melakukan studi pustaka yang menggambarkan secara sistematis data mengenai masalah yang akan dibahas. Data yang terkumpul kemudian dianalisis secara sistematis sehingga dapat ditarik kesimpulan dari seluruh hasil penelitian.[12]

3. Sumber Data

Sumber data yang digunakan dalam pengumpulan data dalam penelitian ini adalah data sekunder yang terdiri dari:

a. Data yang bersumber dari hukum Islam yaitu Al-Qur'an dan Hadist (Sunah Rasul). Data yang bersumber dari hukum Islam tersebut lazim disebut pula sebagai data kewahyuan.
b. Data sekunder yaitu data hukum sekunder merupakan bahan hukum yang menjelaskan bahan hukum primer seperti referensi buku, jurnal, artikel, literatur pada media cetak atau media elektronik yang berkaitan dengan

[12] Soerjono Sockanto dan Sri Mademuji. 2018. Penelitian Hukum Normatif, Jakarta: PT. Raja Grafindo Persada, halaman 20.

permasalahan yang dibahas. Data sekunder terbagi lagi menjadi tiga bahan hukum, meliputi :

1) Bahan hukum primer Bahan hukum primer yaitu bahan-bahan hukum yang mengikat. 3 maka dalam penelitian ini bahan hukum primer terdiri dari Undang-Undang Dasar Republik Indonesia 1945, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016.
2) Bahan hukum sekunder Sebagai bahan hukum sekunder yang terutama adalah buku-buku hukum, termasuk skripsi dan jurnal-jurnal hukum. Peneliti berusaha menggunakan buku-buku dan jurnal yang memang menjadi fokus dalam topik permasalahan yang diangkat pada penelitian tersebut nantinya.
3) Bahan hukum tersier Pada penelitian ini juga digunakan dan didapatkan data-data yang bersumber dari situs internet, khususnya dalam penyertaan beberapa kasus atas topik permasalahan pada penelitian tersebut nantinya

4. Alat Pengumpul

Penelitian ini setidaknya menggunakan tiga jenis alat pengumpulan data, yakni studi dokumentasi dalam penelitian ini dilakukan pada perustakaan Universitas Muhammadiyah Sumatera Utara (Library Research) terhadap dokumen-dokumen yang memiliki kaitan dan relevansi, Pengamatan atau Observasi melalui penelusuran pada situs-situs internet yang terkait..[13]

[13] Fakultas Hukum Muhammadiyah Sumatera Utara, *Op.Cit.*, halaman 21.

5. Analisa Data

Analisis data memiliki sifat seperti deksriptif, evaluatif, dan preskriptif.[14] Penelitian ini menggunakan analisis data secara kualitatif dengan menguraikan dan menjelaskan permasalahan yang berkaitan dengan kasus yang diteliti. Dengan mengolah dan menganalisis data yang diperoleh berdasarkan rumusan masalah yang telah diterapkan sehingga diharapkan dapat memperoleh gambaran yang jelas.

[14] Mukti Fajar dan Yulianto Achmad, *Op.cit*., halaman.183-184

BAB II

TINJAUAN PUSTAKA

A. Kebijakan Hukum Pidana

Istilah kebijakan berasal dari bahasa Inggris policy atau dalam bahasa Belanda politie. Secara umum kebijakan dapat diartikan sebagai prinsip-prinsip umum yang berfungsi untuk mengarahkan pemerintah dalam mengelola, mengatur atau menyelesaikan urusan-urusan publik, masalah-masalah masyarakat atau bidang-bidang penyusunan peraturan perundang-undangan dan pengaplikasian hukum/peraturan, dengan suatu tujuan yang mengarah.

Upaya perlindungan masyarakat (social defence) dan upaya mencapai kesejahteraan masyarakat (social welfare) pada hakikatnya merupakan bagian integral dari kebijakan atau upaya penanggulangan kejahatan .[15]

Pengertian kebijakan atau politik hukum pidana dapat dilihat dari politik hukum maupun politik kriminal. Menurut Sudarto, "Politik Hukum" adalah :

1. Usaha untuk mewujudkan peraturan-peraturan yang baik sesuai dengan keadaan dan situasi pada suatu saat
2. Kebijakan dari negara melalui badan-badan yang berwenang untuk menetapkan peraturan-peraturan yang dikehendaki yang diperkirakan bisa digunakan untuk mengekspresikan apa yang terkandung dalam masyarakat dan untuk mencapai apa yang dicita-citakan. [16]

[15] Barda Nawawi Arief, Bunga Rampai . 2013 . Kebijakan Hukum Pidana, Bandung : Citra Aditya Bakti . halaman 32

[16] Sudarto. 2012 . Hukum dan Hukum Pidana, Jakarta : Rajawali pers . halaman 44-48.

Bertolak dari pengertian demikian Sudarto selanjutnya menyatakan, bahwa melaksanakan "politik hukum pidana" berarti mengadakan pemilihan untuk mencapai hasil perundang-undangan pidana yang paling baik dalam arti memenuhi syarat keadilan dan daya guna.

Dalam kesempatan lain beliau menyatakan, bahwa melaksanakan "politik hukum pidana" berarti, "usaha mewujudkan peraturan perundang-undangan pidana yang sesuai dengan keadaan dan situasi pada suatu waktu dan untuk masamasa yang akan datang. Dengan demikian, dilihat sebagai bagian dari politik hukum, maka politik hukum pidana mengandung arti, bagaimana mengusahakan atau membuat dan merumuskan suatu peraturan perundang-undangan pidana yang baik.

Pengertian demikian terlihat pula dalam definisi "*penal policy*" dari Marc Ancel yakni "suatu ilmu sekaligus seni yang bertujuan untuk memungkinkan peraturan hukum positif dirumuskan secara lebih baik". Melihat dari uraian di atas yang dimaksud dengan "peraturan hukum positif" (*the positive rules*) dalam definisi Marc Ancel itu jelas adalah peraturan perundangundangan dengan hukum pidana. Dengan demikian, istilah "*penal policy*" menurut Marc Ancel adalah sama dengan istilah "kebijakan atau politik hukum pidana" yang dikemukakan oleh Sudarto.

Melihat penjelasan di atas dapat ditegaskan, bahwa pembaharuan hukum pidana (*penal reform*) merupakan bagian dari kebijakan/politik hukum pidana (*penal policy*). Latar belakang diadakannya pembaharuan hukum pidana dapat ditinjau dari aspek sosiopolitik, sosiofilosofis, sosiokultural, atau dari berbagai aspek kebijakan khususnya kebijakan sosial, kebijakan kriminal, dan kebijakan penegakan hukum. Artinya, pembaharuan hukum pidana pada hakikatnya harus

merupakan perwujudan dari perubahan dan pembaruan terhadap berbagai aspek dan kebijakan yang melatarbelakangi pembaharuan tersebut.

Menurut Moeljatno, hukum pidana adalah bagian dari keseluruhan hukum yang berlaku disuatu negara yang mengadakan dasar-dasar dan aturan aturan untuk :

1. Menentukan perbuatan-perbuatan mana yang tidak boleh dilakukan, yang dilarang, dengan disertai ancaman atau sanksi yang berupa pidana tertentu bagi yang telah melanggar larangan tersebut;
2. Menentukan kapan dan dalam hal apa kepada mereka yang telah melanggar larangan-larangan itu dapat dikenakan atau dijatuhi sanksi pidana sebagaimana yang telah diancamkan.
3. Menentukan dengan cara bagaimana pengenaan pidana itu dapat dilaksanakan apabila ada orang yang disangka telah melanggar larangan tersebut.[17]

Menurut C. S. T. Kansil, hukum pidana adalah peraturan atau hukum yang mengatur tentang pelanggaran-pelanggaran dan kejahatan-kejahatan terhadap kepentingan umum, dan bagi pelanggarnya diancam dengan hukuman yang merupakan suatu penderitaan dan siksaan dengan tujuan untuk menimbulkan efek jera pada penerima sanksi tersebut. Mengenai penentuan suatu perbuatan pidana, hukum Indonesia menganut asas legalitas yakni suatu perbuatan tidak dapat dihukum selain atas kekuatan aturan pidana dalam undang-undang, yang diadakan

[17] Raharjo, Agus . 2002 . *Cyber Crime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi* .Bandung: PT Citra Aditya Bakti. halaman 132.

sebelum perbuatan itu terjadi (Pasal 1 ayat (1) KUHP). Hal ini dirumuskan oleh Anselm Von Feuderbach sebagai berikut:

"Nulla Poena Sinelege"

"Nulla Poena sine crimine"

"Nullum crimen sine poena legali "

Artinya:

"Tidak ada hukuman, kalau tidak ada undang-undang"

"Tidak ada hukuman, kalau tak ada kejahatan"

"Tidak ada kejahatan, kalau tidak ada hukuman yang berdasarkan undangundang".[18]

B. Pengertian Pembajakan Akun Cyber Crime

Istilah *cyber crime* saat ini merujuk pada suatu tindakan kejahatan yang berhubungan dengan dunia maya *(cyber space*) dan tindakan kejahatan yang menggunakan komputer. Ada ahli yang menyamakan antara tindak kejahatan *cyber* (*cyber crime*) dengan tindak kejahatan komputer, dan ada ahli yang membedakan diantara keduanya. Beberapa penggunaan kata untuk merujuk pada *cyber crime* yang umum digunakan dalam berbagai literatur adalah kejahatan dunia maya, kejahatan komputer, kejahatan mayantara, kejahatan dibidang teknologi informasi, dan masih banyak lagi[19]

[18] Abdulla Wahid. Dkk. 2005. *Kejahatan Mayantara (Cyber Crime)* .Bandung : Refika Aditamag . halaman 74

[19] Wahid, Abdul. 2014. *Kejahatan Mayantara (Cyber Crime).* PT Refika Aditama. Bandung. Halaman 3-4

Konsep hukum *cyber space*, *cyber law*, dan *cyber line* yang dapat menciptakan komunitas pengguna jaringan internet yang luas 60 juta, yang melibatkan 160 negara menimbulkan kegusaran para praktisi hukum untuk menciptakan pengamanan melalui regulasi, khususnya perlindungan terhadap milik pribadi.[20]

Didik M. Arief Mansur dan elisatris Gultom dalam bukunya "*cyber law* aspek hukum teknologi informasi" menyebutkan secara umum yang dimaksud dengan kejahatan komputer atau kejahatan di dunia maya adalah : "perubahan dan atau kerusakan pada fasilitas komputer yang dimasuki atau digunakan tersebut"[21]

Barda Nawawi Arief menunjuk pada kerangka (sistematik) Draf *Convention on Cyber Crime* dari dewan eropa (Draf No. 25, Desember 2000). Beliau menyamakan peristilahan antara keduanya dengan memberikan defenisi *cyber crime* sebagai "*crime related to technologi,computer, and the internet*" atau secara sederhana berarti kejahatan yang berhubungan dengan teknologi, komputer dan internet.[22]

Dalam beberapa literatur, *cyber crime* sering di identikkan sebagai *computer crime*. Andi Hamzah dalam bukunya "Aspek-aspek Pidana di Bidang Komputer" mengartikan *cyber crime* sebagai kejahatan di bidang computer. secara umum dapat diartikan sebagai penggunaan komputer secara ilegal. Menurut freddy haris, *cyber crime* merupakan suatu tindak pidana dengan karakteristik-karakteristik sebagai berikut:

---

[20] Suparni, Neniek . 2012 . *Cyber Space Problematika & Antisipasi Pengaturannya*. Sinar Grafika. Jakarta.halaman 48.

[21] Ibid. halaman 5

[22] Ibid. halaman 13

1. *Unauthorized access* (dengan maksud untuk memfasilitasi kejahatan),
2. *Unauthorized alteration or destruction of data*,
3. Menggangu/merusak operasi komputer,
4. Mencegah/menghambat akses pada komputer.[30]

Menurut Muladi, sampai saat ini belum ada definisi yang seragam tentang *cyber crime* baik nasional maupun global. Kebanyakan masih menggunakan *soft law* berbentuk *code of conduct* seperti Jepang dan Singapura.

Barda Nawawi Arief, *Cyber Crime menurut Convention on Cyber Crime* 2001 di Budapest Hongaria adalah sebagai berikut :

1. *Illegal access* yaitu sengaja memasuki atau mengakses sistem komputer tanpa hak.
2. *Illegal interception* yaitu sengaja dan tanpa hak mendengar atau menangkap secara diam-diam pengiriman dan pemancaran data komputer yang tidak bersifat publik dari atau di dalam sistem komputer dengan menggunakan alat bantu teknis.
3. *Data interference* yaitu sengaja dan tanpa hak melakukan perusakan, penghapusan, perubahan atau penghapusan data komputer.
4. *System interference* yaitu sengaja melakukan gangguan atau rintangan serius tanpa hak terhadap berfungsinya sistem komputer
5. *Misuse of Devices* yaitu penyalahgunaan perlengkapan komputer, termasuk program komputer, password komputer, kode masuk *(access code).*

6. *Computer related Forgery* yaitu pemalsuan dengan sengaja dan tanpa hak memasukkan, mengubah, menghapus data autentik menjadi tidak autentik dengan maksud digunakan sebagai data autentik.
7. *Computer related Fraud* yaitu penipuan dengan sengaja dan tanpa hak menyebabkan hilangnya barang/kekayaan orang lain dengan cara memasukkan, mengubah, menghapus data computer atau dengan mengganggu berfungsinya komputer/sistem komputer, dengan tujuan untuk memperoleh keuntungan ekonomi bagi dirinya sendiri atau orang lain.[23]

Di lihat dari beberapa definisi di atas, tampak bahwa belum ada kesepakatan mengenai definisi tentang *cyber crime* atau kejahatan dunia *cyber*. Menurut Muladi, sampai saat ini belum ada definisi yang seragam tentang *cyber crime* baik nasional maupun global. Kebanyakan masih menggunakan *soft law* berbentuk *code of conduct* seperti Jepang dan Singapura. Berdasarkan jenis aktifitas yang dilakukannya, *cyber crim*e dapat digolongkan menjadi beberapa jenis:

Hacking adalah kegiatan menerobos program komputer milik orang/pihak lain. *Hacker* adalah orang yang gemar eksplorasi komputer, memiliki keahlian membuat dan membaca program tertentu, dan terobsesi mengamati keamanan (*security*). "*Hacker*" memiliki 2 wajah ganda: "*WHITE HAT HACKER"* memberi tahu kepada admin yang komputernya diterobos, bahwa adanya lemahankelemahan pada program yang dimiliki dan punya potensi disusup. Karakteristik *White Hat Hacker* ini adalah memberikan informasi bukan merusak yang pasti

[23] Remy Syahdeini, Sutan. 2011. *Kejahatan & Tindak Pidana Komputer*. Jakarta : PT Pustaka Utama Grafiti. halaman 93.

menguntungkan/membantu korbannya. *"BLACK HAT HACKER*", menerobos program orang lain untuk merusak, manipulasi/merubah serta mencuri datanya. Karakteristik *Black Hat Hacker* ini adalah melakukan aktifitas kriminal yang pasti merugikan korbannya.

Cracking adalah *hacking* untuk tujuan jahat. Sebutan pelaku *cracking* adalah *"cracker"* Aktfitas *Cracker* sejenis dengan "*hacker* bertopi hitam" (*BLACK HAT HACKER*). Berbeda dengan "*carder*" yang hanya mengintip kartu kredit, *"cracker*" mengintip simpanan para nasabah di berbagai bank atau pusat data sensitif lainnya untuk keuntungan diri sendiri. Meski sama-sama menerobos keamanan komputer orang lain, "*hacker*" lebih fokus pada prosesnya. Sedangkan "*cracker"* lebih fokus untuk menikmati hasilnya.

Carding adalah Aktifitas berbelanja secara *online* tertapi menggunakan nomor dan identitas kartu kredit orang lain, yang diperoleh secara ilegal, pelaku *carding* biasa disebut *carder*. Sebanyak 20 persen transaksi melalui internet yang berasal dari Indonesia adalah hasil *carding*. Akibatnya, banyak situs belanja online yang memblokir *IP address* (alamat komputer internet) yang berasal dari Indonesia. Menurut *ICT Watch*, Lembaga Swadaya Masyarakat yang mengamati dunia internet di Indonesia, para *carder* sekarang beroperasi semakin jauh, *carder* juga melakukan penipuan melalui forum-forum di milis dan ruang chatting di *mIRC*.

Defacing adalah kegiatan mengubah halaman situs pihak lain, seperti yang terjadi pada situs Presiden SBY, Kemenkominfo dan Partai Golkar, BI dan situs KPU saat pemilu 2004 lalu. Banyaknya kasus *deface* saat ini yang bermotif iseng belaka mereka ingin unjuk kebolehan, pamer kemampuan membuat program, tapi

ada juga pelaku *deface* yang jahat, mereka melakukan aktifitas *deface* untuk mencuri data dan dijual kepada pihak lain.

Fishing atau Phising adalah kegiatan memancing pengguna internet dengan harapan agar *user* secara tidak sadar memberikan informasi data *user* dan *password* nya pada *website* yang sudah dilakukan *deface.*

Spamming adalah pengiriman berita atau iklan lewat surat elektronik *(email)* yang tak dikehendaki. *Spam* sering disebut juga sebagai *bulk email* atau *junk email* alias "sampah". Meski demikian, banyak juga orang yang terkena dan menjadi korbannya. [24]

C. Media Soaial

Secara sederhana, istilah media bisa dijelaskan sebagai alat komunikasi sebagaimana defenisi yang selama ini diketahui. Terkadang media ini cenderung lebih dekat terhadap sifatnya yang massa karena terlihat dari berbagai teori yang muncul dalam komunikasi massa. Kata sosial dalam media sosial secara teori semestinya didekati oleh ranah sosiologi.

Kata sosial secara sederhana merujuk pada relasi sosial. Relasi sosial itu sendiri bias dilihat dalam kategori aksi sosial dan relasi sosial. Dua pengertian dasar tentang medoa dan sosial telah dijelaskan, namun tidak mudah membuat sebuah defenisi tetang media sosial berdasarkan perangkat teknologi semata. Diperlukan pedekatan teori-teori sosial yang memperjelas apa yang membedakan antara media sosial dan media lainnya di internet sebelum pada kesimpulan apa yang dimaksud

[24] Garda T. Paripurna. 2008 . *Sekilas Tentang Kejahatan Transnasional* . Riset Hukum Kejahatan Transnasional

dengan media sosial. Media Sosial adalah medium di internet yang memungkinkan pengguna merepresentasikan dirinya maupun berinteraksi, bekerjasama, berbagi, berkomunikasi dengan pengguna lain, dan membentuk ikatan sosial secara virtual.[25]

Media sosial merupakan sebuah media online melalui aplikasi berbasis internet, dapat digunakan untuk berbagi, berpartisipasi dan menciptakan konten berupa blog, wiki, forum, jejaring sosial dan ruang 11 dunia virtual yang didukung oleh teknologi multimedia yang semakin canggih dan hebat.Media sosial memiliki kelebihan yaitu cepat dalam penyebaran informasi, sebaliknya kelemahannya yaitu mengurangi intensitas interaksi interpersonal secara langsung atau tatap muka, kecanduan yang berlebihan serta persoalan hukum karena kontennya yang melanggar moral, privasi serta peraturan. [26]

Klasifikasi Media Sosial Klasifikasi media sosial menurut R.sudiyatmoko dibagi menjadi 6 bagian: [27]

a. Proyek Kolaborasi (Collaroborative projects) Proyek kolaborasi merupakan bentuk demokrasi dari media sosial di mana banyak pengguna internet dapat berkolaborasi untuk menambahkan, mengubah, ataupun menghapus informasi dalam wiki, yaitu situs yang menyediakan layanan bagi pengguna atau pembaca untuk melakukan perubahan-perubahan tersebut. Contoh dari bentuk proyek kolaborasi adalah Wikipedia. Sebuah ensiklopedia online yang menyediakan beragam informasi dalam berbagai bahasa.

[25] Nasrullah, Rulli. (2015). Media Sosial Perspektif Komunikasi, Budaya dan Sosioteknologi. Bandung: Simbiosa Rekatama Media

[26] Sudiyatmoko, R. (2015). Panduan optimalisasi media sosial untuk kementrian perdagangan RI.

[27] Ibid

b. Blog (Blogs) Blog merupakan salah satu bentuk media sosial terlama yang memperbolehkan penggunanya menulis entri baru berdasarkan urutan waktu penulisan. Blog telah digunakan oleh banyak orang dan memiliki fungsi yang beragam untuk masyarakat. Dari sekedar media untuk menyalurkan pengalaman sehari-hari atau yang sering juga disebut sebagai diary sampai sebagai media berbagi informasi dan bahkan sebagai media jual beli.Contoh blog salah satunya adalah Wordpress.

c. Konten Komunitas (*Content Community*) Konten Komunitas adalah media sosial yang tujuan utamanya untuk menampung konten dari pengguna dan membaginya ke pengguna lainnya. Contoh dari media ini adalah YouTube untuk berbagi video, SlideShare untuk berbagi file presentasi, Flickr untuk berbagi file gambar, dan lain sebagainya.

d. Dunia Game Virtual (*Virtual Game Worlds)* Dunia Game Virtual tentu berkaitan dengan Game Online di mana pemain memiliki profil dan karakter sendiri di dunia game tersebut. Karakter mereka dapat berkomunikasi dengan karakter pemain lainnya dan melakukan aktivitas dalam game tersebut bersama-sama. Contoh dari dunia game virtual adalah game online seperti *World of Warcraft, Watch Dogs, dan Need For Speed*.

e. Dunia Sosial Virtual (*Virtual Social Worlds*) Dunia Sosial Virtual hampir sama dengan Dunia Game Virtual hanya saja dengan tujuan murni untuk membangun “kehidupan” lain di luar kehidupan nyata, dengan aspek yang sama seperti dunia nyata hanya saja pengguna dapat berperan sebagai orang lain. Contoh dari dunia sosial virtual adalah Second Life. f. Situs Jejaring

Sosial (*Social Networking Sites*) Situs jejaring sosial adalah tempat di mana setiap pengguna memiliki profil yang berisi informasi pribadi (seperti Tanggal lahir, Alamat, Jenis kelamin) dan dapat berkomunikasi dengan pengguna lainnya melalui profil tersebut.Antar pengguna juga dapat melakukan chatting atau mengirim pesan teks, gambar, suara, maupun video. Pada situs tertentu, pengguna juga dapat mengikuti kegiatan keseharian dari teman-teman profil mereka melalui status update yang memberikan opsi kepada pengguna untuk membagi pengalaman keseharian mereka kepada temantemannya. Contoh dari media sosial ini adalah Facebook, Friendster, dan *MySpace*.Dari keenam bagian ini Instagram termasuk dalam jenis situs jejaring sosial.

1. Karakteristik Media Sosial

Karakteristik Media Sosial Media sosial memiliki karakteristik khusus yang tidak dimiliki oleh beberapa media siber lainnya.Ada batasanbatasan dan ciri khusus tertentu yang hanya dimiliki oleh media sosial dibanding dengan media lainnya. Adapun karakteristik media sosial yaitu: [28]

a. Jaringan (*network*). Media sosial memiliki karakter jaringan sosial.Media sosial terbangun dari struktur sosial yang terbentuk di dalam jaringan atau internet. Jaringan yang terbentuk antar pengguna (*users*) merupakan jaringan yang secara teknologi dimediasi oleh perangkat teknologi, seperti komputer, telepon

[28] Nasrullah, Rulli. (2015). Media Sosial Perspektif Komunikasi, Budaya dan Sosioteknologi. Bandung: Simbiosa Rekatama Media

genggam atau tablet.Jaringan yang terbentuk antar pengguna ini pada akhirnya membentuk komunitas, contohnya seperti *Facebook, twitter* dan lain-lain.

b. Informasi (*information*) Di media sosial, informasi menjadi komoditas yang dikonsumsi oleh pengguna. Komoditas tersebut pada dasarnya merupakan komoditas yang diproduksi dan didistribusikan antar pengguna itu sendiri. Dari kegiatan konsumsi inilah pengguna dan pengguna lain membentuk sebuah jaringan yang pada akhirnya secara sadar atau tidak bermuara pada institusi masyarakat berjejaring.

c. Arsip (*archive*) Bagi pengguna media sosial, arsip menjadi sebuah karakter yang menjelaskan bahwa informasi telah tersimpan dan bisa diakses kapan pun dan melalui perangkat apa pun. Setiap informsi apa pun yang diunggah di Facebook informasi itu tidak hilang begitu saja saat pergantian hari, bulan bahkan sampai tahun.

d. Interaktif (*interactivity*) Karakter dasar dari media sosial adalah terbentuknya jaringan antar pengguna.Jaringan ini tidak sekedar memperluas hubungan pertemanan atau pengikut di internet semata, tetapi juga harus dibangun dengan interaksi antar pengguna tersebut.

e. Simulasi Sosial Interaksi di media sosial memang menggambarkan bahkan mirip dengan realitas, akan tetapi ada juga interaksi yang terjadi adalah simulasi dan terkadang berbeda sekali. Sebagai contoh, di media sosial indentitas menjadi cair dan bisa berubah-ubah. Perangkat di media sosial bisa memungkinkan siapa pun untuk menjadi siapa saja, bahkan bisa jadi pengguna

yang berbeda sekali dengan realitasnya, seperti pertukaran identitas jenis kelamin, hubungan perkawinan, sampai dengan foto profil.

f. Konten olahraga Term ini menunjukkan bahwa di media sosial konten sepenuhnya milik dan berdasarkan kontribusi pengguna atau pemilik akun. User generated content merupakan hubungan simbiosis dalam budaya media baru yang memberikan kesempatan dan keleluasaan pengguna untuk berpartisipasi.

2. Ciri-Ciri Media Sosial

Menurut Abbas menyebutkan ciri – ciri media sosial sebagai berikut: [29]

a. Konten yang disampaikan dibagikan kepada banyak orang dan tidakterbatas pada satu orang tertentu.
b. Isi pesan muncul tanpa melalui suatu gatekeeper dan tidak ada gerbang penghambat.
c. Isi disampaikan secara online dan langsung.
d. Konten dapat diterima secara online dalam waktu lebih cepat dan bisa jugatertunda penerimaannya tergantung pada waktu interaksi yang ditentukansendiri oleh pengguna.
e. Media sosial menjadikan penggunanya sebagai kreator dan aktor yangmemungkinkan dirinya untuk beraktualisasi diri.
f. Dalam konten medsos terdapat sejumlah aspek fungsional seperti identitas,percakapan (interaksi), berbagi (sharing), kehadiran (eksis), hubungan (relasi), reputasi (status) dan kelompok (group).

[29] Abbas, M. R. (2014). Panduan Optimalisasi Media Sosial untuk kementrian perdagangan RI. Jakarta. Kementrian Perdagangan RI.

3. Jenis-jenis Media Sosial

Aplikasi media sosial hingga saat ini memang sudah tak terhitung jumlahnya, namun tidak semuanya mendapatkan perhatian dari masyarakat. Menurut media sosial dapat dibagi menjadi 6 jenis :[30]

1) Proyek kolaborasi website, penggunaanya dapat mengubah, menambah ataupun membuang konten-konten yang termuat di website tersebut, seperti Wikipedia.
2) Blog dan microblog, pengguna dapat bebas mengungkapkan suatu hal di blog itu, seperti memberikan informasi tentang suatu hal, merivew sesuatu dan lainnya.
3) Konten atau isi, pengguna di website saling membagikan berbagai konten multimedia, seperti e-book, video, foto, dan lain-lain.
4) itus jerjaring sosial, pengguna terkoneksi dengan membuat informasi pribadi maupun sosial sehingga dapat diakses oleh orang lain. Beberapa situs jejaring sosial antara lain :
    a. *Facebook*, merupakan sebuah situs jejaring sosial dimana para user dapat bergabung dalam sebuah komunitas seperti kota, kerja, sekolah dan daerah untuk melakukan komunikasi atau interaksi dengan orang lain. Kita dapat memasukkan daftar teman-teman, mengirim pesan, memperbarui foto profil pribadi, mengirim foto, status, video bahkan grup khusus.

[30] Sudiyatmoko, Ani. (2014). Panduan Optimalisasi Media Sosial untuk Kementrian Perdagangan RI. Jakarta: Pusat Humas Kemendag RI

b. *Youtube*, merupakan situs berbagi konten video terpopuler didunia yang memungkinkan penggunanya untuk melakukan pencarian berbagai macam video dan menontonnya langsung. Setiap pengguna youtube juga dapat berpartisipasi menggungah video ke server dan membagikannya ke seluruh dunia.Youtube saat ini sangat digemari para remaja karena adanya „vlog', vlog sebenarnya adalah sebuah video dokumentasi jurnalistik yang berisi tentang hidup, aktivitas, dan opini. Namun, remaja banyak memanfaatkan vlog untuk menunjukkan betapa menariknya kehidupan mereka dengan mengunggah aktivitas keseharian mereka hingaa menunjukkan isi kamar dan rumah mereka.

c. *Twitter*, merupakan layanan media sosial dan mikroblog yang memungkinkan penggunanya untuk mengirim dan membaca pesan berbasis teks hingga 140 karakter, dikenal dengan sebuah kicauan (tweet). Dengan batas karakter yang disediakan, pengguna twitter akan memposting atau biasa disebut „ngetwit" dengan kalimat yang singkat dan padat. Umumnya pengguna twitter melakukan sharing informasi berita yan up to date di akunnya secara otomatis dapat dilihat oleh seluruh orang yang berteman dengannya. Namun tak jarang juga orang-orang menggunakan twitter sebagai diary online dan tempat bergumam hal yang tidak informative kepada orang lain. Batas-batas pada ruang sosial seakan kabur, semua orang bebas

menuangkan apa yang ia rasakan hingga menumpahkan kekesalan di media sosial twitter ini.

d. *Friedster*, sebelum diluncurkan sebagai situs game, Friendster merupakan layanan jejaring sosial yang dulunya popular di awal abad-21, situs ini memungkinkan pengguna terhubung dengan teman mereka. Situs ini dulunya digunakan untuk berkencan dan mencari tahu tentang acara baru, band, dan hobi. Pengguna dapat berbagi video, foto, pesan, dan komentar dengan anggota lain melalui profil dan jaringan mereka. Friendster juga dianggap sebagai salah satu jejaring sosial asli dan bahkan "kakek"-nya semua jejaring sosial.Layanan ini dulunya sangat popular di kawasan Asia Tenggara.

e. *Instagram*, adalah aplikasi media sosial dengan bentuk komunikasi baru diamana para penggunanya bisa mengunggah dan mengedit foto dimanapun dan kapanpun untuk diperlihatkan kepada orang lain. Kini instagram juga menambah fitur baru bernama "snapgram" dimana penggunanya dapat berbagi foto, boomerang dan video. Selain itu terdapat "instalive" dimana user dapat live video kegiatan yang sedang dilakukan.

f. *Path*, merupakan aplikasi media sosial yang dianggap sebagai lahan untuk ajang pamer saja daripada untuk bersosialisasi. Mulai dari update foto, update lokasi dimana pengguna sedang berada, update music yang sedang didengarkan, film yang sedang ditonton, buku

yang sedang dibaca, bahakan sampai tidur dan bangun tidur jam berapa dapat di update pada aplikasi path.

g. Snapchat, termasuk aplikasi media sosial baru yang disinyalir berhasil menarik perhatian para remaja dengan menyajikan cara berkomunikasi yang lebih menyenangkan. Pengguna snapchat bisa saling mengirim foto dan video pendek yang diimbuhi pesan kepada teman snapchatnnya yang kemudian secara otomatis akan hilang dalam beberapa detik. Fitur snapchat yang paling digemari penggunanya adalah snapchat story, dimana fitur ini memungkinkan pengguna untuk menyiarkan live video personal dirinya ke seluruh teman snapchatnya yang dapat dilihat dalam tempo 24 jam dan kemudian dihapus otomatis oleh aplikasi tersebut.

h. Virtual game World adalah platform yang mereplikasi lingkunga tiga dimensi dimana pengguna muncul dalam bentuk avatar yang dipersonalisasi dan berinteraksi sesuai dengan aturan mainnya. Mereka mendapatkan popularitas dengan dukungan perangkat seperti MicrosoftXbox dan Sony’s Play Station. Pengguna dapat berinteraksi dengan orang lain yang mengambilwujud avatar layaknya di dunia nyata melalui aplikasi 3D, contoh online game. Contohnya adalah World of Warcraft. 6.Virtual social Media memungkinkan user untuk berperilaku lebih leluasa dan hidup (dalam bentuk avatar) di dunia maya, mirip dengan kehidupan nyata mereka Seperti Second Life.

4. Manfaat Media Sosial

Media sosial merupakan bagian dari sistem relasi, koneksi dan komunikasi. Berikut ini sikap yang harus kita kembangkan terkait dengan peran, dan manfaat media sosial :

a. Sarana belajar, mendengarkan, dan menyampaikan. Berbagai aplikasi media sosial dapat dimanfaatkan untuk belajar melalui beragam informasi, data dan isu yang termuat di dalamnya. Pada aspek lain, media sosial juga menjadi sarana untuk menyampaikan berbagai informasi kepada pihak lain. Konten-konten di dalam media sosial berasal dari berbagai belahan dunia dengan beragam latar belakang budaya, sosial, ekonomi, keyakinan, tradisi dan tendensi.Oleh karena itu, benar jika dalam arti positif, media sosial adalah sebuah ensiklopedi global yang tumbuh dengan cepat.Dalam konteks ini, pengguna media sosial perlu sekali membekali diri dengan kekritisan, pisau analisa yang tajam, perenungan yang mendalam, kebijaksanaan dalam penggunaan dan emosi yang terkontrol.
b. Sarana dokumentasi, adminitrasi dan integrasi. Bermacam aplikasi media sosial pada dasarnya merupakan gudang dan dokumentasi beragam konten, dari yang berupa profil, informasi, reportase kejadian, rekaman peristiwa, sampai pada hasil-hasil riset kajian. Dalam konteks ini, organisasi, lembaga dan perorangan dapat memanfaatkannya dengan cara membentuk kebijakan penggunaan media sosial dan pelatihannya bagi segenap karyawan, dalam rangka memaksimalkan fungsi media sosial sesuai dengan target-target yang telah dicanangkan. Beberapa hal yang bisa dilakukan dengan media

sosial, antara lain membuat blog organisasi, mengintegrasikan berbagai lini di perusahaan, menyebarkan konten yang relevan sesuai target di masyarakat, atau memanfaatkan media sosial sesuai kepentingan, visi, misi, tujuan, efisiensi, dan efektifitas operasional organisasi.

c. Sarana perencanaan, strategi dan manajemen. Akan diarahkan dan dibawa ke mana media sosial, merupakan domain dari penggunanya.Oleh sebab itu, media sosial di tangan para pakar manajemen dan marketing dapat menjadi senjata yang dahsyat untuk melancarkan perencanaan dan strateginya.Misalnya saja untuk melakukan promosi, menggaet pelanggan setia, menghimpun loyalitas customer, menjajaki market, mendidik publik, sampai menghimpun respons masyarakat.

d. Sarana kontrol, evaluasi dan pengukuran. Media sosial berfaedah untuk melakukan kontrol organisasi dan juga mengevaluasi berbagai perencanaan dan strategi yang telah dilakukan.Ingat, respons publik dan pasar menjadi alat ukur, kalibrasi dan parameter untuk evaluasi. Sejauh mana masyarakat memahami suatu isu atau persoalan, bagaimana prosedur-prosedur ditaati atau dilanggar publik, dan seperti apa keinginan dari masyarakat, akan bisa dilihat langsung melalui media sosial. Pergerakan keinginan, ekspektasi, tendensi, opsi dan posisi pemahaman publik akan dapat terekam dengan baik di dalam media sosial. Oleh sebab itu, media sosial juga dapat digunakan sebagai sarana preventif yang ampuh dalam memblok atau memengaruhi pemahaman publik.

BAB III

HASIL PENELITIAN DAN PEMBAHASAN

A. Kebijkan Hukum Pidana Dalam Pembajakan Akun Media Sosial di Indonesia

1. Kasus Pembajakan Akun di Indonesia

Situs milik KPU (Komisi Pemilihan Umum) *Defacing* oleh *hacker*. Peristiwa tersebut terjadi pada tanggal 17 April 2004 dengan target situs http://tnp.kpu.go.id. Tampilan lambang 24 partai diganti dengan nama partai lucu „partai jambu‟, „partai cucak rowo‟, „Partai Kolor Ijo‟ dan lainnya. Pelakunya, diketahui, bernama Dani Firmansyah 24 tahun mahasiswa asal Yogyakarta yang kemudian ditangkap Polda Metro Jaya. Motivasi pelaku, hanya ingin menjajal sistem pengamanan di *server* KPU yang dibeli sangat mahal dan anti bobol katanya saat itu. Tapi ternyata berhasil di tembus oleh Dani. Ketiadaan undangundang *cyber* di Indonesia membuat Dani Firmansyah dijerat dengan pasal-pasal Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi mengancam pidana terhadap perbuatan: "memanipulasi akses ke jaringan telekomunikasi, menimbulkan gangguan fisik dan eletromagnetik terhadap penyelenggaraan telekomunikasi".

Dani Firmansyah, juga dijerat melakukan tindak pidana yang melanggar pasal 22 huruf a, b, c, Pasal 38 dan Pasal 50 Undang-Undang Nomor 36 tahun1999 tentang Telekomunikasi. Pada pasal 22 UU Telekomunikasi berbunyi:

Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah atau memanipulasi akses ke jaringan telekomunikasi dan atau akses ke jasa telekomunikasi; dan atau akses ke jaringan telekomunikasi khusus. Sedangkan

bunyi pasal 50 UU No 36/1999 tentang Telekomunikasi berbunyi “Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 22, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah).”

Kasus klik bca merupakan kasus *domain name* yang memanfaatkan kesalahan ketik yang bisa dilakukan oleh para nasabahnya. Steven Haryanto membeli 5 domain plesetan pada situs target www.klikbca.com yakni www.klikbca.com, kilkbca.com, clikbca.com, klickbca.com dan klikbca.com. Target dari Steven Haryanto adalah nasabah BCA yang melakukan salah ketik dalam penulisan klikbca, tampilan *homepage web* plesetan sama persis dengan *homepage* BCA. *User* akan melakukan login disitus-situs *phising* tersebut, *username* dan *PIN* internet korban akan terkirim pada sang pemilik situs. StevenHaryanto yang sudah meminta maaf dan menyerahkan semua *user ID* dan *PIN* kepada BCA. Kasus tsb tidak dilanjutkan ke pengadilan karena Steven memberikan informasi security BCA yang masih lemah. Saat itu pihak BCA tengah memikirkan alternatif lain ketimbang melaporkan Steven ke polisi. Steven Haryanto merupakan contoh karakteristik ”*WHITE HAT HACKER”*.

Membobol Komputer dan/atau Sistem Elektronik yang bertujuan selain untuk mengakses juga untuk menaklukkan sistem pengamanan dari sistem komputer yang diakses itu. Larangan melakukan perbuatan tersebut diatur dalam Pasal 30 ayat (3) yang berbunyi: Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan. Melanggar

larangan Pasal 30 ayat (3) dipidana berdasarkan Pasal 46 ayat (3) yang berbunyi: Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/ atau denda paling banyak Rp 800.000.000,00 (delapan ratus juta rupiah). Actus reus dari tindak pidana tersebut di atas adalah "mengakses". Mens rea dari tindak pidana tersebut di atas adalah "dengan sengaja".

Objek dari *actus reus* tindak pidana tersebut adalah sama saja dengan objek dari actus reus dalam Pasal 30 ayat (l) dan ayat (2), yaitu "Komputer dan/atau Sistem Elektronik". Namun yang berbeda adalah tujuan pelakunya. Peretasan Situs Negara www.presidensby.info, Pada 9 Januari 2013 situs www.presidensby.info di retas. Saat diretas, Halaman depan diganti dengan latar belakang hitam dengan tulisan warna hijau di bagian atas "*Hacked by MJL007*", sementara di bawahnya tertera sebuah logo dan tulisan "Jemberhacker Team" berwarna putih. Wildan ditangkap setelah melakukan *deface* situs SBY www.presidensby.info Wildan Yani S (22 th) peretas situs SBY lulusan SMK tahun 2010, Wildan memang tidak melanjutkan kuliah karena terhambat biaya.

Wildan bekerja sebagai operator warung Internet di Jember. Wildan ditangkap pada 25 Januari lalu, terancam dengan melanggar Pasal 50 jo. Pasal 22 huruf b Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi. Wildan terancam hukuman pidana penjara paling lama 6 tahun penjara dan atau denda paling banyak Rp 600 juta. Wildan juga dinilai melanggar Pasal 46 Ayat (1), (2), dan (3) jo. Pasal 30 Ayat (1), (2), dan (3) serta Pasal 48 Ayat (1) juncto Pasal 32 Ayat (1) UndangUndang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Serangkaian pasal itu mengancam Wildan dengan hukuman penjara 6 hingga 10 tahun serta denda mencapai Rp 5 miliar.

Namun, Kepolisian menganggap motif Wildan hanya iseng mengganti tampilan situs tersebut tanpa ada maksud politik. Bareskrim Polri mendata, Wildan akan direkrut sebagai staf *cyber crime* Mabes Polri. Tetapi Kepolisian tetap memproses kasus Wildan. Saat ini sedang tahap penyelesaian perkara. Penangkapan Wildan ini kemudian memicu reaksi dari kelompok *hacker* internasional terkemuka, *ANONYMOUS*. Mereka meminta wildan di bebaskan dari segala tuntutan karena aksi wildan tidak merusak sistem maupun datanya tapi bersifat memberitahu dan mengingatkan bahwa pengelolaan situs penting milik pemerintah belum maksimal menjaga keamanannya, bila tuntutannya tidak dipenuhi mereka menyatakan "perang" terhadap situs Pemerintah Republik Indonesia dengan menumbangkan situs-situs berdomain "go.id". Situs-situs yang sudah dilumpuhkan antara lain beberapa sub domain di situs KPPU, BPS, KBRI Tashkent,Kemenkumham, Depsos, dan Kemenparekraf, bahkan Indonesia.go.id.[31]

2. Kebijakan Pembajakan Akun Media Sosial Melalui Pendekatan KUHP

Hukum Pidana yaitu bagian dari keseluruhan hukum yang berlaku disuatu Negara, yang mengadakan dasar-dasar dan peraturan untuk menentukan perbuatan perbuatan yang tidak boleh dilakukan, menentukan kapan dan hal apa kepada mereka yang telah melanggar larangan-larangan itu dapat dikenakan atau dijatuhi

[31] Arifiyadi Teguh . 2008 . *Menjerat Pelaku Cyber Crime dengan KUHP*. Pusat Data Departemen Komunikasi dan Informatika diakses pada tanggal 27 september 2019 dari www. depkominfo.go.id

pidana sebagaimana yang telah diancamkan, menentukan dengan cara bagaimana pengenaan pidana itu dapat dilaksanakan apabila ada orang yang disangka telah melanggar tersebut.

Tindak Pidana dapat juga dikatakan dengan perbuatan pidana yang memiliki definisi sebagai berikut : “Perbuatan yang dilarang oleh suatu aturan hukum larangan mana disertai ancaman (sanksi) yang berupa pidana tertentu, bagi barang siapa melanggar larangan tersebut”.

Saat ini, Indonesia sudah memiliki Undang Undang *cyber law* yang mengatur mengenai *cyber crime* .Rancangan undang undang tersebut sudah ada sejak tahun 2000 dan revisi terakhir dari rancangan undang-undang tindak pidana di bidang teknologi informasi sejak tahun 2016 sudah dikirimkan ke Sekretariat Negara RI oleh Departemen Komunikasi dan Informasi serta dikirimkan ke DPR namun dikembalikan kembali ke Departemen Komunikasi dan Informasi untuk diperbaiki.

Kitab Undang-Undang Hukum Pidana (KUHP) merupakan hukum nasional adalah sumber hukum sekaligus payung hukum untuk menindak berbagai macam tindak pidana yang terjadi di Indonesia. Dalam kaitannya dengan masalah *cyber crime*, KUHP nasional pengaturannya dapat digolongkan menjadi dua, yaitu pengaturan secara umum/tidak langsung dan pengaturan secara khusus/ langsung. Pengaturan secara langsung artinya mengatur secara eksplisit tindak pidana yang berhubungan dengan kejahatan *cyber crime*.

Kebijakan kriminalisasi Cyber Crime (CC) dalam Rancangan Undang-Undang Pemanfaatan Teknologi Informasi (RUU-PTI) tertuang dalam Bab XIV

yang berjudul "Ketentuan Pidana" mulai Pasal 35-40. Undang-Undang Pemanfaatan Teknologi Informasi (RUU-PTI) pada intinya memuat perumusan tindak pidana seperti apa yang terdapat dalam Konvensi *Cyber Crime* Dewan Eropa (*Council of Europe Cyber Crime Convention*) 2001 yaitu: [32]

Pasal 35:

- Memuat Perumusan delik mengenai "penggunaan nama domain yang bertentangan dengan Hak Kekayaan Intelektual milik orang lain";
- Dalam Konvensi *Cyber Crime*, delik serupa ini termasuk "*infringement of copyright"*.

Pasal 36:

- Memuat perumusan delik mengenai "mengaksis data komputer/media elektronik lainnya secara melawan hukum";
- Dalam Konvensi Cyber Crime, delik ini disebut dengan istilah "illegal access".

Pasal 37:

- Ayat (1) memuat perumusan delik mengenai perbuatan "menahan atau mengintersepsi pengiriman data melalui komputer/media elektronik lainnya secara melawan hukum"; dan ayat (2)-nya memuat perumusan delik mengenai perbuatan. "mengintersepsi secara melawan hukum pengiriman data melalui komputer/media elektronik yang menghambat komunikasi dalam sistem komputer/jaringan komputer/sistem komunikasi lainnya";

[32] Barda Nawawi Arief, 2012 . *Kapita Selekta Hukum Pidana,* Bandung: PT. Citra Aditya Bakti, , halaman 256-258.

- Dalam Konvensi *Cyber Crime*, delik dalam Pasal 37 di atas, disebut "*illegal interception*" untuk ayat (1) dan termasuk "*interference system*" untuk ayat (2)

Pasal 38:

- Ayat (1) memuat perumusan delik mengenai perbuatan „memasukkan, mengubah, menambah, menghapus atau merusak data komputer/program komputer/data elektronik lainnya secara melawan hukum". Delik pada ayat (1) itu diperberat ancaman pidananya apabila "mengakibatkan kerugian ekonomi bagi orang lain" ayat (2) dan "mengakibatkan terganggunya fungsi sistem komputer atau sistem media elektronik lainnya ayat (3);
- Dalam Konvensi *Cyber Crime*, delik dalam ayat (1) dan ayat (2) tergolong"*data interference*" dan ayat (3) termasuk "*system interference*".

Pasal 39:

- Memuat perumusan delik mengenai penggunaan kartu kredit/alat pembayaran elektronik lainnya milik orang lain secara melawan hukum dalam transaksi elektronik.
- Delik ini dalam Konvensi *Cyber Crime* termasuk "*computer related offences"*, khususnya "*computer related fraud*".

Pasal 40:

- Ayat (1) memuat ketentuan mengenai perbuatan "membuat, menyediakan, mengirimkan, mendistribusikan, data/tulisan/gambar/rekaman yang isinya melanggar kesusilaan dengan menggunakan komputer/media elektronik

lainnya". Delik pada ayat (1) diperberat ancaman pidananya dalam ayat (2) apabila objeknya adalah anak.

- Dalam Konvensi *Cyber Crime*, hanya disebutkan adanya "*child pornography*" seperti pada ayat (2) di atas.Tindak pidana di atas Pasal 35-40 diancam dengan pidana penjara (maksimumnya berkisar antara 1 (satu) sampai dengan 5 (lima) tahun dan/atau pidana denda (maksimumnya berkisar antara Rp. 100.000.000,00 (seratus juta rupiah) sampai dengan Rp. 500.000.000,00 (lima ratus juta rupiah).

Dalam Upaya Menangani kasus kasus yg terjadi khususnya yang ada kaitannya dengan *cyber crime*, para Penyidik (khususnya Polri) melakukan analogi atau perumpamaan dan persamaan terhadap pasal-pasal yang ada dalam KUHP Pasal yang dapat dikenakan dalam KUHP pada *cyber crime* antara lain:

a. KUHP (Kitab Undang-Undang Hukum Pidana), pasal-pasal yang terkait :
    1. Pasal 362 KUHP tentang pencurian (Kasus *carding*) *Carding* sendiri dalam versi Polri meliputi:
        a) Mendapatkan nomor kartu kredit dari tamu hotel, khususnya orang asing;
        b) Mendapatkan nomor kartu kredit melalui kegiatan *chatting* di Internet;
        c) Melakukan pemesanan barang ke perusahaan di luar negeri dengan menggunakan Jasa Internet;
        d) Mengambil dan memanipulasi data di Internet;

e) Memberikan keterangan palsu, baik pada waktu pemesanan maupun pada saat pengambilan barang di Jasa Pengiriman;

f) *Carding* (pelakunya biasa disebut *carder*), adalah kegiatan melakukan transaksi *e-commerce* dengan nomor kartu kredit palsu atau curian. Pelaku tidak harus melakukan pencurian atau pemalsuan kartu kredit secara fisik, melainkan pelaku cukup mengetahui nomor kartu dan tanggal kadaluarsanya saja;

g) Pasal 378 KUHP tentang Penipuan (Penipuan melalui *website* seolah-olah menjual barang);

h) Pasal 311 KUHP Pencemaran nama Baik (melalui media internet dengan mengirim email kepada Korban maupun teman-teman korban);

i) Pasal 303 KUHP Perjudian (permainan judi online);

j) Pasal 282 KUHP *Pornografi* (Penyebaran *pornografi* melalui media internet).

2. Undang-Undang Nomor 19 Tahun 2002 tentang Hak Cipta, Khususnya tentang Program Komputer atau software
3. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomukasi, (penyalahgunaan Internet yang mengganggu ketertiban umum atau pribadi).
4. Undang-Undang Nomor 25 Tahun 2003 tentang Perubahan atas Undang- Undang No.15 Tahun 2002 tentang Pencucian Uang.

5. Undang-Undang Nomor 5 Tahun 2018 tentang Pemberantasan Tindak Pidana Terorisme.

Beberapa langkah penting yang harus dilakukan dalam penanggulangan *cyber crime* adalah :

a. Melakukan modernisasi hukum pidana nasional beserta hukum acaranya, yang diselaraskan dengan konvensi internasional yang terkait dengan kejahatan tersebut.
b. Meningkatkan sistem pengamanan jaringan komputer nasional sesuai standar internasional
c. Meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yang berhubungan dengan *cyber crime*
d. Meningkatkan kesadaran warga negara mengenai masalah *cyber crime* serta pentingnya mencegah kejahatan tersebut terjadi
e. Meningkatkan kerjasama antar negara, baik bilateral, regional maupun multilateral, dalam upaya penanganan *cyber crime*, antara lain melalui perjanjian ekstradisi dan *mutual assistance treaties*.

3. Kebijakan Pembajakan Akun melalui pendekatan UU ITE

Kejahatan merupakan entitas yang selalu melekat dengan dinamika perkembagan peradaban umat manusia. Kejahatan yang oleh Saparinah Sadli disebut sebagai perilaku menyimpang, selalu ada dan melekat pada setiap bentuk masyarakat; tidak ada masyarakat sepi dari kejahatan.

Oleh karena itu, upaya penanggulangan kejahatan sesungguhnya merupakan usaha yang terus menerus dan terus berkesinambungan. Semakin majunya peradaban manusia, sebagai implikasi dari perkembangan ilmu pengetahuan dan teknologi,muncul berbagai jenis kejahatan berdimensi baru, yang termasuk di dalamnya *cyber crime*. Sejalan dengan itu diperlukan upaya penanggulangan untuk menjamin ketertiban dalam masyarakat. Dalam perspektif hukum, upaya ini direalisasikan dengan hukum pidana. Hukum pidana diharapkan mampu memenuhi ketertiban masyarakat. Akan tetapi dalam menghadapi perkembangan masyarakat, hukum pidana tidak selamanya mampu menjawab terhadap dampak negatif yang timbul dari kejahatan. Hal ini dikarenakan teknologi yang membawa perubahan dalam masyarakat berkembang begitu pesat, sementara hukum pidana merupakan produk sejarah tertentu berjalan dengan logika sejarah yang menaunginya walaupun dalam batas tertentu mempuntyai prediktabilitas atas perkembangan masyarakat.

Dua muatan besar yang diatur dalam UU ITE ialah mengenai pengaturan tranksaksi elekronik dan mengenai tindak pidana siber. Materi UU ITE tersebut merupakan implementasi dari beberapa prinsip ketentuan internasional. Pada UU ITE dimuat tentang perbuatan yang dilarang pada Pasal 27 sampai Pasal 36. Pada pasal 42 UU ITE diatur pula mengenai ketentuan penyidikan yang berbunyi : “penyidikan sebagaimana dimaksud dalam undang-undang ini, dilakukan berdasarkan ketentuan dalam Hukum Acara Pidana dan ketentuan dalam undang undang ini”. Dengan demikian, sistem pembuktian yang dianut adalah sistem/teori pembuktian berdasar undang-undang secara negatif, yaitu sistem yang dianut dalam

KUHAP dan berdasar Pasal 183 KUHAP, yang berbunyi sebagai berikut: “hakim tidak boleh menjatuhkan pidana kepada sesorang kecuali apabila dengan sekurang-kurangnya dua alat bukti yangsah ia memperoleh keyakinan bajwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukannya”. Dengan demikian, artinya pembuktian harus didasarkan ketentuan undang-undang, yakni alat bukti yang sah yang diatur dalam Pasal 184 KUHAP disertai keyakinan hakim yang diperoleh dari alat-alat bukti tersebut. Berikut beberapa alat bukti yang diatur dalam Pasal 184 KUHAP sebagai acuan dalam pembuktian kejahatan mayantara (*cyber crime*), yaitu:

a. Keterangan saksi Syarat formal keterangan saksi yang diatur dalam KUHAP ialah, antara lain, dinyatakan di persidangan dan mengucapkan sumpah atau janji sebelum saksi memberikan keterangan. Sedangkan syarat materiil untuk keterangan saksi antara lain:
    1) Keterangan yang diberikan ialah mengenai peristiwa yang ia dengar, lihat, dan alami sendiri dengan menyebutkan alasan pengetahuannya.
    2) Bukan pendapat, rekaan, maupun keterangan ahli
    3) Ada lebih dari satu orang saksi yang sesuai asas *unus testis nullus testis*;bukan keterangan yang dia peroleh dari orang lain (*testimonium de auditu);*
    4) Adanya persesuaian antara keterangan saksi yang satu dengan yang lain dan keterangan saksi yang satu dengan alat bukti yang lain.
    5) Pada kasus *cyber crime*, dikarenakan sifatnya yang *virtual*, maka pembuktian dengan menggunakan keterangan saksi tidak dapat

diperoleh secara langsung. Keterangan saksi hanya dapat berupa hasil pembicaraan atau hanya mendengar orang lain. Kesaksian ini dikenal dengan *testimonium de auditum atau hearsay evidence*, meskipunkesaksian sejenis ini tidak diperkenakan sebagai alat bukti, akan tetapi dalam praktiknya tetap dapat dipergunakan sebagai bahan pertimbangan bagi hakim untuk memperkuat keyakinannya sebelum menjatuhkan putusan. Kemungkinan yang dapat dijadikan keterangan saksi ialah melalui hasil interaksi dalam dunia *cyber*, seperti *chatting* dan *e-mail* antara pengguna internet, atau juga dapat melalui keterangan seorang administrator sistem komputer yang telah disertifikasi.

b. Keterangan ahli Dalam Pasal 186 KUHAP diatur mengenai syarat formil keterangan ahli bahwa keterangan ahli ialah apa yang seorang ahli nyatakan di sidang pengadilan. Yang disebut sebagai ahli ialah ahli kedokteran kehakiman dan ahli lainnya. Keterangan ahli menjadi signifikan penggunaannya jika jaksa mengajukan alat bukti elektronik untuk membuktikan kesalahan pelaku *cyber crime.* Peran keterangan ahli disini adalah untuk memberikan suatu penjelasan dalam persidangan bahwa dokumen/data elektronik yang diajukan adalah sah dan dapat dipertanggungjawabkan secara hukum

c. Alat bukti surat (Pasal 184 huruf c dan Pasal 187 KUHAP) Jenis surat yang diakui berdasarkan alat bukti ialah surat yang dibuat diatas sumpah jabatan atau dikuatkan dengan sumpah sebagaimana yang tertuang dalam pasal 187 KUHAP. “Surat” dalam kasus *cyber crime* mengalami perubahan dari

bentuknya yang tertulis menjadi tidak tertulis dan bersifat *online.* Alat bukti dalam komputer yang telah disertifikasi ada dua kategori. Pertama, bila sebuah sistem komputer yang telah disertifikasi oleh badan yang berwenang, maka hasil print out komputer dapat dipercaya keotentikannya. Contohnya *receipt* yang dikeluarkan oleh suatu bank dalam transaksi ATM. Alat bukti ini mempunyai kekuatan pembuktian meskipun dalam persidangan dibutuhkan keterangan lebih lanjut. Kedua, bukti sertifikasi dari badan yang berwenang tersebut dapat dikategorikan sebagai bukti surat, karena dibuat oleh dan atau pejabat yang berwenang. Jenis alat bukti surat lainnya dapat berupa bukti elektronik yang dapat dicetak dan surat yang terpampang dalam layar monitor sebuah jaringan komputer. Selama kedua bukti ini dikeluarkan/dibuat oleh yang berwenang dalam sebuah sistem jaringan komputer dan sebuah sistem jaringan komputer tersebut dapat dipercaya, maka surat tersebut memiliki kekuatan pembuktian yang sama dengan alat bukti surat sebagaimana yang ditentukan dalam KUHAP.

d. Alat bukti petunjuk (Pasal 184 (1) huruf d dan Pasal 188 KUHAP) KUHAP mengatur secara *limitatif* mengenai sumber petunjuk, yaitu bahwa petunnjuk hanya dapat diperoleh dari keterangan saksi, surat, dan keterangan terdakwa. Untuk dapat dijadikan sumber petunjuk, ketiga alat bukti tersebut harus sah, dan oleh karena itu, petunjuk yang dihasilkan juga menjadi sah.Dalam *cyber crime,* pengumpulan alat bukti secara fisik akan sulit dipenuhi. Yang paling mudah dalam melakukan pengumpulan bukti-bukti adalah mencari petunjuk-petunjuk yang mengindikasi telah adanya

suatu niat jahat berupa akses secara tidak sah. Misalnya dengan melihat dan mendengarkan keterangan saksi di pengadilan, atau surat elektronik atau hasil *print out data*, atau juga dari keterangan terdakwa di pengadilan.

e. Keterangan terdakwa (Pasal 184 huruf e dan Pasal 189 KUHAP) Keterangan terdakwa ialah apa yang terdakwa nyatakan di sidang tentang perbuatan yang ia lakukan atau yang ia ketahui sendiri atau alami sendiri. Agar keterangan terdakwa dapat dinyatakan sah, syarat formil,yaitu dinyatakan di sidang dan syarat materiil keterangan tersebut tentang perbuatan yang terdakwa lakukan atau ketahui atau alami sendiri – harus dipenuhi. Dalam Undang-undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik pasal 5 ayat 1 dan 2 mendeskripsikan bahwa Dokumen Elektronik dan Informasi Elektronik adalah merupakan alat bukti yang sah. Selain dalam pasal 44 Undang-undang yang sama mengatakan : "Alat bukti penyidikan, penuntutan dan pemeriksaan di sidang pengadilan menurut ketentuan undang undang ini adalah sebagai berikut :

1) alat bukti sebagaimana dimaksud dalam ketentuan Perundangundangan.
2) alat bukti lain berupa Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud dalam Pasal 1 angka 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3).

Informasi Elektronik dan Dokumen Elektronik dapat dijadikan sebagai alat bukti yang sah menurut undang-undang tentang Teknologi Informasi dan Transaksi Elektronik, walaupun sulit untuk diklasifikasikan termasuk alat bukti yang sah sebagaimana dimaksud Pasal 184 ayat (1) KUHAP. Informasi Elektronik dan/atau

Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik sesuai ketentuan yang diatur dalam UU ITE.[33]

B. Penegakan Hukum Pembajakan Akun / Cyber Crime di Indonesia melalui sarana penal dan non penal

1. Penegakan Hukum *Cyber Crime* Melalui Sarana Penal.

Sebelum penulis membahas penegakan hukum *cyber crime* dengan sarapenal, penulis lebih dulu akan mengemukakan masalah intrumen internasional yang berkaitan dengan kejahatan *cyber*. Intrumen internasional yang berkaitan dengan *cyber crime* adalah *Convention on Cyber Crime* tanggal 23 November 2001 di kota Budapest Hongaria telah membuat dan menyepakati *Convention on Cyber Crime* yang kemudian dimasukkan dalam *European Treaty Series* dengan nomor 185.[34]

Convention on Cyber Crime 2001 dibentuk dengan pertimbangan antara lain:[38]Pertama, masyarakat internasional menyadari perlunya kerjasama antara negara dan industri dalam memerangi kejahatan *cyber* dan adanya kebutuhan untuk melindungi kepentingan yang sah di dalam penggunaan serta pengembangan teknologi informasi. Kedua, Konvensi saat ini diperlukan untuk meredam penyalahgunaan sistem, jaringan dan data komputer untuk melakukan perbuatan kriminal. Dengan demikian perlunya adanya kepastian dalam proses penyelidikan dan penuntutan pada tingkat internasional dan domestik melalui suatu mekanisme kerjasama internasional yang dapat dipercaya dan cepat. Ketiga, saat ini sudah semakin nyata adanya kebutuhan untuk memastikan suatu kesesuaian antara

---

[33] Sehatapy, J.E. 2004 . *Pisau Analisis Kriminologi*. . Bandung. : PT Citra Aditya Bakti . halaman 113

[34] Ahmad M.Ramli . 2012 . *Cyber Law dan HAKI Dalam Sistem Hukum Indonesia* . Bandung: PT Refika Aditama . halaman 23

pelaksanaan penegakan hukum dan hak azasi manusia sejalan dengan Konvensi Dewan Eropa untuk perlindungan Hak Azasi Manusia danm Kovenan Perserikatan Bangsa-Bangsa 1966 tentang Hak Politik dan Sipil yang memberikan perlindungan kebebasan berpendapat seperti hak berekpresi, yang mencakup kebebasan untuk mencari, menerima, dan menyebarkan informasi dan pendapat.

Dilihat dari kebijakan kriminal (kebijakan penanggulangan kejahatan), hukum pidana bukan merupakan sarana kebijakan yang strategis. Kebijakan yang strategis adalah mencegah dan meniadakan faktor faktor penyebab atau kondisi yang menimbulkan kejahatan. Dilihat dari sudut *criminal policy*, upaya penanggulangan kejahatan (termasuk penanggulangan *cyber crime*) tentunya tidak dapat dilakukan secara parsial dengan hukum pidana (sarana penal), tetapi harus ditempuh pula dengan pendekatan integral/sistemik. Sebagai salah satu bentuk dari high tech crime, merupakan hal yang wajar jika upaya penanggulangan *cyber crime* juga harus ditempuh dengan teknologi (*techno prevention*).

Disamping itu diperlukan pula pendekatan budaya/kultural, pendekatan moral/edukatif, dan bahkan global (kerjasama internasional) karena *cyber crime* dapat melampaui batas-batas negara (bersifat *transnational transborder*).Walaupun sarana penal mempunyai keterbatasan, namun dilihat dari sudut "perencanaan kebijakan penanggulangan kejahatan dengan hukum pidana" (*penal policy*), tahap kebijakan legislasi/formulasi merupakan tahap paling strategis. Kesalahan/kelemahan kebijakan legislatif merupakan kesalahan strategis yang

dapat menjadi Penghambat upaya pencegahan dan penanggulangan kejahatan pada tahap aplikasi dan eksekusi[35]

Dalam upaya atau kebijakan penanggulangan *cybercrime* dengan hukum pidana, lokakarya/workshop mengenai *"computer related crime*" yang diselenggarakan dalam kongres PBB X (April 2000) menyatakan, bahwanegaranegara anggota harus berusaha melakukan harmonisasi ketentuan-ketentuan yang berhubungan dengan kriminalisasi, pembuktian, dan prosedur. Jadi masalahnya bukan sekedar bagaimana membuat kebijakan hukum pidana (kebijakan kriminalisasi, formulasi, dan legislasi) di bidang penanggulangan *cyber crime*, tetapi bagaimana ada harmonisasi kebjakan penal di berbagai negara. Ini berarti, kebijakan kriminalisasi tentang masalah *cyber crime* bukan semata-mata masalah kebijakan nasional (Indonesia) tetapi juga terkait dengan kebijakan regional dan internasional.

Kebijakan kriminalisasi merupakan suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana (tidak dipidana) menjadi suatu tindak pidana (perbuatan yang dapat dipidana). Jadi pada hakekatnya, kebijakan kriminalisasi merupakan bagian dari kebijakan kriminal (*criminal policy*) dengan menggunakan sarana hukum pidana (penal), dan oleh karena itu termasuk bagian dari "kebijakan hukum pidana" (*penal policy),* khususnya kebijakan formulasinya.

Ketentuan hukum pidana positif yang dikriminalisasi terkait kejahatan dunia maya (*cyber crime*) dapat kita lihat pada Undang-Undang Nomor 19 Tahun 2016 perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan

[35] Barda Nawawi Arif, op , cit ,.halaman 53

ransaksi Elektronik, sebagaimana yang dimuat pada Pasal 27 sampai dengan Pasal 36. Terdapat pula pada Undang-undang Nomor 20 Tahun 2001 tentang Perubahan atas Undang-undang Nomor 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi, dimana sisi mayantara dari tindak pidana korupsi ini adalah bahwa kejahatan tersebut telah menggunakan media internet sebagai alat untuk melakukan korupsi ataupun memperlancar tindak dilakukannya tindak pidana tersebut meskipun tidak secara eksplisit diatur dalam undang-undang ini. Beberapa peraturan perundang-undangan yang mengkriminalisasi kejahatan mayantara di dalamnya adalah : Undang-undang Nomor 44 Tahun 2008 tentang Pornografi, Undang-undang Nomor 5 Tahun 2018 tentang Pemberantasan Tindak Pidana Terorisme, Undang-undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang, dan Undang-undang Nomor 35 Tahun 2009 tentang Narkotika.

Ada beberapa peraturan perundang-undangan yang berkaitan dengan masalah pembajakan akun, di antaranya adalah sebagai berikut:

Pasal 30 ayat 1, ayat 2, dan atau ayat 3 UU No 11/2008 tentang Informasi dan Transaksi Elektronik (ITE), berbunyi

1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik orang lain dengan cara apa pun.
2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.

3) (3) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Selain itu juga Pasal 32 ayat 1 UU No 11/2008 tentang Informasi dan Transaksi Elektronik (ITE), yang berbunyi (1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik orang lain atau milik publik.

Aturan lainnya, Pasal 22 huruf B Undang-Undang 36/1999 tentang Telekomunikasi yang berbunyi Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi akses ke jaringan telekomunikasi; dan atau akses ke jasa telekomunikasi; dan atau akses ke jaringan telekomunikasi khusus.

Selain mengancam pelanggaran dalam Pasal 30 UU ITE tersebut dengan pidana di Pasal 46 UU ITE. UU ITE juga melakukan pemberatan penjatuhan pidana atas tindakan peretasan, yaitu sesuai dengan objek dan subjek tindakan peretasannya.

Berdasarkan objek peretasannya diberatkan dengan Pasal 52 ayat (2) UU ITE, yaitu pemberatan penjatuhan hukuman pidana apabila objek diretas adalah sistem elektronik yang dimiliki oleh pemerintah atau sistem yang dipergunakan untuk pelayanan publik.

Kemudian, juga diberatkan dalam Pasal 52 ayat (3) UU ITE, yaitu pemberatan penjatuhan hukuman pidana apabila objek yang di retas adalah situs web milik pemerintah yang berhubungan langsung dengan keamanan dan stabilitas negara.

Lalu berdasarkan subjek peretasannya, di beratkan dalam Pasal 52 ayat (4) UU ITE, yaitu pemberatan penjatuhan hukuman pidana dilakukan apabila pelaku peretasan dilakukan oleh korporasi atau perusahaan.

Jerat hukum peretasan oleh *hacker* dapat dipertanggungjawabkan berdasarkan ketentuan Pasal 30 UU ITE. Seseorang dapat dipidana apabila orang tersebut mengakses sistem elektronik atau komputer korban dan juga dalam pasal ini menentukan bahwa cara yang dilakukan adalah dengan cara apapun selama hal tersebut dilakukan dengan cara tanpa haknya.

2. Penegakan Hukum *Cyber Crime* Melalui Sarana Non Penal.

Pendekatan non penal menurut Hoefnagels adalah pendekatan pencegahan kejahatan tanpa menggunakan sarana pemidanaan (*prevention without punisment)*, yaitu antara lain perencanaan kesehatan mental masyarakat (*community planning mental health*), kesehatan mental masyarakat secara nasional (*national mental health*), *social worker and child welfare* (kesejahteraan anak dan pekerja sosial), serta penggunaan hukum civil dan hukum administrasi (*administrative & civil law*).

Kebijakan penanggulangan kejahatan lewat jalur “non penal” lebih bersifat zindakan pencegahan sebelum terjadinya kejahatan. Oleh karena itu, sasaran utamanya adalah menangani faktor-faktor kondusif penyebab terjadinya kejahatan yang berpusat pada masalah-masalah atau kondisi-kondisi sosial yang secara langsung atau tidak langsung dapat menimbulkan atau menumbuh suburkan

kejahatan. Dengan demikian dilihat dari kebijakan penanggulangan kejahatan, maka usaha-usaha non penal ini mempunyai kedudukan yang strategis dan memegang peranan kunci yang harus diintensifkan dan diefektifkan.

Beberapa masalah dan kondisi sosial yang dapat merupakan faktor kondusif penyebab timbulnya kejahatan, jelas merupakan masalah yang tidak dapat diatasi semata–mata dengan "penal". Di sinilah keterbatasan jalur "penal" dan oleh karena itu, harus ditunjang oleh jalur "non penal". Salah satu jalur "non penal" untuk mengatasi masalah–masalah sosial seperti dikemukakan diatas adalah lewat jalur "kebijakan sosial" (*social policy*), dimana G.P. Hoefnagels juga memasukkan dalam jalur "prevention without punishment". Kebijakan sosial pada dasarnya adalah kebijakan atau upaya-upaya rasional untuk mencapai kesejahteraan masyarakat. Jadi identik dengan kebijakan atau perencanaan pembangunan nasional yang meliputi berbagai aspek yang cukup luas dari pembangunan.

Cyber Crime membutuhkan *global action* dalam penanggulangannya mengingat kejahatan tersebut seringkali bersifat transnasional. Beberapa langkah penting yang harus dilakukan setiap negara dalam penanggulangan *cyber crime* adalah:

a. Melakukan modernisasi hukum pidana nasional beserta hukum acaranya, yang diselaraskan dengan konvensi internasional yang terkait dengan kejahatan tersebut.
b. Meningkatkan sistem pengamanan jaringan komputer nasional sesuai standar internasional.

c. Meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yang berhubungan dengan *cyber crime*

d. Meningkatkan kesadaran warga negara mengenai masalah *cyber crime* serta pentingnya mencegah kejahatan tersebut terjadi.

e. Meningkatkan kerjasama antar negara, baik bilateral, regional maupun multilateral, dalam upaya penanganan *cyber crime,* antara lain melalui perjanjian ekstradisi dan *mutual assistance treaty.*

f. Harmonisasi mengenai masalah yurisdiksi untuk menegakkan kedaulatan negara yang berlaku karena sifatnya transnasional.

Meskipun hukum pidana digunakan sebagai ultimum remidium atau alat terakhir apabila bidang hukum yang lain tidak dapat mengatasinya, tetapi harus disadari bahwa hukum pidana memiliki keterbatasan kemampuan dalam menanggulangi kejahatan. Keterbatasan-keterbatasan tersebut dikemukakan oleh Barda nawawi Arief sebagai berikut :

a. Sebab-sebab kejahatan yang demikian kompleks berada di luar jangkauan hukum pidana;

b. Sebab-sebab kejahatan yang demikian kompleks berada di luar jangkauan hukum pidana;

c. Hukum pidana hanya merupakan bagian kecil (subsistem) dari sarana kontrol sosial yang tidak mungkin mengatasi masalah kejahatan sebagai masalah kemanusiaan dan kemayarakatan yang sangat kompleks (sebagai

masalah sosio-psikologis, sosio-politik, sosio-ekonomi, sosio-kultural dan sebagainya);

d. Penggunaan hukum pidana dalam menanggulangi kejahatan hanya merupakan "*kurierenam symptom*", oleh karena itu hukum pidana hanya merupakan pengobatan simptomatik dan bukan pengobatan kausatif;
e. Sanksi hukum pidana merupakan *remedium* yang mengandung sifat kontradiktif/paradoksal dan mengandung unsur-unsur serta efek sampingan yang negatif;
f. Sistem pemidanaan bersifat *fragmentair* dan individual/personal, tidak bersifat struktural/fungsional;
g. Keterbatasan jenis sanksi pidana dan sistem perumusan sanksi pidana yang bersifat kaku dan imperatif;
h. Bekerjanya/berfungsingnya hukum pidana memerlukan sarana pendukung yang lebih bervariasi dan memerlukan "biaya tinggi".

Keterbatasan-keterbatasan hukum pidana inilah yang tampaknya dialami oleh Polri yang menggunakan hukum pidana sebagai landasan kerjanya. Sebab kejahatan yang kompleks ini terlambat diantisipasi oleh Polri sehingga ketika terjadi kasus yang berdimensi baru mereka tidak secara tanggap menanganinya.

Untuk itu, pencegahan kejahatan tidak melulu harus menggunakan hukum pidana. Agar penegakan hukum *cyber crime* ini dapat dilakukan secara menyeluruh maka tidak hanya pendekatan yuridis atau penal yang dilakukan, tetapi dapat juga dilakukan dengan pendekatan non-penal.

Dari paparan penegakan hukum dengan sarana non-penal ini, maka menurut penulis cara non- penal inilah yang lebih diutamakan dari pada sarana penal dengan konsekwensi segera menyiapkan penegak hukum yang menguasai teknologi informasi. Atau lebih jelasnya kita sangat membutuhkan Polisi *cyber*, Jaksa *cyber*, Hakim *cyber* dalam rangka penegakan hukum *cyber crime* di Indonesia tanpa adanya penegak hukum yang mempuni di bidang teknologi informasi, maka akan sulit menjerat penjahat-penjahat *cyber* oleh karena kejahatan *cyber* ini *locus delicti* bisa lintas negara.

C. Faktor-Faktor Yang Mempegaruhi Dalam Penanggulan Peretasan Akun Media Sosial di Indonesia

Hukum tumbuh bukan dari perbuatan pemerintah, tetapi dari fakta-fakta sosial di dalam suatu komunitas. Aturan hukum merupakan pencerminan kaidahkaidah ekonomi dan moral yang didasarkan pada pengakuan masyarakat tentang kesignifikanannya bagi ikatan masyarakatnya. Oleh sebab itu keberadaan aturan yang mengatur mengenai prostitusi *cyber* didasarkan pada kaidah ekonomi dan moral.

Secara umum kejahatan komputer dapat dicegah melalui faktor-faktor lingkungan yaitu:

1. Pendidikan komputer sejak dini yang dimulai dari bangku sekolah, sehingga dapat meningkatkan pengetahuan dan kesadaran atas bentukbentuk perbuatan dalam menggunakan sarana komputer yang salah.
2. Pengawasan terhadap warnet-warnet yang ada di masyarakat, untuk mencegah warnet sebagai sarang penggunaan situs yang melanggar hukum.

3. Pengawan orang tua terhadap anak pengguna komputer dan internet.
4. Membuat wadah bagi anak-anak yang memiliki kelebihan dibidang jaringan internet. Filterisasi situs-situs yang merusak norma anak muda oleh pemerintah.
5. Sanksi yang tegas bagi pemilik warnet jika tidak menegur users nya yang sedang menggunaan situs *cyber gambling*, *cyberporn* , dll.
6. Banyaknya komunitas *black hat* (hacker hitam) di Indonesia sebagai salah satu dampak penyebab maraknya terjadi kejahatan di dunia maya, lemahnya *system computer*, dan begitu kecilnya gaji para ahli IT di Indonesia menyebabkan para master computer berbuat criminal demi mencukupi kebutuhan *financialnya* , jadi perlu peningkata taraf hidup bagi para ahli IT.

1. Faktor penangulangan *cyber crime* melalui para penegak hukum

Strategi Penanganan Pemerintah Penyempurnaan perangkat hukum, Polri, Kemenkominfo, DPR, pakar hukum dan organisasi lainnya yang sangat berkepentingan atau keamanan usahanya tergantung dari kesempurnaan undangundang di bidang *cyber space* (pengusaha *e-commerce dan banking*) sedang memproses untuk merancangnya agar di Indonesia terwujud UU ITE yang sempurna. UU ITE diharapkan bersifat *lex specialist*, menyempurnakan undang undang pendukungnya dan melakukan sintesa serta analogi yang lebih luas terhadap KUHP. UU ITE yang sudah ada perlu direvisi terutama pasal / ayat yang karet (multitafsir), setidaknya tidak boleh dipakai sebagai rujukan hukum hingga nanti terbit PP dan Permen/Kepmen Kominfo yang menjadi turunan hukumnya. Perlu dilakukan Komitmen dan kerja sama yang intensif antara Kemenkominfo

dengan para pakar dari universitasuniversitas dan pelaku bisnis ICT khususnya ISP dan *Computer Network Security* dalam mengantisipasi perkembangan *cyber crime* di Indonesia. Mendidik para penyidik, Dalam hal menangani kasus *cyber crime* diperlukan penyidik yang mempunyai cukup pengalaman (bukan penyidik pemula), pendidikannya diarahkan untuk menguasai teknis penyidikan dan menguasai administrasi penyidikan serta dasar-dasar pengetahuan di bidang komputer dan profil *hacker*.

Untuk itu diperlukan pengiriman aparat hukum Polisi, Jaksa, Hakim untuk melakukan pendidikan mengenai *cyber crime* di negara maju khususnya Amerika Serikat. Membangun Fasilitas *Forensic Computing,* Keberadaan *Fasilitas Forensic Computing* sangat penting dan vital dalam membongkar kasus *cyber crime.* Fasilitas *Forensic Computing* yang akan didirikan Polri diharapkan akan dapat melakukan tiga hal penting, yaitu; *Evidence Collection* (pengumpulan bukti), *Forensic Analysis* (analisis forensik), *Expert Witness* (saksi ahli).

Diharapkan nantinya Para ahli forensik komputer bisa memanfaatkan fasilitas tsb untuk mendeteksi lokasi kejahatan yang tepat dan juga mendukung dalam pemulihan dokumen yang hilang atau sengaja dirusakkan. Ahli Komputer forensik menangani dengan setiap kasus dengan sangat hati-hati ketika akan melakukan pemeriksaan forensik, Setiap melakukan kesalahan penempatan akan berakibat korupsi data atau dapat merusak sistem secara keseluruhan. Komputer forensik memungkinkan ahli forensik dapat mengetahui masing-masing dari setiap file. Baik file yang disimpan di tempat biasa dan maupun yang tersembunyi dan file yang dilindungi oleh security. Hal tersebut dapat dilakukan melalui *tool forensik.*

Forensik komputer ini juga memainkan peran sebagai analisa teknis sehingga mampu menyelidiki bagian yang paling sulit terjangkau dari perangkat digital. Meningkatkan Upaya Penyidikan Dan Kerja Sama Internasional, Indonesia melalui Kepolisian RI bekerja sama dengan Amerika Serikat (AS) melalui *International Criminal Investigative Training Assistance Program (ICITAP*) melatih lebih dari 100 orang polisi se-Jawa timur mengenai cara mengatasi "*Cyber Crime"* (Tindak Kejahatan Dunia Maya). Selain itu Aparatur kepolisian melalui Kepolisian negara-negara Asean terus berkoordinasi dan bekerjasama untuk memerangi kejahatan di dunia maya atau *cyber crime.*

Untuk meningkatkan kemampuannya, sebanyak 70 perwira dari kepolisian se-Asean mengikuti pelatihan selama dua hari di Bandung. Pelatihan ini juga melibatkan para ahli dari *Interpol, Apcert, Microsoft,* kepolisian Korea dan Kepolisian Federal Australia. Kerjasama Kepolisian Republik Indonesia (Polri) dengan *Australia Federal Police* (AFP), dalam bidang penanganan kejahatan *cyber*, diharapkan mampu meningkatkan kinerja penyidik dalam menangani bukan hanya kasus *cyber crime*, namun juga terorisme di Indonesia.

2. Solusi Kebijakan Hukum Pidana Terhadap Penanggulangan *Cyber Crime* di Indonesia

Terjadinya kasus cyber crime, pihak kepolisian telah melakukan berbagai upaya penanggulangan cyber crime upaya tersebut adalah upaya preventif dan represif.

a. Upaya Preventif

Dalam melakukan upaya preventif ini pihak kepolisian khususnya unit *cyber crime* polisi telah melakukan berbagai upaya seperti memberikan himbauan ke masyarakat melalui media elektronik maupun media sosial dengan menyebarkan *broadcast* berupa himbauan-himbauan terkait *cyber crime* untuk di *forward* ke masyarakat luas. Selain itu dilakukan juga penerangan ke masyarakat melalui media surat kabar dan radio, serta pada saat mengisi acara *talkshow* pihak kepolisian tidak henti-hentinya memberikan himbauan kemasyarakat.

b. Upaya Represif

Pihak kepolisian bekerja sama dengan *stakeholder* yang ada yaitu bagaimana menangkap pelaku yang tertangkap tangan melakukan kejahatan ataupun melalui laporan masyarakat kemudian mendatangi tempat kejadian perkara (TKP) guna melakukan penangkapan dan penahanan terhadap tersangka kasus *cyber crime,* setelah dilakukan penangkapan kemudian diproses dikepolisian dan sebelum dilimpahkan berkas perkaranya ke kejaksaan terlebih dahulu diadakan konferensi pers dengan media dimana pihak media hadir untuk mewawancarai tersangka dan petugas yang menangani kasus tersebut. Lalu hasil wawancara tersebut disiarkan atau disebarkan kemasyarakat luas, sehingga masyarakat mengetahui kasus-kasus yang ditangani oleh aparat kepolisian

c. Pelaksanaan Undang Informasi dan Transaksi

Dalam mengahadapi *cyber crime,* hukum positif di Indonesia masih bersifat *lex locus delicti*. Namun beda halnya dengan situasi dan kondisi pelanggaran hukum yang terjadi atas *cyber crime* dimana pelaku kejahatan *cyber* dan korban berada di

tempat yang berbeda. Wilayah kejahatan dunia maya yang begitu luas namun mudah diakses menyebabkan maraknya terjadi kejahatan. Kepolisian Republik Indonesia (POLRI) sebagai salah satu alat kelengkapan negar dalam menegakkan hukum tidak dapat lagi tinggal diam setelah lahirnya Undang-Undang Nomor 19 Tahun 2016 perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Aparat penegak hukum dalam hal ini penyidik kepolisian harus bergerak secara aktif untuk menindak kejahatan di dunia maya. Aparat kepolisian harus dapat menangani kasus-kasus kejahatan yang terjadi di dunia maya.[36]

Undang-Undang Nomor 19 Tahun 2016 perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE) :

1. Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleteks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.
2. Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan Komputer, jaringan Komputer, dan/atau media elektronik lainnya.

[36] M.Ramli, Ahmad. 2006 . *Cyber Law dan HAKI Dalam Sistem Hukum Indonesia*, Bandung: PT Refika Aditama.halaman 98.

3. Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi.
4. Dokumen Elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.
5. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.
6. Penyelenggaraan Sistem Elektronik adalah pemanfaatan Sistem Elektronik oleh penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat penyelenggara sistem elektronik adalah setiap Orang, penyelenggara negara, Badan Usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik, baik secara sendiri-sendiri maupun bersama-sama kepada pengguna sistem elektronik untuk keperluan dirinya dan/atau keperluan pihak lain.

7. Jaringan Sistem Elektronik adalah terhubungnya dua sistem elektronik atau lebih, yang bersifat tertutup ataupun terbuka.
8. Agen Elektronik adalah perangkat dari suatu sistem elektronik yang dibuat untuk melakukan suatu tindakan terhadap suatu informasi elektronik tertentu secara otomatis yang diselenggarakan oleh orang.
9. Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat tanda tangan elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam transaksi elektronik yang dikeluarkan oleh Penyelenggara sertifikasi elektronik.
10. Penyelenggara Sertifikasi Elektronik adalah badan hukum yang berfungsi sebagai pihak yang layak dipercaya, yang memberikan dan mengaudit Sertifikat Elektronik.
11. Lembaga Sertifikasi Keandalan adalah lembaga independen yang dibentuk oleh profesional yang diakui, disahkan, dan diawasi oleh Pemerintah dengan kewenangan mengaudit dan mengeluarkan sertifikat keandalan dalam transaksi elektronik.
12. Tanda Tangan Elektronik adalah tanda tangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.
13. Penanda Tangan adalah subjek hukum yang terasosiasikan atau terkait dengan tanda tangan elektronik.
14. Komputer adalah alat untuk memproses data elektronik, magnetik, optik, atau sistem yang melaksanakan fungsi logika, aritmatika, dan penyimpanan.

15. Akses adalah kegiatan melakukan interaksi dengan Sistem Elektronik yang berdiri sendiri atau dalam jaringan.
16. Kode Akses adalah angka, huruf, simbol, karakter lainnya atau kombinasi di antaranya, yang merupakan kunci untuk dapat mengakses Komputer dan/atau Sistem Elektronik lainnya.
17. Kontrak Elektronik adalah perjanjian para pihak yang dibuat melalui Sistem Elektronik.
18. Pengirim adalah subjek hukum yang mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik.
19. Informasi Elektronik dan/atau Dokumen Elektronik dari Pengirim.
20. Nama Domain adalah alamat internet penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat, yang dapat digunakan dalam berkomunikasi melalui internet, yang berupa kode atau susunan karakter yang bersifat unik untuk menunjukkan lokasi tertentu dalam internet.
21. Orang adalah orang perseorangan, baik warga negara Indonesia, warga negara asing, maupun badan hukum.
22. Badan Usaha adalah perusahaan perseorangan atau perusahaan persekutuan, baik yang berbadan hukum maupun yang tidak berbadan hukum.
23. Pemerintah adalah Menteri atau pejabat lainnya yang ditunjuk oleh Preside *Cyber crime* di Indonesia khususnya dalam (UU ITE) dapat dibagi dalam dua kategori, yaitu perbuatan yang menggunakan komputer sebagai sarana kejahatan, dan perbuatanperbuatan yang menjadikan komputer sebagai sasaran kejahatan. Kejahatan yang menggunakan komputer sebagai sarana

adalah setiap tindakan yang mendayagunakan data komputer, sistem komputer, dan jaringan komputer sebagai alat untuk melakukan kejahatan di ruang maya bukan ruang nyata. Kejahatan yang menjadikan komputer sebagai sasaran adalah setiap perbuatan dengan menggunakan komputer yang diarahkan pada data komputer, sistem komputer, atau jaringan komputer, atau ketiganya secara bersama-sama. Perbuatan tersebut dilakukan di ruang maya bukan ruang nyata, sehingga seluruh aktivitas yang dilarang oleh peraturan perundangundangan terjadi di ruang maya. [37]

[37] Undang – undang ITE No.19 tahun 2016

BAB IV

KESIMPULAN DAN SARAN

A. Kesimpulan

1. Kebijakan Hukum Pidana melalui pendekatan KUHP untuk menangggulangi tindak pidana Pembajakan Akun media sosial di Indonesia masih memiliki tumpang tindih hukum dan masih belum seutuhnya terkandung didalam produk KUHP ,terjadi banyak analogi terkait penjeratan hukum terhadap tersangka *cyber crime* seperti kasus Hacking yang dikaitkan dengan pasal pencurian yakni, pasal 368 KUHP. Juga terjadi pada pendekatan UU ITE yang belum seluruhnya mengatur berbagai tindak pidana *cybercrime* itu sendiri sehingga belum memiliki payung hukum yang pasti.
2. Penegakan Hukum *cyber crime* di Indonesia secara penal, masih mengacu pada sistem Kitab Undang-Undang Hukum Acara Pidana (KUHAP) secara mutlak. Sedangkan secara non penal dilakukan melalui metode atau pendekatan sosial seperti informasi himbauan,jalur pendidikan, pembinaan, dan juga terkait hal-hal pencegahan *cyber crime* tersebut.
3. Faktor – faktor yang mempengaruhi dalam penanggulangan tindak pidana *cyber crime* di indonesia. Upaya Preventif dalam melakukan upaya preventif ini pihak kepolisian khususnya unit *cyber crime* polisi telah melakukan berbagai upaya seperti memberikan himbauan ke masyarakat melalui media elektronik . Upaya Represif Pihak kepolisian bekerja sama dengan *stakeholder* yang ada yaitu bagaimana menangkap pelaku yang

tertangkap tangan melakukan kejahatan ataupun melalui laporan masyarakat kemudian mendatangi tempat kejadian perkara (TKP) guna melakukan penangkapan dan penahanan terhadap tersangka kasus pembajakan akun media sosial.

B. Saran

1. Dalam mewujudkan penegakan hukum perlu peran aktif aparat penegak hukum yaitu dengan dibekali keahlian khusus dalam melakukan penyidikan dan penyelidikan guna memperlancar pembuktian kejahatan dunia maya (*cyber crime*) tersebut. Peningkatan sarana prasarana dan kemampuan aparat penegak hukum di bidang teknologi dan informasi, pengetahuan, keyakinan dan pandangan yang luas hakim dalam menafsirkan hukum sebagai upaya penegakan hukum dunia mayantara di Indonesia.
2. Dalam mewujudkan penegakan hukum perlu peran aktif aparat penegak hukum yaitu dengan dibekali keahlian khusus dalam melakukan penyidikan dan penyelidikan guna memperlancar pembuktian kejahatan mayantara (*cyber crime*) tersebut. Peningkatan sarana prasarana dan kemampuan aparat penegak hukum di bidang teknologi dan informasi, pengetahuan, keyakinan dan pandangan yang luas hakim dalam menafsirkan hukum sebagai upaya penegakan hukum dunia mayantara di Indonesia. Dan perlu peningkatan kelengkapan alat teknologi informasi dan komunikasi untuk memperlancar proses pembuktian kejahatan tersebut serta peningkatan kerjasama internasional dalam rangka penegakan hukum untuk memberantas kejahatan dunia maya (*cyber crime).*

3. Terkait faktor penanggulangan *cyber crime* sejauh ini cukup memuaskan, namun diperlukan sosialisasi atau seminar dari pihak Kepolisian yang bekerja sama dengan perwakilan pemerintah melalui Menkominfo terkait *cyber crime* dan juga unsur serta klasifikasi terkait tindak pidana tersebut.

DAFTAR PUSTAKA

A. Kitab

Suci: Kitab Suci Al-Qur'an, diterbitkan oleh Diponegoro: Bandung.

B. Buku:

Abdul Manan. 2013. *Aspek –Aspek Pengubah Hukum*. Jakarta: Kencana.

Abdul wahid dan Mohammad Labib. 2015. *Kejahatan Mayantara (Cyber Crime).* Jakarta: PT Refika Aditama.

Arifiyadi Teguh. 2008. *Menjerat Pelaku Cyber Crime dengan KUHP*. Pusat Data Departemen Komunikasi dan Informatika.

Barda Nawawi Arief. 2016. *Pembaharuan Hukum Pidana dalam Perspektif Kajian Perbandingan*. Jakarta: Prena Media Group.

Budi Suhariyanto. 2012. *Tindak Pidana Teknologi Informasi (Cybercrime)*. Jakarta: RajaGrafindo Persada.

Didik M. Arief Mansyur, (dkk). 2015. *Cyber Law Aspek Hukum Teknologi Informasi*. Bandung: Reflika Aditama.

Elaw dan Pewit. 2016. *Kebijakan Publik*. Jakarta: Pustaka Prima.

Garda T. Paripurna. 2008. *Sekilas Tentang Kejahatan Transnasional*. Riset Hukum Kejahatan Transnasional.

Ida Hanifah, (dkk). 2018. *Pedoman Penulisan Tugas Akhir Mahasiswa*. Medan: UMSU Pers.

M. Ramli, Ahmad. 2006. *Cyber Law dan HAKI Dalam Sistem Hukum Indonesia*. Bandung: PT Refika Aditama.

Prasetyo, Teguh, dan Barkatullah, Abdul Halim. 2011. *Politik Hukum Pidana Kajian Kebijakan Kriminalisasi dan Dekriminalisasi.* Yogyakarta: Pustaka Pelajar.

Rahardi, H. Pudi, Hukum Kepolisian . 2014. *Kemandirian, Profesionalisme Dan Reformasi Polri*. Surabaya: Laks Bang Grafika.

Remy Syahdeini, Sutan. 2011. *Kejahatan & Tindak Pidana Komputer*. Jakarta : PT Pustaka Utama Grafiti.

Rukmini. 2014. *Aspek Hukum Pidana dan Kriminologi (Sebuah Bunga Rampai).* Bandung: P.T. Alumni.

Sehatapy, J.E. 2004. *Pisau Analisis Kriminologi*. Bandung: PT Citra Aditya Bakti.

Soerjono Soekanto. 2013. *Faktor-Faktor yang Mempengaruhi Penegakan Hukum*. Jakarta: PT. RajaGrafindo Persada.

Sudarto. 2012. *Hukum dan Hukum Pidana*. Jakarta: Rajawali Pers.

Suparni, Neniek . 2012 . *Cyber Space Problematika & Antisipasi Pengaturannya*. Jakarta: Sinar Grafika.

Widodo . 2013. "*Sistem Pemidanaan dalam Cyber Crime Alternatif Ancaman Pidana Kerja Sosial dan Pidana Pengawasan Bagi Pelaku Cyber Crime",*Yogyakarta: Laksbang Mediatama

B. Artikel, Majalah dan Jurnal Ilmiah

Ach Tahir, *"Penegakan Hukum Cyber Crime di Indonesia". Vol. 3 No. 1*

Dista Amaliah Arifah, "Kasus Cyber Crime Di Indonesia". Jurnal Bisnis dan Ekonomi. Vol. 18 No. 2, September 2011.

Hardianto Djanggih, " Kebijakan Hukum Pidana Dalam Penanggulangan Tindak Pidana Cyber Crime Di Bidang Kesusilaan". Jurnal Media Hukum. Vol. 1 No. 2, September 2013.

Ineu Rahmawati, "Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Peningkatan Cyber Defense". Jurnal Pertahanan dan Bela Negara. Vol 7 No. 2

Rudi Hermawan, "Kesiapan aparatur pemerintah dalam menghadapi cyber crime di Indonesia". Jurnal Media Hukum. Vol. 6 No. 1 , 25 September 2019.

C. Peraturan Perundang-Undangan

Kitab Undang-Undang Hukum Pidana (KUHP)

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik selanjutnya disebut Undang-Undang ITE

Undang-Undang Republik Indonesia Nomor 36 Tahun 1999 tentang Telekomunikasi