# KEJAHATAN SIBER SEBAGAI DAMPAK NEGATIF DARI PERKEMBANGAN TEKNOLOGI DAN INTERNET DI INDONESIA BERDASARKAN UNDANG-UNDANG NO. 19 TAHUN 2016 PERUBAHAN ATAS UNDANG-UNDANG NO. 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK DAN PERSFEKTIF HUKUM PIDANA

**JURNAL HUKUM**

**Diajukan Untuk Melengkapi dan Memenuhi Syarat-Syarat Untuk Memperoleh Gelar Sarjana Hukum**

**Oleh:**

**ANA MARIA F. PASARIBU**

**NIM: 130200107**

**DEPARTEMEN HUKUM PIDANA**

**FAKULTAS HUKUM**

**UNIVERSITAS SUMATERA UTARA**

**MEDAN**

**2017**

**LEMBAR PENGESAHAN**

# KEJAHATAN SIBER SEBAGAI DAMPAK NEGATIF DARI PERKEMBANGAN TEKNOLOGI DAN INTERNET DI INDONESIA BERDASARKAN UNDANG-UNDANG NO. 19 TAHUN 2016 PERUBAHAN ATAS UNDANG-UNDANG NO. 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK DAN PERSFEKTIF HUKUM PIDANA

**JURNAL**

*Disusun dan Diajukan dalam Rangka Memenuhi Persyaratan Memperoleh Gelar Sarjana Hukum pada Fakultas Hukum Universitas Sumatera Utara*

Oleh:

ANA MARIA F. PASARIBU

NIM: 130200107

Disetujui Oleh:

Penanggung Jawab,

(Dr. M. Hamdan, S.H., M.H.)

NIP. 195703261986011001

Pembimbing,

(Prof. Dr. Alvi Syahrin, S.H., M.S.)

NIP. 196303311987031001

**FAKULTAS HUKUM**

**UNIVERSITAS SUMATERA UTARA**

**MEDAN**

**2017**

**LEMBAR PENGESAHAN**

# KEJAHATAN SIBER SEBAGAI DAMPAK NEGATIF DARI PERKEMBANGAN TEKNOLOGI DAN INTERNET DI INDONESIA BERDASARKAN UNDANG-UNDANG NO. 19 TAHUN 2016 PERUBAHAN ATAS UNDANG-UNDANG NO. 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK DAN PERSFEKTIF HUKUM PIDANA

**JURNAL**

*Disusun dan Diajukan dalam Rangka Memenuhi Persyaratan Memperoleh Gelar Sarjana Hukum pada Fakultas Hukum Universitas Sumatera Utara*

Oleh:

ANA MARIA F. PASARIBU

NIM: 130200107

Disetujui Oleh:

Penanggung Jawab,

(Dr. M. Hamdan, S.H., M.H.)

NIP. 195703261986011001

Pembimbing,

(Syafruddin Hasibuan, S.H., M.Hum.)

NIP. 196305111989031001

**FAKULTAS HUKUM**

**UNIVERSITAS SUMATERA UTARA**

**MEDAN**

**2017**

**BIODATA DIRI**

Nama Lengkap : Ana Maria F. Pasaribu

Tempat, Tgl. Lahir : Siandor-andor, 08 April 1995

Jenis Kelamin : Perempuan

Status : Belum Menikah

Agama : Kristen

Kebangsaan : Indonesia

Alamat Lengkap : Jalan Terompet No. 13 Pasar 1, Padang Bulan, Kecamatan Medan Baru, Medan.

Orang Tua : H. Pasaribu

L. Manalu

Email : annamaria96am08@gmail.com

No. HP : 082168346895

**Pendidikan:**

- 2001 – 2007 : SD Negeri 175769 Hasibuan
- 2007 – 2010 : SMP Negeri 2 Pagaran
- 2010 – 2013 : SMA Negeri 1 Pagaran
- 2013 – 2017 : Program Sarjana (S-1) Ilmu Hukum Universitas Sumatera Utara

## ABSTRAK

# KEJAHATAN SIBER SEBAGAI DAMPAK NEGATIF DARI PERKEMBANGAN TEKNOLOGI DAN INTERNET DI INDONESIA BERDASARKAN UNDANG-UNDANG NO. 19 TAHUN 2016 PERUBAHAN ATAS UNDANG-UNDANG NO. 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK DAN PERSFEKTIF HUKUM PIDANA

Ana Maria F. Pasaribu[*]
Alvi Syahrin[**]
Syafruddin Hasibuan[***]

Perkembangan teknologi informasi dan arus globalisasi membawa pengaruh besar dalam berbagai bidang kehidupan manusia dunia ini saat ini. Dimulai sejak abad ke 20, perkembangan ini membawa perubahan dalam kehidupan manusia yang hidup dalam zaman yang semakin modern dengan berbagai kecanggihan alat teknologi. Dalam hal berkomunikasi, awalnya dilakukan secara langsung, kemudian melalui surat menyurat dan sekarang menggunakan alat canggih, misalnya saja Handphone (HP) sebagai alat komunikasi yang ditawarkan dengan berbagai kecanggihan lain di dalamnya. Di awali dengan lahirnya komputer yang menggunakan mesin teknologi yang canggih yang selalu dikembangkan setiap waktu guna memperbaiki kekurangan dan melakukan inovasi baru terhadap produk yang dibuat. Lahirnya teknologi sebagai perkembangan dari ilmu pengetahuan bukan hanya membawa dampak positif dalam kehidupan, tetapi juga dampak negatif yang besar, karena kejahatan teknologi lahir setelah itu. Tindak pidana yang dilakukan dalam bidang teknologi ini, diatur secara khusus dalam satu undang-undang.

Permasalahan yang timbul dari uraian di atas berbicara mengenai beberapa hal, yaitu bagaimana pengaturan hukum tentang kejahatan siber, bagaimana faktor penyebab perkembangan kejahatan siber di Indonesia, serta bagaimana upaya yang dilakukan untuk menanggulangi kejahatan siber. Metode penelitian yang digunakan adalah penelitian hukum yuridis normatif. Penelitian hukum ini adalah penelitian hukum yang meletakkan hukum sebagai bangunan sistem norma, dimana berbicara mengenai asas-asas, norma, kaidah, dari peraturan perundang-undangan, perjanjian, serta doktrin. Adapun teknik pengumpulan data menggunakan studi pustaka terhadap bahan-bahan hukum, baik bahan hukum primer, bahan hukum sekunder maupun bahan hukum tersier. Penelitian ini menggunakan bahan hukum sekunder yang diperoleh dari berbagai literatur buku dan peraturan yang berkaitan dengan penulisan skripsi ini.

Tindak pidana dalam skripsi ini diatur dalam Undang-Undang No. 19 Tahun 2016 tentang Perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Kitab Undang-Undang Hukum Pidana (KUHP). Tindak pidana kejahatan siber terjadi karena pemanfaatan teknologi yang salah oleh orang-orang yang ingin mengambil keuntungan pribadi atau kelompok yang merugikan orang lain yang juga menggunakan teknologi tersebut.



Kata kunci: Perkembangan kejahatan, Teknologi dan Internet, Kejahatan Siber



## ABSTRACT

# CYBER CRIME AS THE NEGATIVE IMPACT OF THE DEVELOPMENT OF TECHNOLOGY AND THE INTERNET IN INDONESIA IS BASED ON LAW NO.



[*] Mahasiswa Fakultas Hukum Universitas Sumatera Utara
[**] Dosen Pembimbing I
[***] Dosen Pembimbing II

# 19 OF THE YEAR 2016 CHANGES IN THE LAW NO. 11 YEAR 2008 ABOUT INFORMATION AND ELECTRONIC TRANSACTION PERSFEKTIF AND CRIMINAL LAW

Ana Maria F. Pasaribu[*]
Alvi Syahrin[**]
Syafruddin Hasibuan[***]

The development of information technology and the current globalization brings great influence in many areas of human life in this world at this time. Started since the 20th century, this development brings changes in human life which live in an age of increasingly modern sophistication with a variety of technology tools. In terms of communicating, originally done directly, then through correspondence and now use sophisticated tools, for example Mobile (HP) as a means of communication offered by many others in it. At the start with the birth of the computer using sophisticated technology that has always developed each time in order to remedy the shortcomings and innovating new products are created. Inception technologies as the development of science not only bring positive impact in your life, but also a big negative impact, because evil technology born after that. Criminal acts performed in the fields of technology, is set specifically in one act.

The problems arising from the above description talks about a few things, how the arrangements law about cyber crime, how the development of the cause of the cyber crime factor in Indonesia, as well as how the efforts made to tackling cyber crime. The research method used is the juridical normative legal research. This is a legal research legal research that lays the legal system building of norms, which talks about the principles, norms, rules, and regulations, of agreements, as well as doctrine. As for the data collection technique to use library materials against the law, both primary legal materials, legal secondary materials as well as legal materials tertiary. This study uses secondary law obtained from different literature books and regulations pertaining to the writing of this thesis.

The crime in this thesis is regulated in Act No. 19 of the year 2016 about changes in the law No. 11 Year 2008 about information and Electronic Transaction law and the criminal law (the CRIMINAL CODE). Cyber crime criminal acts occurred because the wrong technology utilization by those who want to take advantage of private or group that harms other people who also use the technology.

Key words: Development crime, Technology and Internet, Cyber crime

## I. PENDAHULUAN

### A. Latar Belakang

Perkembangan teknologi informasi sekarang ini telah menjadi pedang bermata dua, karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi sarana efektif terjadinya perbuatan melawan

[*] College Students Of The Law Faculty Of The University Of North Sumatra
[**] Lecturer Supervisor I
[***] Lecturer Supervisor II

hukum. Dengan terjadinya perbuatan-perbuatan melawan hukum tersebut, maka ruang lingkup hukum harus diperluas untuk menjangkau perbuatan-perbuatan tersebut. Teknologi pada dirinya sendiri adalah tidak baik maupun tidak jahat, dan menyalahkannya seperti mencela gunung es karena telah menenggelamkan kapal Titanic. Kecanggihan teknologi dan perkembangan sistem transportasi dan komunikasi yang menghasilkan ketergantungan antar bangsa telah mengakibatkan menciutnya dunia ini, sehingga menjelma menjadi suatu desa sejagat. Tidak ada satu bagian dari dunia ini pun yang terlepas dari pengamatan dan pemantauan. Kita telah atau sedang dimanjakan oleh produk teknologi, karena kita dengan gampang bisa mengunjungi belahan bumi lain dari yang kita tempati dan menjalin komunikasi global, atau bercengkerama dengan orang lain, mencari pacar baru, dan bahkan belajar bagaimana menjadi teroris, menjadi anggota jaringan mafia, atau menjadi bagian dari kejahatan terorganisir[1].

Munculnya kejahatan baru sebagai akibat dari perkembangan arus teknologi di dunia melalui globalisasi juga berkembang pesat seperti pesatnya perkembangan teknologi itu sendiri, diantaranya kejahatan *manipulasi data, spionase, sabotase, provokasi, money laundering, hacking, pencurian software, penipuan on-line dan berbagai macamnya*. Bahkan pemerintah belum punya kemampuan yang cukup untuk mengimbangi kejahatan melalui internet ini sehingga sulit untuk mengendalikannya. Dengan munculnya beberapa kasus kejatan siber (*cyber crime*) di Indonesia telah menjadi ancaman stabilitas keamanan dan ketertiban nasional dengan eskalatif yang cukup tinggi. Pemerintah dan perangkatnya belum mampu mengimbangi teknik kejahatan yang dilakukan dengan teknologi komputer khususnya di jaringan internet dan internet (*internetwork)*. Perbuatan melawan hukum *cyber* sangat tidak mudah diatasi dengan mengandalkan hukum positif konvensional, karena berbicara mengenai kejahatan itu tidak dapat dilepaskan dari 5 (lima) faktor yang saling berkaitan, yaitu pelaku kejahatan, korban kejahatan, reaksi sosial atas kejahatan dan hukum. Hukum memang menjadi instrumen penting dalam pencegahan dan penanggulangan kejahatan. Akan tetapi, untuk membuat suatu ketentuan hukum terhadap bidang hukum yang berubah sangat cepat, seperti teknologi informasi ini bukanlah hal yang mudah. Disinilah sring kali hukum (peraturan) tempak cepat menjadi usang manakala mengatur bidang yang mengalami perubahan yang cepat, sehingga situasinya seperti mengalami kekosongan hukum (*vacuum recht)*. Terhadap kejahatan di internet atau *cyber crime* ini tampaknya memang terjadi kekosongan hukum[2].

---

[1] Abdul Wahid & Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)*, Bandung: PT Refika Aditama, 2005, hlm. 8.

[2]Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi Pengaturan dan Celah Hukumnya*, Jakarta: PT RajaGrafindo Persada, 2012 , hlm. 3.

## B. Permasalahan

Adapun yang menjadi permasalahan adalah:

1. Bagaimanakah pengaturan tentang kejahatan siber di Indonesia?
2. Bagaimanakah faktor penyebab perkembangan kejahatan siber di Indonesia?
3. Upaya apakah yang dapat digunakan untuk menanggulangi kejahatan siber?

## II. PENGATURAN TENTANG KEJAHATAN SIBER

### A. Sejarah Lahirnya Undang-Undang Nomor 19 Tahun 2016 Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

1. Rekomendasi Perserikatan Bangsa-Bangsa (PBB) Tentang Kriminalisasi Cyberspace

Kejahatan siber merupakan keseluruhan bentuk kejahatan yang ditujukan terhadap komputer, jaringan komputer dan para penggunanya, dan bentuk-bentuk kejahatan tradisional yang menggunakan atau dengan bantuan komputer. Dapat disimpulkan bahwa kejahatan siber adalah setiap aktivitas seseorang, sekelompok orang, badan hukum yang menggunakan komputer sebagai sarana melakukan kejahatan, dan komputer sebagai sasaran kejahatan. Kejahatan tersebut adalah bentuk-bentuk kejahatan yang bertentangan dengan peraturan perundang-undangan. Indonesia sebagai negara hukum, selalu mengutamakan semua kegiatan kenegaraan dan kemasyarakatan didasarkan pada ketentuan hukum. Karena hal itu, Indonesia selalu berusaha untuk melakukan pembaharuan Hukum Pidana, salah satunya dengan menerbitkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Karena penyelenggaraan kegiatan dalam bidang teknologi yang berbasis komputer sangat penting bagi masyarakat dan rawan melakukan pelanggaran hak asasi manusia, maka dalam melakukan kriminalisasi, Indonesia dapat memperhatikan himbauan, anjuran, rekomendasi dari Perserikatan Bangsa-Bangsa.

Berkaitan dengan kriminalisasi terhadap perbuatan yang berkategori kejahatan siber (*cyber crime)*, PBB menentukan bahwa ketentuan pidana dalam perbuatan perundang-undangan setiap negara wajib melakukan perumusan ketentuan pidana secara jelas (*lex certa)*. Dimana hal ini dilakukan dalam rangka memberikan perlindungan hukum bagi rakyat Indonesia, memberikan kejelasan, menjamin kepastian ketentuan hukum, agar tidak terjadi ambiguitas penafsiran. Setiap negara dihimbau agar melakukan aksi nasional pemberantasan kejahatan siber secara bersama-sama melalui kerjasama karena kejahatan siber sering dilakukan lintas negara. Kebijakan penanggulangan kejahatan siber yang diharapkan oleh kongres PBB adalah melakukan kriminalisasi terhadap penyalahgunaan teknologi informasi. Selanjutnya dalam uraian PBB dikemukakan bahwa ketentuan hukum pidana tersebut hanya boleh dilakukan dalam kasus-kasus serius, terutama yang berkaitan dengan data yang sangat sensitif atau informasi rahasia yang dilindungi oleh hukum.

Berdasarkan pada pencerahan dari PBB tersebut dan juga karena kebutuhan bangsa Indonesia untuk membangun, sejak 21 April 2008, bangsa Indonesia memasuki babak baru dalam pengaturan mengenai penggunaan teknologi informasi dan transaksi

elektronik yaitu adanya pengesahan Rancangan Undang-Undang Tentang Informasi dan Transaksi Elektronik yang kemudian diundangkan menjadi Undang-Undang Negara Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (LN Republik Indonesia Tahun 2008 Nomor 58; TLN Republik Indonesia Nomor 4843)[3]. Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (selanjutnya disingkat UU-ITE) merupakan undang-undang pertama di Indonesia yang secara khusus mengatur tindak pidana siber, undang-undang ini memiliki sejarah tersendiri dalam pembentukan dan pengundangannya. Rancangan UU-ITE mulai dibahas sejak Maret 2003 oleh Kementrian Negara Komunikasi dan Informatika dengan nama Rancangan Undang-Undang Informasi Komunikasi dan Transaksi Elektronik. Pada awalnya, RUU ini merupakan penyatuan dua rancangan undang-undang yang disusun oleh dua kementrian yaitu Departemen Perhubungan dengan Departemen Perindustrian dan Perdagangan, bekerja sama dengan Lembaga Kajian Hukum dan Teknologi Universitas Indonesia, Tim dari Fakultas Hukum Universitas Padjajaran, serta Tim Asistensi dari Institut Teknologi Bandung. Kemudian, berdasarkan surat Presiden RI. No. R. /70/Pres/9/2005 tanggal 5 September 2005, naskah UU-ITE secara resmi disampaikan kepada DPR RI. Pada tanggal 21 April 2008, undang-undang ini disahkan; dengan demikian proses pengundangan UU-ITE telah berlangsung sekitar lima tahun. Oleh karena itu, UU-ITE terdiri dari 13 Bab dan 54 Pasal ini merupakan undang-undang yang relatif baru baik dari segi pengundangannya dan juga segi materi yang diatur. Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik tersebut multak diperlukan bagi negara Indonesia, karena saat ini Indonesia merupakan slah satu negara yang telah menggunakan dan memanfaatkan teknologi informasi secara luas dan efisien, dan secara faktual belum banyak memiliki ketentuan hukum terutama dari aspek hukum pidana.

Dua muatan besar yang diatur dalam UU-ITE ialah mengenai pengaturan transaksi elektronik dan mengenai tindak pidana siber. Materi UU-ITE tersebut merupakan implementasi dari beberapa prinsip ketentuan internasional, cakupan materi UU-ITE, secara umum antara lain berisi tentang informasi dan dokumen elektronik, pengiriman dan penerimaan surat elektronik, tanda tangan elektronik, sertifikat elektronik, penyelenggaraan sistem elektronik, transaksi elektronik, hak atas kekayaan intelektual dan privasi, serta ketentuan pidana yang berkaitan dengan pemanfaatan informasi dan transaksi elektronik.

2. Tindak Pidana dalam Cybercrime dalam Undang-Undang Nomor 19 Tahun 2016 perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

[3] Josua Sitompul, op.cit. hlm. 135-136.

Dalam perspektif yuridis, khususnya dalam ruang lingkup hukum pidana, banyak terobosan yang penting dalam UU-ITE tersebut, antara lain sebagai berikut;

a) Penegasan secara cermat beberapa istilah yang berkaitan dengan dunia mayantara, misalnya pengertian komputer, data, transaksi elektronik, dan lain-lain;
b) Tindak pidana yang diatur banyak yang sudah merujuk pada ketentuan yang diatur dalam *Convention on Cyber crime*, baik tindak pidana yang menjadikan komputer sebagai sasaran maupun menggunakan komputer sebagai alat kejahatan;
c) Beberapa kejahatan tradisional yang menggunakan komputer, misalnya perjudian, pornografi, perbuatan tidak menyenangkan, pencemaran nama baik, penghinaan dan lain-lain yang sudah dijadikan tindak pidana;
d) Ancaman bagi setiap orang yang melakukan tindak pidana berupa jenis pidana (*strafsourt)* menggunakan sistem ancaman kumulatif-alternatif, dan lama pemidanaan atau besarnya ancaman denda (*strafmaad)* cukup tinggi dibandingkan dengan ancaman dalam hukum pidana konvensional;
e) Tanda tangan elektronik (*digital signature)* diakui sebgai alat bukti yang memiliki kekuatan hukum yang sama dengan tanda tangan konvensional yang menggunakan tinta basah dan bermaterai. Surat elektronik (*e-mail)*, *website*, dan perangkat-perangkat virtual lainnya sudah diakui sebagai alat bukti yang sah sehingga dapat digunakan sebgai alat bukti yang sah dalam proses peradilan pidana, selain sebagaimana diatur dalam Pasal 184 KUHAP;
f) Jika korporasi melakukan tindak pidana juga diancam dengan pidana, ahkan ancaman dendanya lebih berat dibandingkan dengan dilakukan manusia;
g) Ruang lingkup keberlakuan UU-ITE adalah untuk setiap orang yang melakukan perbuatan hukum di wilayah Indonesia maupun di luar negeri yang memiliki akibat hukum di Indonesia.

## B. Kejahatan Siber ditinjau dari Kitab Undang-Undang Hukum Pidana

1. Pengertian kejahatan dalam Hukum Pidana

Secara empiris defenisi kejahatan dapat dilihat dari dua prespektif, *pertama* adalah kejahatan dalam perspektif yuridis dimana kejahatan dirumuskan sebagai perbuatan yang oleh negara diberi pidana, pemberian pidana ini dimaksudkan untuk mengembalikan keseimbangan yang terganggu akibat perbuatan itu. Perbuatan atau kejahatan yang demikian dalam ilmu Hukum Pidana biasa disebut dengan Tindak Pidana.

*Kedua,* kejahatan dalam perpektif sosiologis (kriminologis) merupakan suatu perbuatan yang dari sisi sosiologis merupakan kejahatan, tapi dari segi yuridis bukan suatu kejahatan[4].

Van Bammelen merumuskan, kejahatan adalah tiap kelakuan yang bersifat tidak susila dan merugikan, menimbulkan begitu banyak ketidaktenangan dalam suatu masyarakat tertentu, sehingga masyarakat berhak mencelanya dan menyatakan penolakannya atas kelakuan itu dalam bentuk nestapa dengan sengaja diberikan karena kelakuan tersebut. Menurut W.A. Bonger, kejahatan adalah perbuatan yang sangat anti sosial yang memperoleh tantangan dengan sadar dari negara berupa pemberian penderitaan (hukuman)[5].

2. Ruang Lingkup Berlakunya Hukum Pidana dalam Kejahatan Siber

Kitab Undang-Undang Hukum Pidana (KUHP) Indonesia telah memberikan pengaturan yang jelas mengenai batas-batas berlakunya aturan perundang-undangan hukum pidana. Hal ini diatur dalam Bab I Buku Kesatu KUHP yang terdiri dari 9 pasal mulai dari Pasal 1 sampai Pasal 9. Dalam Pasal 1 KUHP diatur mengenai batas-batas berlakunya hukum pidana menurut waktu atau saat terjadinya perbuatan. Sedangkan Pasal 2 sampai dengan Pasal 9 KUHP mengatur mengenai batas-batas berlakunya perundang-undangan hukum pidana menurut tempat terjadinya perbuatan. Pada dasarnya, ada dua hal yang menyebabkan pengaturan dalam KUHP memiliki daya jangkau yang terbatas, yaitu:

a) Keterbatasan pengaturan mengenai jenis-jenis tindak pidana

   Hal ini sangat wajar terjadi mengingat suasana yang mempengaruhi pada saat penyusunan KUHP kita sangat jauh berbeda dengan kondisi sekarang yang sarat dengan perkembangan teknologi informasi yang pesat.

b) Keterbatasan dalam pengaturan mengenai pelaku tindak pidana

   Dalam era teknologi informasi seperti sekarang ini penentuan siapa yang dapat dikualifikasikan sebagai pelaku tindak pidan lebih kompleks sifatnya.

3. Hukum Pidana di Bidang Kejahatan Siber di Indonesia

Sebelum diberlakukan UU-ITE, pengadilan menggunakan ketentuan dalam mengadili kejahatan siber adalah KUHP dan ketentuan dalam undang-undang di luar KUHP yang mengatur tindak pidana. Ketentuan dalam KUHP yang digunakan untuk menangani kejahatan siber adalah ketentuan tentang Pemalsuan (Pasal 263-276), Penipuan (Pasal 378-395), Perusakan Barang (Pasal 407-412). Sedangkan ketentuan

[4] Abdul Wahid & Mohammad Labib,op.cit, hlm .37-38.
[5] M.Ridwan & Ediwarman, *Asas-asas Kriminologi,* Medan: USU Press,1994,hlm.1-2.

perundang-undangan di luar KUHP yang dapat digunakan dalam menangani kejahatan siber (hukum pidana materil atau formil) antara lain sebagai berikut;

a) Undang-Undang RI No. 3 Tahun 1971 tentang Pemberantasan Tindak Pidana Korupsi, yang kemudian diganti dengan UU RI No. 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi, dan terakhir diubah dengan UU RI No. 20 Tahun 2001 tentang Perubahan atas UU RI No. 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi;
b) UU RI No. 6 Tahun 1982 tentang Hak Cipta, kemudian diubah melalui UU RI No. 7 Tahun 1987 tentang Perubahan atas UU RI No. 6 Tahun 1982 tentang Hak Cipta. Akhirnya kedua UU tersebut diganti dengan UU RI No. 19 Tahun 2002 tentang Hak Cipta, UU RI No. 28 Tahun 2014 tentang Hak Cipta pengganti UU RI No. 19 Tahun 2002 tentang Hak Cipta;
c) UU RI No. 7 Tahun 1992 tentang Perbankan *junto* UU No. 10 Tahun 1998 tentang Perbankan;
d) UU RI No. 5 Tahun 1999 tentang Persaingan Usaha;
e) UU RI No. 36 Tahun 1999 tentang Telekomunikasi;

## C. Kejahatan Siber dan Teknologi

1. Istilah dan Pengertian

Istilah *cyber crime* (kejahatan siber) saat ini merujuk pada suatu tindakan kejahatan yang berhubungan dengan dunia maya (*cyber space*) dan tindakan kejahatan yang menggunakan komputer. Secara umum, yang dimaksud kejahatan komputer atau kejahatan di dunia siber adalah "*upaya memasuki atau menggunakan fasilitas komputer tanpa ijin dan dengan melawan hukum dengan atau tanpa menyebabkan perubahan dan atau kerusakan pada fasilitas komputer yang dimasuki atau digunakan tersebut*"[6]. Ruang lingkup cakupan kejahatan siber yaitu, (a) pembajakan; (b) penipuan; (c) pencurian; (d) pornografi; (e) pelecehan; (f) pemalsuan; (g) pemfitnahan; (h) perjudian; dan lainnya.

Berdasarkan literatur serta praktiknya, kejahatan siber memiliki beberapa karakteristik, yaitu;

a) Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis tersebut terjadi dalam ruang/wilayah siber/*cyber space*, sehingga tidak dapat dipastikan yurisdiksi negara mana yang berlaku terhadapnya.
b) Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang terhubung dengan internet.

[6] Dikdik M.Arif Mansur & Elisatris Gultom, op.cit. hlm. 8.

c) Perbuatan tersebut mengakibatkan kerugian materil maupun immateril yang cenderung lebih besar dibandingkan dengan kejahatan konvensional.
d) Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya.
e) Perbuatan tersebut sering dilakukan secara transnasional/melintasi batas negara.

2. Bentuk-bentuk Kejahatan Siber

Beberapa bentuk kejahatan yang berhubungan erat dengan penggunaan teknologi informasi yang berbasis utama komputer dan jaringan telekomunikasi ini, dalam beberapa literatur dan praktiknya dikelompokkan dalam beberapa bentuk, antara lain:[7]

a) Unauthorized Acces Computer System and Service

Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa ijin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya.

b) Illegal Contents

Merupakan kejahatan dengan menggunakan data atau informasi ke internet tentang suatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum.

c) Data Forgery

Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* melalui internet.

d) Cyber Espionage

Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer pihak sasaran.

e) Cyber Sabotage and Extortion

Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.

f) Offense Against Intellectual Property

Kejahatan ini ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di internet. Contoh, peniruan tampilan pada *web page* suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di internet yang ternyata merupakan informasi rahasia dagang orang lain dan sebagainya.

[7] Dikdik M.Arif Mansur & Elisatris Gultom, op.cit. hlm. 9.

## D. Jenis-jenis Kejahatan Siber

Kejahatan siber yang diatur dalam UU ITE diatur dalam Bab VII tentang perbuatan yang dilarang; perbuatan-perbuatan tersebut dikategorikan menjadi beberapa kelompok, yaitu;

1. Akses Tidak Sah *(Illegal Access)*
2. Penyadapan atau Intersepsi Tidak Sah (*Intersepting)*
3. Gangguan Terhadap Data Komputer (*Data Interference) &* Gangguan terhadap Sistem Komputer (*System Interference)*

## III. FAKTOR PERKEMBANGAN KEJAHATAN SIBER

### A. Faktor Perkembangan Teknologi dan Internet yang Cepat

Kemajuan teknologi dan internet yang merupakan hasil budaya manusia di samping membawa dampak positif, juga menimbulkan dampak negatif terhadap perkembangan manusia dan peradabannya. Dampak negatif ini berkaitan dengan dunia kejahatan. Salah satu kejahatan yang ditimbulkan adalah kejahatan yang berkaitan dengan dunia internet, dalam istilah asing disebut dengan *Cyber Crime* (kejahatan siber)[8].

Di Indonesia, perkembangan kejahatan siber sudah mencapai tingkat yang memprihatinkan. Akibatnya, Indonesia dijuluki dunia sebagai negara kriminal internet. Pada tahun 2002, pihak Kepolisian Indonesia telah mengungkap 109 kasus tindak pidana Teknologi Informasi (TI) yang dilakukan oleh 124 orang tersangka yang merupakan warga negara Indonesia yang melakukan berbagai aksinya di berbagai kota di Indonesia. Secara garis besar, kejahatan yang berkaitan dengan teknologi informasi ini dibagi menjadi dua. Pertama, kejahatan yang bertujuan untuk merusak atau menyerang sistem atau jaringan komputer. Kedua, kejahatan yang menggunakan komputer atau internet sebagai alat bantu dalam melancarkan kejahatan. Dalam beberapa literatur dan siitus-situs yang mengetengahkan kejahatan siber, berpuluh jenis kejahatan siber yang terjadi. Yang termasuk dalam kategori kejahatan umum yang difasilitasi teknologi antara lain penipuan kartu kredit, penipuan bursa efek, penipuan perbankan, pornografi anak, perdagangan narkoba, serta terorisme. Sedangkan kejahatan yang menggunakan teknologi informasi adalah *defacing*, *cracking*, ataupun *phreaking*.

### B. Faktor Sosial dan Ekonomi

Kehadiran teknologi dan internet, walaupun masih merupakan industri baru dan masih dalam fase pertumbuhan telah mengokohkan keyakinan tentang pentingnya teknologi dalam pencapaian tujuan finansial. Teknologi dan internet dapat dimanfaatkan untuk melakukan transaksi perdagangan, dan banyak situs di internet yang menawarkan jasa pemasangan iklan. Disamping manfaat yang diperoleh atas penggunaan teknologi dan internet ini, ada kenyataan bahwa para pengusaha baru mulai membuat *net companies* setelah terinspirasi dari keberhasilan yang diraih oleh para pengusaha digital di berbagai negara maju. Perkembangan teknologi dan internet ini terjadi diberbagai bidang kehidupan manusia terutama dibidang sosial dan ekonomi. Pergaulan hidup masyarakat modern saat ini lebih banyak di dunia virtual/maya dibandingkan dengan berinteraksi secara langsung dengan manusia lain. Pergeseran ini membuat masyarakat perlahan mulai meninggalkan dunia nyata dan menghabiskan waktu dengan berinteraksi dengan orang

[8] Ibid

lain melalui internet, hal ini terjadi bahkan lintas negara dari negara satu ke negara lain yang saling terhubung. Dibidang ekonomi, saat ini di Indonesia sudah banyak berkembang berbagai transaksi melalui jaringan internet yang lebih memudahkan suatu transaksi tanpa bertemu secara langsung[9].

Banyak aktivitas bisnis yang berkembang pada tahun 2000-an, dinamika perdagangan dan bisnis industri perbankan melahirkan model transaksi yang eksistensinya lahir karena kemajuan teknologi dan internet di era globalisasi, yaitu *electronic commerce transaction (e-commerce)*. *E-commerce* merupakan model bisnis modern yang *non-face* dan *non-sign* yang melakukan pertukaran data melalui internet dimana kedua belah pihak yaitu penjual dan pembeli melakukan transaksi. Saat ini, *e-commerce* sudah seperti gaya hidup di mana-mana termasuk di Indonesia. Berkembangnya *e-commerce* di ikuti pula dengan berkembangnya kejahatan teknologi canggih ini, dikenallah istilah *cybank crime, internet banking crime, online business crime, cyber/electronic money laudering*, dan lain-lain. Kejahatan *e-commerce* tidak hanya ditujukan pada pencurian data, tetapi juga pada penggunaan, pengungkapan, penghapusan, perusakan data, atau bertujuan untuk menggangu atau merusak sistem transfer. Kejahatan yang terjadi pada transaksi ini tentu sangat merugikan, dari aspek ekonomi, perbankan, politik dan keamanan nasional[10].

## C. Faktor Penegakan Hukum

Rasa aman tentu akan dirasakan oleh pelaku kejahatan siber saat melakukan aksinya, hal ini terjadi karena internet lazim dipergunakan ditempat tertutup seperti rumah, kamar, tempat kerja, perpustakaan dan lain-lain. Aktivitas ini akan membuat orang lain sulit untuk diketahui oleh orang lain, sehingga orang lain jarang mengetahui bahwa seseorang itu sedang melakukan suatu tindak pidana kejahatan siber. Hal ini tentu berbeda dengan kejahatan yang bersifat konvensional yang mana pelaku dapat diketahui karena melakukan aksinya secara fisik. Disamping itu, pelaku juga dapat menghapus jejak kejahatan yang telah dilakukannya mengingat internet menyediakan fasilitas untuk menghapus data/file yang ada. Akibatnya pelaku sulit untuk ditangkap karena aparat penegak hukum sulit untuk menemukan alat bukti. Faktor penegak hukum juga sering menjadi penyebab dari berkembang kejahatan siber itu. Hal ini dilatarbelakangi oleh sedikitnya aparat penegak hukum yang memahami tentang seluk beluk teknologi informasi, sehingga saat pelaku ditangkap mereka kesulitan untuk mencari bukti-bukti untuk menjerat pelaku terlebih apabila kejahatan siber yang dilakukan memiliki sistem

[9] Dikdik M. Arief Mansur & Elisatris Gultom, op.cit, hlm. 143.

[10] Barda Nawawi Arief, *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di* Indonesia, Jakarta: PT RajaGrafindo Persada, 2006. hlm. 52.

pengoperasian yang sulit untuk dimengerti. Maka peningkatan kualitas dari aparat penegak hukum sangat diperlukan untuk dapat menangani berbagai kejahatan siber yang saat ini marak terjadi dan berkembang[11].

[11] *Ibid*

## IV. UPAYA PENANGGULANGAN KEJAHATAN SIBER

### A. Sarana Penal (Kebijakan Penal)

Kebijakan Penal (kebijakan dalam hukum pidana) adalah salah satu kebijakan dalam penanggulangan kejahatan dengan menggunakan hukum pidana.. kebijakan tersebut dioperasikan dengan cara menerapkan hukum pidana, yaitu pidana materiil, hukum formil dan penitentier dalam masyarakat. Dalam Kongres PBB ke-4 yang berlangsung di Kyoto disepakati bahwa usaha pencegahan kejahatan, termasuk penerapan hukum pidana merupakan bagian integral dari rencana pembangunan nasional[12]. Kebijakan hukum pidana pada hakikatnya merupakan usaha untuk mewujudkan peraturan perundang-undangan pidana agar sesuai dengan keadaan pada waktu tertentu (*ius constitutum)* dan masa yang akan datang (*ius constituendum)*[13]. Dalam upaya menanggulangi kejahatan siber, resolusi Kongres PBB VIII/1990 mengenai *computer related crimes* mengajukan beberapa kebijakan antara lain:

1. Menghimbau negara anggota untuk mengintensifkan upaya-upaya penanggulangan penyalahgunaan komputer lebih efektif dengan mempertimbangkan langkah-langkah berikut;
   a) Melakukan modernisasi hukum pidana meateriil dan hukum acara pidana
   b) Mengembangkan tindakan-tindakan pencegahan dan pengamanan komputer
   c) Melakukan langkah-langkah untuk membuat peka warga masyarakat, aparat penegak hukum, dan pengadilan terhadap pentingnya pencegahan kejahatan yang berhubungan dengan komputer
   d) Melakukan upaya-upaya pelatihan bagi para hakim, penegak hukum, pejabat mengenai kejahatan dibidang ekonomi dan kejahatan siber
   e) Memperluas *rules of ethics* dalam penggunaan komputer dan mengajarkannya melalui kurikulum informatika
   f) Mengadopsi kebijakan perlindungan korban sesuai deklarasi PBB mengenai korban, dan mengambil langkah-langkah untuk mendorong korban melaporkan adanya kejahatan siber.
2. Menghimbau agar negara anggota meningkatkan kegiatan internasional dalam upaya penanggulangan kejahatan siber,
3. Merekomendasikan kepada Komite Pengendalian dan Pencegahan Kejahatan PBB untuk;
   a) Menyebarluaskan pedoman dan standar untuk membantu negara anggota menghadapi kejahatan siber ditingkat nasional, ragional dan internasional,

---

[12] Widodo, op.cit, hlm. 188.

[13] Lilik Mulyadi, *Bunga Rampai Hukum Pidana Prespektif, Teoritis dan Praktik*, Bandung: PT. Alumni, 2008, hlm. 390.

b) Mengembangkan penelitian dan analisis lebih lanjut guna menemukan cara-cara baru menghadapi permasalahan kejahatan siber dimasa mendatang,
c) Mempertimbangkan kejahatan siber sewaktu meninjau pengimplementasian perjanjian ekstradisi dan bantuan kerjasama dibidang penangulangan kejahatan[14].

**B. Sarana Non Penal (Kebijakan Non Penal)**

Kebijakan non penal dapat ditempuh dengan cara memperbaiki perekonomian nasional, melakukan pendidikan budi pekerti kepada setiap orang baik secara formal maupun secara non formal terutama kepada pihak yang rentan melakukan kejahatan, memperbaiki sistem kesehatan mental masyarakat, mengefektifkan kerjasama internasional dalam pemberantasan kejahatan siber, memperbaiki sistem pengamanan komputer, serta mengefektifkan hukum administrasi dan hukum perdata yang berhubungan dengan penyelenggaraan sistem dan jaringan komputer. Hal ini senada dengan *Convention on Cyber Crime*, bahwa kerjasama internasional yang perlu dilakukan dalam rangka penanggulangan kejahatan siber adalah perjanjian ekstradisi, *mutual assistence in criminal matters*, pemberian informasi secara spontan, dan pembentukan jaringan yang dikelola oleh tenaga profesional dalam rangka menjamin terselenggaranya bantuan secepatnya untuk investigasi dan peradilan untuk mengumpulkan alat bukti elektronik. Bantuan-bantuan tersebut berupa fasilitas atau bantuan lain, dengan syarat dan ijin oleh hukum nasional masing-masing negara, dalam hal ini diatur pula pertanggungjawaban korporasi, baik dalam hukum pidana maupun dalam hukum perdata dan hukum administrasi.

[14] Barda Nawawi Arief, *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia*, op.cit, hlm. 3.

# V. KESIMPULAN DAN SARAN

## A. Kesimpulan

Berdasarkan pembahasan pada Bab sebelumnya, maka kesimpulan yang dapat diambil sebagai berikut:

1. Pengaturan mengenai tindak pidana kejahatan siber di Indonesia diatur dalam Undang-Undang No. 19 Tahun 2016 Perubahan Atas Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Undang-Undang ini lahir sebagai dasar hukum dalam penegakan tindak pidana kejahatan siber, karena Indonesia membutuhkan aturan ini mengingat Indonesia termasuk pengguna teknologi dan informasi yang setiap tahun bertambah penggunanya. Untuk itu, peraturan ini secara khusus dibuat guna mengatasi kejahatan siber yang sering terjadi di tanah air dalam skala yang besar. KUHP tidak memuat secara khusus aturan mengenai kejahatan ini, maka UU-ITE inilah yang mengaturnya dengan sanksi pidananya.
2. Faktor perkembangan teknologi, internet, sosial, ekonomi dan penegakan hukum berperan besar dalam melahirkan berbagai kejahatan siber di Indonesia. Teknologi dan internet sendiri sudah menjadi kebutuhan masyarakat modern saat ini, hal ini juga mempengaruhi kehidupan sosial dan ekonomi masyarakat dan global. Faktor penegakan hukum yang tidak dapat mengikuti perkembangan kejahatan, juga mempengaruhi perkembagan kejahatan itu sehingga semakin kompleks.
3. Sarana dan kebijakan yang ada diharapkan dapat mengatasi kejahatan teknologi tersebut, walaupun tidak bisa sepenuhnya bisa mengatasi kejahan tersebut. Peningkatan sarana dan kebijakan dalam menanggulangi kejahatan ini sangat dibutuhkan.

## B. Saran

Saran yang dapat penulis berikan berdasarkan bahasan dalam skripsi ini, ada beberapa yaitu:

1. Kepada pemerintah, agar semakin jeli melihat perkembangan kejahatan teknologi yang berkembang saat ini dan peraturan yang ada bisa disesuaikan dengan kebutuhan dalam penegakan kejahatan yang semakin kompleks.
2. Kepada pemerintah juga diharapkan agar aktif dalam mensosialisasikan mengenai perkembangan kejahatan dan sanksi pidana yang akan menjerat apabila terjadi pelanggaran. Sosialisasi ini dapat menyadarkan masyarakat untuk taat pada peraturan yang ada, khususnya dibidang teknologi.

3. Kepada pengguna teknologi dan internet, diharapkan menggunakannya dengan baik agar tidak menimbulkan kerugian bagi orang lain. Khususnya pengguna media sosial, agar jangan menggunakannya sebagai sarana melakukan kejahatan.

# DAFTAR PUSTAKA

## BUKU


Mansur, Dikdik M. Arif & Elisatris Gultom, 2005, *Cyber Law (Aspek Hukum Teknologi Informasi)*, PT Refika Aditama, Bandung.

Mulyadi, Lilik, 2008, *Bunga Rampai Hukum Pidana Prespektif, Teoritis dan Praktik*, PT. Alumni, Bandung.

Nawawi Arief, Barda, 2006, *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di* Indonesia, PT RajaGrafindo Persada, Jakarta.

Ridwan, M & Ediwarman, 1994, *Asas-asas Kriminologi*, USU Press, Medan.

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

Suhariyanto, Budi, 2012, *Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi Pengaturan dan Celah Hukumnya*, PT RajaGrafindo Persada, Jakarta.

Wahid, Abdul & Mohammad Labib, 2005, *Kejahatan Mayantara (Cyber Crime)*, PT Refika Aditama, Bandung.

Widodo, 2013, *Aspek Hukum Pidana Kejahatan Mayantara*, Aswaja Pressindo, Yogyakarta.


## Undang-Undang


Kitab Undang-Undang Hukum Pidana