FUNGSI KEPOLISIAN DALAM PENANGGULANGAN TINDAK PIDANA SIBER DI POLDA SULAWESI BARAT

TESIS

REYNALDI EKO SAPUTRA
NIM : 4616101043

Untuk Memenuhi Salah Satu Persyaratan Guna Memperoleh Gelar Magister Hukum

PROGRAM STUDI ILMU HUKUM
PROGRAM PASCASARJANA
UNIVERSITAS BOSOWA MAKASSAR
2019

HALAMAN PENGESAHAN

J u d u l	:	**FUNGSI KEPOLISIAN DALAM PENANGGULANGAN TINDAK PIDANA SIBER DI POLDA SULAWESI BARAT**
Nama Mahasiswa	:	**REYNALDI EKO SAPUTRA**
NIM	:	**4616101043**
Program Studi	:	**Ilmu Hukum**

Menyetujui

Komisi Pembimbing

Pembimbing I	Pembimbing II
Dr. H. Abdul Salam Siku, S.H., M.H.	**Dr. Baso Madiong, S.H., M.H.**
NIDN. 0025075902	**NIDN. 0909096702**

Mengetahui :

Direktur Program Pascasarjana	Ketua Program Studi Ilmu Hukum
Prof. Dr. Ir. Batara Surya, M.Si.	**Dr. Baso Madiong, S.H., M.H.**
NIDN. 0913017402	**NIDN. 0909096702**

HALAMAN PENERIMAAN

Pada Hari / Tanggal : Jumat, 25 Januari 2019

Tesis atas Nama : **REYNALDI EKO SAPUTRA**

NIM : **4616101043**

Telah Diterima oleh Panitia Ujian Tesis Program Pascasarjana untuk memenuhi salah satu syarat guna memperoleh gelar Magister Hukum pada Program Studi Ilmu Hukum.

PANITIA UJIAN TESIS

Ketua : Dr. H. Abdul Salam Siku, S.H., M.H. (…….)
(Pembimbing I)

Sekretaris : Dr. Baso Madiong, S.H., M.H. (…….)
(Pembimbing II)

Anggota Penguji : 1. Dr. Yulia A. Hasan, S.H., M.H. (…….)

2. Dr. Zulkifli Makkawaru, S.H., M.H. (…….)

Makassar, 25 Januari 2019
Direktur,

Prof. Dr. Ir. Batara Surya, M.Si.
NIDN. 0913017402

PERNYATAAN KEASLIAN TESIS

Yang Bertanda Tangan di bawah ini :

Nama	:	**REYNALDI EKO SAPUTRA**
NIM	:	**4616101043**
Program Studi	:	**ILMU HUKUM**
Judul Tesis	:	**FUNGSI KEPOLISIAN DALAM PENANGGULANGAN TINDAK PIDANA SIBER DI POLDA SULAWESI BARAT**

Menyatakan bahwa Tesis yang saya tulis ini sepanjang pengetahuan saya di dalam naskah Tesis ini tidak terdapat karya ilmiah yang pernah diajukan oleh orang lain untuk memperoleh gelar akademik disuatu perguruan tinggi dan tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali secara tertulis dikutip dalam naskah ini dan disebutkan dalam sumber kutipan dan daftar pustaka.

Demikian pernyataan ini saya buat dengan sebenarnya dan jika dikemudian hari terbukti ada unsur plagiat maka gelar akademik yang saya peroleh dinyatakan batal demi hukum.

Makasar, 25 Januari 2019
Yang Membuat Pernyataan,

REYNALDI EKO SAPUTRA
NIM. 4616101043

PRAKATA

Assalamu Alaikum Wr. Wb

Dengan menyebut Asma Allah yang Maha Pengasih dan Maha Penyayang, Puji syukur kita panjatkan kehadirat Allah SWT, yang telah melimpahkan rahmat serta hidayahNya sehingga Tesis Ini dapat terselesaikan dengan judul " **Fungsi Kepolisian Dalam Penanggulangan Tindak Pidana Siber Di Polda Sulawesi Barat** ". Sholawat serta salam semoga tetap terlimpahkan kepada Nabi Muhammad SAW, keluarga beliau, para sahabat beliau dan orang-orang yang mengikuti ajaran beliau sampai akhir zaman nanti.

Tesis ini disusun dan diajukan sebagai salah satu syarat guna mencapai gelar Magister Hukum (M.H) di Universitas Bosowa.

Terselesaikannya Tesis ini dengan baik berkat dukungan, motivasi, petunjuk dan bimbingan dari berbagai pihak. Oleh karena itu penulis mengucapkan terima kasih kepada :

1. Bapak Prof. Dr. Ir. H. Muhammad Saleh Pallu, M.Eng, selaku Rektor Universitas Bosowa ;
2. Bapak Prof. Dr. Ir. Batara Surya, M.Si, selaku Direktur Program Pascasarjana Universitas Bosowa ;
3. Bapak Dr. Baso Madiong, S.H., M.H, selaku Ketua Program Studi Magister Ilmu Hukum Universitas Bosowa;
4. Bapak Dr. H. Abdul Salam Siku, S.H., M.H, selaku Dosen Pembimbing I yang tidak pernah bosan dan lelah dalam membimbing, guna menyelesaikan Tesis ini ;

5. Bapak Dr. Baso Madiong, S.H., M.H,. selaku Dosen Pembimbing II yang selalu memberikan masukan, saran dan petunjuk dalam proses menyelesaikan Tesis ini ;
6. Penghargaan Setinggi-tingginya kepada orang tuaku Bapak Rusman Alisapa, S.E dan Ibu Hj. Ratna yang mendidik dan menyekolahkan saya hingga perguruan tinggi dan selalu memberikan dorongan moral, spiritual dan material sehingga penulisan tesis ini dapat terselesaikan dengan baik. Semoga Allah SWT mencatat pengorbanannya sebagai amal ibadah, dan mengantinya dengan nikmat yang lebih besar di dunia dan akhirat. Semoga Allah SWT memberikan iman, kesejahteraan, kebahagiaan, kesehatan dan umur yang Panjang agar bisa melihat dan menikmati keberhasilan anaknya di masa tuanya. *Amin ya robbal alamin.*
7. Semua Bapak dan Ibu Dosen Program Pascasarjana Magister Ilmu Hukum Universitas Bosowa yang telah mengajarkan dan memberikan banyak ilmu dengan tulus. Semoga Ilmu yang di berikan dapat bermanfaat di dunia dan akhirat ;
8. Seluruh Staf Program Pascasarjana Universitas Bosowa tanpa terkecuali yang telah banyak memberikan kemudahan kepada penulis terutama dalam hal administrasi akademik.
9. Rekan-rekan Mahasiswa Program Pascasarjana Magister Ilmu Hukum yang telah membantu dan mendorong saya dalam penyelesaian Tesis ini.
10. Kepada Semua Pihak yang tidak sempat saya sebutkan namanya, saya mengucapkan banyak-banyak terima kasih atas motivasi dan bantuannya sehinga terselesainya Tesis ini dengan baik.

Penulis menyadari bahwa dalam penyusunan Tesis ini, masih banyak kekurangan dan banyak mengalami kendala, oleh karena itu bimbingan, arahan, kritikan dan saran dari berbagai pihak yang bersifat membangun sangat penulis harapkan demi hasil yang lebih baik.

Semoga Tesis ini bermanfaat bagi penulis khususnya dan juga bagi pembaca umumnya serta mampu menjadi referensi untuk teman-teman yang lain dalam penyusunan Hasil penelitian dikemudian hari. Atas bimbingan serta petunjuk yang telah diberikan dari berbagai pihak akan memperoleh imbalan yang setimpal dari ALLAH SWT.

Wabillahi Taufik Wal Hidayah.

Wassalamu Alaikum Warahmatullahi Wabarakatu.

Makassar, 25 Januari 2019

Penulis

ABSTRAK

REYNALDI EKO SAPUTRA, 46 16 101 031 . *Fungsi Kepolisian Dalam Penanggulangan Tindak Pidana Siber Di Polda Sulawesi Barat* . (Dibimbing oleh Abdul Salam Siku dan Baso Madiong).

Penelitian ini bertujuan untuk mengetahui faktor-faktor penyebab terjadinya tindak pidana siber di wilayah polda Sulawesi barat, dan kendala yang dialami kepolisian dalam penanggulangan tindak pidana siber di wilayah polda Sulawesi barat.

Penelitian ini dilaksanakan di Kepolisian Negara Republik Indonesia Daerah Sulawesi Barat (Polda Sulbar). Metode penelitian yang digunakan adalah hukum normatif yaitu merupakan penelitian yang mengkaji studi dokumen, yakni menggunakan berbagai bahan hukum primer dan sekunder adapun bahan hukum yang digunakan yaitu bahan hukum primer melalui wawancara langsung kepada narasumber yang berkaitan dengan tulisan ini, dan bahan hukum sekunder dengan mengumpulkan data dari berbagi literatur yang ada, berupa buku, artikel-artikel yang diperoleh dari penelusuran internet, termasuk aturan perundang-undangan yang terkait dengan permasalahan dalam penelitian ini.

Hasil yang penulis peroleh dari penelitian ini, yaitu (1) Upaya Penanggulangan Tindak Pidana Siber Oleh Aparat Kepolisian yaitu Upaya *Preventif* dan *Represif*. (2) faktor-faktor penyebab terjadinya tindak pidana siber di wilayah polda Sulawesi barat terdiri dari dua faktor yaitu : faktor internal terdiri dari terbatasnya personil tenaga ahli, aspek alat bukti dan aspek fasilitas, kemudian faktor eksternal terdiri dari faktor ekonomi, faktor lingkungan, faktor sosial budaya dan faktor intelektual. (3) Kendala yang dialami kepolisian dalam penanggulangan tindak pidana siber di wilayah polda sulbar yaitu kendala internal terdiri dari dengan lemahnya pengawasan pemerintah dan kepolisian, terbatasnya anggaran operasional dan aspek yuridiksi, kemudian kendala eksternal terdiri dari kurangnya kesadaran hukum masyarakat, kurangnya respon masyarakat terhadap sosialisasi atau penyuluhan yang dilakukan pihak kepolisian dan kurangnya laporan masyarakat.

Kata Kunci : Tindak Pidana Siber, Penanggulangan, Fungsi Kepolisian.

ABSTRACT

REYNALDI EKO SAPUTRA, 46 16 101 031 . ***The function of the police in the tackling of cyber crime in the Regional Police of West Sulawesi.*** **(*Supervised by* Abdul Salam Siku *and* Baso Madiong).**

This study aims to determine the factors that cause cyber crime in the Regional Police of West Sulawesi, and the obstacles experienced by the police in eradicate cyber crime in the Regional Police of West Sulawesi.

This research was conducted at the Police of the Republic of Indonesia Regional West Sulawesi (West Sulawesi Regional Police). The research method used is normative law, namely research that examines document review, which uses various primary and secondary legal materials, while the legal material used is primary legal material through direct interviews with informants related to this paper, and secondary law. material by collecting data. from sharing existing literature, in book form, articles obtained from internet searches, including laws relating to the problems in this study.

The results of the study that the authors obtained from this study, namely (1) Police Crime Response Measures by Polri Officers namely Prevention and Repressive Efforts. (2) factors that cause cyber crime in the West Sulawesi Regional Police consists of two factors: internal factors consisting of limited experts, evidence aspects and facilities aspects, then external factors consist of economic factors, environmental factors, socio-cultural factors and intellectual factors. (3) The obstacle experienced by the police in overcoming cyber crime in the West Sulawesi regional police is an internal obstacle consisting of weak government and police supervision, limited operational budgets and aspects of jurisdiction, the external constraints consist of a lack of public legal awareness, lack of public socialization or counseling conducted by the police and lack of public reports.

Keywords : Cyber Crime, Prevention, Police Function.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Pada saat ini kita telah berada di suatu era yang disebut era teknologi. Teknologi dapat diartikan sebagai pelaksanaan ilmu atau juga disebut dengan ilmu terapan, sedangkan informasi dalam Kamus Besar Bahasa Indonesia adalah sesuatu yang dapat diketahui. Undang-undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik dalam pasal 1 sub - 3 menegaskan pengertian teknologi informasi di Indonesia sebagai suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisa, dan menyebarkan informasi.

Pada awal mulanya peralatan komputer hanya terbatas sebagai alat penghitung, namun dalam perkembangannya pemakaian peralatan komputer semakin diperluas. Mengingat permasalahan di dalam kehidupan masyarakat dari waktu ke waktu semakin kompleks dan menyeluruh, maka dalam rangka pengambilan keputusan secara cepat, tepat, dan akurat; diperlukan alat bantu yang dikenal dengan komputer. Semakin banyak minat orang untuk menggunakan komputer, mengakibatkan semakin besar ketergantungan orang terhadap peralatan canggih tersebut. Kita ketahui bersama bahwa perkembangan teknologi itu sangat berpengaruh terhadap sikap tindak dan sikap mental setiap anggota masyarakat

Teknologi sendiri merupakan satu hal yang tidak bisa dipisahkan dari kehidupan manusia. Di Era modern ini, kebutuhan akan internet dan/atau teknologi jaringan komputer semakin meningkat. Internet menjadi bagian

terpenting dan tidak dapat dipisahkan dari kehidupan manusia, baik anak kecil maupun orang dewasa mengakses informasi dari internet dan/atau jaringan komputer. Perkembangan Teknologi Informasi dan Komunikasi dalam kehidupan sehari-hari sekarang ini sangat pesat

Dalam perkembangannya, komputer telah memunculkan sesuatu yang baru didalam kehidupan kita yaitu Internet. Internet telah menjadi sangat penting bagi manusia di seluruh dunia. Perkembangan teknologi informasi yang berwujud internet ini telah mengubah pola interaksi masyarakat, seperti interaksi bisnis, ekonomi, sosial, dan budaya. Para pelaku bisnis, pejabat pemerintah, dan banyak orang di seluruh dunia menggunakan internet sebagai bagian dari bisnis nasional dan internasional serta kehidupan pribadi manusia sehari-hari. Eksistensi dari beberapa jenis bisnis justru tidak mungkin berlangsung tanpa adanya internet. Manusia menjadi makin nyaman dalam menyelenggarakan kegiatan pribadinya sehari-hari, dan mereka yang telah terbiasa dengan internet menjadi tidak nyaman apabila aksesnya kepada internet terganggu.

Peranan teknologi informasi dan komunikasi di era globalisasi telah menempatkan pada posisi yang amat strategis karena menghadirkan suatu dunia tanpa batas, jarak, ruang, dan waktu. Pengaruh globalisasi dengan penggunaan sarana teknologi informasi dan komunikasi telah mengubah pola hidup masyarakat, dan berkembang dalam tatanan kehidupan baru dan mendorong terjadinya perubahan sosial, budaya, ekonomi, pertahanan, keamanan, dan penegakan hukum.

Teknologi informasi dan komunikasi telah dimanfaatkan dalam kehidupan sosial masyarakat, dan telah memasuki berbagai faktor kehidupan baik sektor pemerintahan, bisnis, perbankan, pendidikan, kesehatan, dan kehidupan pribadi. Manfaat teknologi informasi dan komunikasi selain memberikan dampak positif juga disadari memberi peluang untuk dijadikan sarana untuk melakukan tindak kejahatan baru Tindak Pidana Siber. Sehingga dapat dikatakan bahwa teknologi informasi dan komunikasi bagaikan pedang bermata dua, dimana selain memberikan kontribusi positif bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, juga menjadi sarana potensial dan sarana efektif untuk melakukan perbuatan melawan hukum.

Di samping menciptakan berbagai peluang baru dalam kehidupan Masyarakat, perkembangan teknologi internet juga menciptakan peluang-peluang baru bagi kejahatan. Hal-hal negatif tersebut yang merupakan efek sampingnya antara lain adalah timbulnya kejahatan di dunia maya atau lebih dikenal dengan kejahatan mayantara *(cyber crime)*. Di dunia maya orang melakukan kejahatan yang justru tidak dapat dilakukan di dunia nyata, yaitu menggunakan komputer sebagai sarana perbuatannya. Kejahatan masa kini yang mendapat perhatian luas di dunia internasional.

Terkait dengan dampak negatif yang ditimbulkan dari perkembangan ilmu pengetahuan dan teknologi, Indonesia mempunyai pengaturan khusus tentang informasi dan teknologi yang diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik untuk melindungi

masyarakat dari perkembangan teknologi yang mengarah ke hal-hal yang bersifat negatif.

Kemajuan teknologi informasi dan ilmu pengetahuan juga menjadi faktor yang menyebabkan perubahan cara berpikir, cara bertindak dan cara bersikap. Perubahan sikap, pandangan dan orientasi masyarakat inilah yang mempengaruhi kesadaran hukum dan penilaian terhadap suatu tingkah laku. Pertanyaannya apakah perubahan sikap warga masyarakat ini dianggap lazim atau menjadi suatu tindakan yang tidak lazim bahkan dapat menjadi suatu tindak yang mengancam ketertiban sosial. Perbuatan yang mengancam ketertiban sosial yang tergolong dalam kejahatan, sering kali memanfaatkan sarana teknologi informatika. Kejahatan yang menggunakan sarana teknologi informatika ini tergolong baru serta berbahaya bagi ketertiban dan kesejahteraan masyarakat.

Tindak Pidana Siber merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian luas di dunia internasional. Tindak Pidana Siber merupakan salah satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negatif yang sangat luas bagi seluruh bidang kehidupan modern saat ini. Perbuatan melawan hukum di dunia maya merupakan fenomena yang sangat mengkhawatirkan, mengingat tindakan *carding*, *hacking*, penipuan, terorisme dan penyebaran informasi destruktif telah menjadi bagian dari aktivitas kejahatan di dunia maya. Kenyataan itu, demikian sangat kontras dengan ketiadaan regulasi yang mengatur pemanfaatan teknologi informasi dan komunikasi di berbagai sektor. Oleh

karena itu untuk menjamin kepastian hukum, pemerintah berkewajiban melakukan regulasi terhadap berbagai aktivitas terkait dengan pemanfaatan teknologi informasi dan komunikasi tersebut.

Demikian pesatnya perkembangan dan kemajuan teknologi informasi dan komunikasi merupakan salah satu penyebab perubahan kegiatan manusia dalam berbagai bidang yang secara langsung mempengaruhi lahirnya bentuk-bentuk perbuatan hukum baru. Pemanfaatan teknologi informasi dan komunikasi harus terus dikembangkan untuk menjaga, memelihara, dan memperkukuh persatuan dan kesatuan Indonesia demi kepentingan nasional. Pemerintah perlu mendukung pengembangan teknologi informasi melalui infrastruktur hukum dan pengaturannya, untuk mencegah penyalahgunaannya.

Kegiatan yang dilakukan melalui jaringan sistem komputer dan sistem komunikasi, baik dalam lingkup lokal maupun global (internet) dengan memanfaatkan teknologi informasi berbasis sistem komputer yang merupakan sistem elektronik yang dapat dilihat secara virtual. Permasalahan hukum yang seringkali dihadapi adalah ketika terkait dengan penyampaian informasi, komunikasi, dan/atau transaksi secara elektronik, khususnya dalam hal pembuktian dan hal yang terkait dengan perbuatan hukum yang dilaksanakan melalui sistem elektronik.

Dilihat dari perspektif hukum pidana upaya penanggulangan Tindak Pidana Siber dapat dilihat dari berbagai aspek, antara lain aspek kebijakan kriminalisasi (formulasi tindak pidana), aspek pertanggungjawaban pidana atau pemidanaan (termasuk aspek alat bukti/pembuktian), dan aspek jurisdiksi.

Perumusan tindak pidana di dalam KUHPidana kebanyakan masih bersifat konvensional dan belum secara langsung dikaitkan dengan perkembangan Tindak Pidana Siber. Di samping itu, mengandung berbagai kelemahan dan keterbatasan dalam menghadapi perkembangan teknologi dan *high tech crime* yang sangat bervariasi.

Undang-Undang RI Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik hadir sebagai wujud dari tanggung jawab yang harus diemban oleh Negara, untuk memberikan perlindungan maksimal pada seluruh aktivitas pemanfaatan teknologi informasi dan komunikasi di dalam negeri agar terlindung dengan baik dari potensi kejahatan dan penyalahgunaan teknologi. Akibat pengaruh globalisasi informasi, telah menempatkan Indonesia sebagai bagian dari masyarakat informasi dan transaksi elektronik di tingkat nasional sehingga pembangunan teknologi informasi dapat dilakukan secara optimal, merata, dan menyebar ke seluruh lapisan masyarakat guna mencerdaskan kehidupan bangsa.

Ruang lingkup keberlakuan undang-undang ini, diatur dalam Pasal 2 UU Nomor 19 Tahun 2016 yang mana undang-undang ini berlaku untuk setiap orang yang melakukan perbuatan hukum, baik yang berada di wilayah hukum Indonesia, maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah Indonesia dan/atau di luar wilayah hukum Indonesia baik oleh warga Negara Indonesia, maupun warga negara asing atau badan hukum Indonesia maupun asing yang memiliki akibat hukum di Indonesia, mengingat

pemanfaatan teknologi informasi untuk informasi elektronik dan transaksi elektronik dapat bersifat lintas territorial atau universal.

Dalam kenyataannya kegiatan siber tidak lagi sederhana, karena kegiatannya tidak lagi dibatasi oleh teritori suatu negara, yang mudah diakses kapan pun, dan dimana pun. Kerugian dapat terjadi, baik pada pelaku transaksi, maupun pada orang lain, yang tidak melakukan transaksi di internet. Di samping itu, pembuktian merupakan faktor yang sangat penting, mengingat informasi elektronik bukan saja belum terakomodasi dalam sistem hukum acara di Indonesia secara komprehensif, melainkan juga ternyata sangat rentan untuk diubah, disadap, dipalsukan, dan dikirim ke berbagai penjuru dunia dalam waktu yang sangat singkat. Dengan demikian dampak yang diakibatkannya pun bisa demikian kompleks dan rumit.

Kenyataan ini, menunjukkan bahwa konvergensi di bidang teknologi informasi, media, dan informatika (telematika) berkembang terus tanpa dapat dibendung, seiring dengan ditemukannya perkembangan baru di bidang teknologi informasi, media dan komunikasi. Kegiatan melalui media sistem elektronik yang disebut juga ruang siber (*cyber space*) meskipun sifatnya virtual dapat dikategorikan sebagai tindakan atau perbuatan hukum yang nyata. Secara yuridis kegiatan pada ruang siber tidak dapat didekati dengan ukuran dan kualifikasi hukum konvensional saja, sebab jika cara ini yang ditempuh akan terlalu banyak kesulitan dan hal yang lolos dari pemberlakuan hukum.

Kegiatan dalam ruang siber adalah kegiatan virtual yang berdampak sangat nyata meskipun alat buktinya bersifat elektronik. Perlu diperhatikan sisi

keamanan dan kepastian hukum dalam pemanfaatan teknologi informasi, media, dan komunikasi, agar dapat berkembang secara optimal. Untuk mengatasi gangguan keamanan dalam penyelenggaraan sistem secara elektronik maka pendekatan hukum bersifat mutlak, karena tanpa kepastian hukum persoalan pemanfaatan teknologi informasi menjadi tidak optimal.

Upaya penanganan Tindak Pidana Siber membutuhkan keseriusan semua pihak mengingat teknologi informasi khususnya internet telah dijadikan sebagai sarana untuk membangun masyarakat yang berbudaya informasi. Keberadaan undang-undang yang mengatur tindak pidana siber memang diperlukan, akan tetapi apalah arti undang-undang jika pelaksana dari undang-undang tidak memiliki kemampuan atau keahlian dalam bidang itu dan masyarakat yang menjadi sasaran dari undang-undang tersebut tidak mendukung tercapainya tujuan pembentukan hukum tersebut.

Masalah Tindak Pidana Siber yang dilakukan oleh orang yang tidak bertanggung jawab sangatlah bertentangan oleh norma-norma hukum, kesusilaan, adat istiadat dan agama pada bangsa Indonesia. Oleh karena itu haruslah ada usaha untuk menanggulangi tindak pidana Siber ini.

Penulis beranggapan bahwa tindak pidana siber merupakan kejahatan yang dilakukan di dimensi lain yang membutuhkan penanganan yang serius melalui instrument hukum yang baik mengingat dampaknya dapat dirasakan dikehidupan nyata. Oleh karena itu aparat kepolisian dalam hal ini Polda Sulawesi Barat sebagai pelaksana dan penegak hukum peraturan perundang-undangan harus segera menanggulangi Tindak Pidana Siber dengan serius.

Berdasarkan uraian-uraian yang telah disampaikan di atas, maka penulis tertarik untuk mengangkat judul tentang **" Fungsi Kepolisian Dalam Penanggulangan Tindak Pidana Siber di Polda Sulawesi Barat ".**

B. Rumusan Masalah

Berdasarkan latar belakang tersebut di atas, maka masalah dalam penelitian ini adalah :

1. Apakah faktor-faktor penyebab terjadinya Tindak Pidana Siber di wilayah Polda Sulawesi Barat ?
2. Bagaimanakah Kendala yang dialami kepolisian dalam penanggulangan tindak pidana Siber di wilayah Polda Sulawesi Barat ?

C. Tujuan Penelitian

Adapun Tujuan Penelitian ini Sebagai Berikut :

1. Untuk mengetahui faktor-faktor penyebab terjadinya Tindak Pidana Siber di wilayah Polda Sulawesi Barat.
2. Untuk mengetahui dan menjelaskan kendala yang dialami kepolisian dalam penanggulangan Tindak Pidana Siber di wilayah Polda Sulawesi Barat.

D. Manfaat Penelitian

Dari hasil penelitian ini nantinya diharapkan dapat memberikan manfaat sebagai berikut :

1. Manfaat Praktis

   Penelitian ini nantinya diharapkan dapat memberikan penjelasan kepada instansi-instansi terkait, khusunya aparat penegak hukum untuk bagaimana melakukan upaya untuk pencegahan Tindak Pidana Siber.

2. Manfaat Teoritis

   Dari hasil penelitian ini diharapkan dapat dijadikan bahan kepustakaan dan bahan referensi hukum bagi mereka yang berminat pada kajian-kajian ilmu hukum pada umumnya dan hukum pidana khusunya.

BAB II

KAJIAN TEORI DAN KERANGKA PIKIR

A. Tindak Pidana

1. Pengertian Tindak Pidana

Menurut Adami Chazawi (2008 : 69) Istilah tindak pidana berasal dari hukum pidana Belanda yang dikenal dengan *strafbaar feit* yang terdiri dari tiga kata yaitu, *straf*, *baar*, dan *feit*. *straf* diterjemahkan dengan pidana dan hukum. *baar* diterjemahkan dengan dapat dan boleh. Sementara itu, untuk kata *feit* diterjemahkan dengan tindak, peristiwa, pelanggaran, dan perbuatan.

Istilah tindak pidana merupakan terjemahan umum untuk istilah *strafbaar feit*. Andi Zainal Abidin (dalam Erdianto Effendi, 2011 : 96) adalah salah seorang ahli hukum pidana Indonesia yang tidak sepakat dengan penerjemahan *strafbaar feit* menjadi tindak pidana. Adapun alasannya adalah sebagai berikut:

a. Tindak tidak mungkin dipidana, tetapi orang yang melakukanlah yang dapat dijatuhi pidana;
b. Ditinjau dari segi bahasa Indonesia, tindak adalah kata benda dan pidana juga kata benda. Yang lazim ialah kata benda selalu diikuti kata sifat;
c. Istilah *strafbaar feit* bersifat eliptis yang kalau diterjemahkan secara harfiah adalah peristiwa yang dapat dipidana.

Untuk istilah “tindak” memang telah lazim digunakan dalam peraturan perundang-undangan walaupun masih dapat diperdebatkan ketepatannya. Tindak menunjuk pada hal kelakuan manusia dalam arti positif (*handelen*) semata, dan tidak termasuk kelakuan manusia yang pasif atau negative (*nalaten*). Padahal pengertian sebenarnya dalam istilah *feit* itu termasuk perbuatan aktif maupun pasif tersebut.

Perbuatan aktif artinya suatu bentuk perbuatan yang untuk mewujudkannya diperlukan adanya suatu gerakan dari tubuh atau bagian dari tubuh manusia. Sementara itu, perbuatan pasif adalah suatu bentuk tidak melakukan suatu bentuk perbuatan fisik apa pun yang oleh karenanya seseorang tersebut telah mengabaikan kewajiban hukumnya, misalnya perbuatan tidak menolong (Pasal 531 KUHPidana) atau perbuatan membiarkan (Pasal 304 KUHPidana).

Adapun beberapa istilah-istilah yang dipergunakan didalam Bahasa Indonesia antara lain :

a. Peristiwa pidana
b. Perbuatan pidana
c. Tindak pidana
d. Pelanggaran pidana

Dari beberapa istilah diatas yang paling popular dipakai adalah istilah tindak pidana. hal ini dapat dilihat pada beberapa buku hukum pidana, serta peraturan perundang-undangan hukum pidana yang pada umumnya mempergunakan istilah tindak pidana.

Namun ada beberapa sarjana yang mempergunakan istilah lain. Moeljato (2009 : 23) misalnya, menganggap lebih tepat menggunakan istilah perbuatan pidana dengan alasan-alasan sebagai berikut :

1. Perkataan peristiwa tidak menunjukkan bahwa yang menimbulkan *handeing* atau *gedraging* seseorang, mungkin juga hewan atau kekuatan alam.
2. Perkataan tindak berarti langkah dan baru dalam bentuk tindak tanduk atau tingkah laku.
3. Perkataan perbuatan sudah lazim dipergunakan dalam percakapan sehari-hari, seperti perbuatan tidak senonoh, perbuatan jahat, dan sebagainya. Dan juga istilah seperti perbuatan melawan hukum (*onrecht matigedaad*).

Mengenai apa yang dimaksud atau apa yang diartikan dengan perbuatan pidana, tindak pidana atau peristiwa pidana, berikut penulis kemukakan beberapa pandangan pakar hukum pidana antara lain :

Moeljatno (2009 : 4) mengartikan s*trafbaarfeit* sebagai berikut :

> s*trafbaarfeit* itu sebenarnya adalah "suatu kelakuan manusia yang diaancam pidana oleh peraturan perundang-undangan".

Sementara Indriyanto Seno Adji Adji (dalam Erdianto Effendi, 2011 : 10) yang mengartikan tindak pidana sebagai :

> Perbuatan seseorang yang diancam pidana, perbuatannya bersifat melawan hukum, terdapat suatu kesalahan dan bagi pelakunya dapat dipertanggungjawabkan atas perbuatannya.

s*trafbaarfeit* diartikan juga oleh Pompe (dalam P. A. F. Lamintang dan Francius Theojunior Lamintang, 2014 : 17) sebagai :

> Suatu pelanggaran norma (gangguan terhadap tertib hukum) yang dengan sengaja ataupun dengan tidak sengaja telah dilakukan oleh seorang pelaku, dimana penja Tuhan hukuman terhadap pelaku tersebut adalah perlu demi terpeliharanya tertib hukum.

Simon (dalam P. A. F. Lamintang dan Francius Theojunior Lamintang, 2014 : 17) merumuskan s*trafbaarfeit* adalah :

> Suatu tindakan melanggar hukum yang telah dilakukan dengan sengaja oleh seseorang yang dapat dipertanggungjawabkan atas tindakannya dan yang oleh undang-undang telah dinyatakan sebagai suatu tindakan yang dapat dihukum.

R. Tresna (dalam P. A. F. Lamintang dan Francius Theojunior Lamintang, 2014 : 17) menjelaskan bahwa :

> s*trafbaarfeit* atau peristiwa pidana adalah suatu perbuatan atau rangkaian perbuatan manusia, yang bertentangan dengan undangundang atau peraturan perundangan lainnya terhadap perbuatan mana diadakan tindakan penghukuman.

Walaupun istilah tindak pidana diterjemahkan bermacam-macam sebagaimana yang telah dipaparkan diatas, dapat disimpulkan bahwa tindak pidana adalah suatu perbuatan melawan hukum, dimana pelakunya dapat dipidana.

Tindak pidana juga diartikan sebagai suatu dasar yang pokok dalam menjatuhi pidana pada orang yang telah melakukan perbuatan pidana atas dasar pertanggungjawaban seseorang atas perbuatan yang telah dilakukannya, tapi sebelum itu mengenai dilarang dan diancamnya suatu perbuatan yaitu mengenai perbuatan pidanannya sendiri, yaitu berdasarkan asas legalitas (*principle of legality*) asas yang menentukan bahwa tidak ada perbuatan yang dilarang dan diancam dengan pidana jika tidak ditentukan terlebih dahulu dalam perundang-undangan, biasanya ini lebih dikenal

dalam Bahasa latin sebagai *nullum delictum nulla poena sine praevia lege* (tidak ada delik, tidak ada pidana tanpa peraturan lebih dahulu).

2. Unsur – Unsur Tindak Pidana

Dalam mengkaji unsur-unsur tindak pidana dikenal dua aliran yaitu aliran monistis dan aliran dualistis Masruchin Rubah (2001 : 23). Aliran monistis, memandang semua syarat untuk menjatuhkan pidana sebagai unsur tindak pidana. Aliran ini tidak memisahkan unsur yang melekat pada perbuatannya (*criminal act*) dengan unsur yang melekat pada orang yang melakukan tindak pidana (*criminal responsibility* atau *criminal liability* yang berarti pertanggungan-jawab dalam hukum pidana). Sarjana-sarjana yang termasuk kelompok aliran monistis diantaranya: Simon, Mezger, dan Wirdjono Prodjodikoro.

Simon (dalam P. A. F. Lamintang dan Francius Theojunior Lamintang, 2014 : 13) mengemukakan unsur-unsur tindak pidana sebagai berikut :

a) Perbuatan manusia (positif atau negatif).
b) Diancam dengan pidana.
c) Melawan hukum.
d) Dilakukan dengan kesalahan.
e) Oleh orang yang mampu bertanggung jawab.

Unsur-unsur tersebut oleh Simon dibedakan antara unsur objektif dan unsur subjektif. Yang termasuk dalam unsur objektif adalah: perbuatan orang, akibat yang kelihatan dari perbuatan itu, dan kemungkinan adanya

keadaan tertentu yang menyertai, misalnya unsur “dimuka umum” dalam pasal 218 KUHP. Yang termasuk dalam unsur subjektif adalah: orang yang mampu bertanggung jawab dan melakukan kesalahan.

Sedangkan E. Mezger (dalam P. A. F. Lamintang dan Francius Theojunior Lamintang, 2014 : 14) mengemukakan unsur-unsur tindak pidana sebagai berikut :

1. Perbuatan dalam arti yang luas dari manusia.
2. Sifat melawan hukum.
3. Dapat dipertanggungjawabkan kepada seseorang.
4. Diancam pidana

Wirdjono Prodjodikoro (dalam Adami Chazawi, 2008:24) mengemukakan unsur-unsur tindak pidana sesuai dengan definisi yang dikemukakannya sebagai berikut: “tindak pidana berarti suatu perbuatan yang pelakunya dapat dikenakan pidana”. Unsur-unsur tindak pidana menurut Wirdjono meliputi unsur perbuatan dan pelaku.

Moeljatno (2009 : 11) mengemukakan unsur-unsur tindak pidana sebagai berikut :

1. Perbuatan (manusia).
2. Memenuhi rumusan undang-undang.
3. Bersifat melawan hukum.

Memenuhi rumusan undang-undang merupakan syarat formil. Keharusan demikian merupakan konsekuensi dari asas legalitas. Bersifat melawan hukum merupakan syarat materiil. Keharusan demikian, karena

perbuatan yang dilakukan itu harus betul-betul oleh masyarakat dirasakan sebagai perbuatan yang tidak patut dilakukan. Menurut Moeljatno bersifat melawan hukum itu merupakan syarat mutlak untuk tindak pidana.

3. Jenis Tindak Pidana

a. Tindak Pidana Menurut Doktrin

1) Kejahatan

Secara doktrinal kejahatan adalah *rechtdelicht*, yaitu perbuatan-perbuatan yang bertentangan dengan keadilan, terlepas apakah perbuatan itu diancam pidana dalam suatu undang-undang atau tidak. Sekalipun tidak dirumuskan sebagai delik dalam undang-undang, perbuatan ini benarbenar dirasakan oleh masyarakat sebagai perbuatan yang bertentangan dengan keadilan.

2) Pelanggaran

Jenis tindak pidana ini disebut *wetsdelicht*, yaitu perbuatanperbuatan yang oleh masyarakat baru disadari sebagai suatu tindak pidana, karena undang-undang merumuskannya sebagai delik dan diancam sanksi pidana bagi pelanggarnya.

Tindak pidana secara kualitatif atas kejahatan dan pelanggaran tidak dapat diterima. Tidak semua kejahatan merupakan perbuatan yang benar-benar telah dirasakan sebagai perbuatan yang bertentangan dengan keadilan, sebelum dirumuskan dalam undang-undang. Terdapat juga pelanggaran yang memang benar-benar telah dirasakan oleh masyarakat sebagai perbuatan yang bertentangan dengan keadilan,

sekalipun perbuatan tersebut belum dirumuskan sebagai tindak pidana dalam undang-undang. (P.A.F. Lamintang, 2014 : 118)

b. Tindak Pidana Formil dan Materil

1) Tindak Pidana Formil

Tindak pidana yang perumusannya dititik beratkan pada perbuatan yang dilarang. Tindak pidana formil adalah tindak pidana yang telah dianggap terjadi/selesai dengan telah dilakukannya perbuatan yang dilarang dalam undang-undang, tanpa mempersoalkan akibat.

2) Tindak Pidana Materil

Tindak pidana yang perumusannya dititik beratkan pada akibat yang dilarang. Tindak pidana materiil adalah tindak pidana yang baru dianggap telah terjadi, atau dianggap telah selesai apabila akibat yang dilarang itu telah terjadi. (P.A.F. Lamintang, 2014 : 97)

c. Tindak Pidana Sengaja dan Tindak Pidana Kelalaian

Menurut Adami Chazawi (2008 : 127) Tindak pidana sengaja (*doleus delicten*) adalah tindak pidana yang dalam rumusannya dilakukan dengan kesengajaan atau mengandung unsur kesengajaan. Sementara itu tindak pidana kelalaian (*culpose delicten*) adalah tindak pidana yang dalam rumusannya mengandung unsur kelalaian (*culpa).*

d. Tindak Pidana Aktif (Delik *commisionis*) dan Tindak Pidana Pasif (Delik *omisionis*)

Menurut Adami Chazawi (2008 : 129) Tindak pidana aktif (*delicta commissionis*) adalah tindak pidana yang perbuatannya berupa

perbuatan aktif (positif). Perbuatan aktif disebut juga perbuatan materiil merupakan perbuatan yang untuk mewujudkannya disyaratkan adanya gerakan dari anggota tubuh orang yang berbuat. Dengan berbuat aktif, orang melanggar larangan. perbuatan aktif ini terdapat, baik dalam tindak pidana yang dirumuskan secara formil maupun materiil.

Berbeda dengan tindak pidana pasif, terdapat suatu kondisi atau keadaan tertentu yang mewajibkan seseorang dibebani kewajiban hukum untuk berbuat tertentu, yang apa bila ia tidak melakukan (aktif) perbuatan itu, ia telah melanggar kewajiban hukumnya tadi. Di sini ia telah melakukan tindak pidana pasif. Tindak pidana ini dapat disebut juga tindak pidana pengabaian suatu kewajiban hukum.

e. Tindak Pidana Terjadi Seketika dan Tindak Pidana Berlangsung Terus

Menurut Adami Chazawi (2008 : 129) Tindak pidana yang dirumuskan sedemikian rupa sehingga untuk terwujudnya atau terjadinya dalam waktu seketika atau waktu singkat saja, disebut juga dengan *afolpende delicten* Misalnya pencurian (362), jika perbuatan mengambilnya selesai, tindak pidana itu menjadi selesai secara sempurna.

Sebaliknya ada tindak pidana yang dirumuskan sedemikian rupa, sehingga terjadinya tindak pidana itu berlangsung lama, yakni setelah perbuatan dilakukan, tindak pidana itu masih berlangsung terus, yang disebut juga dengan *voortdurende delicten*. Kejahatan ini

berlangsung lama, tidak selesai seketika. Seperti Pasal 333, perampasan kemerdekaan itu berlangsung lama, bahkan sangat lama, dan akan terhenti setelah korban dibebaskan/terbebaskan.

f. Tindak Pidana Umum dan Tindak Pidana Khusus

Menurut Adami Chazawi (2008 : 131) Tindak pidana umum adalah semua tindak pidana yang dimuat dalam KUHPidana sebagai kodifikasi hukum pidana materiil. Sementara itu, tindak pidana khusus adalah semua tindak pidana yang terdapat diluar kodifikasi tersebut.

Adanya tindak pidana diluar KUHPidana merupakan suatu keharusan yang tidak dapat dihindari. Perbuatan-perbuatan tertentu yang dinilai merugikan masyarakat dan patut diancam dengan pidana itu terus berkembang sesuai dengan perkembangan teknologi dan kemajuan ilmu pengetahuan, yang tidak cukup efektif dengan hanya menambahkannnya pada kodifikasi (KUHPidana).

g. Tindak Pidana *communia* dan Tindak Pidana *propria*

Menurut Adami Chazawi (2008 : 139) Jika dilihat dari subjek hukum tindak pidana, tindak pidana itu dapat dibedakan antara tindak pidana yang dapat dilakukan oleh semua orang (*delicta communia*) dan tindak pidana yang hanya dapat dilakukan oleh orang tertentu (*delicta propria*).

Pada umumnya, tindak pidana itu dibentuk dan dirumuskan untuk berlaku pada semua orang, dan memang bagian terbesar tindak pidana itu dirumuskan dengan maksud yang demikian. Akan tetapi, ada

perbuatan-perbuatan yang tidak patut tertentu yang khusus hanya dapat dilakukan oleh orang yang berkualitas saja, misalnya pegawai negeri (pada kejahatan jabatan) atau nahkoda (pada kejahatan pelayaran) dan sebagainya.

h. Tindak Pidana Biasa (*gewone delicten*) dan Tindak Pidana Aduan (*klacht delicten*)

Menurut Adami Chazawi (2008 : 132) Tindak pidana biasa merupakan tindak pidana yang untuk dilakukannya penuntutan pidana terhadap pembuatnya tidak disyaratkan adanya pengaduan dari yang berhak. Sementara itu, tindak pidana aduan merupakan tindak pidana yang untuk dapatya dilakukan penuntutan pidana disyaratkan untuk terlebih dahulu adanya pengaduan oleh yang berhak mengajukan pengaduan, yakni korban atau wakilnya dalam perkara perdata atau keluarga tertentu dalam hal-hal tertentu atau orang yang diberi kuasa khusus untuk pengaduan oleh yang berhak.

i. Tindak Pidana dalam Bentuk Pokok, yang Diperberat dan yang Diperingan

Menurut Adami Chazawi (2008 : 134) Tindak pidana dalam bentuk pokok dirumuskan secara lengkap, artinya semua unsurnya dicantumkan dala rumusan. Karena disebutkan secara lengkap unsur-unsurnya, pada rumusan bentuk pokok terkandung pengertian yuridis dari tindak pidana tersebut.

Sementara itu, pada bentuk yang diperberat dan atau yang diperingan, tidak mengulang kembali unsure-unsur bentuk pokok itu, melainkan sekedar menyebut kualifikasi bentuk pokoknya atau Pasal bentuk pokoknya, kemudian disebutkan atau ditambahkan unsur yang bersifat memberatkan atau meringankan secara tegas dalam rumusan.

j. Tindak Pidana Tunggal dan Tindak Pidana Berangkai

Menurut Adami Chazawi (2008 : 136) Tindak pidana tunggal (*enkelvoudige delicten*) adalah tindak pidana yang dirumuskan sedemikian rupa sehingga untuk dipandang selesainya tindak pidana dan dapat dipidannya pelaku cukup dilakukan satu kali perbuatan saja.

Sementara itu, tindak pidana berangkai adalah tindak pidana yang dirumuskan sedemikian rupa sehingga untuk dipandang sebagai selesai dan dapat dipidananya pembuat, disyaratkan dilakukan secara berulang.

4. Teori Penanggulangan Kejahatan

Dalam usaha untuk menanggulangi kejahatan dengan dua cara yaitu tindakan *preventif* (mencegah sebelum terjadinya kejahatan), dan tindakan *represif* (usaha sesudah terjadinya kejahatan). Berikut ini diuraikan pula masing-masing usaha tersebut :

a. Tindakan *preventif*

Tindakan *preventif* adalah tindakan yang dilakukan untuk mencegah atau menjaga kemungkinan akan terjadinya kejahatan, dalam kaitannya untuk melakukan tindakan *preventif* adalah

mencegah kejahatan lebih baik dari pada mendidik penjahat menjadi baik kembali, sebab bukan saja diperhitungkan segi biaya, tapi usaha ini lebih mudah dan akan mendapat hasil yang memuaskan atau mencapai tujuan.

Selanjutnya Bonger (1982:15) berpendapat cara menanggulangi kejahatan yang terpenting adalah :

1) *preventif* kejahatan dalam arti luas, meliputi reformasi dan prevensi dalam arti sempit
2) *prevensi* kejahatan dalam arti sempit meliputi :
    a. *moralistik* yaitu menyebarluaskan sarana-sarana yang dapat memperteguhkan moral seseorang agar dapat terhindar dari nafsu berbuat jahat.
    b. *abalionistik* yaitu berusaha mencegah tumbuhnya keinginan kejahatan dan meniadakan faktor-faktor yang terkenal sebagai penyebab timbulnya kejahatan, Misalnya memperbaiki ekonomi (pengangguran, kelaparan, mempertinggi peradapan, dan lain-lain);
3) Berusaha melakukan pengawasan dan pengontrolan terhadap kejahatan dengan berusaha menciptakan;
    a. Sistem organisasi dan perlengkapan kepolisian yang baik,
    b. Sistem peradilan yang objektif
    c. Hukum (perundang-undangan) yang baik.

4) Mencegah kejahatan dengan pengawasan dan patroli yang teratur;

5) Pervensi kenakalan anak-anak sebagai sarana pokok dalam usaha prevensi kejahatan pada umumnya.

b. Tindakan *represif*

Menurut Soedjono D (1976 : 32) Tindakan *represif* adalah segala tindakan yang dilakukan oleh aparatur penegak hukum sesudah terjadinya tindakan pidana. Tindakan represif lebih dititik beratkan terhadap orang yang melakukan tindak pidana, yaitu antara lain dengan memberikan hukum (pidana) yang setimpal atas perbuatannya. Tindakan ini sebenarnya dapat juga dipandang sebagai pencegahan untuk masa yang akan datang. Tindakan ini meliputi cara aparat penegak hukum dalam melakukan penyidikan, penyidikan lanjutan, penuntutan pidana, pemeriksaan di pengadilan, eksekusi dan seterusnya sampai pembinaan narapidana.

Menurut Simanjuntak B (1980 : 399) Penanggulangan kejahatan secara *represif* ini dilakukan juga dengan teknik rehabilitas, dengan dua konsepsi mengenai cara atau tekhnik rehabilitasi, yaitu :

1. Menciptakan sistem program yang bertujuan untuk menghukum penjahat, sistem ini bersifat memperbaiki antara lain hukuman bersyarat dan hukuman kurungan.

2. Lebih ditekankan pada usaha agar penjahat dapat berubah menjadi orang biasa, selama menjalankan hukuman dicarikan pekerjaan bagi terhukum dan konsultasi psikologis, diberikan kursus keterampilan agar kelak menyesuaaikan diri dengan masyarakat.

Tindakan *represif* juga disebutkan sebagai pencegahan khusus, yaitu suatu usaha untuk menekankan jumlah kejahatan dengan memberikan hukuman (pidana) terhadap pelaku kejahatan dan berusaha pula melakukan perbuatan dengan jalan memperbaiki si pelaku yang berbuat kejahatan. Jadi lembaga permasyarakatan bukan hanya tempat untuk mendidik narapidana untuk tidak lagi menjadi jahat atau melakukan kejahatan yang pernah dilakukan.

Kemudian upaya penanggulangan kejahatan yang sebaik-baiknya harus memenuhi persyaratan sebagai berikut:

(1) Sistem dan operasi Kepolisian yang baik.
(2) Peradilan yang efektif.
(3) Hukum dan perundang-undangan yang berwibawa.
(4) Koodinasi antar penegak hukum dan aparatur pemerintah yang serasi.
(5) Partisipasi masyarakat dalam penanggulangan kejahatan.
(6) Pengawasan dan kesiagaan terhadap kemungkinan timbulnya kejahatan.
(7) Pembinaan organisasi kemasyarakatan

B. Tindak Pidana Siber

1. Pengertian Tindak Pidana Siber

Pada masa awalnya, *cyber crime* didefinisikan sebagai kejahatan komputer (tindak pidana siber). *The British Law Commission*, mengartikan "tindak pidana siber" sebagai manipulasi komputer dengan cara apa pun yang dilakukan dengan itikad buruk untuk memperoleh uang, barang atau keuntungan lainnya atau dimaksudkan untuk menimbulkan kerugian kepada pihak lain. Mandell (dalam Budi Sahariyanto, 2013 : 10) membagi "tindak pidana siber" atas dua kegiatan, yaitu:

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

Menurut Budi Sahariyanto (2013 : 11) Sistem teknologi informasi berupa internet telah dapat menggeser paradigma para ahli hukum terhadap definisi kejahatan komputer, pada awalnya para ahli hukum terfokus pada alat/perangkat keras yaitu komputer. Namun dengan adanya perkembangan teknologi informasi berupa jaringan internet, maka fokus dari identifikasi terhadap definisi tindak pidana siber lebih diperluas lagi yaitu seluas aktivitas yang dapat dilakukan di dunia *cyber* / maya melalui sistem informasi yang digunakan.

Jadi tidak sekedar pada komponen *hardware*-nya saja kejahatan itu dimaknai sebagai tindak pidana siber, tetapi sudah dapat diperluas dalam lingkup dunia yang dijelajah oleh sistem teknologi informasi yang bersangkutan. sehingga lebih tepat jika pemaknaan dari tindak pidana siber adalah kejahatan teknologi informasi, juga sebagai kejahatan mayantara.

Pada dasarnya tindak pidana siber meliputi semua tindak pidana yang berkenaan dengan sistem informasi itu sendiri, serta sistem informasi yang merupakan sarana untuk penyampaian/pertukaran informasi kepada pihak lainnya.

Menurut Maskun (2017 : 23) Teknologi telekomunikasi telah membawa manusia kepada suatu peradaban baru dengan struktur sosial beserta tata nilainya. Artinya, masyarakat berkembang menuju masyarakat baru yang berstruktur global. Sistem tata nilai dalam suatu masyarakat berubah, dari yang bersifat lokal-partikular menjadi global universal. Hal ini pada akhirnya akan membawa dampak pada pergeseran nilai, norma, moral, dan kesusilaan.

Dampak pergeseran tersebut ditemukanya perkembangan dan kemajuan ilmu pengetahuan dan teknologi, terjadilah konvergensi antara keduanya. Kemajuan teknologi yang merupakan hasil budaya menusia di samping membawa dampak positif, dalam arti dapat diperdayagunakan untuk kepentingan umat manusia juga membawa dampak negatif terhadap perkembangan manusia dan peradabannya. Dampak negatif yang dimaksud adalah yang berkaitan dengan dunia kejahatan.

Menurut J. E Sahetapy (2002 : 45) telah menyatakan dalam tulisannya, bahwa kejahatan erat kaitanya dan bahkan menjadi sebagian dari hasil budaya itu sendiri. Ini berarti semakin tinggi tingkat budaya dan semakin modern suatu bangsa, maka semakin modern pula kejahatan itu dalam bentuk, sifat dan cara pelaksanaanya.

Menurut Josua Sitompul (2017 : 46) Perkembangan teknologi komputer, teknologi informasi, dan teknologi komunikasi juga menyebabkan munculnya tindak pidana baru yang memiliki karakteristik yang berbeda dengan tindak pidana konvensional. Penyalahgunaan komputer sebagai salah satu dampak dari ketiga perkembangan teknologi tersebut itu tidak terlepas dari sifatnya yang khas sehingga membawa persoalan yang rumit dipecahkan berkenaan dengan masalah penanggulangannya (penyelidikan, penyidikan hingga dengan penuntutan).

Salah satu kejahatan yang ditimbulkan oleh perkembangan dan kemajuan teknologi informasi atau telekomunikasi adalah kejahatan yang berkaitan dengan aplikasi internet. Kejahatan ini dalam istilah asing sering disebut dengan *cybercrime.* Tindak pidana Siber merupakan bentuk kejahatan yang relatif baru apabila dibandingkan dengan bentuk-bentuk kejahatan lain yang sifatnya konvensional (*street crime*). Tindak Pidana Siber muncul bersamaan dengan lahirnya revolusi teknologi informasi. Sebagaimana dikemukakan oleh Didik M. Arif Mansur (2005 : 78) bahwa:

> *Interaksi sosial yang meminimalisir kehadiran secara fisik, merupakan ciri lain revolusi teknologi informasi. Dengan interaksi semacam ini, penyimpangan hubungan sosial yang berupa*

kejahatan (crime) akan menyesuaiakan bentuknya dengan karakter baru tersebut.

Ringkasnya, sesuai dengan ungkapan "kejahatan merupakan produk dari masyarakat sendiri" *(crime is a product of society its self)*, "habitat" baru ini, dengan segala bentuk pola interaksi yang ada didalamya, akan menghasilkan jenis-jenis kejahatan yang berbeda dengan kejahatan-kejahatan lain yang sebelumnya telah dikenal. Kejahatan-kejahatan ini berada dalam satu kelompok besar yang dikenal dengan istilah Tindak Pidana Siber.

Pengertian Tindak Pidana Siber menurut Andi Hamzah (1992 : 13) adalah setiap aktivitas seseorang, sekelompok orang, badan hukum yang menggunakan komputer sebagai sarana melakukan kejahatan, atau menjadikan komputer sebagai sasaran kejahatan. Semua kejahatan tersebut adalah bentuk-bentuk perbuatan yang bertentangan dengan peraturan perundang-undangan, baik dalam arti melawan hukum secara material maupun melawan hukum secara formal. Kemudian, definisi lain mengenai kejahatan komputer ini dikeluarkan oleh *organization of european community development (OECD)* yaitu sebagai berikut: " *any illegal, unethicall or unauthorized behavior relating to the authomathic processing and/or the transmission of data"*. Dari definisi tersebut, kejahatan komputer ini termasuk segala akses illegal atau akses secara tidak sah terhadap suatu transmisi data. Sehingga telihat bahwa segala aktivitas yang tidak sah dalam suatu system komputer merupakan suatu kejahatan.

Batasan atau definisi dari kejahatan komputer juga diberikan oleh Andi Hamzah (1992 : 26), bahwa “kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara illegal. Dari pengertian yang diberikan oleh Andi Hamzah dapat disimpulkan bahwa beliau memperluas pengertian kejahatan komputer, yaitu segala aktivitas tidak sah yang memanfaatkan komputer untuk tindak pidana. Sekecil apapun dampak atau akibat yang ditimbulkan dari penggunaan komputer secara tidak sah atau illegal merupakan suatu kejahatan.

Menurut Widodo (2009 : 76) Tindak Pidana Siber memiliki beberapa karakteristik, yaitu:

a. Perbuatan yang dilakukan secara illegal, tanpa hak atau tidak etis tersebut terjadi dalam ruang / wilayah siber / *cyber* (*cyberspace*), sehingga tidak dapat dipastikan yurisdiksi negara mana yang berlaku terhadapnya.
b. Perbuatan tersebut dilakukan dengan menggunakan peralatan apa pun yang terhubung dengan internet.
c. Perbuatan tersebut mengakibatkan kerugian materill maupun immaterial (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasian informasi) 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 / melintas batas negara.

Kejahatan dalam bidang teknologi informasi secara umum terdiri dari dua kelompok, yaitu :

a. Kejahatan konvensional yang menggunakan bidang teknologi informasi sebagai alat bantunya, contohnya pembelian barang dengan menggunakan nomor kartu kredit curian melalui media internet;
b. Kejahatan timbul setelah adanya internet, dengan menggunakan sistem komputer sebagai korbannya, contoh kejahatan ini ialah perusak situs internet (*cracking*), pengiriman virus atau program-program komputer yang bertujuan untuk merusak sistem kerja komputer.

Menurut Maskun (2017 : 13) Tindak Pidana Siber disebut juga sebagai kejahatan lahir sebagai dampak negatif dari perkembangan aplikasi internet. Dari pengertian ini bahwa Tindak Pidana Siber mencakup semua jenia kejahatan beserta modus operandinya yang dilakukan sebagai negatif aplikasi internet. Secara umum yang dimaksud kejahatan komputer atau kejahatan didunia siber yaitu upaya memasuki dan atau menggunakan fasilitas komputer atau jaringan komputer tanpa izin dan dengan melawan hukum dengan atau tanpa menyebabkan perubahan dan atau kerusakan pada fasilitas komputer yang dimasuki atau digunakan tersebut.

Dengan demikian jelaslah bahwa jika seseorang menggunakan komputer atau bagian dari jaringan komputer tanpa seijin yang berhak, tindakan tersebut sudah tergolong kejahatan komputer. Perkembangan Tindak Pidana Siber yang masih relatif baru mengakibatkan belum adanya definisi yang final terhadap tindak pidana siber itu sendiri.

Menurut Barda Nawawi Arief (dalam Widodo, 2009 : 23), pengertian *computer related crime* sama dengan Tindak Pidana Siber. Ronny R. Nitibaskara berpendapat, bahwa kejahatan yang terjadi melalui atau pada jaringan komputer di dalam internet disebut Tindak Pidana Siber atau cybercrime, kejahatan ini juga dapat disebut kejahatan yang berhubungan dengan komputer (*computer related crime*), yang mencakup dua hal kategori kejahatan, yaitu kejahatan yang menggunakan komputer sebagai sarana atau alat dan menjadikan komputer sebagai sasaran atau objek kejahatan.

Goodman dan Brenner (dalam Didik Herman Sulistyo Sutanto, 2015 : 27) melakukan survey mengenai Tindak Pidana Siber. Survey ini menunjukan bahwa di negara – negara yang relatif maju teknologi informasinya Tindak Pidana Siber dapat dibedakan menjadi delapan kategori, yaitu: akses yang tidak sah, merubah dan memanipulasi data pada komputer secara tidak sah, sabotase terhadap komputer, pemanfaatan sistem informasi secara melawan hukum, penipuan dengan komputer (*computer fraud*, spionase (industrial, keamananan dan lain lain), dan pelanggaran privasi.

Lastwoka dan Hunter (dalam Budi Sahariyanto, 2013 : 14) mendefinisikan Tindak Pidana Siber sama dengan apa yang biasanya disebut sebagai *virtual crime* (kejahatan maya), yaitu suatu kejahatan dilakukan terhadap komputer atau dengan alat bantu komputer. Meskipun gambaran mengenai Tindak Pidana Siber cukup beragam, pada dasarnya terdapat karakteristik tertentu yang dapat digunakan untuk mengenali Tindak Pidana Siber. Pada umumnya Tindak Pidana Siber memiliki ciri – ciri sebagai berikut: *non-violence* (tanpa kekerasan), sedikit melibatkan kontak fisik (*minimum of physical contact*), menggunakan peralatan dan teknologi, memanfaatkan jaringan telematika global (Edmon Makarim, 2003 : 56).

Berdasarkan ciri – ciri tersebut, terutama ciri yang terakhir, Tindak Pidana Siber dapat terjadi dengan mengaitkan beberapa wilayah hukum atau beberapa negara sekaligus. Hal ini sesuai dengan rekomendasi yang dikeluarkan oleh negara-negara G-8 yang menyatakan bahwa *high tech* dan *computer relate crimes* termasuk ke dalam *transnational crime*. Masuknya *cybercrime* ke dalam kategori *transnational crime* berarti bahwa tindak pidana siber melibatkan lintas yurisdiksi.

Menurut Sutan Remy Syahdeini (2009 : 40) Di Indonesia *cybercrime* dapat diartikan dengan tindak pidana komputer. Definisinya adalah perilaku yang dilakukan oleh pelakunya dengan menggunakan program komputer sebagai sarana untuk menggunakan program komputer sebagai sarana untuk melakukan perbuatan tersebut atau yang dilakukan

oleh pelakunya terhadap sistem komputer sebagai sasarannya dan telah dikriminalisasi oleh undang – undang pidana sebagai tindak pidana.

Berdasarkan definisi – definisi di atas, dapatlah dirumuskan bahwa tindak pidana siber itu merupakan segala tindakan yang merugikan orang lain dengan menggunakan komputer sebagai alat untuk melakukan kejahatan serta sistem dan data di dalamnya sebagai target. Atau, Tindak Pidana Siber dirumuskan sebagai perbuatan melawan hukum yang dilakukan dengan memakai komputer sebagai sarana/alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. Secara ringkas tindak pidana siber ini dapat didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan teknologi komputer canggih (A. Dipanegara, 2009 : 26).

Menurut Petrus Reinhard Golose (dalam Budi Sahariyanto, 2013 : 15) dalam kasus kejahatan dunia maya, baik korban maupun pelaku tidak berhadapan langsung dalam 1 (satu) tempat kejadian perkara. Dalam beberapa kasus, baik korban maupun pelaku dapat berada pada negara yang berbeda. Hal tersebut menggambarkan bahwa kejahatan dunia maya merupakan salah satu bentuk kejahatan lintas negara (*transnational crime*), dan tak berbatas (*borderless*), tanpa kekerasan (*non violence*), tidak ada kontak fisik (*no phisically contact*) dan tanpa nama (*anonimity*).

2. Jenis-Jenis Tindak Pidana Siber

Menurut Hermawan Sutanto Sulistyo (2002 : 78), Seperti pengertiannya, jenis-jenis tindak pidana siber secara umum banyak sekali

dan berbeda-beda karena pandangan setiap ahli hukum memiliki pandangan masing-masing selain itu juga belum ada kesepakatan yang seragam mengenai pengertian tindak pidana siber itu sendiri sehingga membuat terjadinya perbedaan. Banyak jenis kejahatan komputer yang telah berkembang secara pesat sejak diperkenalkannya Internet berkaitan dengan pengembangan dan perkembangan teknologi informasi. Perkembangan dari waktu ke waktu jenis-jenis tindak pidana siber bermunculan dengan upaya pembentukan undang-undang untuk mengkriminalisasi kejahatan-kejahatan baru tersebut menjadi tindak pidana. Disetiap negara berbeda-beda dalam mengatur tindak pidana siber. Berikut ini jenis-jenis tindak pidana siber secara umum adalah :

a. Kejahatan Terhadap Harta Kekayaan

banyak jenis kejahatan komputer yang telah muncul sejak diperkenalkannya Internet berkaitan dengan pengembangan dan perkembangan teknologi informasi. Dari waktu ke waktu jenis-jenis kejahatan komputer bermunculan dan berpacu dengan upaya pembentuk undang-undang untuk menkriminalisasi kejahatan-kejahatan baru tersebut menjadi tindak pidana.

1) cybersquatting

domain name adalah aset yang sangat berharga karena dapat diperjual-belikan, disewa, dapat menjadi situs pemasangan iklan sehingga menjadi sumber keuangan, bahkan dapat dijaminkan, maka para penjahat melihat peluang untuk menjadikan *domain name*

sebagai objek perdagangan, yaitu dengan melakukan *cybersquatting*. *cybersquatting* adalah perbuatan yang dilakukan oleh seorang spekulator untuk mendaftarkan suatu *domain name* mendahului pihak lain, yaitu pihak yang sesungguhnya akan menggunakan *domain name* tersebut.

Tujuan pelaku mendahului mendaftarkan *domain name* tersebut adalah untuk ditawarkan kepada pihak yang sesungguhnya akan menggunakan *domain name* tersebut adalah untuk ditawarkan kepada pihak yang sesungguhnya akan menggunakan *domain name* tersebut dengan memperoleh keuntungan besar. Pelaku *cybersquatting* disebut *cybersquatter*. Pada kejahatan *cybersquatting*, pendaftaran *domain name* dilakukan dengan menggunakan nama orang apabila korbannya adalah seorang tokoh ternama yang di era Internet ini tentunya perlu memiliki website pribadi. Tokoh – tokoh terkenal itu misalnya tokoh politik dan para selebritis seperti bintang film, apabila korbanya adalah perusahaan, yang digunakan adalah nama perusahaan atau *trademark* atau *service merk* perusahaan tersebut.

Sejak internet menjadi sumber marketing yang sangat penting dipertengahan Tahun 1990-an, muncul berbagai sengketa mengenai pendaftaran-pendaftaran *domain name*. Sengketa tersebut dapat terjadi antar perusahaan yang terkait dengan nama yang sama atau serupa dengan *domain name* tersebut di berbagai sektor industri

atau antar negara. Sengketa tersebut banyak terjadi antara para pemilik asli dari nama – nama terkenal atau merek – merek dagang yang telah terlebih dahulu didaftarkan oleh para spekulator. Tujuan dari para spekulator adalah untuk menjual *domain name* tersebut kepada para pemilik asli nama – nama yang telah dipakai dalam *domain name* tersebut.

Oleh karena perusahaan pendaftar penerima permohonan pendaftaran nama tersebut berdasarkan asas "siapa duluan dia yang akan dilayani terlebih dahulu" (*on first come, first served basis*), maka dimungkinkan bagi pendaftar untuk mencuri start terlebih dahulu mendaftarkan nama perusahaanperusahaan maupun tokoh-tokoh tersebut. Inilah awal mula terjadinya tindak pidana komputer menyangkut perihal *domain name* yang disebut dengan *cybersquatting.* Hal yang paling penting dengan pendaftaran *domain name* adalah kecepatan. Artinya secepatnya mendaftarkan *domain name* yang memuat nama ada *trademark* atau *service mark* perusahaannya sebelum orang lain melakukannya.

Salah satu contoh kasus yang terkenal ada kasus *microsoft corporation. domain name www.microsoft.org* telah didaftarkan oleh Amit Mehtora jauh sebelum *microsoft corporation* bermaksud untuk mendaftarkan *domain name*-nya. Keterlambatan *Microsoft Corporation* bermaksud untuk mendaftarkan domain name yang mengandung namanya sendiri atau trademark-nya sebelum orang

lain mendaftarkan nama tersebut mengakibatkan munculnya masalah hukum bagi *microsoft coorporation*. Sekalipun *microsoft coorporation* tidak dapat memakai *www.microsoft.org* sebagai *domain name*-nya berlakunya asas "*on first come, first served basis*" dalam pendaftaran domain name.

2) Pembajakan HAKI

Internet telah menimbulkan masalah baru dibidang Hak Atas Kekayaan Intelektual (HAKI). *copyright, trademark, patent, trade secret,* dan *moral right* sangat terpengaruh oleh Internet. Internet memiliki beberapa karakteristik teknis yang membuat masalah – masalah HAKI tumbuh dengan subur. Salah satu masalah yang timbul adalah berkaitan dengan pembajakan hak cipta.

b. Kejahatan Menyangkut Identitas

Menurut Hermawan Sutanto Sulistyo (2002 : 82), Kejahatan – kejahatan komputer yang menyangkut identitas berupa pencurian identitas orang lain yang tersimpan secara *computerized,* yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materil maupun immateri. Salah satu bentuk kejahatan tersebut adalah menggunakan identitas orang lain guna memalsukan kartu kredit dalam kejahatan yang disebut dengan *carding.*

1) phising atau identity theft

phising merupakan salah satu bentuk dari kejahatan Internet yang disebut *identity theft.* phishing adalah pengiriman *e-mail* palsu

atau *spoofed e-mail* kepada seseorang atau suatu perusahaan atau suatu organisasi dengan menyatakan bahwa pengirim adalah suatu entitas bisnis yang sah. Pengiriman *e-mail* tersebut menampilkan *e mail* itu dalam bentuk dan dengan isi seperti suatu *e-mail* yang bukan *e-mail* palsu. Penerima yang mengira bahwa *e-mail* yang diterimanya itu adalah *e-mail* yang bukan *e-mail* palsu akan menanggapi *e-mail* tersebut dengan mengunjungi *website* pengirim *e-mail* dan kemudian terpancing untuk mengungkapkan informasi mengenai diri dari penerima *email* palsu tersebut, antara lain mengungkapkan password, nomor *credit card,* nomor *social security* dan nomor rekening bank sebagaimana yang diminta oleh pengirim *e-mail* dalam *e-mail* nya itu. *website* tersebut sengaja dibuat untuk mencuri informasi pribadi korbannya. Pada umumnya *phising* memang dilakukan melalui email, tetapi ada pula yang dilakukan melalui sms pada *handphone.*

Sekalipun banyak *e-mail* palsu tersebut tampil menyakinkan seperti yang asli, yaitu lengkap dengan logo perusahaan dan menampilkan *links* kepada *website* yang asli, tetapi banyak yang tampil sangat menggelikan karena dilakukan oleh seseorang yang bukan profesional. Hal itu tampak dari formatnya yang cenderung seperti asal – asalan, terjadinya kesalahan -kesalahan *grammar* dalam kalimat – kalimat yang ditulis, dan terjadinya kekeliruan *spelling* dari kata-kata yang digunakan.

2) carding

carding atau *credit card fraud* adalah suatu kejahatan kartu kredit, merupakan salah satu bentuk dari pencurian *(theft)* dan kecurangan *(fraud)* di dunia internet yang dilakukan oleh pelakunya dengan menggunakan kartu kredit *(credit card)* curian atau kartu kredit palsu yang dibuatnya sendiri Tujuannya tentu saja adalah untuk membeli barang secara tidak sah atas beban rekening dari pemilik kartu kredit yang sebenarnya atau untuk menarik dana secara tidak sah dari suatu rekening bank milik orang lain. Modus operasi dari *carding* ini adalah :

a) Dengan mencuri kartu kredit atau *credit card;*
b) Dengan menanamkan *spyware parasites;*
c) *spyware parasites* ini dapat melakukan pencurisn identitas (*identity theft*) dan dapat menelusuri nomor-nomor kartu kredit ketika seorang pemegang kartu kredit menggunakan kartu kreditnya untuk berbelanja secara *online;*
d) Seorang petugas toko *(merchant)* menyalin tanda tangan terima penjualan *(sale receipt)* dari barang yang dibeli oleh pelanggan dengan tujuan untuk dapat digunakan melakukan kejahatan dikemudian hari;
e) Dengan melakukan *skimming. Skimming* merupakan suatu *hi-tech method,* yaitu si pelaku memperoleh informasi mengenai izin pribadi korban atau mengenai rekening korban dari kartu

kredit, surat izin mengemudi (SIM), kartu tanda penduduk (KTP), atau paspor anda. Pelaku menggunakan suatu alat elektronik *(electronic device)* untuk informasi tersebut.

c. Kejahatan Terhadap Privasi

Kejahatan terhadap privasi adalah kejahatan komputer terhadap privasi pihak lain. Korban yang dapat menjadi sasaran kejahatan ini dapat berupa seseorang, organisasi bukan badan hukum, badan hukum swasta antara lain yayasan, koperasi, perusahaan, partai politik yang berbadan hukum dan milik negara yang antara lain BUMN, bank sentral, lembaga – lembaga negara , pemerintah, lembaga swadaya masyarakat, komunitas masyarakat dan lain sebagainya.

1) *cyberstalking*

Seperti halnya dengan kejahatan – kejahatan komputer pada umunya, demikian juga definisi dari *cyberstalking* belum ada yang sudah diterima secara universal. *cyberstalking* berasal dari dua kata, yaitu *"cyber"* dan *"stalking"*. Arti *cyber* telah kita diketahui bersama sebelumnya. Arti yuridis dari *"stalking"* adalah:

> *harass somebody persistently: to harass somebody criminally by persistent, inappropriate, and unwanted attention, e.g. by constantly following, telephoning, e-mailing, or writting to him or her.*

Gangguan baru dapat dikatakan *stalking* hanya apabila gangguan tersebut dilakukan terus-menerus atau tidak henti-hentinya dengan melakukan perbuatan-perbuatan yang tidak diinginkan oleh pihak pengganggu. Misalnya mengikuti, menelepon,

mengirim *e-mail*, mengirim surat kepada seseorang terus-menerus tanpa henti dalam waktu berhari – hari lamanya. Sudah tentu isi dari telepon, isi *e-mail*, isi surat dari penganggu tersebut sangat tidak disukai oleh orang yang diganggu sehingga sangat menjengkelkan.

Apabila *stalking* itu dilakukan dengan menggunakan Internet maka perbuatan *stalking* itu disebut *cybertalking*. c*yberstalking* adakalanya disebut *cyberharassment*, kebanyakan orang menyebut dua kata itu dalam tindak pidana ini. Sedangkan pelaku kejahatanya disebut *cyberstalker*.

2) *cyberterrorism*

Dengan perkembangan teknologi informasi yang sangat pesat, terutama perkembangan Internet, telah muncul bentuk terorisme baru yang disebut dengan *cyberterrorism*. Dari istilah ini saja secara mudah dapat diduga bahwa terorisme tersebut pasti dilakukan dengan menggunakan program komputer sebagai sarananya.

Untuk melakukan *cyberterrorism*, pelaku *cyberterrorism* yang disebut *cyberterrorist*, harus terlebih dahulu mampu membobol sistem komputer pihak yang akan diteror. Dengan demikian, sebelum melakukan teror pelaku harus berhasil melakukan hacking terhadap sistem komputer pihak yang akan diteror. Dengan kata lain seorang *cyberterrorist* adalah *hacker* atau

cracker yang dalam melakukan *hacking* bertujuan untuk melakukan teror.

Dengan munculnya terorisme melalui jaringan komputer atau menggunakan program komputer, maka terorisme dapat terjadi baik didunia nyata atau didunia virtual. *cyberterrorism* adalah terorisme dengan menggunakan komputer atau melalui dunia virtual. Ternyata belum ada definisi mengenai terorisme itu sendiri yang disepakati secara global. Oleh karena itu belum pula terdapat kesepakatan mengenai apa yang disebut dengan *cyberterrorism*.

d. Kejahatan Terhadap Sistem Komputer

Kejahatan yang dilakukan dengan memasuki ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan *(hacker)* melakukan dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun begitu, ada juga yang melakukannya hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi.

hacking and cracking Dalam dunia komputer, terdapat dua istilah yang semula berbeda artinya tetapi dalam perkembangannya menjadi dua istilah yang memiliki arti yang sama. Kedua istilah itu adalah *hacking* dan *cracking. hacking* adalah perbuatan membobol sistem komputer. Tindak pidana didunia maya ini adalah melakukan

perbuatan memasuki sistem komputer orang lain tanpa izin atau otoritasi dari pemiliknya. Pelaku *hacking* adalah *hacker.* Menurut Susan W. Brenner (dalam Budi Sahariyanto, 2013 : 20) :

> *hacking is gaining unauthorised access to a computer system and, as such is conceptually analogous to realworld tresspassing*.

Sementara itu yang dimaksudkan dengan cracking menurut Brenner adalah:

> *Gaining unathorised accsess to a computer system for the purpose of committing a crime "inside" the system, is conceptually analogues to burglary"*.

Apabila hal itu terjadi di dunia nyata, *cracking* sama dengan *burglary* atau pencurian. Menurut para *hacker,* tujuan *cracker* adalah membobol *secure system* dari komputer, sedangkan tujuan para *hacker* hanyalah untuk memperoleh pengetahuan tentang system-sistem komputer. Media massa telah menggunakan istilah *hacker* bagi orang-orang yang mengakses sistem-sistem komputer tanpa memperoleh otorisasi dengan tujuan untuk mencuri dan menyalahgunakan data yang tersimpan dalam system-sistem komputer tersebut, yaitu istilah *hacker* seharusnya disebut *cracker*, bukan *hacker.*

e. Kejahatan Terhadap Ketertiban Umum

Merupakan kejahatan dengan memasukan data atau informasi ke Internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Sebagai contohnya, pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau harga diri pihak lain, hal – hal yang

berhubungan dengan pornografi atau pemuatan suatu informasi yang merupakan rahasia negara, agitasi dan propaganda untuk melawan pemerintahan yang sah dan sebagainya.

1) Perjudian di Internet

Perjudian Internet *(internet gambling, online gambling,* atau *cyberspace gambling)* ternyata merupakan merupakan industri yang berkembang sangat pesat kelahirannya. Perjudian Internet telah memusingkan perusahaan-perusahaan penerbit kartu kredit berkenaan dengan penggunaan kartu kredit oleh para penjudian. Para penegak hukum mengemukakan bahwa perjudian di Internet dapat digunakan untuk melakukan pencucian uang. Para penegak hukum mengemukakan bahwa masalah-masalah anonimitas *(anonymity)* dan yurisdiksional *(jurisdictional)* yang merupakan ciri dari perjudian Internet merupakan sarana yang sangat menguntungkan bagi para pencuci uang.

2) Pornografi Anak di Internet

Pornografi anak atau *child pornography* atau *child porn* adalah bahan-bahan porno yang menampilkan anak-anak. Kebanyakan negara menyebutkan hal ini dengan sebagai bentuk dari *child sexual abuse* dan merupakan hal yang melanggar hukum. Dimana *child pornography* berupa foto-foto yang menampilkan anak-anak yang terlibat dalam perilaku seksual dan memproduksi bahan-bahan tersebut dengan sendirinya dilarang hukum sebagai *child sexual abuse* di kebanyakan

negara. Perkembangan dan meningkatnya akses kepada Internet, serta penggunaan teknologi *home-computer* telah mengubah besar-besaran cara distribusi gambar – gambar porno ini karena mudahnya melakukan akses kepada Internet dan makin murahnya biaya produksi dan distribusi gambar-gambar tersebut terutama secara lintas batas negara. Teknologi komputer telah mentransformasikan produksi dari gambar – gambar ini ke dalam suatu industri global yang canggih

3. Pengaturan Tindak Pidana Siber di Indonesia

a. Undang-Undang No 36 Tahun 1999 tentang Telekomunikasi

Dalam undang-undang tersebut terdapat beberapa pasal yang mengatur perbuatan yang dilarang yang termasuk tindak pidana *cybercrime*. Sebelum ada Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, undang-undang ini yang digunakan untuk mengancam pidana bagi perbuatan yang dikategorikan dalam tindak pidana *cybercrime*. Namun undang-undang ini hanya mengatur beberapa tindak pidana yang termasuk tindak pidana *cybercrime* yang masih bersifat umum dan luas, dan hanya berkaitan dengan telekomunikasi, sehingga belum dapat mengakomudir tindak-tindak pidana yang berkaitan dengan komputer.

Pasal 22 yang berbunyi**: "**Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi :

1) Akses ke jaringan telekomunikasi; dan atau
2) Akses ke jasa telekomunikasi; dan atau

3) Akses ke jaringan telekomunikasi khusus."

Pasal 38 yang berbunyi : Setiap orang dilarang melakukan perbuatan yang dapat menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi.

Pasal 40 yang berbunyi : Setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun.

Bentuk-bentuk tindak pidana *cybercrime* dalam Undang-undang Nomor 36 tahun 1999 tentang Telekomunikasi adalah Akses Illegal yakni tanpa hak, tidak sah, atau memanipulasi akses ke jaringan telekomunikasi, menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi dan penyadapan informasi melalui jaringan telekomunikasi. Hal ini merujuk pada pengertian *cybercrime* yang diberikan oleh Konferensi PBB yang menyatakan *cybercrime* adalah perbuatan yang tidak sah yang menjadikan komputer atau jaringan komputer, baik pada system keamananya. Telekomunikasi merupakan salah satu bentuk jaringan dan sistem komputer sehingga perbuatan yang dilarang dalam pasal-pasal tersebut dapat dikategorikan menjadi tindak pidana *cybercrime*.

b. Undang-Undang No 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang No 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

Tanggal 25 November 2016 telah diundangkan Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi

Elektronik (ITE). Undang-undang ini bukanlah undang-undang tindak pidana khusus, melainkan juga memuat tentang pengaturan mengenai pengelolaan informasi dan transaksi elektronik dengan tujuan pembangunan, namun undang undang ini juga mengantisipasi pengaruh buruk dari pemanfaatan kemajuan teknologi ITE tersebut, yakni dengan diaturnya hukum pidana khususnya tentang tindak pidana yang menyerang kepentingan hukum orang pribadi, masyarakat, atau kepentingan hukum Negara dengan memanfaatkan kemajuan teknologi ITE, atau sering disebut tindak pidana *cybercrime*.

UU ITE telah menetapkan perbuatan-perbuatan mana yang termasuk tindak pidana di bidang ITE (*cybercrime*) dan telah ditentukan unsur-unsur tindak pidana dan penyerangan terhadap berbagai kepentingan hukum dalam bentuk rumusan-rumusan tindak pidana tertentu. Tindak Pidana c*ybercrime* dalam UU ITE diatur dalam 9 pasal, dari pasal 27 sampai dengan pasal 35. Dalam 9 pasal tersebut dirumuskan 20 bentuk atau jenis tindak pidana ITE. Pasal 36 tidak merumuskan bentuk tindak pidana ITE tertentu, melainkan merumuskan tentang dasar pemberatan pidana yang diletakkan pada akibat merugikan orang lain pada tindak pidana yang diatur dalam Pasal 27 sampai dengan Pasal 34. Sementara ancaman pidananya ditentukan didalam Pasal 45 sampai Pasal 52.

Dari uraian rumusan pasal-pasal bentuk-bentuk tindak pidana Siber menurut Undang-undang Nomor 19 Tahun 2016 tentang perubahan atas undang-undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik dapat diklasifikasikan menjadi 2 bentuk yakni :

1) *cybercrime* yang menggunakan komputer sebagai alat kejahatan, yakni Pornografi Online (c*yber-Porno*), Perjudian Online, Pencemaran nama baik melalui media sosial, penipuan melalui komputer, pemalsuan melalui komputer, pemerasan dan pengancaman melalui komputer, penyebaran berita bohong melalui komputer, pelanggaran terhadap hak cipta, *cyber terrorism.*
2) *cybercrime* yang berkaitan dengan komputer, jaringan sebagai sasaran untuk melakukan kejahatan, yakni akses tidak sah (*illegal acces),* menggangu sistem komputer dan data komputer, penyadapan atau intersepsi tidak sah, pencurian data, dan menyalahgunakan peralatan komputer.

4. Bentuk-Bentuk Tindak Pidana Siber

Menurut Didik M. Arif Mansur (2005 : 15) Tindak Pidana Siber mempunyai bentuk beragam, karena setiap negara tidak selalu sama dalam melakukan krimininalisasi. Begitu pula, dalam setiap negara dalam menyebut apakah suatu perbuatan tergolong kejahatan *cybercrime* atau bukan kejahatan *cybercrime* juga belum tentu sama. Secara teoritik,

berkaitan dengan konsepsi kejahatan. Didik M. Arif Mansur mengemukakan bahwa asas *mala in se* mengajarkan bahwa suatu perbuatan dikategorikan sebagai kejahatan karena masyarakat dengan sendirinya menganggap perbuatan tersebut jahat. Sedangkan berdasarkan asas *mala prohibita,* suatau perbuatan dianggap jahat karena melanggar peraturan perundang-undangan. Asas *mala prohibita* menghasilkan konsep si kejahatan dalam arti yuridis (yaitu sebagaimana diatur dalam peraturan perundang-undangan tertulis).

Tindak Pidana Siber meliputi pelanggaran hak kekayaan intelektual, fitnah atau pencemaran nama baik, pelanggaran terhadap kebebasan pribadi (*privacy*), ancaman dan pemerasan, ekploitasi seksual anak-anak dan pencabulan, perusakan sistem komputer, pembobolan kode akses, dan pemalsuan tanda tangan digital. Semua perbuatan tersebut dapat dipertanggungjawabkan secara pidana sesuai dengan yurisdiksinya. Tindak Pidana Siber juga dapat berbentuk pemalsuan data, penyebaran virus komputer ke jaringan komputer atau sistem komputer, penambahan atau pengurangan sistem instruksi dalam jaringan komputer, pembulatan angka, perusakan data, dan pembocoran data rahasia.

Berdasarkan uraian *handbook on computer crime, cybercrime* dikategorikan menjadi tiga. Kategori pertama, *cybercrime* adalah kejahatan ekonomi yang terkait dengan komputer, meliputi penipuan dengan manipulasi komputer, pembajakan perangkat lunak komputer, spionase komputer, sabotase, pencurian jasa, akses tidak sah ke dalam

sistem atau jaringan komputer, komputer sebagai alat untuk menyerang bisnis tradisional. Kategori ke dua, adalah pelanggaran terhadap keleluasaan pribadi, yaitu penggunaan data yang tidak benar, pengumpulan data secara tidak sah, penyalahgunaan data, pelanggaran rahasia perusahaan. Sedangkan kategori ke tiga, misalnya melakukan penyerangan terhadap dan kepentingan politik, dan penyerangan terhadap kebebasan pribadi orang per orang.

Selain penggolongan Tindak Pidana Siber sebagaimana terjabar di atas, (Jonathan Rosenoer, 1997 : 67) mengklasifikasikan bentuk bentuk Tindak Pidana Siber ke dalam empat klarifikasi berikut :

1. Komputer sebagai Objek Dalam kategori ini, bentuk-bentuk *cybercrime* termasuk kasus-kasus perusakan terhadap komputer, data atau program yang terdapat di dalamnya atau perusakan terhadap sarana-sarana komputer seperti *air condutouring (AC)* dan peralatan yang menunjang pengoprasian komputer.
2. Komputer sebagai Subjek Komputer dapat pula menimbulkan tempat atau lingkungan untuk melakukan kejahatan, misalnya pencurian, penipuan, dan pemalsuan yang menyangkut harta benda dalam bentuk baru yang tidak dapat disentuh (*intangible*), misalnya pulsa elektronis dan guratan-guratan magnetis.
3. Komputer sebagai Alat Komputer digunakan sebagai alat melakukan kejahatan sehingga sifat peristiwa kejahatan tersebut adalah sangat kompleks dan sulit diketahui. Salah satu contoh adalah seseorang

pelaku kejahatan yang mengambil warkat-warkat setoran darai suatu bank dan menulis nomor rekening pelaku dengan tinta magnetis pada warkat-warkat tersebut kemudian meletakkan kembali ke tempat semula. Nasabah yang akan memasukkan uang akan mengambil dan mengisi warkat yang sudah dibubuhi nomor rekening pelaku kejahatan memproses warkat-warkat nasabah, komputer secara otomatis akan mengredit sejumlah uang pada rekening pelaku kejahatan. Salah satu, pelaku kejahatan menarik uang dengan cek dari rekeningnya sebelum peram nasabah yang menyetor mengajukan komplain ke bank.

4. Komputer sebagai simbol Suatu komputer dapat digunakan sebagai simbol untuk melakukan penipuan atau ancaman, dalam kategori ini termasuk penipuan “Biro Jodoh” yang menyatakan bahwa biro jodoh tersebut memakai komputer untuk membantu si koraban mencari jodoh, akan tetapi ternyata birojodoh tersebut sama sekali tidak memakai komputer untuk keperluan tersebut.

Berdasarkan ringkasan ketentuan dalam *convention on cybercrime* dapat dipahami bahwa dalam bagian 1, Pelanggaran terhadap kerahasiaan, ketersediaan dan integeritas sistem dan data komputer, terdiri atas perbutan berikut :

1. Akses tidak sah, yaitu sengaja memasuki atau mengakses komputer tanpa hak (Pasal 2);

2. Intersepsi tidak sah, yaitu sengaja dan tanpa hak mendengar atau menangkap secara diam-diam pengiriman transmisi dan pemancaraan (emisi) data komputer yang tidak bersifat public ke, dari atau di dalam sisitem komputer dengan menggunakan alat bantu teknis (Pasal 3);
3. Gangguan atau perusakan data, yaitu sengaja dan tanpa hak melakukan perusakan.
4. Penghapusan, perubahan atau penghapusan data computer (Pasal 4) ;
5. Gangguan atau perusakan sistem, yaitu sengaja melakukan gangguan atau rintangan secara serius tanpa hak terhadap berfungsinya sistem komputer (Pasal 5);
6. Penyalahgunaan peralatan, yaitu penyalahgunaan perlengkapan komputer, termasuk program komputer, *password* komputer, kode masuk (*access code*) (Pasal 6).

Kemudian dalam bagian 2, diatur tentang pelanggaran yang berhubungan dengan komputer, yaitu dalam bentuk berikut :

1. Pemalsuan yang berhubungan dengan komputer (Pasal 7), yaitu pemalsuan (dengan sengaja dan tanpa hak memasukkan, mengubah, menghapus data otentik menjadi tidak otentik dengan maksud untuk digunakan sebagai data otentik);
2. Penipuan yang berhubungan dengan komputer (Pasal 8), yaitu penipuan (dengan sengaja dan tanpa hak menyebabkan hilangnya barang atau kekayaan orang lain dengan cara memasukkan, mengubah, menghapus data komputer, atau dengan mengganggu

berfungsinya komputer, dengan tujuan untuk memperoleh keuntungan ekonomi bagi dirinya sendiri atau orang lain).

Selanjutnya dalam bagian 3 tentang Pelanggaran yang berhubungan dengan isi, yaitu berkaitan dengan delik-delik yang berhubungan dengan pornografi anak (Pasal 9), yaitu meliputi perbuatan :

1. Memproduksi dengan tujuan mendistribusikan melalui system komputer;
2. Menawarkan melalui sistem komputer;
3. Mendistribusikan atau mengirim melaui sistem komputer;
4. Memperoleh melalui sistem komputer;
5. Memiliki dalam sistem komputer atau di dalam media penyimpanan data.

Akhirnya dalam bagian 4 tentang Pelanggaran yang berhubungan dengan Hak Cipta (Pasal 10), yaitu delik-delik yang terkait dengan pelanggaran hak cipta. Sedangkan pada bagian 5, diatur tentang pertanggungjawabkan pidana dan sanksi; Percobaan dan Pembantuan (Pasal 11); Pertanggungjawaban Korporasi (Pasal 12); Sanksi dan tindakan (Pasal 13).

Berdasarkan ketentuan-ketentuan dalam konvensi tersebut dapat disimpulkan bahwa delik-delik *cybercrime* suadah diatur secara umum dalam konvensi. Meskipun demikian, setiap Negara diberi peluang untuk mengembangkan dan mengharmonisasikan dengan kebutuhan Negara yang bersangkutan tanpa mengesampingkan kepentingan masyarakat

internasional. Karena itu, bahasa yang digunakan bersifat netral, dan bentuk-bentuk kejahatan yang diatur dalam konvensi adalah ketentuan standar minimum.

5. Tindak Pidana Siber di Indonesia

Tindak Pidana Siber yang marak di Indonesia meliputi penipuan kartu kredit, penipuan perbankan, *defacing*, *cracking*, transaksi seks, pornografi, judi online, penyebaran berita bohong melalui internet dan terorisme. Terdapat beberapa jenis kasus tindak pidana siber yang banyak terjadi di Indonesia berdasarkan modusnya, yaitu:

a) Pencurian Nomor Kredit

Menurut Rommy Alkatiry, penyalahagunaan kartu kredit milik orang lain di internet merupakan kasus *cyber crime* terbesar yang berkaitan dengan dunia bisnis internet di Indonesia. Penyalahgunaan kartu kredit milik orang lain memang tidak terlalu rumit dan bisa dilakukan secara fisik atau *online*. Nama dan kartu kredit orang lain yang diperoleh di berbagai tempat (restaurant, hotel, atau segala tempat yang melakukan transaksi pembayaran dengan kartu kredit) dimasukkan diaplikasi pembelian barang di Internet.

b) Memasuki, Memodifikasi, atau Merusak *homepage* (*hacking*)

Seiring tahun berlalu, kasus *hacking* atau peretasan semakin sering terjadi. Kasus peretasan umumnya bertujuan untuk mengambil data-data tertentu yang dimiliki target. Tapi ada juga peretasan yang

bertujuan menghancurkan data atau sistem tertentu sehingga berdampak seperti kerusakan digital.

Menurut John. S. Tumiwa pada umumnya tindakan *hacker* Indonesia belum separah aksi di luar negeri. Perilaku *hacker* Indonesia masih sebatas masuk ke suatu situs komputer orang lain yang ternyata rentan penyusupan dan memberitahukan kepada pemiliknya untuk berhati-hati. Di luar negeri *hacker* sudah memasuki sistem perbankan dan merusak data base bank. (Budi Sahariyanto, 2013 : 18)

c) Penyerangan Situs atau *e-mail* melalui virus atau s*pamming*

spamming merupakan sistem pengriman pesan/berita iklan secara massal dan seringkali *spammers* (pelaku *spamming*) mengirimkan *spam*-nya secara bertubi-tubi dalam jumlah yang banyak dan tanpa kehendak si penerima.

spam dikirimkan oleh pengiklan dengan biaya operasional yang sangat rendah, karena *spam* tidak memerlukan senarai (*mailing list*) untuk mencapai para pelanggan yang diinginkan. Karena hambatan masuk yang rendah maka banyak *spammers* yang muncul dan jumlah pesan yang tidak diminta menjadi sangat tinggi.

Akibatnya, banyak pihak yang dirugikan, selain pengguna internet itu sendiri, *ISP* (Penyelenggara Jasa Internet atau (*internet service provider*), dan masyarakat umum juga merasa tidak nyaman. *Spam* sering mengganggu dan terkadang menipu penerimanya.

Berikut ini beberapa contoh kasus *spam* yang terjadi di Indonesia:

1. Kasus penipuan yang dialami beberapa korban yang juga merupakan konsumen dan juga pengguna situs jual beli di dunia maya, seperti:
    a. Kasus yang bersumber dari postingan F David Talalo, diforum fotografer.net, dimana korban memberikan informasi mengenai dirinya yang telah menjadi korban penipuan. *"Baru baru ini saya tergiur dengan iklan penawaran kamera digital SLR disitus tokobagus.com disitu ditawarkan oleh seorang pengiklan bernama charles zhang yg berdomisili di medan, kamera Nikon D200 body only hanya seharga 2,8 jt. Pengiklan menyertakan alamat lengkap beserta nama toko - Miracle Komputer di Shopping Centre YUKI Suka Ramai Lt. 2 no.29 dan nomor telepon 061-76503903. Bodohnya, saya terlanjur mentransfer uang sejumlah 2,8jt ke rekening milik bpk. Syukran. Baru kemudian setelah itu konfirmasi dari pihak mall dimedan menyatakan bahwa toko itu sudah tutup. Barang tidak sampai, nota pembelian pun tidak difax"*
    b. Kasus yang bersumber dari Facebook toko bagus yang beralamat Facebook.com/tokobagus, dimana korban memberikan informasi mengenai dirinya yang telah menjadi korban penipuan. "*Saya ditipu, saya kemaren membeli BB torch 9800 dan sudah mentransfer sejumlah Rp.800.000,- Ke BRI dengan NO REK 530601012007534 AN. RICKY EDISYAH PUTRA dengan nomor HP 085760868349 setelah uang ditransfer HP tidak aktif dan*

barang pun tidak ditrima, saya sangat kecewa setelah belanja OL di situs tokobagus.com"

2. Kasus penipuan yang akibat spamming melalui email hingga mengalami kerugian milyaran rupiah seperti kasus berikut ini :

   Penipuan yang terjadi terhadap seorang rektor Universitas Swasta di Jakarta dengan kerugian sejumlah 1,8 miliar. Kasus tersebut bermula ketika pada tanggal 3 september 2007 rektor tersebut menerima sebuah email yang berisi penugasan seorang warga Nigeria yang bernama Prince Shanka Moye yang membawa barang senilai US$ 25 Juta Ke indonesia. Barang yang bernilai mahal tersebut milik seorang pengusaha jerman yang telah mengalami kecelakaan pesawat di Perancis, namun terdapat syarat untuk mendapatkan barang berharga tersebut dimana rektor tersebut diminta untuk menyetorkan uang senilai Rp 1,8 miliar untuk biaya administrasi.

   Untuk lebih meyakinkan sang korban, Prince Shanka Moye menggunakan sebuah tipu muslihat dimana pelaku mengetahui secara detail mengenai pekerjaan sang rektor, "*Dia tahu betul pekerjaan saya. Dia tahu saya pernah kerja di PBB dan membantu proyek kemanusiaan. Makanya saya tertarik dan percaya."* kata rektor yang minta agar nama dan universitasnya dirahasiakan ini di Polda Metro Jaya, Jakarta, Rabu (26/9/2007).

Setelah masuk perangkap si pelaku, rektor tersebut mentransfer sejumlah uang ke rekening Moye.

Rektor tersebut diperintahkan untuk mentransfer uang Rp 56,7 Juta ke BCA Cabang Mandala pada 6 September 2007. Kemudian pada hari yang sama, rektor tersebut bertemu dengan Moye dan dimintai uang Rp 350 juta. Pertemuan tersebut berlanjut, Rektor dan Moye bertemu kembali pada 7 September di Hotel Mulia, Senayan Jakarta. Korban mengatakan "*Sudah menjual 2 rumah dan hasil kerja 40 tahun musnah. Saya terlalu mengebu-gebu mendapatkan barang itu. Saya ingin membangun kampus yang membutuhkan dana besar,".* Setelah uang Rp 1,8 miliar selesai ditransfer, karena barang berharga yang dijanjikan tidak kunjung didapatkan, rektor tersebut akhirnya melaporkan modus penipuan ini ke Polda Metro Jaya.

Karena itu, melihat sejarah kasus *spamming* di Indonesia dari jumlah presentasi dari tahun ke tahun semakin mengkhawatirkan dan melihat macam-macam kerugian atau dampak yang ditimbulkan maka wajar apabila jenis kejahatan ini dikriminalisasikan

d) *defacing*

defacing merupakan kegiatan mengubah halaman situs/website pihak lain, seperti yang terjadi pada situs Menkominfo dan Partai Golkar serta BI beberapa waktu lalu dan situs KPU saat pemilu 2004.

Tindakan *deface* ada yang semata-mata iseng, unjuk kebolehan, pamer kemampuan membuat program, tapi ada juga yang melakukannya untuk mencuri data dan dijual kepada pihak lain.

6. Penegakan Hukum Terhadap Tindak Pidana Siber

Menurut Satjipto Rahardjo (2009 : 24) Penegakan hukum merupakan suatu proses untuk mewujudkan keinginan-keinginan hukum menjadi kenyataan. Keinginan hukum inilah yang nantinya menjadi pikiran badan pembuat undang-undang yang dirumuskan dalam peraturan-peraturan hukum. Perumusan pikiran pembuat hukum dituangkan dalam peraturan hukum yang nantinya menentukan bagaimana penegakan hukum itu dijalankan.

Pada kenyataannya proses penegakan hukum memuncak pada pelaksanaannya oleh para pejabat penegak hukum. Aparat penegak hukum di Indonesia adalah hakim, jaksa, polisi. Hakim adalah salah satu aparat penegak hukum yang melaksanakan suatu sistem peradilan yang mempunyai tugas untuk menerima dan memutus perkara dengan seadil-adilnya. Hakim adalah pejabat yang melakukan kekuasaan kehakiman yang diatur dalam Undang-undang Nomor 48 Tahun 2009 tentang kekuasaan kehakiman.

Dalam rangka penegakan hukum di Indonesia tugas hakim adalah menegakkan hukum dan keadilan melalui perkara-perkara yang dihadapkan kepadanya. Jaksa adalah aparat penegak hukum yang merupakan pejabat fungsional yang diberikan wewenang oleh undang-

undang dan pelasanaan putusan pengadilan. Selanjutnya adalah Polisi, polisi sebagai penegak hukum dituntut melaksanakan profesinya secara baik dengan dilandasi etika profesi. Etika profesi tersebut berpokok pangkal pada ketentuan yang menentukan peranan polisi sebagai penegak hukum. Polisi dituntut untuk melaksanakan profesinya dengan adil dan bijaksana, serta mendatangkan keamanan dan ketenteraman.

Penegakan hukum selalu akan melibatkan manusia di dalamnya dan dengan demikian hal tersebut tingkah laku manusia terlibat di dalamnya. Hukum tidak bisa tegak dengan sendirinya sehingga melibatkan aparat penegak hukum, dan aparat dalam mewujudkan tegaknya hukum harus dengan undang-undang, sarana, dan kultur, sehingga hukum dapat ditegakkan dengan seadil-adilnya sesuai dengan cita hukum itu sendiri.

Hal ini menunjukan bahwa tantangan yang dihadapi oleh aparat penegak hukum bukan tidak mungkin sangatlah banyak Penegak hukum tidak hanya dituntut untuk professional dan tepat dalam menerapkan normannya akan tetapi juga dituntut dapat membuktikan kebenaran atas dakwaan kejahatan yang terkadang dipengaruhi oleh rangsangan dari prilaku masyrakat untuk sama-sama menjadi pelanggar hukum.

Pendapat Soerjono Soekanto (1981 : 21) mengatakan bahwa pokok penegakan hukum terletak pada faktor-faktor yang mempengaruhinya. Faktor-faktor tersebut, adalah sebagai berikut :

1. Faktor hukumnya sendiri, yaitu peraturan perundang-undangan yang berlaku di Indonesia.

2. Faktor penegak hukum, yakni pihak-pihak yang membentuk maupun menerapkan hukum.
3. Faktor sarana atau fasilitas yang mendukung penegakan hukum
4. Faktor masyarakat, yakni lingkungan dimana hukum tersebut berlaku atau diterapkan.
5. Faktor kebudayaan, yakni sebagai hasil karya, cipta dan rasa yang didasarkan pada karsa manusia didalam pergaulan hidup.

Dari kelima faktor tersebut saling berkaitan dengan eratnya karena antara yang satu dengan yang lainnya saling mempengaruhi. Kelima faktor tersebut dapat dikatakan esensi dari penegakan hukum, dan dapat dijadikan tolok ukur daripada keefektifitasan penegak hukum di Indonesia.

Kejahatan teknologi informasi atau tindak pidana siber memiliki karakter yang berbeda dengan tindak pidana lainnya baik dari segi pelaku, korban, modus operandi dan tempat kejadian perkara sehingga butuh penanganan dan pengaturan khusus di luar Kitab Undang-Undang Hukum Pidana (KUHP) dan juga Kitab Undang-Undang Hukum Acara Pidana (KUHAP). Terkait dengan hukum pembuktian biasanya akan memunculkan sebuah posisi dilema, di salah satu sisi diharapkan agar hukum dapat mengikuti perkembangan zaman dan teknologi, di sisi yang lain perlu juga pengakuan hukum terhadap berbagai jenis-jenis perkembangan teknologi digital untuk berfungsi sebagai alat bukti di pengadilan.

Pembuktian memegang peranan yang penting dalam proses pemeriksaan sidang pengadilan. Pembuktian inilah yang menentukan bersalah atau tidaknya seseorang yang diajukan di muka pengadilan. Apabila hasil pembuktian dengan alat bukti yang ditentukan dengan undang-undang tidak cukup membuktikan kesalahan dari orang tersebut maka akan dilepaskan dari hukuman, sebaliknya apabila kesalahan dapat dibuktikan maka dinyatakan bersalah dan dijatuhi hukuman. Oleh karena itu harus berhati-hati, cermat dan matang dalam menilai dan mempertimbangkan masalah pembuktian.

Muncul kesulitan dalam penerapan hukum dan penegakan hukum terhadap tindak pidana siber yakni dalam penyelesaian tindak pidana tersebut , kondisi yang *paperless* (tidak menggunakan kertas) ini menimbulkan masalah dalam pembuktian mengenai informasi yang diproses, disimpan, atau dikirim secara elektronik. mendasar penggunaan bukti elektronik dalam proses pembuktian perkara pidana, khususnya yaitu tidak adanya patokan atau dasar penggunaan bukti elektronik di dalam perundang-undangan kita. Selain itu sulitnya mengungkap tindak pidana tersebut baik pelaku, dan kejahtan yang sering sekali sulit untuk dibuktikan sehingga hal tersebut menjadi tantangan tersendiri dalam penegakan hukum tindak pidana *cybercrime*. Setiap penegak hukum diberi kewenangan berdasarkan Peraturan Perundang-undangan yang berlaku untuk menjelaskan tugasnya.

Dalam penanganan tindak pidana *cybercrime,* hukum acara yang digunakan yaitu hukum acara berdasarkan KUHAP. Hal tersebut memang tidak disebutkan secara jelas dalam atas Undang-undang Nomor 19 tahun 2016 tentang Informasi dan Transaksi Elektronik, tetapi karena undang-undang tersebut tidak menetukan lain maka KUHAP berlaku bagi tindak pidana yang termuat dalam Undang-undang Nomor 19 tahun 2016. Dalam Pasal 42 UU Undang-undan Nomor 19 tahun 2016 disebutkan :

> Penyidikan terhadap tindak pidana sebagimana dimaksud dalam undang-undang ini dilakukan berdasarkan ketentuan dalam Hukum Acara Pidana dan Ketentuan dalam Undang-undang ini.

Hal tersebut juga ditegaskan dalam UU No 19 Tahun 2016 tentang perubahan atas UU No 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, bahwa dalam perubahan tersebut sama sekali tidak merubah Pasal 43 Berdasarkan pasal tersebut sehingga dapat ditafsirkan bahwa Hukum Acara Pidana yang diatur dalam KUHAP merupakan *le*x *genaralis,* sedangkan ketentuan acara dalam UU No 11 tahun 2008 tentang Informasi dan Transaksi Elektronik dan UU No 19 Tahun 2016 tentang perubahan atas UU No 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, ini merupakan *lex specialis*.

Dengan demikian sepanjang tidak terdapat ketentuan lain maka ketentuan hukum acara yang digunakan seperti yang terdapat dalam KUHAP. Ketentran yang diatur lain dalam UU ITE ini yaitu menyangkut proses penyidikan dan penambahan satu alat bukti lain dalam penanganan tindak pidana yang diatur dalam UU ITE. Pelaksanaan penyelidikan tindak

pidana *cybercrime* agak sedikit berbeda dengan penyelidikan tindak pidana lainya, pejabat dalam hal ini adalah pejabat polisi Negara Republik Indonesia yang diberi wewenang oleh undang-undang ini untuk melakukan penyelidikan (Pasal 1 angka 4 KUHAP) dihadapkan pada masalah dari mana dan dimana penyelidikan harus dimulai. Akibat perbuatan tindak pidana *cybercrime* seperti *cyber porno, cyber terrorism, hacking , dll* baik yang diketahui pertama kali oleh penyelidik yang sedang melukan *cyber-patroling* maupun berdasarkan laporan dari korban tindak pidana *cybercrime*, diketahui melalui layar monitor suatu komputer yang terhubung dengan jaringan melalui koneksi internet, ataupun terjun langsung ke warnet-warnet.

Proses awal penyelidikan harus melibatkan komputer, alat elektronik seperti handphone maupun android, tablet, dan jaringannya yang terkoneksi dengan suatu jaringan dan terkoneksi melalui internet. Bukti-bukti dalam suatu tindak pidan *cybercrime* biasanya sealu dapat tersimpan di dalam istem alat alat elektronik tersebut ataupun system komputer. Dengan Demikian inti dari suatu proses penyelidikan adalah bagaimana menemukan dan selanjutnya menyita alat alat atau barang elektronik maupun komputer milik tersangka. Dari komputer tersebutlah penyelidikan dapat menentukan apakah ada bukti-bukti tindak pidana.

Karakteristik tindak pidana *cybercrime* berbeda dengan tindak pidana yang lain , karakteristik bentuk tindak pidana *cybercrime* antara yang satu dengan yang lain pun berbeda hal ini dikarenakan modus

operandi yang digunakan berbeda. Sehingga dengan demikian dalam penegakan hukum dan dalam proses beracaranya dari tahap penyelidikan dan penyidikan memerlukan ketentuan khusus.

Ketentuan khusus yang berkaitan dengan acara pidana yang terdapat dalam Undang-undang Nomor 11 Tahun 2008, yang telah dirubah oleh Undang-undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-undang Nomor 11 Tahun 2008 tentang informasi dan transaksi elektronik adalah sebagai berikut :

1. Diakuinya alat bukti elektronik yang berupa informasi elektronik dan dokumen elektronik sebagai alat bukti yang sah dalam pembuktian tindak pidana *cybercrime.*
2. Adanya wewenang khusus yang diberikan kepada Pejabat Pegawai Negeri Sipil tertentu dilingkungan Pemerintah yang lingkup tugas dan tanggungjawabnya di bidang Teknologi Informasi dan transaksi elektronik sebagai penyidik
3. Adanya kewenangan penyidik, penuntut umum, dan hakim untuk meminta keterangan kepada penyedia jasa dan penyelenggara sistem elektronik mengenai data-data yang berhubungan dengan tindak pidana, dengan tetap terikat terhadap privasi, kerahasian, dan kelancaran layanan publik, integritas data dan keutuhan data.
4. Adanya wewenang terhadap penyidik untuk melakukan penggeledahan, penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan atas izin ketua

pengadilan negeri setempat, hal ini menghindari agar sistem elektronik tersebut tidak bias hapus oleh pelaku dan menghindari agar pelacakan pelaku berjalan cepat, sehingga jejak pelaku mudah untuk ditemukan.

Upaya penegakan hukum terhadap tindak pidana siber selain dengan aturan-aturan tersebut seharusnya juga diimbangi dengan skill dan kemampuan penegak hukumnya dalam pemberantasan tindak pidana *cybercrime.* Hal ini dikarenakan modus-modus tindak pidana *cybercrime* semakin hari semakin berkembang dikhawatirkan kejahatan tersebut akan merajalela dan pelaku-pelaku sulit untuk dilacak dan ditangkap, sehingga dapat merugikan masyarakat dan Negara dan bahkan dunia luas.

C. Kepolisian Negara Republik Indonesia

1 . Pengertian Kepolisian

Menurut Momo Kelana (1972 : 18) Kata polis berasal dari bahasa Yunani " *politeia*" yang berarti seluruh pemerintahan negara kota. Di Negara Belanda pada zaman dahulu istilah polisi dikenal melalui konsep catur praja dan Van Vollenhonen yang membagi pemerintahan menjadi 4 (empat) bagian, yaitu Bestuur, Politie, Rechtspraak, dan Regelling.

Dengan demikian polities dalam pengertian ini sudah dipisahkan dari Bestuur dan merupakan bagian pemerintahan tersendiri. Pada pengertian ini polisi termasuk organ-organ pemerintahan yang mempunyai wewenang melakukan pengawasan terhadap kewajiban-kewajiban.

Menurut Charles Reith (dalam Momo Kelana, 1972 : 25) dalam bukunya *the blind eye of history* mengemukakan pengertian polisi dengan terjemahan kedalam bahasa Indonesia sebagai tiap-tiap usaha untuk memperbaiki atau menertibkan susunan kehidupan masyarakat. Didalam Encyclopedia and social science dikemukakan bahwa pengertian polisi meliputi bidang fungsi, tugas yang luas, yang digunakan untuk menjelaskan berbagai aspek daripada pengawasan keseharian umum.

Dalam Kamus Bahasa Indonesia W.J.S Poerwodarmita dikemukakan bahwa istilah polisi mengandung pengertian merupakan badan pemerintahan yang bertugas memelihara keamananan dan ketertiban umum, dan merupakan pegawai negeri yang bertugas menjaga keamanan dan ketertiban umum. Dalam pengertian ini, istilah polisi mengandung 2 (dua) pengertian ini makna polisi tugas dan sebagai organnya.

Polisi adalah aparat penegak hukum dan menjaga kamtibmas yang setiap saat harus berhubungan dengan masyarakat luas. Dalam hubungan dengan masyarakat itu polisi mengharapkan kesadaran hukum dan sikap tertib dari masyarakat. Sebaliknya, masyarakat menghendaki agar kepolisian selalu bijaksana dan cepat dalam bertindak serta senantiasa berpegang teguh pada hukum tanpa mengabaikan kepentingan dan perasaan masyarakat.

Kata Polri adalah singkatan dari Polisi Republik Indonesia. Sekarang yang dikatakan polisi adalah badan pemerintahan yang bertugas

memelihara keamanan dan ketertiban umum. Pembentukan Kepolisian Negara Republik Indonesia atau yang lazim disebut POLRI yaitu berdasarkan UU Republik Indonesia Nomor 2 Tahun 2002 tentang Kepolsian Negara Republik Indonesia yang selanjutnya disebut UU Kepolisian. Dalam Pasal 1 ayat (1) UU No.2 tahun 2002 menyatakan bahwa yang dimaksud dengan Kepolisian adalah segala hal-ikhwal yang berkaitan dengan fungsi dan lembaga polisi sesuai dengan peraturan perundang-undangan.

2. Tugas dan Fungsi Kepolisian

a. Tugas

Sebagaimana dalam Bab III UU No.2 Tahun 2002 tentang Tugas dan Wewenang, dinyatakan bahwa tugas pokok Kepolisian Negara Republik Indonesia adalah :

1) Memelihara keamanan dan ketertiban masyarakat;
2) Menegakkan hukum;
3) Memberikan perlindungan, pengayoman, dan pelayanan kepada masyarakat.

Pasal 14 ayat (1) UU Nomor 2 Tahun 2002, menyatakan bahwa dalam melaksanakan tugas pokoknya, Kepolisian Negara Republik Indonesia bertugas :

1) Melaksanakan pengaturan, penjagaan, pengawalan, dan patroli terhadap kegiatan masyarakat dan pemerintah sesuai kebutuhan;

2) Menyelenggarakan segala kegiatan dalam menjamin keamanan, ketertiban, dan kelancaran lalu lintas di jalan;
3) Membina masyarakat untuk meningkatkan partisipasi masyarakat. Kesadaran hukum masyarakat serta ketaatan warga masyarakat terhadap hukum dan peraturan perundang-undangan;
4) Turut serta dalam pembinaan hukum nasional;
5) Memelihara ketertiban dan menjamin keamanan umum;
6) Melakukan koordinasi, pengawasan, dan pembinaan teknis terhadap kepolisian khusus, penyidik pegawai negeri sipil, dan bentuk-bentuk pengamanan swakarsa;
7) Melakukan penyelidikan dan penyidikan terhadap semua tindak pidana sesuai dengan hukum acara pidana dan peraturan perundang-undangan lainnya;
8) Menyelenggarakan identifikasi kepolisian, kedokteran kepolisian, laboratorium forensik dan psikologi kepolisian untuk kepentingan tugas kepolisian;
9) Melindungi keselamatan jiwa raga, harta benda, masyarakat, dan lingkungan hidup dari gangguan ketertiban dan/atau bencana termasuk memberikan bantuan dan pertolongan dengan menjunjung tinggi Hak Asasi Manusia;
10) Melayani kepentingan warga masyarakat untuk sementara sebelum ditangani oleh instansi dan/atau pihak yang berwenang;

11) Memberikan pelayanan kepada masyarakat sesuai dengan kepentingannya dalam lingkup tugas kepolisian; serta
12) Melaksanakan tugas lain sesuai dengan peraturan perundang-undangan.

b. Fungsi

Kepolisian Negara Republik Indonesia merupakan alat negara yang berperan dalam memelihara keamanan dan ketertiban masyarakat, menegakkan hukum, serta memberikan perlindungan, pengayoman, dan pelayanan kepada masyarakat dalam rangka terpeliharanya keamanan dalam negeri.

Sebagaimana penetapan Pasal 2 UU No.2 Tahun 2002 bahwa " fungsi kepolisian adalah salah satu fungsi pemerintahan Negara yaitu dalam hal pemeliharaan keamanan dan ketertiban masyarakat, penegak hukum, perlindungan, dan pelayanan kepada masyarakat."

Selain fungsi tersebut, terdapat juga tujuan pembentukan Kepolisian Negara Republik Indonesia sebagaimana terdapat pada Pasal 4 UU No.2 Tahun 2002, yaitu mewujudkan keamanan dan ketertiban masyarakat, tertib dan tegaknya hukum, terselenggaranya perlindungan, pengayoman, dan pelayanan kepada masyarakat serta terbinanya ketenteraman masyarakat dengan menjunjung tinggi hak asasi manusia.

Pasal 3 UU No.2 Tahun 2002 mengatur tentang pengembang fungsi Kepolisian, dimana kepolisian dalam melaksanakan fungsinya dibantu oleh:

1) Kepolisian khusus;
2) Penyidik pegawai Negeri Sipil; dan/atau
3) Bentuk-bentuk pengamanan swakarsa.

Ketiga pengemban fungsi kepolisian tersebut dalam melaksanakan fungsi kepolisian sesuai dengan peraturan perundang-undangan yang menjadi dasar hukumnya masing-masing.

Guna mengefektifkan pelaksanaan tugas dan fungsinya, Kepolisian Negara Republik Indonesia diberi wewenang yang diatur dalam UU No.2 Tahun 2002, Pasal 15, yaitu :

Ayat (1)

1) Menerima laporan dan/atau pengaduan;
2) Membantu menyelesaikan perselesihan warga maasyarakat yang dapat membantu ketertiban umum;
3) Mencegah dan menanggulangi tumbuhnya penyakit masyarakat;
4) Mengawasi aliran yang dapat menimbulkan perpecahan atau mengancam persatuan dan kesatuan bangsa;
5) Mengeluarkan peraturan kepolisian dalam lingkup kewenangan administrative kepolisian;
6) Melaksanakan pemeriksaan khusus sebagai bagian dari tindakan kepolisian dalam rangka pencegahan;

7) Melakukan tindakan pertama di tempat kejadian;
8) Mengambil sidik jari dan identitas lainnya serta memotret seseorang;
9) Mencari keterangan dan barang bukti;
10) Menyelenggarakan pusat informasi kriminal nasional;
11) Mengeluarkan surat izin dan/ atau surat keterangan yang diperlukan dalam rangka pelayanan masyarakat;
12) Memberikan bantuan pengamanan dalam sidang dan pelaksanaan putusan pengadilan, kegiatan instansi lain, serta kegiatan masyarakat;
13) Menerima dan menyimpan barang temuan untuk sementara waktu.

Ayat (2)

Kepolisian Negara Republik Indonesia sesuai dengan peraturan perundang-undangan lainnya berwenang :

1) Memberikan izin dan mengawasi kegiatan keramaian umum dan kegiatan masyarakat lainnya;
2) Menyelenggarakan registrasi dan identifikasi kendaraan bermotor;
3) Memberikan surat izin kendaraan bermotor;
4) Menerima pemberitahuan tentang kegiatan politik;
5) Memberikan izin dan melakukan pengawasan senjata api, bahan peledak dan senjata tajam;

6) Memberikan izin operasional dan melakukan pengawasan terhadap badan usaha di bidang jasa pengamanan;
7) Memberikan petunjuk, mendidik, dan melatih aparat kepolisian khusus dan petugas pengamanan swakarsa dalam bidang teknis kepolisian;
8) Melakukan kerjasama dengan kepolisian Negara lain dalam menyidik dan memberantas kejahatan internasional;
9) Melakukan pengawasan fungsional kepolisian terhadap orang asing yang berada di wilayah Indonesia dengan koordinasi dengan instansi terkait;
10) Mewakili pemerintah Republik Indonesia dalam organisasi kepolisian internasional;

Dalam rangka penyelenggaraan tugas dibidang proses pidana sebagaimana diatur dalam Pasal 16 ayat (1) UU No.2 Tahun 2002, Kepolisian Negara Republik Indonesia berwenang untuk :

1) Melakukan penangkapan, penahanan, penggeledahan, dan penyitaan;
2) Melarang setiap orang meninggalkan dan/atau memasuki tempat kejadian perkara untuk kepentingan penyidikan;
3) Membawa dan menghadapkan orang kepada penyidik dalam rangka penyidikan;
4) Menyuruh berhenti orang yang dicurigai dan menanyakan serta memeriksa tanda pengenal diri;

5) Melakukan pemeriksaan dan penyitaan surat;
6) Memanggil orang untuk didengar dan diperiksa sebagai tersangka atau saksi;
7) Mendatangkan orang ahli yang diperlukan dalam hubungannya dengan pemeriksaan perkara;
8) Mengadakan penghentian penyidikan;
9) Menyerahkan berkas perkara kepada penuntut umum;
10) Mengajukan permintaan secara langsung kepada pejabat imigrasi dalam keadaan mendesak atau mendadak untuk mencegah atau menangkal orang yang disangka melakukan tindak pidana;
11) Memberi petunjuk dan bantuan penyidikan kepada penyidik pegawai negeri sipil serta menerima hasil penyidikan, penyidik pegawai negeri sipil untuk diserahkan kepada penuntut umum;
12) Mengadakan tindakan lain menurut hukum yang bertanggung jawab.

Dalam penyelenggaraan tugas dan wewenangnya, pihak kepolisian harus senantiasa memperhatikan peraturan perundang-undangan, serta kode etik profesi Kepolisian Negara Republik Indonesia, dan juga bertindak berdasarkan norma hukum dan mengindahkan norma agama, kesopanan, kesusilaan, serta menjunjung tinggi hak asasi manusia, sebagaimana diatur dalam Pasal 18-19 UU No.2 Tahun 2002.

D. Kerangka Pikir

Dalam penelitian ini dikembangkan suatu konsep atau kerangka pikir dengan tujuan untuk mempermudah peneliti dalam melakukan penelitian. Dengan adanya kerangka pikir ini maka tujuan yang akan dicapai oleh peneliti dalam penelitian akan lebih terarah karena telah terkonsep secara jelas.

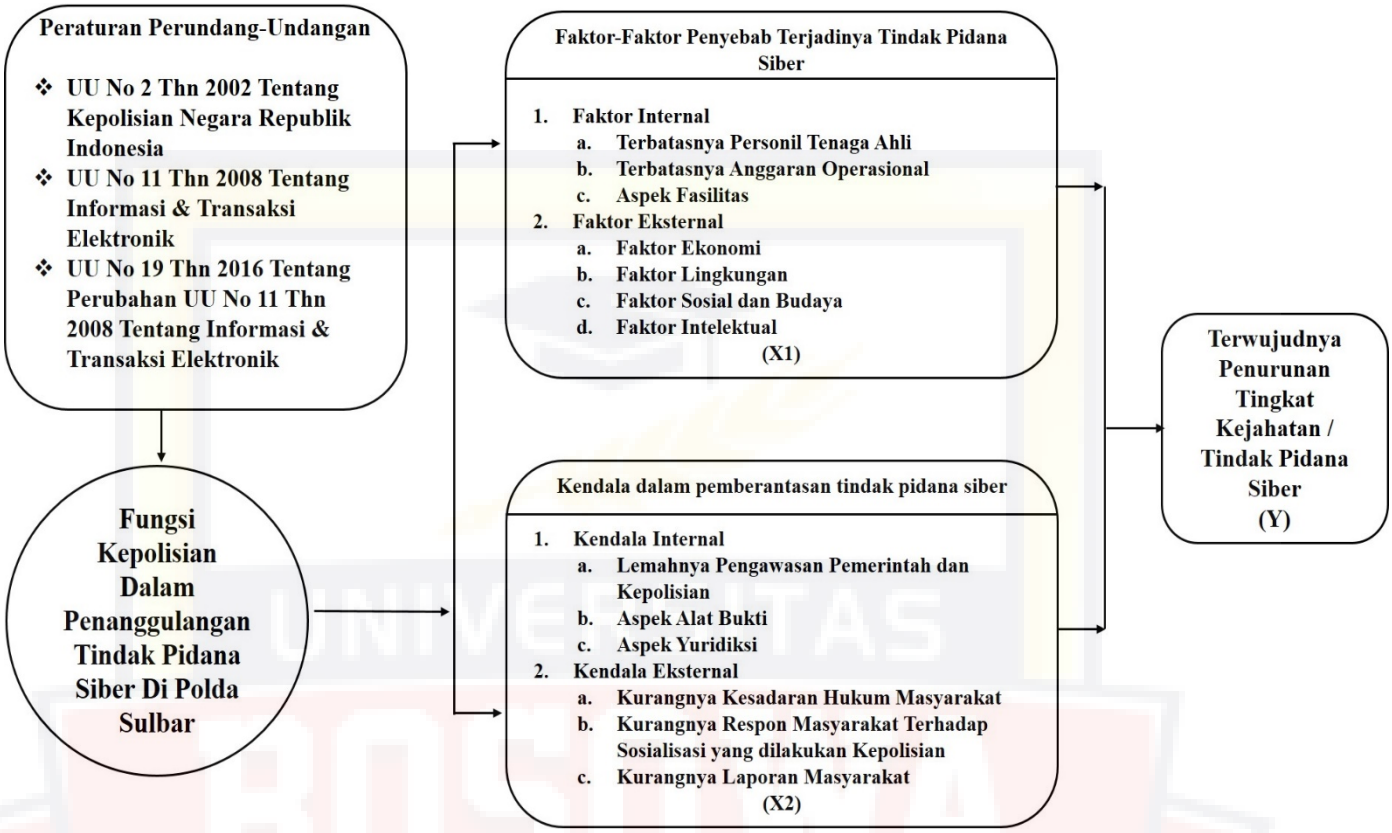
Kerangka pikir yang menjadi garis besar dalam penelitian ini adalah Fungsi Kepolisian dalam penanggulangan Tindak Pidana Siber di Polda Sulawesi Barat. Beberapa tahun terakhir perkembangan teknologi komunikasi dan informasi berkembang dengan pesat, hampir dalam segala bidang akan perkembangan teknologi tersebut. Munculnya berbagai penemuan baru memberikan kemudahan dalam kehidupan manusia, khususnya dalam bidang komunikasi dengan diketemukanya internet yang memberikan dampak yang cukup besar.

Dengan adanya internet bukan hanya memberikan manfaat terhadap kehidupan manusia, namun juga memunculkan dampak negatif yang tidak dapat dihindari. Salah satu dampak negatif yang muncul dari adanya internet adalah tindak pidana siber.

Polisi sebagai pengayom dan penegak hukum dalam struktur kehidupan masyarakat memiliki tanggung jawab khusus untuk memelihara ketertiban masyarakat serta menangani dan mengatasi setiap tindakan baik kejahatan maupun pelanggaran yang terjadi di masing-masing wilayah, Polisi memiliki peranan penting dalam pencegahan dan penanggulangan tindak pidana siber, karena polisi merupakan garda terdepan dalam penegakan hukum

dan pemberantasan berbagai tindak pidana khususnya tindak pidana siber yang terjadi dalam lingkungan masyarakat.

Adapun Faktor Penyebab terjadinya tindak pidana siber di wilayah polda sulbar terdiri dari dua faktor yaitu : faktor internal terdiri dari terbatasnya personil tenaga ahli, aspek alat bukti dan aspek fasilitas, kemudian faktor eksternal terdiri dari faktor ekonomi, faktor lingkungan, faktor sosial budaya dan faktor intelektual. Adapun kendala yang dialami kepolisian dalam penanggulangan tindak pidana siber di wilayah polda sulbar yaitu kendala internal terdiri dari dengan lemahnya pengawasan pemerintah dan kepolisian, terbatasnya anggaran operasional dan aspek yuridiksi, kemudian kendala eksternal terdiri dari kurangnya kesadaran hukum masyarakat, kurangnya respon masyarakat terhadap sosialisasi atau penyuluhan yang dilakukan pihak kepolisian dan kurangnya laporan masyarakat.



Gambar 2.1. Bagan Kerangka Pikir

E. Definisi Operasional

Untuk memudahkan pembahasan dalam tesis ini perlu adanya definisi operasional yang jelas untuk menghindari kesalahpahaman sehubungan dengan judul di atas.

Personil Tenaga Ahli	:	adalah orang yang mahir, mengerti, dan sangat paham mengenai bidang ilmu atau keterampilan tentang *cybercrime*.
Anggaran Operasional	:	adalah jumlah uang yang dikeluarkan untuk membiayai kegiatan yang akan dilaksanakan.
Fasilitas	:	Adalah segala sesuatu yang dapat memudahkan atau melancarkan pelaksanaan suatu usaha.
Faktor Ekonomi	:	Adalah Inti dari masalah yang dihadapi manusia dan kenyataan bahwa kebutuhan manusia jumlahnya tidak terbatas, sedangkan alat pemuas kebutuhan manusia jumlahnya terbatas.
Faktor Lingkungan	:	Adalah kondisi pergaulan yang turut menentukan pembentukan mental dan karakter seseorang.
Faktor Sosial Budaya	:	Adalah segala sesuatu yang dihasilkan / diciptakan oleh manusia untuk kelangsungan

hidup bermasyarakat dan telah berkembang dari generasi ke generasi.

Faktor Intelektual : Adalah orang yang menggunakan kecerdasannya untuk bekerja, belajar, mengagas, atau menyoal dan menjawab persoalan tentang berbagai gagasan.

Pengawasan Pemerintah dan Kepolisian : Adalah proses untuk memastikan bahwa segala aktifitas yang terlaksana sesuai dengan apa yang telah direncanakan pemerintah dan Kepolisian.

Alat Bukti : Adalah alat-alat yang ada hubungannya dengan suatu tindak pidana, dimana alat-alat tersebut dapat dipergunakan sebagai bahan pembuktian guna menimbulkan keyakinan hakim atas kebenaran adanya suatu tindak pidana yang telah dilakukan oleh terdakwa.

Yuridiksi : Adalah wilayah / daerah tempat berlakunya sebuah undang-undang yang berdasarkan hukum.

Kurangnya kesadaran hukum masyarakat	:	adalah setiap orang menaati aturan-aturan atau norma-norma hukum yang dibuat oleh pemerintah
Kurangnya Respon Masyarakat terhadap Sosialisasi dan penyuluhan	:	Adalah tingkah laku masyarakat yang kurang responsif terhadap proses penyebaran informasi yang berkaitan dengan upaya pencegahan terhadap perjudian.
Kurangnya Laporan Masyarakat	:	tingkah laku masyarakat yang kurang terbuka terhadap perilaku-perilaku meyimpang yang sering di lakukan oleh seseorang

BAB III

METODE PENELITIAN

A. Jenis Penelitian

Penelitian yang digunakan adalah penelitian hukum normatif yaitu merupakan penelitian yang mengkaji studi dokumen, yakni menggunakan berbagai bahan hukum primer dan sekunder seperti peraturan perundang-undangan, keputusan pengadilan, teori hukum, dan dapat berupa pendapat para ahli.

B. Lokasi Penelitian

Penelitian dilakukan berlokasi di Kota Mamuju merupakan ibu kota dari provinsi Sulawesi Barat. Khususnya di Polda Sulawesi Barat.

C. Teknik Pengumpulan dan Sumber Bahan Hukum

Adapun teknik pengumpulan data yang dilakukan dalam penelitian ini adalah dengan cara penelitian kepustakaan (*library research*) dan objek lapangan (*field research*). Penelitian ini dilakukan untuk memperoleh bahan hukum primer dan bahan hukum sekunder yang terdiri dari :

a. Bahan Hukum Primer

Bahan hukum primer yaitu data dan informasi yang diperoleh langsung dari sumber pertama. Adapun sumber data yang penulis peroleh berasal dari hasil wawancara dengan anggota kepolisian yang berwenang menangani kasus yang diteliti oleh penulis.

b. Bahan Hukum Sekunder

Bahan hukum sekunder yaitu data dan informasi yang penulis peroleh secara tidak langsung, yakni melalui data dan dokumen yang telah tersedia pada instansi atau lembaga tempat penelitian penulis. Adapun sumber data yang penulis peroleh berasal dari peraturan perundang-undangan, pendapat pakar hukum, serta laporan yang ada.

D. Analisis Bahan Hukum

Setelah bahan dikumpulkan dengan lengkap, maka tahap berikutnya adalah adalah mengolah dan menganalisis bahan. bahan penelitian akan dianalisis dengan menggunakan analisis deskriptif kualitatif. deskriptif kualitatif adalah merupakan analisis bahan dengan cara memaparkan semua bahan, baik yang berupa bahan primer maupun bahan sekunder yang telah diperoleh.

BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

A. Faktor Penyebab Terjadinya Tindak Pidana Siber

Kejahatan mayantara (*cyber crime*) menjadi semakin berkembang dan canggih dan memiliki dampak ekonomi yang lebih parah dari pada kejahatan pada umumnya. Teknologi dan orang-orang yang terampil dibidang ini memiliki tingkat kejahatan yang lebih luas dibnding kejahatan pada umumnya dan sifat kejahatan dunia maya mempunyai struktur yang berbeda.

Mekanisme yang menjadi penyebab sebuah tindakan kriminal berbeda untuk tiap tipe kejahatan. Sebuah pemahaman yang lebih rinci tentang mekanisme tersebut, yaitu, struktur biaya, keuntungan, dan daya Tarik dari kejahatan dunia maya menjadi penting untuk menanggulangi jenis kejahatan baru ini. Berikut adalah faktor-faktor penyebab terjadinya Tindak Pidana Siber:

1. Faktor Internal

a. Terbatasnya Personil Tenaga Ahli

Keterbatasan tenaga ahli pada pihak kepolisian memang merupakan faktor yang sangat besar, dengan jumlah anggota ahli yang terbatas ini pengungkapan dan penyidikan kasus kejahatan dunia maya tidak bisa diselesaikan dengan waktu yang cepat, sehingga akan membuat para pelaku lebih leluasa dalam beraksi.

Menurut Kombes (Pol) Wisnu Andayana, Direktur Kriminal Khusus Polda Sulbar (Wawancara Pada Tanggal 31 September 2018)

Penyidik kepolisian memiliki peran penting dalam upaya penanggulangan tindak pidana siber, dimana kemampuan penyidik sangat dibutuhkan untuk mengungkap kasus-kasus *cyber crime*. Adanya unit *cybercrime* dilingkungan kepolisian membuktikan bahwa dibutuhkannya penyidik khusus yang memiliki kemampuan di bidang informasi dan transaksi elektronik guna menangani kejahatan-kejahatan di dunia maya. oleh karena itu dibutuhkaannya pendidikan khusus untuk memberikan pengetahuan terkait *cyber* kepada para penyidik yang khusus menangani masalah *cyber crime*

Secara umum penyidik masih sangat minim dalam penguasaan operasional komputer dan pemahaman terhadap komputer serta kemampuan melakukan penyidikan terhadap komputer serta kemampuan melakukan penyidikan terhadap kasus-kasus itu.

Beberapa faktor yang sangat berpengaruh adalah:

a. Kurangnya pengetahuan tentang komputer
b. Kurangnya pengetahuan teknis dan pengalaman para penyidik dalam menangani kasus-kasus *cybercrime*
c. Faktor sistem pembuktian yang menyulitkan para penyidik

Menurut Pendapat Penulis Selain itu perlu juga diketahui bahwa dalam melakukan penyidikan terhadap tindak pidana siber. Kepolisian maupun penyidik dari Pegawai Negeri Sipil harus berkoordinasi dan dapat menerima bantuan ahli yang diperlukan

dalam melakukan penyidikan bahkan Kepolisian dan penyidik dari Pegawai Negeri Sipil tersebut dapat menerima bantuan dari penyidik negara lain untuk berbagai informasi dan alat bukti.

Dari informasi yang didapat penulis anggota kepolisian masih belum terlalu melek akan teknologi, bahkan banyak diantara anggota *cyber police* Indonesia masih baru memakai komputer. Bisa dikatakan kemampuan polisi Indonesia dalam dunia maya masih dalam tahap standar atau pemula. Keterbatasan jumlah personil tenaga ahli sebenarnya bisa diatasi dengan adanya pelatihan-pelatihan baik oleh kepolisian atau pihak universitas dan perguruan tinggi negri atau swasta yang terdapat fakultas teknologi informasi. Langkah ini perlu dilakukan untuk merekrut tenaga-tenaga ahli teknologi informasi terutama sekali para pelajar dan mahasiswa yang memiliki keahlian dibidang IT (*Information technology*) pihak dosen dan mahasiswa memiliki peran yang sangat startegis sebab merekalah yang paling bisa mengikuti perkembangan IT.

Para praktisi juga bisa memberikan peran penting dalam memberikan masukanmasukan kepada pihak pemerintah dalam keamanan jaringan computer dan internet. Mendesaknya kebutuhan tenaga ahli juga harus diimbangi dengan adanya sarana dan prasarana serta fasilitas peralatan yang canggih dan maju dalam mendukung keamanan jaringan dan juga untuk memudahkan pelacakan pelaku

kejahatan agar kasus kejahatan dunia maya dapat di atasi dengan cepat.

b. Terbatasnya Anggaran Operasional

Kendala lain yang krusial adalah terbatasnya dana anggaran operasional, penulis mengutip pernyataan Kombes (Pol) Wisnu Andayana, Direktur Kriminal Khusus Polda Sulbar (Wawancara Pada Tanggal 3 September 2018) masalah yang cukup krusial selain perangkat hukum, yaitu SDM yang belum mencukupi, anggaran serta sarana dan prasarana untuk menunjang pengungkapan kasus-kasus *cyber crime*. Sekarang ini anggaran yang ada hanya cukup untuk satu perkara per satu bulan. Padahal kenyataanya satu bulan bisa sampai 10 kasus-kasus.

Menurut Analisis Penulis Jumlah anggaran yang kurang menjadi penyebab faktor yang sangat besar dalam pengungkapan kasus kejahatan siber, dengan keterbatasan anggaran maka akan berdampak langsung pada peralatan yang digunakan oleh pihak kepolisian untuk melacak pelaku kejahatan siber. Seperti yang dikutip dari situs berita kriminalitas.com, Sebagai contoh perbandingan penulis membandingkan rancangan anggaran cyber di Amerika Serikat yang mencapai USD 19. miliar dollar pada tahun 2017, keadaan ini mengahruskan pemerintah Amerika Serikat karena menambah anggaran yang cukup besar tersebut disebabkan oleh

ancaman dunia maya (*cyber*) di Amerika Serikat juga angat meningkat tajam.

Pemerintah amerka serikat dibawah kordinasi langsung presiden barack obama peningkatan anggaran untuk keamanan cyber di amerika tidak lepas dari berbagai ancaman-ancaman yang cukup besar terutama yang datang dari luar Negara amerika, selain ancaman pencurian data intelejen, pencurian data diri warga sipil Amerika dan perbankan, ancaman yang paling serius ialah *cyber terrorism*.

Presiden obama juga menandatangani perintah eksekutif untuk membentuk dewan privasi federal, sebuah lembaga kordinasi untuk yang bertugas mengembangkan buku acuan komprhensif mengenai pengumpulan dan penyimpanan data pribadi warga, selain itu usulan anggaran pemerintah akan mengalokasikan dana sebesar 62 juta dolar untuk mempekerjakan pakar dunia maya bagi pemerintah. Sudah saatnya pemerintah melalui KOMINFO dan pihak institusi kepolisisan mulai menambah anggaran untuk keamanan *cyber* agar kasus penyalahgunaan teknologi informasi dapat diminimalisir. Program kerja yang dilakukan oleh presiden amerika barack obama tersebut selain menambah anggaran untuk keamanan dunia maya, pemerintah Amerika Serikat juga ikut melibatkan dan memberdayakan para pakar-pakar dan tenaga ahli dunia maya agar dapat ambil bagian untuk menjaga keamanan dunia maya dinegara tersebut.

Langkah yang dilakukan oleh Presiden Amerika serikat Barack Obama juga bisa diterapkan di Indoensia dengan memberdayakan dan mempekerjakan para pakar dan tenaga ahli dunia maya di Indonesia untuk keamanan jaringan, walaupun membutuhkan waktu yang tidak sebentar setidaknya langkah tersebut bisa diterapkan oleh pemerintah Indonesia untuk mengurangi keterbatsan tenaga ahli. Kejahatan dunia maya diindonesia yang paling banyak ialah kejahatan perbankan dengan motif untuk mendapatkan keuntungan berupa uang. Walau masih bersifat kejahatan perbankan, namun jika terus dibiarkan maka bukan tidak mungkin cepat atau lambat *cyber terorrism* juga akan mengancam Indonesia.

c. Aspek Fasilitas

Menurut AKP H. Muh. Agus, Kasubdit II Direktorat Krimsus Polda Sulbar, (Wawancara Pada Tanggal 3 September 2018) Dalam mengungkap kasus-kasus *cyber crime* dibutuhkan fasilitas yang mampu menunjang kinerja aparat kepolisian. Fasilitas tersebut berupa laboratorium forensik komputer yang digunakan untuk mengungkap data-data yang bersifat digital serta merekam dan menyimpan bukti-bukti yang berupa *soft copy* (gambar, program, html, suara, dan lain sebagainya).

Komputer forensik merupakan salah satu cabang ilmu forensik yang berhubungan dengan bukti hukum yang ditemukan dalam komputer maupun media penyimpanan secara digital. Komputer

forensik dikenal sebagai digital forensic. Adapun tujuannya ialah untuk mengamankan dan menganalisis bukti digital, serta memperoleh berbagai fakta yang objektif dari sebuah kejadian atau pelanggaran keamanan dari sistem informasi.

Berbagai fakta tersebut akan menjadi bukti yang akan digunakan dalam proses hukum. Contohnya, melalui Internet Forensik, kita dapat megetahui siapa saja orang yang mengirim email kepada kita, kapan dan dimana keberadaan pengirim. Dalam contoh lain kita bisa melihat siapa pengunjung website secara lengkap dengan informasi *ip address*, komputer yang dipakainya dan keberadaannya serta kegiatan apa yang dilakukan pada website kita tersebut.

Kemampuan digital forensik menggunakan fasilitas yang hanya dimiliki oleh laboratorium forensik komputer. Terkait dengan hal tersebut unit *cyber crime* polda sulbar belum memiliki fasilitas berupa laboratorium forensic komputer, yang mengakibatkan terkendalanya upaya penanggulangan tindak pidana siber diwilayah hukum polda sulbar.

Menurut Analisis Penulis bahwa fasilitas yang digunakan unit *cyber crime* Polda Sulbar bukannya kurang memadai tetapi memang sangat tidak memadai untuk mendukung proses penanganan kasus tindak pidana siber sehingga menyulitkan kinerja petugas kepolisian dan hal ini harusnya menjadi bahan perhatian oleh pemerintah agar

segera menyediakan Laboratorium *computer forensic* di setiap polda yang ada diseluruh Indonesia .

2. Faktor Eksternal

a. Faktor Ekonomi

Menurut Kombes (Pol) Wisnu Andayana, Direktur Kriminal Khusus Polda Sulbar (Wawancara Pada Tanggal 31 September 2018), Salah satu yang mendorong terjadinya kejahatan ini adalah rendahnya tingkat pendidikan dari orang yang melakukan kejahatan ini, sehingga mengakibatkan pasaran tenaga kerja tidak dapat menyerap keahliannya dengan alasan rendahnya tingkat pendidikan. Hal tersebut mengakibatkan pelaku kejahatan menjadi pengangguran. Karena menjadi pengangguran dan kesulitan untuk memenuhi kebutuhan sehari-hari maka pelaku kejahatan tersebut terdorong untuk mencari jalan pintas guna mendapatkan penghasilan demi memenuhi kebutuhannya. Bukannya mencari pekerjaan yang halal tapi justru lebih tergiur untuk melakukan kejahatan demi mendapatkan uang. Salah satu kejahatan yang cenderung mudah dilakukan yaitu seperti melakukan penipuan berbasis siber. Selain itu juga pelaku melakukan pemerasan, bahkan sampai pada tingkat pembobolan atau pencurian mengingat media yang digunakan cukup mudah diakses dan sulit dilacak.

Menurut Analisis Penulis Dengan demikian, perkembangan tindak pidana siber di Indonesia merupakan fakta sosial yang harus

dicegah, ditindak dan ditanggulangi. Dengan bertambahnya pengguna internet maka kemungkinan terjadinya tindak pidana siber akan semakin terbuka apalagi terdorong oleh tuntutan ekonomi yang mendesak.

b. Faktor Lingkungan

Hubungan antara faktor ekonomi dan faktor lingkungan sangat kuat, di mana pelaku yang awalnya tidak mempunyai pekerjaan akhirnya mulai belajar dari orang yang telah atau pernah melakukan tindak pidana siber, yang masih memiliki hubungan keluarga ataupun pertemanan, karena berasal dari lingkungan atau daerah yang sama.

Lingkungan pergaulan turut menentukan pembentukan mental dan karakter seseorang. Seseorang yang pada awalnya bukan merupakan pelanggar hukum, akibat bergaul pada lingkungan yang sering melakukan pelanggaran hukum maka orang tersebut cenderung terdorong oleh lingkungannya dan akan menjadi pelanggar hukum. Fakta ini memperkuat teori asosiasi diferensial yang dikemukakan oleh Sutherland.

Seseorang yang melakukan kejahatan cenderung diakibatkan oleh kondisi lingkungan sosialnya dimana pelaku telah belajar atau mendapat pelajaran dari lingkungannya bahwa tingkah laku kriminal atau perbuatan melanggar hukum lebih baik dan menguntungkan daripada tingkah laku non-kriminal atau melakukan perbuatan taat pada hukum.

c. Faktor Sosial dan Budaya

Menurut AKP H. Muh. Agus, Kasubdit II Direktorat Krimsus Polda Sulbar, (Wawancara Pada Tanggal 28 Agustus 2018), Faktor Sosial dan Budaya yang menjadi faktor penyebab terjadinya tindak pidana siber yaitu:

a. Kemajuan Teknologi Informasi

Perkembangan ilmu pengetahuan dan teknologi (IPTEK) yang cukup pesat dewasa ini terutama segi teknologi informasi (*information technology*) seperti halnya internet (*interconnected computer network*) sangat menunjang profesi dan pekerjaan setiap orang untuk mencapa tujuan hidup dalam waktu singkat. Dengan menggunakan internet kita diberikan kenyamanan kemudahan dalam mengakses segala sesuatu tanpa ada batasannya. Dengan kenyamanan itulah yang merupakan faktor utama bagi sebagian oknum untuk melakukan tindak kejahatan.

Tindak pidana atau kejahatan mayantara adalah sisi buruk yang amat berpengaruh terhadap kehidupan modern dari masyarakat informasi akibat kemajuan teknologi informasi tanpa batas. Indikatornya adalah peningkatan setiap tahun peristiwa kejahatan mayantara melalui sarana komputer. Keadaan tindak pidana ini mudah dibayangkan, betapa kejahatan mayantara ini membawa dampak buruk yang dapat ditiru dan merugikan orang,

lembaga dan negara lain akibat pelanggaran hukum tersebut menyebabkan berkembangnya kejahatan berdimensi baru.

b. Sumber Daya Manusia (SDM)

Sumber daya manusia dalam teknologi informasi mempunyai peranan penting sebagai pengendali sebuah alat. Teknologi dapat dimanfaatkan untuk kemakmuran namun dapat juga untuk perbuatan yang mengakibatkan petaka akibat dari penyimpangan dan penyalahgunaan. Para pelaku merupakan orang yang pada umumnya cerdas, mempunyai rasa ingin tahu yang besar, dan fanatik akan teknologi komputer. Pengetahuan pelaku kejahatan dunia maya tentang cara kerja sebuah komputer jauh diatas operator komputer. Hal ini merupakan faktor yang sulit untuk dihindari, karena kelebihan atau kecerdasan dalam mengakses internet yang dimiliki seseorang di zaman sekarang ini banyak yang disalah gunakan demi mendapatkan keuntungan semata sehingga sulit untuk dihindari.

c. Munculnya fenomena komunitas baru

Dengan adanya teknologi sebagai suatu sarana elektronik untuk mencapai suatu tujuan, di antaranya internet sebagai suatu media untuk berkomunikasi, secara sosiologis terbentuklah komunitas baru di internet atau dunia maya yang saling menghubungkan para pengguna dalam berkomunikasi. terdapat 2 sisi yang saling melatarbelakangi, yaitu sisi komunitas di antara

para pelaku tindak pidana siber dimana mereka saling berkomunikasi untuk keperluan modus operandi mereka, serta sisi lainnya di mana pelaku tindak pidana siber melakukan modus operandi mereka dengan menggunakan *social media* seperti *Facebook* atau *Whatsapp* untuk mendapatkan korban.

d. Faktor Intelektual

Menurut Analisis Penulis Faktor intelektual memiliki hubungan yang erat dengan faktor-faktor yang telah penulis sebutkan di atas. Faktor intelektual ini dilatarbelakangi oleh kemampuan orang yang terlebih dahulu menjadi pelaku *cyber crime,* yang kemudian mengajarkan atau menularkan kemampuannya kepada orang lain yang berada disekitarnya atau memiliki keadaan yang sama dengannya. Bahkan terkadang pelaku *cyber crime* masih tergolong *newbie* atau pemula yang baru mulai melakukan tindakan-tindakan kejahatan dari tingkatan terkecil hingga terbesar akibat didorong dengan faktor intelektual yang cenderung disalahgunakan.

B. Upaya Penanggulangan Tindak Pidana Siber oleh Aparat Kepolisian

Dalam menanggulangi terjadinya kasus Tindak Pidana Siber, pihak kepolisian telah melakukan berbagai upaya penanggulangan Tindak Pidana Siber. Berdasarkan wawancara dengan AKP H. Muh. Agus, Kasubdit II Direktorat Krimsus Polda Sulbar (Wawancara Pada Tanggal 28 Agustus 2018) yang menyatakan bahwa pihak kepolisian telah melakukan upaya-upaya penanggulangan yang bersifat *preventif* dan *represif.*

1. **Upaya *Preventif***

Dalam melakukan upaya preventif ini pihak kepolisian khususnya unit *cyber crime* polda sulbar 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.

Pihak kepolisian juga menjalankan fungsi teknis yang khusus menangani kasus Tindak Pidana Siber, yaitu dengan melakukan penegakan aturan, melakukan penjagaan di lokasi-lokasi yang diduga sering terjadi kasus Tindak Pidana Siber dan melakukan patroli *cyber* rutin di dunia maya seperti media-media sosial.

2. **Upaya *Represif***

Dalam melakukan upaya *represif* ini, pihak kepolisian telah mengambil tindakan dengan memproses setiap kasus Tindak Pidana Siber yang ditangani sesuai dengan aturan yang berlaku. 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 Tindak Pidana Siber, 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 khususnya kepolisian polda sulbar.

C. Pelaksanaan Undang-Undang Informasi dan Transaksi Elektronik terhadap Tindak Pidana Siber

Undang-undang ITE (Informasi dan Transaksi Elektronik) merupakan salah satu peranti hukum di bidang *cyberspace* atau dunia maya yang diharapkan dapat mengakomodir segala persoalan yang menyangkut kejahatan atau pelanggaran di dunia maya (*cyber crime*).

Undang-undang ITE berperan sangat penting dalam pemberantasan tindak pidana siber di Indonesia. Selain memuat perlindungan hukum terhadap pemakai jasa internet juga memuat ancaman sanksi terhadap pelaku kejahatan tindak pidana siber. Dalam mengahadapi tindak pidana siber, hukum positif di Indonesia masih bersifat *lex locus delicti*. Namun beda halnya dengan situasi dan kondisi pelanggaran hukum yang terjadi atas tindak pidana siber dimana pelaku kejahatan siber 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 negara dalam menegakkan hukum tidak dapat lagi tinggal diam setelah lahirnya Undang-Undang Nomor 19

Tahun 2016 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.

Berikut ini akan dipaparkan beberapa kasus tindak pidana siber yang telah ditangani oleh Kepolisan Daerah Sulawesi Barat tahun 2016 – 2018 :

Tabel 4.1.
Jumlah Kasus Tindak Pidana Siber yang ditangani Polda Sulbar
Tahun 2016 – 2018

No.	Kasus	Tahun			Jumlah
		2016	2017	2018	
1	Pornografi	2	4	2	8
2	Penghinaan / Pencemaran Nama Baik	3	5	4	12
3	Penyebaran Berita Bohong dan Penyesatan *(Hoax)*	5	10	11	26
4	*Hacking*	1	2	1	4
	Total				**50**

Sumber : Data Primer yang diolah

Berdasarkan tabel di atas dapat diketahui, bahwa jenis tindak pidana siber yang ditangani oleh Ditreskrimsus Subdit II yang terjadi diwilayah hukum Polda Sulawesi Barat. Antara tahun 2016 sampai dengan tahun 2018 sebanyak 50 kasus, masing-masing kasus yaitu : Pertama 8 kasus Pornografi, Kedua 12 kasus Penghinaan/Pencemaran Nama Baik, Ketiga 26 kasus Penyebaran Berita Bohong atau *hoax*, Keempat 4 kasus *Hacking*. Dari hasil penelitian ini, dapat disimpulkan oleh peneliti bahwa kasus Penyebaran Berita Bohong atau *hoax* merupakan kasus yang terbanyak terjadi dalam kurun waktu 3 tahun terakhir

Menurut AKP H. Muh. Agus, Kasubdit II Direktorat Krimsus Polda Sulbar, (Wawancara Pada Tanggal 28 Agustus 2018), Saat ini masalah pornografi dan pornoaksi sangat memprihatinkan, dan memiliki dampak negatif yang sangat nyata. Orang-orang yang menjadi korban kejahatan kesusilaan ini tidak hanya perempuan dewasa tetapi banyak korban yang masih anak-anak baik perempuan maupun laki-laki. Para pelakunya pun bukan hanya orang yang tidak dikenal, atau orang yang tidak mempunyai hubungan kekeluargaan dengan korban, diantaranya pelaku masih memiliki hubungan darah, atau hubungan semenda, hubungan profesi, hubungan kerja, hubungan tetangga, bahkan sampai pada hubungan pendidikan dengan korban.

Menurut Analisis Penulis Masalah pornografi dan pornoaksi di Indonesia telah melampaui ambang toleransi dan merusak akhlak bangsa. Namun sangat disayangkan penyelesaian terhadap masalah pornografi yang menyangkut kesusilaan ini belum sesuai dengan yang diharapkan. Kenyataan itu dapat dilihat berdasarkan tabel 1 di atas dimana jumlah kasus pornografi dan/atau pelanggaran kesusilaan melalui media elektronik yang ditangani oleh unit *cyber crime* Polda Sulbar yaitu sekitar 8 kasus dari rentan waktu 2016 hingga agustus 2018. Jumlah tersebut penulis nilai sangat minim mengingat banyaknya pornoaksi bahkan pelanggaran kesusilaan yang beredar di internet khususnya pada media sosial. Hal tersebut beralasan mengingat kurangnya pengetahuan dari masyarakat tentang pentingnya menjaga etika baik itu tingkah laku maupun penyebaran *pict* berupa gambar, suara, dan video pada

media sosial yang tidak bermuatan atau mengandung unsur pelanggaran kesusilaan.

Pelanggaran kesusilaan pada media elektronik dan dunia maya merupakan perbuatan yang dilarang sebagaimana diatur dalam Pasal 27 ayat (1) yang berbunyi sebagai berikut :

> Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.

Pasal tersebut memiliki sanksi pidana yang ditentukan dalam Pasal 45 ayat (1), yang berbunyi:

> Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3), dan ayat (4) dipidana degan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp.1.000.000.000,00 (satu miliar rupiah).

Menurut AKP H. Muh. Agus, Kasubdit II Direktorat Krimsus Polda Sulbar, (Wawancara Pada Tanggal 29 Agustus 2018) Penghinaan dan pencemaran nama baik di dunia maya ini merupakan masalah yang sangat popular dan paling sering terjadi di internet khususnya pada media-media sosial dimana banyak orang-orang yang mem-*posting* status bahkan komentar-komentar yang berisi penghinaan bahkan termasuk pencemaran nama baik. Polda Sulbar telah menangani kasus penghinaan dan pencemaran nama baik sebanyak 12 kasus sejak tahun 2016 hingga agustus 2018, jumlah kejadian penghinaan dan pencemaran nama baik cukup sering terjadi di dunia maya namun penanganannya dinilai cukup menyulitkan dimana kebanyakan pelaku menggunakan nama samaran atau identitas palsu dalam menjalankan

kejahatannya. Selain itu polisi kesulitan mengidentifikasi apakah status atau komentar yang di *post* memuat unsur penghinaan tanpa adanya laporan dari korban.

Penghinaan / pencemaran nama baik di internet dimuat dalam Pasal 27 ayat (3) yang berbunyi:

> Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.

Menurut Kombes (Pol) Wisnu Andayana, Direktur Kriminal Khusus Polda Sulbar, (Wawancara Pada Tanggal 3 September 2018) Penyebaran berita bohong dan penyesatan merupakan kata yang semakna dengan penipuan. Penipuan dapat dilakukan dengan motivasi, yaitu untuk menguntungkan dirinya sendiri atau paling tidak untuk merugikan orang lain. Dengan motivasi tersebut, maka penyebaran berita bohong dan penyesatan dapat dikategorikan sebagai penipuan.

Berdasarkan tabel 1 yang telah dipaparkan sebelumnya polda sulbar telah menangani kasus tentang penyebaran berita bohong dan penyesatan melalui media elektronik sebanyak 26 kasus. Hal ini membuktikan bahwa kasus penipuan yang terjadi di kawasan hukum polda sulbar cukup marak terjadi.

Menurut Kombes (Pol) Wisnu Andayana, Direktur Kriminal Khusus Polda Sulbar (Wawancara Pada Tanggal 31 September 2018) mengungkapkan bahwa kejahatan ini marak terjadi dikarenakan korban cenderung mudah ditipu ataupun dibodohi oleh pelaku.

Penyebaran berita bohong atau penyesatan melalui media elektronik dapat dijerat dengan Pasal 28 ayat (1) yang berbunyi:

> Setiap orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transakasi elektronik.

Diancam dengan sanksi pidana pada Pasal 45 ayat (2) yang berbunyi:

> Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 28 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp.1.000.000.000,00 (satu miliar rupiah).

Menurut Kombes (Pol) Wisnu Andayana, Direktur Kriminal Khusus Polda Sulbar, (Wawancara Pada Tanggal 3 September 2018) Salah satu bentuk kejahatan elektronik yang sering ditemukan adalah *hacking* atau *cracking*. Kejahatan ini dapat dilakukan dari luar dan dalam negeri. Semua tindakan yang dapat merugikan kepentingan orang yang dilindungi Indonesia, baik atas tindakan yang dilakukan dengan cara menggunakanatau mengakses komputer dan sistem elektronik lainnya, baik yang dimiliki secara privat atau yang dimiliki dan dilindungi oleh pemerintah, secara tanpa izin atau tanpa hak.

Tujuannya adalah memperoleh, mengubah, merusak, atau menghilangkan informasi demi keuntungannya. Oleh karena itu, *hacking* merupakan salah satu kegiatan yang bersifat negatif. Meskipun pada awalnya memiliki tujuan mulia, yaitu untuk memperbaiki sistem keamanan yang telah dibangun dan memperkuatnya, tetapi dalam perkembangannya *hacking* digunakan untuk keperluan-keperluan lain yang bersifat merugikan. Hal ini tidak terlepas dari penggunaan internet yang semakin meluas sehingga

penyalahgunaan kemampuan *hacking* juga mengikuti luasnya pemanfaatan internet.

Menurut Analisis Penulis Pada dasarnya perbuatan mengakses ke suatu sistem jaringan tanpa izin tersebut dapat dikategorikan sebagai perbuatan tanpa wewenang masuk dengan memaksa ke dalam rumah atau ruangan yang tertutup sehingga dianggap suatu kejahatan. Terkait dengan kejahatan *hacking* ini polda sulbar telah menangani 4 kasus yang menyangkut keamanan privasi. Kasus-kasus tersebut ditangani berdasarkan laporan dari korban.

Begitu banyaknya kejahatan *hacking* yang terjadi namun hanya sedikit yang dapat diproses hukum dikarenakan korban tidak menyadari bahwa sistem perangkat elektroniknya sedang dibobol selain itu pelaku tidak meninggalkan jejak sama sekali dalam melancarkan aksiknya sehingga kegiatan *hacking* tidak dapat dideteksi.

Contoh kasus *Hacking* pada tahun 2018 Indra Wibowo Meretas akun *Facebook* milik Busman, setelah meretas akun tersebut pelaku memposting gambar-gambar pornografi dan meminta sejumlah pulsa dari teman-teman korban di *Facebook* untuk dikirimkan ke nomor handphone pelaku, jumlah yang diminta bervariasi.

Perbuatan *hacking* ini diatur dalam Pasal 30 yang berbunyi:

a) setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun.

b) setiap orang 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.

c) setiap orang 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.

Adapun sanksi yang dikenakan dari perbuatan *hacking* diatur dalam Pasal 46, yang berbunyi :

1) setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp.600.000.000,00 (enam ratus juta rupiah).
2) setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp.700.000.000,00 (tujuh ratus juta rupiah).
3) 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).

D. Kendala yang dialami Kepolisian Daerah Sulawesi Barat dalam Menanggulangi Tindak Pidana Siber

Berikut adalah kendala-kendala yang dialami kepolisian daerah sulawesi barat dalam menanggulangi tindak pidana siber yaitu :

1. Kendala Internal

a. Lemahnya Pengawasan Pemerintah dan Kepolisian

Menurut Kombes (Pol) Wisnu Andayana, Direktur Kriminal Khusus Polda Sulbar (Wawancara Pada Tanggal 4 September 2018) Lemahnya pengawasan penggunaan internet berpotensi besar akan menciptakan peluang terjadinya kejahatan *cyber crime* (dunia maya). Karena kejahatan dengan menggunakan teknologi terjadi jika ada akses internet yang cukup memadai. Fasilitas internet Di indonesia bisa dikatakan sudah memadai baik dari segi kecepatan akses dan kemudahan pemasangan jaringan akses internet. Dalam hal pengawasan pemerintah telah mengontrol pengawasan trafik konten negatif internet yang dapat diakses di indonesia. Seperti pemblokiran situs-situs porno, SARA, kekerasan dan situs-situs website yang dianggap menyalahi norma kesusilaan.

Dari segi prosedur pemasangan jaringan koneksi internet di indonesia dari yang dipaparkan oleh narasumber hampir 95% persen dikendalikan oleh pihak swasta, peran dari pemerintah hanya 5% saja, jika ISP *(internet service provider*) seluruhnya pihak swasta yang menegendalikan maka berakibat pada akan terjadi lemahnya

pengawasan oleh pihak pemerintah, biaya yang cukup murah serta akses kecepatan internet yang cukup memadai maka akan sangat rawan dalam penyalahgunaan penggunaan jaringan internet.

Seperti halnya *provider* XL dan Indosat yang hamper semua sahamnya dimiliki oleh pihak asing merupakan lahan bisnis yang sangat besar bagi pihak swasta untuk meraup keuntungan dari penyediaan jasa internet di indonesia, tongginya pengguna internet di indoensia juga salah satu faktor pihak sawasta melakukan ekspansi ke indonesia. Dengan leluasanya pihak swasta mengendalikan jaringan koneksi di Indonesia dinilai salah satu penyebab maraknya menyalahgunaan internet (*internet misuse*).

Menurut Analisis Penulis Tidak adanya kebijakan dan langkah prventif menjadi faktor utama, para pengguna bisa dengan bebas mengakses data data tertentu yabg mana bisaa disalahgunakan oleh pengguna yang tidak bertamggung jawab. Dalam jangka panjang maka alamat *ip address* dan domain name asal indonesia akan di black list oleh dunia internasional sehingga kerugianpun akan ditanggung oleh rakyat indonesia Penggunaan fasilitas internet sangatlah dibutuhkan oleh pengguna teknologi informasi dalam hal ini pihak yang bertanggung jawab adalah penyedia jasa layanan internet atau ISP (*internet service provider)* yang harus menyediakan pelayanan maupun servis ketika ada kerusakan, namun dikarenakan dikendalikan oleh pihak swasta Maka penulis berpendapat ada celah

hukum yang bias dimanfaatkan oleh pihak yang tidak bertanggung jawab dalam menyalahgunakan fasilitas internet, jika dilihat dari Undang-Undang No 19 Tahun 2016 tentang Informasi Dan Transaksi Elektronik misalnya yang terdapat pada pasal 13, pasal 14, pasal 15 dan pasal 16.

Pasal tersebut lebih fokus untuk menitikberatkan penyelenggaraan sistem elektronik harus sesuai dengan apa yang dibutuhkan oleh pengguna jasa elektronik. Sedangkan pasal 23, pasal 24, pasal 25 dan pasal 26 yang mengatur tentang Nama domain, Hak Kekayaan Intelektual dan Perlindungan Hak Pribadi, Tidak ada satupun pada pasal-pasal tersebut yang menyebutkan pengawasan penggunaan internet .Pasal 23 hingga pasal 26 lebih cenderung fokus pada hak kekayaan intelektual atau semacam hak paten. Dengan adanya campur tangan pemerintah dalam mengawasi perizinan pemasangan akses jaringan internet diharapkan tingkat kejahatan dunia maya dapat diminimalisir.

b. Aspek Alat Bukti

Saat ini sistem pembuktian hukum di Indonesia (khusunya dalam Pasal 184 KUHAP) belum mengenal istilah bukti elektronik/digital *(digital evidence)* sebagai bukti yang sah menurut undang-undang. Masih banyak perdebatan khususnya antara akademisi dan praktisi mengenai alat bukti elektronik tersebut.

Sementara itu dalam proses penyidikan kasus *cyber crime*, alat bukti elektronik memiliki peran penting dalam penanganan kasus.

Alat bukti dalam kasus tindak pidana siber berbeda dengan alat bukti kejahatan lainnya dimana sasaran atau media *cyber crime* merupakan data-data atau sistem komputer / internet yang sifatnya mudah diubah, dihapus, atau disembunyikan oleh pelaku kejahatan. Selain itu saksi korban dalam kasus tindak pidana siber berperan sangat penting dimana jarang sekali terdapat saksi dalam kasus tindak pidana siber dikarenakan saksi korban yang berada di luar daerah atau bahkan berada di luar negeri yang mengakibatkan penyidik sulit untuk melakukan pemeriksaan saksi dan pemberkasan hasil penyelidikan.

Penuntut umum juga tidak mau menerima berkas perkara yang tidak dilengkapi dengan berita acara pemeriksaan saksi khususnya saksi korban dan harus dilengkapi dengan berita acara penyumpahan saksi karena kemungkinan besar saksi tidak dapat hadir di persidangan dikarenakan jarak kediaman saksi yang cukup jauh. Hal tersebut mengakibatkan kurangnya alat bukti yang sah jika berkas perkara tersebut dilimpahkan ke pengadilan untuk disidangkan sehingga terdakwa beresiko akan dinyatakan bebas.

Menurut Analisis Penulis Hal serupa dialami oleh penyidik reskrimsus *cyber crime* polda sulbar dimana sangat kesulitan menangani kasus tindak pidana siber terkait aspek alat bukti karena terkadang alat bukti yang berupa data-data tersebut telah diubah atau

dihapus, namun beda halnya ketika pelaku tindak pidana siber tertangkap tangan dalam melakukan aksi kejahatannya dimana alat bukti dapat langsung diamankan oleh petugas kepolisian.

c. Aspek Yurisdiksi

Menurut AKP H. Muh. Agus, Kasubdit II Direktorat Krimsus Polda Sulbar, (Wawancara Pada Tanggal 3 September 2018), Dalam sistem hukum pidana yang berlaku saat ini, hukum pidana pada umumnya hanya berlaku di wilayah negaranya sendiri (asas territorial) dan untuk warga negaranya sendiri (asas personal/nasional aktif). Hanya delik-delik tertentu yang dapat digunakan asas nasional pasif dan asas universal. Asas-asas berlakunya hukum pidana menurut tempat yang konvensional / tradisional (jurisdiksi fisik) tentunya menghadapi tantangan sehubungan dengan masalah pertanggungjawaban tindak pidana siber.

Penanganan tindak pidana siber tidak akan berhasil jika aspek yurisdiksi diabaikan. Karena pemetaan yang menyangkut kejahatan dunia maya menyangkut juga hubungan antar kawasan, antar wilayah, dan antar negara. Sehingga penetapan jurisdiksi yang jelas mutlak diperlukan.

Yurisdiksi tersebut telah diatur dalam Pasal 2 undang-undang informasi dan transaksi elektronik nomor 19 tahun 2016, yaitu:

> Undang-undang ini berlaku untuk setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam undang-undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia yang

memiliki akibat hukum di wilayah hukum Indonesia dan/atau diluar wilayah hukum indonesia dan merugikan kepentingan Indonesia.

Undang-undang ini memiliki jangkauan yurisdiksi tidak sematamata untuk perbuatan hukum yang berlaku di Indonesia dan/atau dilakukan oleh warga negara Indonesia, tetapi juga berlaku untuk perbuatan hukum yang dilakukan di luar wilayah hukum (yurisdiksi) Indonesia baik oleh warga negara Indonesia (WNI) maupun warga negara asing (WNA) atau badan hukum Indonesia maupun badan hukum asing yang memiliki akibat hukum di Indonesia, mengingat pemanfaatan teknologi informasi untuk informasi dan transaksi elektronik dapat bersifat lintas territorial atau universal.

Yang dimaksud dengan "merugikan kepentingan indonesia" adalah meliputi tetapi tidak terbatas pada merugikan kepentingan ekonomi nasional, perlindungan data strategis, harkat dan martabat bangsa, pertahanan dan keamanan negara, kedaulatan negara, warga negara, serta badan hukum Indonesia.

2. Kendala Eksternal

a. Kurangnya Kesadaran Hukum Masyarakat

Menurut Kombes (Pol) Wisnu Andayana, Direktur Kriminal Khusus Polda Sulbar, (Wawancara Pada Tanggal 3 September 2018), Fungsi hukum pidana di bidang teknologi informasi secara umum adalah mengatur kehidupan manusia dalam kaitannya dengan

kegiatannya dalam dunia maya agar tercipta tatanan masyarakat yang tertib dan damai. Sedangkan fungsi khususnya adalah sebagai berikut.

a. Melindungi kepentingan hukum seluruh anggota masyarakat, baik orang per orang, kepentingan hukum masyarakat, maupun kepentingan hukum negara (misalnya keamanan negara) dalam pemanfaatan teknologi informasi agar dapat mencapai kesejahteraan.
b. Melindungi kepentingan hukum bagi setiap orang (manusia dan badan hukum) yang diduga atau telah terbukti menjadi pelaku kejahatan di bidang teknologi informasi.
c. Melindungi korban tindak pidana di bidang teknologi informasi.

Menurut Analisis Penulis Sampai saat ini, kesadaran hukum masyarakat Indonesia akan fungsi-fungsi tersebut dan dalam hal merespon aktivitas kejahatan mayantara (*cybercrime*) khususnya tindak pidana siber masih dirasakan kurang. Hal ini disebabkan karena kurangnya. Hal ini disebabkan karena kurangnya pemahaman dan pengetahuan masyarakat terhadap apa saja jenis-jenis kejahatan mayantara. Kurangnya pengetahuan ini menyebabkan upaya penanggulangan kejahatan mayantara mengalami kendala yang berkanaan dengan penataan hukum dan pengawasan (*controlling*) masyarakat terhadap setiap kegiatan atau aktivitas yang diduga berkaitan dengan tindak pidana siber.

b. Kurangnya Respon Masyarakat terhadap sosialisasi atau penyuluhan yang dilakukan pihak Kepolisian

Menurut AKP H. Muh. Agus, Kasubdit II Direktorat Krimsus Polda Sulbar, (Wawancara Pada Tanggal 28 Agustus 2018), Kendala yang dihadapi pihak Kepolisian dalam melakukan sosialisasi atau penyuluhan tentang tindak pidana siber yaitu kurangnya respon masyarakat terhadap apa yang dilakukan pihak Kepolisian ini membuktikan bahwa masyarakat masih minim pengetahuan tentang peraturan Undang-undang tentang *cyber crime* karena masyarakat menganggap bahwa teknologi itu merupakan hiburan semata dan menganggap tidak ada peraturan yang mengikat yang akan diberi sanksi ketika dilanggar.

Menurut Analisis Penulis masyarakat perlu untuk diberikan pengetahuan melalui penyuluhan atau sosialisasi yang dapat meningkatkan pengetahuan tentang aturan yang melarang *cyber crime* dan dampak ketika melakukan kejahatan *cyber crime*. Dengan melalui penyuluhan ini pihak kepolisian dapat mewujudkan masyarakat yang taat hukum, sehingga tidak ada lagi penyimpangan yang menyebabkan kesengjangan sosial.

c. Kurangnya Laporan Masyarakat

Menurut Pendapat Penulis Kurangnya laporan masyarakat terhadap yaitu ketika terjadi tindak pidana siber di lingkungan masyarakat, mereka seakan tidak peduli dengan kegiatan tersebut. Hal

ini berpengaruh terhadap kurangnya laporan yang masuk di kepolisian terkait tindak pidana siber. Dari keterangan beberapa warga, mereka tidak melaporkan adanya tindak pidana siber karena kurangnya pengetahuan masyarakat tentang tindak pidana siber dan masyarakat cenderung menanggap hal tersebut biasa-biasa saja, mereka takut berurusan dengan kepolisan dan tidak mau memperpanjang masalah, sehingga untuk pelaporan kecil kemungkinan dilakukan oleh masyarakat.

BAB V

PENUTUP

A. Kesimpulan

1. Faktor-faktor penyebab tindak pidana siber diwilayah Polda Sulawesi Barat terdiri dari dua yaitu : Faktor Internal yang terdiri dari Terbatasnya Personil Tenaga Ahli, Terbatasnya Anggaran Operasional dan Aspek Fasilitas Sedangkan Faktor Eksternal terdiri dari Faktor Ekonomi, Faktor Lingkungan, Faktor Sosial dan Budaya, dan Faktor Intelektual.
2. Kendala yang dialami oleh kepolisian daerah Sulawesi Barat dalam upaya penanggulangan tindak pidana siber terdiri dari dua yaitu : Kendala Internal yang terdiri dari Lemahnya Pengawasan Pemerintah dan Kepolisian, Aspek Alat Bukti dan Aspek Yurisdiksi, Sedangkan Kendala Eksternal terdiri dari Kurangnya kesadaran hukum masyarakat, kurangnya respon masyarakat terhadap sosialisasi atau penyuluhan yang dilakukan pihak kepolisian dan kurangnya laporan masyarakat.

B. Saran

1. Sarana dan Prasarana yang dimiliki oleh aparat penegak hukum untuk mengungkap kasus Tindak Pidana Siber masih sangat terbatas jumlah dan penggunaannya ini perlu dioptimalkan baik dari jumlah dan pengoperasiannya agar dapat mengembalikan kepercayaan masyarakat kepada aparat penegak hukum kita untuk menangani kasus Tindak Pidana Siber.

2. Untuk masyarakat sebaiknya membekali atau meningkatkan sistem keamanan media elektronik yang terhubung dengan internet guna menghindari adanya akses-akses illegal dari pihak luar serta masyarakat juga harus turut membantu penegakan hokum terkait tindak pidana siber, dengan melaporkanya ke aparat kepolisian jika melihat ataupun menjadi korban kejahatan siber.

DAFTAR PUSTAKA

A. Buku

B, Simanjuntak dan Chairil Ali. (1980). *Cakrawala Baru Kriminologi.* Penerbit. Trasito. Bandung.

Bonger. (1982). *Pengantar Tentang Kriminologi*. Penerbit. PT Pembangunan Ghalia Indonesia. Jakarta.

Chazawi, Adami. (2008). *Pelajaran Hukum Pidana I.* Penerbit. PT. Raja Grafindo Persada. Jakarta.

D, Soedjono. (1998). *Konsep Kriminologi Dalam Usaha Penanggulangan Kejahatan (Crime Preventions).* Penerbit. Alumni. Bandung.

Departemen Pendidikan Nasional. (2008). *Kamus Besar Bahasa Indonesia Pusat Bahasa.* Penerbit. PT. Gramedia Pustaka Utama. Jakarta

Dipanegara, A. (2009). *1 Jam Belajar Teknik Hacking*. Penerbit. HP Cyber Community. Jakarta.

Effendi, Erdianto. (2011). *Hukum Pidana Indonesia – Suatu Pengantar.* Penerbit. PT. Refika Aditama. Bandung.

ELCOM. (2011). *Hacking Exposed*. Penerbit. ANDI. Yogyakarta.

Hadi, Ainal, et al. (2012). *Kriminologi dan Viktimologi*. Penerbit. CV Bina Nanggroe. Aceh.

Hamzah, Andi. (1992). *Aspek-aspek pidana dibidang Komputer*. Peerbit. Sinar Grafika. Jakarta.

Kelana, Momo. (1972). *Hukum Kepolisian, Perkembangan di Indonesia Suatu Studi Histories Komparatif.* Penerbit. PTIK. Jakarta.

Lamintang, P. A. F. dan Francius Theojunior Lamintang. (2014), *Dasar-Dasar Hukum Pidana.* Penerbit. Sinar Grafika. Jakarta.

Makarim, Edmon. (2003). *Pengantar Hukum Telematika (Suatu Kajian Kompilasi).* Penerbit. PT. Raja Grafindo Persada. Jakarta.

Mansur, Didik M. Arif. (2005). *Cyber Law Aspek Hukum Teknologi Informasi*. Penerbit. Reflika Aditama. Bandung.

Moeljatno. (2015). *Asas-Asas Hukum Pidana.* Penerbit. PT. Rineka Cipta.Jakarta.

Maskun. (2017). *Kejahatan Siber (Cyber Crime) Suatu Pengantar.* Penerbit. Prenada Media. Depok.

Prana, Gede Artha Azriadi. (1990). *Hacker : Sisi Lain Legenda Komputer*. Penerbit. Adigna. Jakarta.

Rahardjo, Satjipto. (2011). *Penegakan Hukum Suatu Tinjauan Sosiologis.* Penerbit. Genta Publishing. Yogyakarta.

Rosenoer, Jonathan. (1997). *Cyber Law : The Law Of The Internet.* Spring Veriag. New York

Sahariyanto, Budi. (2013). *Tindak Pidana Teknologi Informasi (Cyber Crime) Urgensi Pengaturan dan Celah Hukumnya*. Penerbit. Rajawali Pers. Jakarta.

Sitompul, Josua. (2017). *Cyberspace, Cybercrimes, Cyberlaw, Tinjauan Aspek Hukum Pidana*. Penerbit. PT. Tatanusa. Ciputat.

Sulistyo, Sutanto Hermawan, dan Tjuk Sugiarto. (2002). *Cybercrime-Motif dan Penindakan.* Jakarta *:* Pensil 324.

Syahdeini, Sutan Remy. (2009). *Kejahatan & Tindak Pidana Komputer.* Penerbit. Pustaka Utama Grafiti. Jakarta.

Widodo. (2009). *Sistem Pemidanaan Dalam Cybercrime Alternatif Ancaman Pidana Kerja Sosial dan Pidana Pengawasan bagi Pelaku Cybercrime.* Penerbit. Laksbang Mediatama. Yogyakarta.

B. Undang-Undang

Undang-Undang Nomor 2 Tahun 2002 Tentang Kepolisian Negara Republik Indonesia.

Undang-Undang nomor 11 tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Undang-Undang No 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang nomor 11 tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

C. Karya Ilmiah

Situmorang, Evi Lestari. (2014). *Kajian Yuridis Pembuktian Kejahatan Mayantara (Cyber Crime) dalam Lingkup Transnasional*, Fakultas Hukum Universitas Sumatera Utara (USU), Medan.

Dwi, Pradita Krisna. (2010). *Tindak Pidana Hacking ditinjau dari Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*, Fakultas Hukum, Universitas Sebelas Maret, Surakarta.

D. Internet

URL : http://blogkelompokblog.wordpress.com/2013/06/19/pengertian-cybercrime-menurut-para-ahli/, *Pengertian Cyber Crime Menurut Para Ahli*, diakses pada 25 Juli 2018 pukul 17:00 WITA

URL : http://ogapermana.blogspot.com/2013/04/ pengertian-cybercrime-menurut-para-ahli/_11.html, diakses pada 25 Juli 2018 pukul 17:08 WITA

URL : http://informasinetonline.blogspot.com/2009/02/sejarah-hacking-141s.html, diakses pada 26 Juli 2018 pukul 17:08 WITA

URL : http://forums.soulmateclub.net/showthread.php?/1628-CYBER-CRIME-(Kejahatan-Internet)-amp-Pasal-pasalnya, *CYBER CRIME (Kejahatan-Internet) dan Pasal-pasalnya*, diakses pada 26 Juli 2018 pukul 18:08 WITA

URL : https://andriksupriadi.wordpress.com/2010/04/29/kebijakan-penanganan-dan-pencegahan-cyber-crime/, Penanganan dan Pencegahan Cyber Crime, diakses pada 26 Juli 2018 pukul 16:23 WITA

URL : http://en.wikipedia.org/wiki/Denial/_of_service, *Denial of Service Attack*, diakses pada 26 Juli 2018 pukul 19:05 WITA

DAFTAR PERTANYAAN WAWANCARA

1. Faktor-Faktor yang menyebabkan terjadinya tindak pidana Siber di wilayah sulbar ?
2. kasus tindak pidana Siber apa saja yg telah terjadi di wilayah sulbar ?
3. upaya penangggulanagan apa saja yg dilakukan untuk menaggulanagi terjadinya tindak pidana Siber ?
4. secara keseluruhan, apakah UU ITE telah menjawab kebutuhan dalam melakukan kegiatan atau aktivitas di dunia cyberspace ?
5. menyikapi berbagai kekurangan produk hukum tentang ITE solusi apa yg dapat dilakuakn oleh kepolisian untuk dapat melindunggi masyarakat dalam penggunaan teknologi ?
6. bagaimana kewenangan aparat kepolisian sebagai penegak hukum dalam melakukan penegakan hukum terhadap pelanggaran UU ITE ?
7. kendala aparat kepolisian dalam menanggulangi tindak pidana Siber ?
8. Lembaga-lembaga apa saja yang telah dimiliki oleh Indonesia yang diperluklan dalam menjalankan dan menegakkan UU ITE ?
9. Menyikapi berbagai kekurangan UU ITE apa yang harus dilakukan agar tidak mengganggu aktivitas/transaksi di dunia cyber dan dapat melindungi pengguna serta menjaga budaya bangsa ?
10. Ada beberapa Peraturan Pemerintah yang diamanatkan oleh UU ITE ? Bagaimana pemerintah melaksanakn amanat tersebut ?

FOTO PENELITIAN

KEPOLISIAN NEGARA REPUBLIK INDONESIA
DAERAH SULAWESI BARAT
DIREKTORAT RESERSE KRIMINAL KHUSUS

Nomor : SKP/141/IX/2018
Klasifikasi : B I A S A
Lampiran : -
Perihal : Penyampaian Telah Melaksanakan Penelitian

K e p a d a

Yth. DIREKTUR PROGRAM PASCASARJANA
UNIVERSITAS BOSOWA

Di
Makassar

1. Rujukan Surat Direktur Program Pascasarjana Universitas Bosowa Nomor : 299/B.01/PPs/UNIBOS/VIII/2018 tanggal 25 Agustus 2018 tentang penelitian.
2. Sehubungan dengan rujukan tersebut diatas, disampaikan kepada Bapak bahwa Mahasiswa Program Pascasarjana Universitas Bosowa yang tersebut dibawah ini :

   NAMA : REYNALDI EKO SAPUTRA
   NIM : 4616101043
   PROGRAM STUDI : MAGISTER ILMU HUKUM
   ALAMAT : Jln. Baharuddin Lopa, No. 5

   Telah melaksanakan penelitian pada Dit Reskrimsus Polda Sulbar pada tanggal 27 Agustus s/d 7 September 2018 dengan judul penelitian **"FUNGSI KEPOLISIAN DALAM PENANGGULANGAN TINDAK PIDANA SIBER DI POLDA SULAWESI BARAT"**.

3. Demikian untuk menjadi maklum.

Dikeluarkan di : Mamuju
Pada Tanggal : 7 September 2018
AN. DIREKTUR KRIMINAL KHUSUS
KASUBDIT II

H. MUH. AGUS, S.H.
AKP. NRP 70010105