YURIDIKSI NEGARA PADA CYBERCRIME

SKRIPSI

Disusun untuk memperoleh gelar Sarjana Hukum

Oleh

RYOBI PRADIPTA
NIM : 15.0201.0007

PROGRAM STUDI ILMU HUKUM
FAKULTAS HUKUM
UNIVERSITAS MUHAMMADIYAH MAGELANG
2019

PERSETUJUAN PEMBIMBING

Skripsi dengan judul **"YURIDIKSI NEGARA DALAM *CYBERCRIME*"**, disusun oleh **RYOBI PRADIPTA (NIM. 15.0201.0007)** telah disetujui untuk dipertahankan di hadapan Sidang Ujian Skripsi Fakultas Hukum Universitas Muhammadiyah Magelang, pada:

Hari : Kamis

Tanggal : 7 Februari 2019

Pembimbing I,

YULIA KURNIATY, SH., MH.
NIDN. 0606077602

Pembimbing II,

BASRI, SH., M.Hum.
NIDN. 0631016901

Mengetahui,
Dekan Fakultas Hukum
Universitas Muhammadiyah Magelang

BASRI, SH., M.Hum.
NIK. 966906114

PENGESAHAN PENGUJI

Skripsi

YURIDIKSI NEGARA DALAM *CYBERCRIME*

Oleh:

RYOBI PRADIPTA

NIM. 15.0201.0007

Telah diterima dan disahkan oleh Penguji Skripsi
Fakultas Hukum Universitas Muhammadiyah Magelang

Pada :

Hari : Kamis

Tanggal : 7 Februari 2019

PENGUJI

1. **YULIA KURNIATY, SH., MH.** : .....
   NIDN. 0606077602
   Ketua

2. **BASRI, SH., M.Hum.** : .....
   NIDN. 0631016901
   Sekretaris

3. **AGNA SUSILA, SH., M.Hum.** : .....
   NIDN. 0608155401
   Anggota

Mengetahui
Dekan,

BASRI, SH., M.Hum.
NIK. 966906114

HALAMAN PERNYATAAN ORISINALITAS

Saya yang bertanda tangan di bawah ini :

Nama : Ryobi Pradipta

NPM : 15.0201.0007

menyatakan bahwa skripsi yang berjudul "Yuridiksi Negara Dalam *Cybercrime*" adalah hasil karya saya sendiri, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar. Apabila dikemudian hari adanya plagiasi maka saya siap mempertanggungjawabkan secara hukum.

Magelang, 7 Februari 2019

Yang menyatakan

Ryobi Pradipta
NPM. 15.0201.0007

HALAMAN PERNYATAAN PUBLIKASI

TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Saya yang bertanda tangan di bawah ini :

Nama	: Ryobi Pradipta
NPM	: 15.0201.0007
Program Studi	: Ilmu Hukum (S1)
Fakultas	: Hukum

demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Muhammadiyah Magelang **Hak Bebas Royalti Non-eksklusif** (Non-exclucive Royalty Free Right) atas skripsi saya yang berjudul "Yuridiksi Negara dalam *Cybercrime*" beserta perangka yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-eksklusif ini Universitas Muhammadiyah Magelang berhak menyimpan, mengalihmedia formatkan, mengelola dalam bentuk pengkalan data base, merawat dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenarnya

Magelang, 7 Februari 2019

Yang menyatakan

Ryobi Pradipta
NPM. 15.0201.0007

MOTTO DAN PERSEMBAHAN

MOTTO

Man Jadda Wa Jada
(Siapa yang bersungguh-sungguh akan berhasil)

Man Shobaro Zafiro
(Siapa yang bersabar akan beruntung)

Man Saaro 'Alaa Darbi Washola
(Siapa yang berjalan di jalur-Nya akan sampai)

PERSEMBAHAN

Untuk istri, anak, orang tua, mertua, serta semua keluarga besarku.

Untuk Satuan Polisi Pamong Praja dan Pemadam Kebakaran
Kabupaten Temanggung.

KATA PENGANTAR

Puji dan syukur penulis panjatkan kehadirat Allah Subhanahu Wa Ta'ala yang telah melimpahkan kasih dan sayang-Nya sehingga penulis dapat menyelesaikan skripsi dengan judul "Yuridiksi Negara dalam *Cybercrime*".

Tujuan dari penyusunan skripsi ini dilakukan dalam rangka memenuhi salah satu syarat untuk bisa mencapai gelar Sarjana Hukum pada Program Studi Ilmu Hukum Strata Satu (S-1) Fakultas Hukum di Universitas Muhammadiyah Magelang.

Penyusunan skripsi ini telah melibatkan banyak pihak yang sangat membantu dalam banyak hal. Oleh sebab itu, penulis sampaikan rasa terima kasih kepada:

1. Bapak Ir. Eko Muh Widodo, M.T., selaku Rektor Univesitas Muhammadiyah Magelang;
2. Bapak Basri, S.H., M.Hum., selaku Dekan Fakultas Hukum Universitas Muhammadiyah Magelang;
3. Ibu Puji Sulistyaningsih, S.H.,M.H., selaku Kepala Progam Studi Fakultas Hukum Universitas Muhammadiyah Magelang;
4. Bapak Chrisna Bagus Edhita P, SH., MH ., selaku dosen pembimbing akademik Fakultas Hukum Universitas Muhammadiyah Magelang;
5. Ibu Yulia Kurniaty, SH., MH, selaku dosen pembimbing skripsi I Fakultas Hukum Universitas Muhammadiyah Magelang;
6. Bapak Basri, SH., M.Hum, selaku dosen pembimbing skripsi II Fakultas Hukum Universitas Muhammadiyah Magelang;
7. Seluruh dosen dan karyawan Fakultas Hukum Universitas Muhammadiyah Magelang atas pelayanan yang telah diberikan;
8. Kepala Perpustakaan Universitas Muhammadiyah Magelang yang telah membantu saya memfasilitasi dalam mencari data penelitian.
9. Semua keluarga yang telah mendukung saya dalam penyelesaian kuliah;
10. Seluruh pihak yang telah membantu dalam penyelesaian skripsi ini yang tidak dapat penulis sebutkan satu persatu.

Akhir kata, semoga Allah Subhanahu Wa Ta'ala berkenan membalas segala kebaikan semua pihak yang telah membantu dan semoga skripsi ini membawa manfaat bagi perkembangan ilmu.

Magelang, 07 Februari 2019

Penulis

ABSTRAK

Penelitian ini mengungkapkan secara lebih mendetail lagi tentang yurisdiksi negara dalam menangani kejahatan mayantara (*cybercrime*). Perkembangan kejahatan atau tindak pidana mayantara tanpa diikuti dengan perkembangan hukum akan menjadikan penegakkan hukumnya tidak berimbang. Oleh karena itu, selain menelaah yurisdiksi kriminal yang terdapat dalam UU No. 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, juga membahas Konvensi Dewan Eropa 2001 atau Konvensi Budapest yang memberikan penjelasan tentang kejahatan mayantara dan yurisdiksi sesuai Hukum Internasional. Penulis mencoba untuk memberikan ulasan yang mendalam tentang kejahatan mayantara ini, sehingga dapat dijadikan bahan referensi pengetahuan hukum tentang kajahatan mayantara yang cenderung terus meningkat belakangan ini.

Penelitian ini dilakukan di beberapa tempat, seperti perpustakaan Universitas Muhammadiyah Magelang dan perpustakaann kota.. Tempat-tempat tersebut dapat memberikan data primer untuk penulisan skripsi ini. Dalam penelitian ini juga ditelusuri data-data sekunder yang didapat dari perpustakaan. Wawancara dilakukan terhadap berbagai nara sumber untuk memenuhi kekurangan data penulis, terutama terhadap ahli hukum internasional, penyidik kepolisian, maupun praktisi hukum lainnya, yang menguasai kasus *cybercrime* ini.

Penelitian ini menggunakan metode yuridis normatif yang bersifat kualitatif. Penelitian yuridis normatif ini mengacu pada norma-norma hukum yang ada. Penelitian kualitatif digunakan untuk menganalisis data-data yang diperoleh, baik dari hasil kajian pustaka maupun hasil wawancara.

Hasil penelitian menyimpulkan bahwa: (1) pengaturan *cybercrime* dalam Konvensi Budapest terdiri atas 9 (sembilan) kategori kejahatan yang dilakukan secara sengaja dan tanpa hak); (2) menurut UU ITE, yurisdiksi Indonesia memiliki prinsip teritorial dan prinsip perlindungan: (3) baik UU ITE maupun Konvensi Budapest menggunakan prinsip teritorial dalam yurisdiksinya, dan Konvensi Budapest memiliki prinsip nasional, prinsip bendera kapal, prinsip pesawat terdaftar, yang tidak dimiliki UU ITE, selain itu UU ITE memiliki prinsip perlindungan, yang tidak dimiliki Konvensi Budapest.

Kata Kunci: **Yurisdiksi, *Cybercrime***

ABSTRACT

This research reveals in greater detail again about the jurisdiction of the State in dealing with the evil ofcybercrime. Development of crime or criminal offence the cybercrime legal developments followed without will make enforcement of the law is not balanced. Therefore, in addition to reviewing criminal jurisdiction contained in Act No. 19-year 2016 about changes to the law No. 11 Year 2008 of the information and electronic transactions, also addressed the Council of Europe 2001 Convention or the Convention of Budapest that provide explanation of cybercrime and appropriate international legal jurisdiction. The authors try to provide in-depth reviews about this cybercrime, so that it can be used as reference material legal knowledge about cybercrime tend to be on the rise lately.

The research was carried out in some places, like the library Muhammadiyah University of Magelang and city library. These places can provide primary data for the writing of this thesis. In this study also traced the secondary data obtained from the library. The interview was conducted on various resource person to meet the shortage of data authors, particularly against international law experts, police investigators, as well as other legal practitioner, who ruled the case of cybercrime .

This research uses the normative juridical method is qualitative. Juridical normative research refers to the legal norms that exist. Qualitative research is used to analyze the data obtained, either from the results of the literature review as well as the results of the interview.

Research results concluded that: (1) setting the cybercrime Convention in Budapest consist of 9 (nine) categories of crime committed intentionally and without right); (2) according to the ACT ITE, Indonesia has jurisdiction and the principle of the territorial principle of protection: (3) either the ACT ITE or the Convention of Budapest use the territorial principle in its jurisdiction, and the Convention of Budapest has a principle, the principle of national flag the ship, registered aircraft principles, which are not owned by the ACT ITE, in addition the ACT ITE has a principle of protection, which is not owned by the Budapest Convention.

Keywords**: **Jurisdiction, Cybercrime

DAFTAR ISI

BAB I
PENDAHULUAN

A. Latar Belakang

Kecepatan perkembangan teknologi di bidang digital, terutama internet menjadikan dunia ini terasa tanpa batas. Pada setiap jengkal ruang sudah dapat dideteksi tanpa menghadirkan fisik seseorang ke tempat tersebut. Dengan mengandalkan kemajuan teknologi digital ini pula, semua sudut bumi dapat dilihat dengan nyata pada saat seketika itu juga. Perkembangan kemajuan teknologi ini menjadikan dunia ini seperti dalam genggaman dan tanpa batas sama sekali (*borderless).*

Ini semua berawal dari pengembangan jaringan teknologi komputer *Advanced Research Projects Agency Network* (ARPANET) yang disponsori oleh Militer Amerika Serikat pada tahun 1960 untuk membangun sistem jaringan *(network*), yang sebelumnya dimaksudkan untuk menciptakan alat komunikasi yang mempunyai daya pegas dan aman serta memungkinkan terciptanya koordinasi antar aktivitas militer. Pada tahun 1969, pengembangan ARPANET meningkat dan secara bersamaan pula mulai menghubungkan komunitas peneliti universitas dengan aparat pemerintah. Pengembangan jaringan komputer tersebut merupakan cikal bakal lahirnya internet yang menghubungkan berbagai jaringan komputer di seluruh dunia dan telah menciptakan dunia baru yang disebut *cyberspace.*

Penemuan-penemuan dan pengembangan teknologi komputer dan produk- produk gelombang elektromagnetik (*electromagnetic wave)*

yang semula hanya digunakan untuk meningkatkan kemampuan sistem persenjataan militer, pencarian,

deteksi, akuisisi dan penghancuran sasaran (*search, detection, target, acquisition, and destroy*) dengan tingkat akurasi yang tinggi, telah membawa revolusi teknologi digital dari dunia maya ke dalam dunia kehidupan manusia sehari-hari.

Internet telah membentuk masyarakat dengan kebudayaan baru, dimana saat ini hubungan antara masyarakat dalam dimensi global tidak lagi dibatasi oleh batas- batas teritorial negara *(borderless).* Hadirnya internet dengan segala fasilitas dan program yang menyertainya, telah memungkinkan dilakukannya komunikasi global tanpa mengenal batas negara. Fenomena ini merupakan salah satu bagian dari globalisasi yang melanda dunia saat ini. Derasnya penggunaan teknologi informasi dalam kegiatan yang berbasis transaksi elektronik, seperti layanan anjungan tunai mandiri (ATM), transaksi *internet banking, mobile banking*, transaksi perdagangan dunia maya *(e-commerce*), dan lain-lain; sayangnya belum diikuti dengan perkembangan perangkat hukum. Oleh karena itu, diperlukan kehadiran perangkat hukum yang dapat menyelesaikan permasalahan/sengketa yang terjadi di dunia maya, karena hukum positif yang ada belum cukup dapat menjangkaunya (Efa Laela Fakhriah, 2017: 4).

Dalam perkembangan dunia digital internet selanjutnya, muncullah *e- commerce*. Secara umum *e-commerce* itu merupakan mekanisme

transaksi dalam berbisnis yang tidak menggunakan kertas sebagai sarana mekanismenya, tapi menggunakan teknologi dalam pengertian luas dalam proses dan praktik transaksinya, seperti penggunaan *e-mail* atau bisa melalui *worldwibeweb* (www) (Onno W Purbo dan Aang Arief Wahyudi, 2001: 1-2). Secara singkat dapat diartikan bahwa *e-commerce* merupakan suatu transaksi komersial yang dilakukan antar penjual dan

pembeli atau dengan pihak lain dalam hubungan perjanjian yang sama untuk mengirimkan sejumlah barang, pelayanan atau peralihan hak. Transaksi komersial ini terdapat di dalam media elektronik (media digital) yang secara fisik tidak memerlukan pertemuan para pihak yang bertransaksi dan keberadaan media ini di dalam jaringan umum (*public network)* atau sistem yang berlawanan dengan jaringan pribadi (*private network*).

Pemanfaatan internet yang begitu luas jangkauannya, sehingga membuat perkembangan bisnis di dunia maya *(electronic commerce* atau *e-commerce*) meningkat secara signifikan. Perkembangan *e-commerce* yang begitu pesat membuat tawaran barang dan jasa jadi berkembang lintas benua. Alhasil, perdagangan di dunia maya (*e-commerce*) ini jauh melebihi perkembangan perdagangan di dunia nyata. Pergeseran penjualan barang dan jasa ke dunia maya (*e-commerce*) didukung dengan berbagai kemudahan, antara lain: hampir semua jenis barang yang dibutuhkan ada di dunia maya, hampir segala jenis jasa tersedia, tidak perlu mengeluarkan

uang tunai – cukup hanya menggunakan kartu debit atau kredit – dengan berbagai cara pembayaran, tidak perlu keluar rumah (dapat dilakukan transaksi dari dalam kamar pribadi sekalipun), pilihan barang dan jasa yang hampir tidak terbatas, tidak mengenal waktu (buka 24 jam) serta kemudahan-kemudahan lain yang tidak didapatkan di gerai atau toko di dunia nyata.

Sementara itu, di luar Indonesia, juga banyak tersebar toko dunia maya, seperti amazone.com; alibaba.com; barbie.com; fashion.com; investment.com; dan lain-lain. Semua toko *online* tersebut dapat diakses lewat internet, seketika. Dengan

demikian, pembelian dapat dilakakukan kapan saja, dan dari belahan bumi mana saja, termasuk Indonesia.

Selain untuk kepentingan berjualan *(e-commerce*), internet dapat juga menjadikan ruang promosi suatu instansi (baik pemerintahan maupun swasta) lewat berbagai *website* yang mereka buat. Mereka dapat mempromosikan apapun yang berguna dan menarik untuk dilihat oleh seluruh manusia di muka bumi ini. Mereka dapat memuat berbagai hasil atau produk daerah masing-masing, atau menawarkan untuk berinvestasi di daerah mereka yang potensial untuk pengembangan ekonomi setempat. Itu semua dapat dilakukan lewat internet, dan luar biasanya, dapat dijangkau oleh semua orang yang punya akses internet untuk melihatnya.

Hampir semua instansi pemerintah saat ini telah memiliki laman (*website)* daerah masing-masing. Hal ini dimaksudkan untuk memberi

informasi ke semua khalayak tentang keadaan daerah tersebut, baik data kependudukannya, luas wilayahnya, hasil utama daerah tersebut, hingga potensi ekonomi yang dapat dikembangkan. Oleh karena itu, dengan hanya melihat *website* saja, seseorang dapat mengetahui keadaan suatu daerah tanpa harus mendatanginya. Inilah kelebihan penggunaan internet sebagai sarana komunikasi yang tak dapat ditawar-tawar lagi penggunaannya.

Melihat begitu pentingnya peran internet dalam kehidupan manusia saat ini, maka tak dapat disangkal lagi bahwa internet menjadi kebutuhan utama untuk mencari dan membagi informasi. Lewat informasi yang didapat, berbagai ilmu pengetahuan dan teknologi dapat dikembangkan menjadi lebih baik lagi. Lewat informasi yang disebar, masyarakat dunia dapat mengetahui keberadaan Indonesia,

negeri yang *gemah ripah loh jinawi*. Intinya, pemanfaatan teknologi informasi ini, selain mendorong permintaan atas produk-produk teknologi informasi itu sendiri, juga memudahkan untuk melakukan transaksi bisnis (Maskun dan Wiwik Meilarati,2016: 2).

Secara umum, dampak positif dari penggunaan internet adalah kemudahan komunikasi dengan siapapun di seluruh dunia, sebagai media pertukaran data dengan menggunakan fasilitas mesin pencarian *(search engine*), yang memudahkan pengguna di seluruh dunia dapat bertukar informasi dengan cepat, mudah, penting dan akurat sehingga manusia dapat mengetahui apa saja yang terjadi di belahan bumi lain; digunakan sebagai lahan informasi untuk bidang pendidikan, kebudayaan

dan lain- lain; dan kemudahan bertransaksi dan berbisnis di tempat dalam bidang perdagangan.

Sungguhpun demikian, di setiap peluang kemajuan terdapat potensi kecurangan atau tindakan kejahatan. Kejahatan sangat erat kaitannya dengan perkembangan masyarakat. Semakin maju kehidupan masyarakat, maka kejahatan juga mengiringi kemajuan tersebut. Peluang besar dapat terjadi di dunia internet yang tanpa batas-batas negara (*borderless)* ini sering disebut sebagai kejahatan dunia maya *(cybercrime*). Dan dalam perkembangannya, *cybercrime* ini juga telah melampaui batas-batas negara. Pelaku kejahatan atau tindak pidana dunia maya ini, bisa dilakukan di mana saja dan menimbulkan korban di mana saja, tanpa mengenal batas negara.

Teknologi internet yang berkembang ini kemudian dijadikan sarana untuk melakukan tindak pidana (*cybercrime).* Tindak pidana yang berbasiskan internet, baik berupa tindak pidana berupa membocorkan kerahasiaan (*confidentiality),* tentang integritas *(integrity*), dan keberadaan data (*avaiability*); atau penyerangan terhadap sistem komputer seperti *hacking, cracking, phreaking, virusses* dan lain-lain, maupun tindak pidana yang digunakan melalui media teknologi informasi dan komunikasi sebagai alat, seperti *cyberfraud, credit card fraud, cyberpornography, cyberterrorism* dan lain-lain.

Permasalahan yang muncul kemudian adalah apabila pelaku kejahatan atau tindak pidana ini berada diluar wilayah Indonesia, di

Amerika Serikat, China, Singapura, Malaysia atau negara lainnya. Para pelaku kejahatan internet yang melakukan penjualan manusia *(human traficking)*, berada di Malaysia, sementara korbannya ada di Indonesia. Kejahatan-kejahatan atau penipuan-penipuan berbasis internet yang dilakukan diluar yurisdiksi Indonesia, pastinya mengalami kendala penyelesaiannya. Sungguhpun demikian, upaya hukum harus tetap dilakukan untuk melindungi segenap warga negara Indonesia yang mengalami permasalahan hukum.

Pencegahan dan pemberantasan tindak pidana berbasis internet *(cybercrime*) ini bersifat transnasional dan memiliki karakteristik teknologi informasi dan komunikasi yang membutuhkan adanya harmonisasi peraturan (regulasi) tindak pidana dunia maya dalam hukum nasional negara-negara di dunia. Oleh karena itu, regulasi mengenai *cybercrime* dalam hukum nasional menjadi tidak mudah, karena berkaitan dengan yurisdiksi negara-negara lain. Sayangnya, pengaturan *cybercrime* dalam peraturan perundang-undangan Indonesia belum cukup representatif. Hal ini memiliki implikasi, baik terhadap hukum pidana materiil maupun hukum pidana formal.

Perkembangan teknologi yang begitu pesat tanpa diikuti perkembangan dunia hukum berakibat pada pelemahan sistem hukum yang ada. Para pelaku kejahatan mayantara ini sudah selayaknya untuk dilakukan kriminalisasi agar dapat dijerat secara hukum. Selain itu, regulasi hukum internet (*Cyber Law*) belum cukup untuk menjerat para

pejahat dunia maya ini. Konvensi Dewan Eropa 2001 atau Konvensi Budapest untuk menanggulangi kejahatan mayantara ini dapat dimanfaatkan untuk harmonisasi hukum nasional, walaupun Indonesia belum meratifikasi konvensi tersebut. Tetapi, paling tidak dapat memanfaatkan konvensi tersebut untuk kepentingan penegakan hukum di Indonesia.

Berdasarkan uraian di atas, penulis ingin memberikan ulasan secara mendalam tentang kejahatan atau tindak pidana yang dilakukan seseorang melalui internet *(cybercrime)* dengan memanfaatkan regulasi yang ada, yakni UU No. 19

Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Juga ingin memberikan ulasan tentang yurisdiksi negara dalam menangani kejahatan mayantara ini, sehingga sebagai negara berdaulat dapat memberikan perannya dalam menegakkan hukum secara adil dan profesional. Dengan latar belakang tersebut, penulis berusaha untuk memberikan ulasan secara mendalam lewat sebuah penelitian skripsi dengan judul: **‘‘Yurisdiksi Negara Dalam Cybercrime.**

B. Perumusan Masalah

Berdasarkan uraian latar belakang tersebut di atas, maka perumusan masalahnya adalah sebagai berikut:

1. Bagaimana pengaturan *Yuridiksi Negara* dalam Konvensi Budapest?

2. Bagaimana pengaturan yurisdiksi negara dalam UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diperbaharui dengan UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik?
3. Apakah persamaan dan perbedaan tentang pengaturan yurisdiksi negara dalam *cybercrime* menurut Konvensi Budapest dan UU ITE?

C. Tujuan Penelitian

1. Ingin mengetahui pemgaturan *cybercrime* dalam Konvensi Budapest.
2. Ingin mengetahui pengaturan yurisdiksi negara dalam UU ITE.
3. Ingin mengetahu persamaan dan perbedaan pengaturan yurisdiksi negara dalam *cybercrime* menurut Konvensi Budapest dan UU ITE

D. Kegunaan Penelitian

1. Secara teoritis, penelitian ini berguna untuk pengembangan ilmu hukum, khususnya Hukum Internet (*Cyber Law*), Hukum Internasional yang berkaitan dengan yurisdiksi, Hukum Pidana yang berkaitan dengan tindak pidana dunia maya (*cybercrime*) juga berkaitan dengan Hukum Perdata, khususnya yang berkaitan dengan perjanjian.
2. Secara praktis, penelitian ini diharapkan dapat menjadi acuan untuk bertransaksi di dunia maya agar dilakukan secara bijaksana, sehingga dapat terhindar dari hal-hal yang tidak diinginkan, terutama berkaitan dengan tindak pidana.

E. Sistematika Penulisan

BAB I PENDAHULUAN

Dalam BAB I ini akan diuraikan tentang Latar Belakang, Perumusan Masalah, Tujuan Penelitian, Kegunaan Penelitian dan Sistematika Penulisan.

BAB II TINJAUAN PUSTAKA

BAB II ini secara garis besar akan menjelaskan teori-teori yang dipakai dalam penelitian skripsi ini, yakni Pengertian atau Istilah-istilah yang digunakan tentang Internet, Yurisdiksi, Tindak Pidana Mayantara (*cybercrime)*, UU ITE, Konvensi Dewan Eropa 2001 atau Konvensi Budapest. Dasar Hukum yang digunakan untuk transaksi berbasis internet di Indonesia dan Kerangka Berpikir penelitian skripsi.

BAB III METODE PENELITIAN

Dalam penelitian skripsi ini, pada BAB III ini adalah Metode Penelitian yang meliputi Sifat Penelitian, Tipe Penelitian, Cara Pengumpulan Data, dan Analisis Hasil Penelitian.

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

BAB IV ini merupakan pemecahan perumusan masalah tentang pengaturan yurisdiksi tindak pidana mayatara (*cybercrime)* dalam Konvensi Dewan Eropa 2001 atau Konvensi Budapest, pengaturan yurisdiksi negara dalam UU ITE serta persamaan dan perbedaan yurisdiksi negara menurut Konvensi Budapest dan UU ITE.

BAB V PENUTUP

BAB V ini merupakan intisari dari hasil penelitian dan pembahasan, yang berisikan Kesimpulan dan Saran dari hasil penelitian ini.

BAB II

TINJAUAN PUSTAKA

A. Pengertian Internet

Internet adalah jaringan komputer yang terhubung satu sama lain melalui media komunikasi, seperti kabel telepon, serat optik (*fibre optic*), satelit ataupun gelombang frekuensi.

Internet adalah kependekan dari *interconnection networking* yang berarti seluruh jaringan komunikasi yang menggunakan media elektronik, yang saling terhubung menggunakan standar sistem *Global Transmission Control Protocol/Internet Protocol Suite* (TCP/IP) sebagai protokol pertukaran paket *(packet switching communication protocol*) (Maskun dan Wiwik Meilarati, 2016: 13).

Pengertian lainnya, Internet adalah sebuh jaringan komputer yang saling terhubung dengan menggunakan sistem *standard global transmission control protocol /internet protocol suite* (TCP/IP) yang digunakan sebagai protokol pertukaran paket dalam melayani miliaran pengguna yang terdapat di seluruh dunia, juga dapat diartikan sebagai jaringan komunikasi global yang terbuka dan menghubungkan jutaan atau milyaran jaringan komputer dengan berbagaui tipe komunikasi.

Fungsi internet:

1) Sebagai media komunikasi.
2) Sebagai salah satu media untuk mencari informasi.
3) Sebagai sumber daya dan data.

4) Dapat menyiarkan dan mengakses secara langsung baik itu berita dan bertukar data dengan internet *online* ke seluruh dunia.

Dapat disederhanakan di sini bahwa pengertian Internet adalah sebuah jaringan komputer yang terhubung dengan jaringan komputer lainnya yang milyaran jumlahnya dan digunakan oleh milyaran manusia dengan standar TCP/IP dengan menggunakan berbagai tipe komunikasi.

B. Pengertian Yurisdiksi Negara

Kata "yurisdiksi" dalam bahasa Indonesia berasal dari bahasa Inggris *"Jurisdiction"*. *"Jurisdiction*" berasal dari bahasa Latin *"Yurisdictio",* yang terdiri atas dua suku kata, *yuris* yang berarti kepunyaan menurut hukum, dan *diction* yang berarti ucapan, sabda, sebutan, firman (Cowie, 1989: 679).

Dapat disimpulkan bahwa yurisdiksi negara berarti:

1. Kepunyaan seperti yang ditentukan oleh hukum.
2. Hak menurut hukum.
3. Kekuasaan menurut hukum.
4. Kewenanagan menurut hukum.

Menurut Romli Atmasasmita (1997: 89), yurisdiksi negara itu meliputi:

1. Yurisdiksi untuk menetapkan suatu peraturan perundang-undangan *(jurisdiction to prescribe);*

2. Yurisdiksi untuk melaksanakan penuntutan *(jurisdiction to adjudicate);*

3. Yurisdiksi untuk menetapkan peraturan perundang-undangan *(jurisdiction to enforce).*

Hikmahanto Juwana (2006: 6) mengatakan bahwa yurisdiksi negara terkait dengan kapan hukum suatu negara dapat diberlakukan baik terhadap warga negaranya sendiri maupun warga negara asing. Berdasarkan yurisdiksi aparat penegak hukum dapat menjalankan kewenangannya. Polisi dapat melakukan penangkapan dan penahanan. Jaksa dapat melakukan penuntutan. Pengadilan dapat menyidangkan.

Selanjutnya, Hikmahanto Juwana (2006: 12) menyebutkan bahwa ada 4 (empat) azas yang digunakan dalam menajalankan yuridiski negara dalam hukum internasional, yaitu:

a. Azas Teritorial

Asas teritorial menentukan bahwa Negara dapat menjalankan yurisdiksi atas hukumnya terhadap setiap individu dan badan hukum yang berada di wilayah teritorialnya tanpa melihat status kewarganegaraan individu ataupun badan hukum. WNA bila melakukan kejahatan di Indonesia dapat ditangkap, ditahan dan diadili di Indonesia. Azas ini juga diatur dalam Pasal 2 KUHPidana.

b. Azas Personalitet atau Asas Nasional Aktif

Asas Nasionalitas/ Personalitas menentukan bahwa Negara dapat menjalankan yurisdiksinya berdasarkan kewarganegaraan dari individu atau badan hukum. Asas ini dapat didasarkan

pada kewarganegaraan pelaku (Nasionalitas Aktif) dan kewarganegaraan korban (Nasionalitas Pasif). Ketentuan azas ini sesuai dengan Pasal 5 KUHPidana.

c. Asas Perlindungan atau Asas Nasional Pasif

Asas Kepentingan Negara menentukan bahwa Negara dapat menjalankan yurisdiksinya berdasarkan kepentingan dan keamanan Negara yang merasa terancam, meskipun tindakan di luar negara tersebut dan oleh pelaku yang tidak berkewarganegaraan dari Negara yang terancam. Azas ini sesuai dengan Pasal 4 ayat (1), ayat (2), dan ayat (3). d. Asas Universal.

Asas Universal menentukan bahwa Negara mana saja dan kapan saja dapat menjalankan yurisdiksinya apabila ada individu yang melakukan kejahatan internasional. Asas ini terkait erat dengan individu sebagai subyek hukum internasional. Azas ini sesuai dengan Pasal 4 ayat (2) dan ayat (4).

Asril Sitompul (2001: 17) menyebutkan bahwa yurisdiksi berkaitan dengan pelaku tindak pidana yang berbasiskan internet *(cybercrime*), berkaitan dengan wewenang pengadilan, tempat kejadian perkara, tempat pengajuan gugatan, dan sebagainya.

Menurut Sigid Suseno (2017: 55), yurisdiksi adalah refleksi dari kedaulatan suatu negara, yang dilaksanakan dalam batas-batas wilayahnya. Apabila kedaulatan merupakan atribut atau ciri khusus dari negara, maka yurisdiksi merupakan lambang kedaulatan suatu negara.

Menurut Konvensi Budapest (karena penyelenggaraannya di Budapest, Hongaria, 23 November 2001) atau dikenal juga dengan nama Konvensi Dewan Eropa 2001 (karena penyelenggara dan anggotanya adalan Masyarakat Eropa atau *Council of Europa*, pengertian yurisdiksi negara yang terdapat pada Pasal 22 adalah:

1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Article 2 through 11 of this Convention when the offence committed;

   (1. Pihak Negara harus menerapkan undang-undang dan mengambil tindakan-tindakan lain yang diperlukan untuk menetapkan kewenangan setiap tindak pidana sebagaimana ditetapkan dalam Pasal 2 sampai 11 Konvensi ini, saat pelanggaran dilakukan):

   a. in its territory; or (*di wilayahnya; atau*)
   b. on board a ship flying the flag of that Party; or (*di atas kapal yang mengibarkan bendera dari Pihak tersebut; atau*)
   c. on board an aircraft registered under the laws of that Party; or *(di atas pesawat terdaftar berdasarkan hukum dari Pihak tersebut; atau*)
   d. by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State

(*oleh salah satu warga negaranya, jika pelanggaran dapat dihukum berdasarkan hukum pidana di mana perbuatan tersebut dilakukan atau jika kejahatan dilakukan di luar yurisdiksi wilayah dari setiap negara*).

2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down paragraphs 1.b through 1.d of this article or any part thereof; *(2. Pihak Negara berhak untuk tidak menerapkan atau hanya berlaku dalam kasus-kasus tertentu atau kondisi tertentu tentang aturan yurisdiksi yang ditetapkan dalam paragraf 1.b sampai*

   1.d pasal ini atau setiap bagian daripadanya:).

3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences reffered to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition; *(3. Pihak Negara wajib mengambil tindakan yang mungkin diperlukan untuk menetapkan yurisdiksi atas tindak pidana sebagaimana yang dimaksud dalam Pasal 24 ayat (1) Konvensi ini, dalam kasus-kasus dimana tersangka pelaku berada di wilayahnya dan tidak mengektradisinya untuk pihak lain semata-mata atas dasar kewarganegaraannya, setelah ada permintaan ekstradisi:)*

4. This Convention does not exclude any criminal jurisdiction excercised by a Party in accordance with its domestic law; *(4. Konvensi ini tidak mengesampingkan setiap yurisdiksi kejahatan yang dilakukan oleh Pihak Negara sesuai dengan hukum nasionalnya:)*

5. When more than one Party claims jurisdiction over an alleged offence establish in accordance with this Convention, the Parties involved shal, when appropriate, consult with a view to determining the most appropriate jurisdiction for presecution. *(5. Bila lebih dari satu Pihak Negara mengklaim yurisdiksinya atas suatu dugaan tindak pidana yang ditetapkan sesuai dengan Konvensi ini, Pihak Negara yang terlibat harus, jika perlu, berkonsultasi dengan maksud untuk menentukan yurisdiksi yang paling tepat untuk melakukan penuntutan)* (Maskun dan Meilarati, 2017: 132-133).

Sementara itu, menurut UU No. 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) pada Pasal 2 memberikan pengertian yurisdiksi bahwa setiap orang yang melakukan perbuatan hukum sebagaimana yang diatur UU ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/ atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia.

C. Pengertian Cybercrime

Menurut tipologinya, *cybercrime* berasal dari 2 (dua) kata, yaitu *cyber* dan *crime*. *Cyber* adalah bahasa Inggris yang berarti ruang, maya, mayantara, siber; sedangkan *crime* berarti kejahatan, tindak pidana, peristiwa pidana atau yang sejenisnya (Agus Rahardjo, 2002: 4). Dengan demikian, maka untuk itu diperlukan pengertian tentang tindak pidana dan pengertian tindak pidana mayantara.

1. Tindak Pidana

Menurur Barda Nawawi Arief (2005: 81), tindak pidana pada hakikatnya adalah perbuatan yang melawan hukum, baik secara formal maupun secara material. Sedangkan dalam Konsep KUHP Baru disebutkan dalam Pasal 14 bahwa tindak pidana ialah perbuatan melakukan atau tidak melakukan sesuatu yang oleh peraturan perundang-undangan dinyatakan sebagai perbuatan yang dilarang dan diancam dengan pidana.

Wirjono Prodjodikoro (1981: 50) menyatakan bahwa tindak pidana itu adalah suatu prerbuatan yang pelakunya dapat dikenakan hukuman pidana.

Adam Chazawi (2001: 73) berpendapat bahwa tindak pidana *(strafbaar feit*) atau peristiwa pidana adalah suatu perbuatan atau rangkaian perbuatan manusia, yang bertentangan dengan undang-undang atau peraturan perundang-undangan lainnya, terhadap perbuatan mana diadakan tindakan penghukuman.

Hilman Hadikusuma (2013: 115) menyebutkan bahwa peristiwa pidana, perbuatan pidana, tindak pidana atau delik memiliki pengertian yang sama yaitu semua peristiwa perbuatan yang bertentangan dengan hukum pidana. Jadi, peristiwa itu merupakan pelanggaran hukum dan mengandung anasir melawan hukum. Pelanggaran hukum yang diancam dengan hukuman (pidana) itulah yang dikualifikasi sebagai peristiwa pidana *(strafbaar feit).*

2. Tindak Pidana Mayantara

Cybercrime atau tindak pidana mayantara atau kejahatan dunia maya atau tindak pidana siber adalah aktivitas pengguna internet yang menyimpang atau melanggar hukum dengan memanfaatkan perkembangan teknologi informasi dan komunikasi (TIK) sebagai media baru untuk melakukan kejahatan (Barda Nawawi Arief, 2005: 101).

Cybercrime merupakan tindak kejahatan yang menggunakan koneksi internet untuk melakukannya, yang dapat dilakukan hingga menembus negara lain. Penggunaan istilah *computer crime* maupun *cybercrime* adalah sama, mengingat keduanya menimbulkan akibat hukum yang sama (Maskun dan Wiwik Meilarati,2016: 20).

Tindak pidana siber (*cybercrime*) adalah aktivitas pengguna internet yang menyimpang atau melanggar hukum dengan memanfaatkan perkembangan teknologi informasi dan komunikasi sebagai media baru untuk melakukan kejahatan (Sigid Suseno, 2017: 23).

D. Pengaturan Tindak Pidana Mayantara (Cybercrime)

1. *Cybercrime* Menurut KUHPidana

Menurut Umar Said Sugiarto (2015: 234) hukum pidana dibagi menjadi 2 (dua), hukum pidana material dan hukum pidana formal (hukum acara pidana). Hukum pidana material adalah peraturan atau norma hukum yang mengatur tentang perbuatan-perbuatan apa yang dapat dipidana, siapa yang dapat dipidana, dan macam apa sanksi pidana yang dijatuhkan. Dengan kata lain, hukum pidana (material) adalah keseluruhan peraturan atau hukum yang mengatur perbuatan seseorang atau badan yang dilakukan dengan salah dan melanggar hukum pidana serta diancam dengan sanksi pidana.

Hukum pidana formal (hukum aacara pidana) adalah keseluruhan peraturan atau norma hukum yang mengatur tata cara melaksanakan dan mempertahankan hukum pidana material. Dengan kata lain, hukum acara pidana (hukum pidana formal) adalah segala peraturan atau hukum yang mengatur tindakan-tindakan aparatur negara apabila diduga terjadi perbuatan pidana menurut hukum pidana material (Umar Said Sugiarto, 2015: 234).

Sesungguhnya, setiap tindak pidana mayantara (*cybercrime*), dapat dijerat dengan pasal-pasal yang ada dalam KUHPidana. Dalam Buku II yang mengatur tentang Kejahatan, Buku III mengatur tentang Pelanggaran. Baik kejahatan maupun

pelanggaran yang dilakukan di dunia maya *(cybercrime*) akan dirumuskan

atau dikriminalisasi sehingga dapat dirumuskan pasal-pasal yang dijatuhkan untuk penghukuman.

Maskun (2013: 51) membagi cakupan kejahatan mayantara (dunia maya), meliputi:

a) Pembajakan; (Pasal 363 KUHPidana)

b) Penipuan; (Pasal 378 KUHPidana) c) Pencurian; (Pasal 362 KUHPidana) d) Pornografi; (Pasal 335 KUHPidana) e) Pelecehan; (Pasal 335 KUHPidana)

f) Pemfitnahan; (Pasal 282 KUHPidana ayat (1), (2), (3); dan g) Pemalsuan. (Pasal 244 sampai Pasal 252 KUHPidana).

Keterbatasan cakupan KUHPidana ini sebenarnya dapat dibantu dengan regulasi lain, sehingga para pelaku *cybercrime* dapat dijerat secara hukum. Selain itu, KUHPidana berisikan tindak pidana umum, sedangkan *cybercrime* nerupakan kejahatan yang memiliki karakteristik khusus teknologi informasi dan komunikasi. Kejahatan terhadap *confideciality*, *integrity*, dan *availability* data komputer dan/ atau sistem komputer. Oleh karena itu, pengaturan *cybercrime* lebih tepat bila diatur dalam undang-undang atau regulasi khusus, sebagaimana ketentuan Pasal 103 KUHPidana.

2. *Cybercrime* Menurut UU ITE

Dalam hukum positif Indonesia, tindak pidana mayantara *(cybercrime)* ini telah diatur, yakni dalam UU No. 19 Tahun 2016 tentang Perubahan Atas UU No. 11 tahun 2008 tentang Informasi dan Transaksi

Elektronik (UU ITE). UU ITE ini

merupakan undang-undang khusus yang mengatur berbagai aktivitas manusia di bidang teknologi informasi dan komunikasi, termasuk beberapa tindak pidana mayantara. Kriminalisasi tindak pidana mayantara dalam peraturan perundang- undangan Indonesia tersebut memiliki implikasi terhadap upaya pemberantasan tindak pidana mayantara di Indonesia khususnya dan dunia pada umumnya.

Pengaturan tindak pidana mayantara dalam UU ITE terdapat dalam Pasal 27 hingga Pasal 36 (perbuatan yang dilarang) *juncto* Pasal 45 hingga Pasal 52. Perumusan tindak pidana mayantara dalam UU ITE dilakukan secara terpisah dengan terlebih dahulu merumuskan unsur-unsur tindak pidananya dalam Pasal 27 hingga Pasal 36, dan kemudian sanksi pidananya dalam Pasal 45 hingga Pasal 52.

Pasal 27 UU ITE:

1. 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.
2. 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 perjudian.
3. Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/

atau mentrasnisikan dan/ atau membuat dapat diaksesnya Informasi Elektronik dan/ atau Dokumen Elektronik yang memiliki muatan penghinaan dan/ atau pencemaran nama baik.

4. 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 pemerasan dan/ atau pengancaman.

Pasal 28 UU ITE:

1. Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.
2. Setiap Orang dengan sengaja dan tanpa hak menyebarkan informasi 6yang ditujukan untuk menimbulkan rasa kebencian dan permusuhan individu dan/ atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras dan antargolongan (SARA).

Pasal 29 UU ITE:

Setiap Orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/ atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi.

Pasal 30 UU ITE:

1. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses

   Komputer dan/ atau Sistem Elektronik milik Orang Lain dengan cara apapun.

2. 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.

Pasal 31 UU ITE:

1. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/ atau Dokumen Elektronik dalam suatu Komputer dan/ atau Sistem Elektronik tertentu milik Orang Lain.
2. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/ atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/ atau Sistem Elektronik tertentu milik Orang Lain, baik yang tidak menyebabkan perubahan apapun maupun yang menyebabkan adanya perubahan, penghilangan dan/ atau penghentian Informasi Elektronik dan/ atau Dokumen Elektronik yang sedang ditransmisikan.
3. Kecuali intersepsi sebagaimana dimaksud pada ayat (1) dan ayat (2), intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan dan/ atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang.

4. Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.

Pasal 32 UU ITE:

1. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/ atau Dokumen Elektronik milik Orang Lain atau milik publik.

2. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun memindahkan atau mentransfer Informasi Elektronik dan/ atau Dokumen Elektronik kepada Sistem Elektronik Orang Lain yang tidak berhak.

3. Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/ atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

Pasal 33 UU ITE:

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apapun yang berakibat terganggunya Sistem Elektronik dan/ atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.

Pasal 34 UU ITE:

1. Setiap Orang dengan sengaja dan tanpa haka tau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan atau memiliki:
   a. perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan pasal 33;
   b. sandi lewat Komputer, Kode Akses, atau hal lain yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan pasal 33.

2. Tindakan sebagaimana dimaksud dalam ayat (1) bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian Sistem Elektronik, untuk perlindungan Sistem Elektronik itu sendiri secara sah dan tidak melawan hukum.

Pasal 35 UU ITE:

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/ atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.

Pasal 36 UU ITE:

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian Orang Lain.

Selanjutnya, ketentuan pidana akibat kejahatan mayantara *(cybercrime)*

terdapat pada Pasal 45:

1. Setiap Orang yang memenuhi unsur dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3) atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/ atau denda paling banyak Rp. 1.000.000.000,00 (satu milyar rupiah).
2. 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 milyar rupiah).
3. Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 29 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/ atau denda paling banyak Rp. 2.000.000.000,00 (dua milyar rupiah).

Pasal 46 UU ITE:

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 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 paling lama 8 (delapan) tahun dan/ atau denda paling banyak Rp.800.000.000,00 (delapan ratus juta rupiah).

Pasal 47 UU ITE:

Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 31 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/ atau denda paling banyak Rp.800.000.000,00 (delapan ratus juta rupiah).

Pasal 48 UU ITE:

1. Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/ atau denda paling banyak Rp.2.000.000.000,00 (dua milyar rupiah).

2. Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (sembilan) tahun dan/ atau denda paling banyak Rp.3.000.000.000,00 (tiga milyar rupiah).

3. Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (3) dipidana denga pidana penjara paling lama 10 (sepuluh) tahun dan/ atau denda paling banyak Rp.5.000.000.000,00 (lima milyar rupiah).

Pasal 49 UU ITE:

Setiap Orang yang memenuhi unsur sebagaimana yang dimaksud dalam Pasal 33, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/ atau denda paling banyak Rp.10.000.000.000,00 (sepuluh milyar rupiah).

Pasal 50 UU ITE:

Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 34 ayat (1) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/ atau denda paling banyak Rp.10.000.000.000,00 (sepuluh milyar rupiah).

Pasal 51 UU ITE:

1. Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/ atau denda paling banyak Rp.12.000.000.000,00 (dua belas milyar rupiah).
2. Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 36 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/ atau denda paling banyak Rp.12.000.000.000,00

(dua belas milyar rupiah).

Pasal 52 UU ITE:

1. Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 ayat (1) menyangkut kesusilaan atau ekploitasi seksual terhadap anak dikenakan pemberatan sepertiga dari pidana pokok.
2. Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 37 ditujukan terhadap Komputer dan/ atau Sistem elektronik milik Pemerintah dan/ atau yang digunakan untukkyanan public dipidana dengan pidana pokok ditambah sepertiga.
3. Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/ atau Sistem Elektronik serta Informasi Elektronik dan/ atau Dokumen elektronik milik Pemerintah dan/ atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan diancam dengan pidana maksimal ancaman pidana pokok masing-masing Pasal ditambanh dua pertiga.
4. Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pokok ditambah dua pertiga.

Dari uraian tentang kejahtan mayantara *(cybercrime)* yang diakomodasi UU ITE tampak bahwa kejahatan dilakukan dengan menggunakan teknologi informasi dan komunikasi yang difasilitasi komputer dan jaringan internet. Upaya kriminalisasi terhadap para pelaku tindak pidana mayantara ini pada prinsipnya tidak memberikan

beban berlebih kepada aparat penegak hukum. Kriminalisasi terhadap kejahatan mayantara ini merupakan usaha pencegahan dan pemberantasannya oleh aparat penegak hukum dengan sarana dan prasarana yang memadai. Menurut Muladi (1992:

31), kriminalisasi penyalahgunaan komputer *(computer abuse)* menggunakan pendekatan evolusioner dan pendekatan kompromis. Pendekatan evolusioner adalah pendekatan dengan melakukan pembaharuan atau amandemen perumusan tindak pidana terhadap kejahatan-kejahatan tradisional dengan menambah objek atau cara- cara dilakukannya kejahatan. Pendekatan kompromis adalah pendekatan antara pendekatan global dan pendekatan evolusioner. Pendekatan global adalah pendekatan dengan melakukan pengaturan baru yang bersifat umum tentang kejahatan komputer. Dengan demikian, pendekatan kompromis adalah pendekatan dengan cara mencantumkan komputer dalam kodifikasi hukum pidana.

3. *Cybercrime* Menurut Konvensi Dewan Eropa 2001 atau Konvensi Budapest

Untuk pengaturan, pencegahan, dan kebijakan kriminalisasi terhadap kejahatan mayantara *(cybercrime)* ini dan yurisdiksi negara yang berada di dalamnya serta sebagai sarana harmonisasi untuk mengatasi kejahatan mayantara ini, maka pada tanggal 23 November 2001, negara-negara yang bergabung dalam Uni Eropa *(Council of Europe)* membuat suatu konvensi untuk mengatasi kejahatan ini, yakni *Convention on Cybercrime*, di Kota Budapest, Hungaria. Selanjutnya, konvensi ini diberi nama Konvensi Dewan Eropa 2001 atau Konvensi Budapest, yang pada awalnya dibuat oleh organisasi regional Eropa, tetapi pada perkembangannya dimungkinkan untuk diratifikasi dan diakses oleh negara manapun di dunia yang memiliki komitmen dalam upaya mengatasi kejahatan mayantara (*cybercrime).*

Konvensi Dewan Eropa 2001 telah mengatur hukum pidana subtantif terhadap pelaku *cybercrime* yang terdapat pada Pasal 2 hingga Pasal 11. Daya berlaku hukum pidana subtantif berdasarkan pada ketentuan tentang yurisdiksi negara (Pasal

22), yang mengatur prinsip-prinsip yurisdiksi negara sebagai dasar berlakunya yurisdiksi kriminal terhadap tindak pidana mayantara *(cybercrime).*

Pengaturan yurisdiksi dalam Pasal 22 Konvensi Dewan Eropa 2001 dengan maksud agar negara pihak dalam Konvensi Dewan Eropa ini menetapkan berlakunya yurisdiksi terhadap *cybercrime,* dalam hukum nasional masing-masing negara. Pengaturan yurisdiksi ini juga dimaksudkan untuk menghadapi terjadinya dua atau lebih negara pihak yang menuntut yurisdiksi terhadap *cybercrime.*

Adapun hal-hal yang termasuk *cybercrime* menurut Konvensi Dewan Eropa

2001 atau Konvensi Budapest adalah:

a) Pasal 2 tentang Pelanggaran Terhadap Akses Illegal *(Illegal Access);*

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under the domestic law, when committed intentionally, the acces to the whole or any part of a computer system without right; A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system. (*Pihak Negara harus menerapkan undang-undang dan mengambil tindakan-tindakan lain yang diperlukan untuk ditetapkan sebagai tindak pidana berdasarkan hukum nasionalnya, jika dilakukan dengan sengaja, akses ke seluruh atau sebagian dari suatu sistem komputer*

tanpa hak; Pihak Negara dapat meminta pelanggaran yang dilakukan oleh pelanggar untuk memperoleh data komputer atau

dengan maksud tidak jujur, atau berhubungan dengan sistem komputer yang terhubung ke sistem komputer lainnya, demi keamanan komputer.)

b) Pasal 3 tentang Pelanggaran Terhadap Penyadapan Illegal (*Illegal*

Intercepcion);

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data; A Party may require that the offence be committed is conenected to another computer system. (*Pihak Negara harus menerapkan undang-undang dan mengambil tindakan-tindakan lain yang diperlukan untuk ditetapkan sebagai tindak pidana berdasarkan hukum nasionalnya, jika dilakukan dengan sengaja, penyadapan tanpa hak, dilakukan dengan cara teknis, transmisi non publik data komputer untuk, dari atau dalam sistem komputer, termasuk emisi elektromagnetik dari sebuah sistem komputer yang membawa data komputer tersebut. Pihak Negara mensyaratkan bahwa apa yang dilakukan merupakan tindakan tidak jujur berkaitan dengan sistem komputer yang berhubungan dengan sistem komputer lainnya).*

c) Pasal 4 tentang Pelanggaran Melakukan Gangguan Data (*Data*

Interference);

1. Each Party shall adopt such the legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alternation or suppression of computer data without right; (*1. Pihak Negara harus menerapkan undang-undang dan mengambil tindakan- tindakan lain yang diperlukan unttuk ditetapkan sebagai tindak pidana: pengrusakan,penghapusan, pemburukan, perubahan atau penahanan data komputer tanpa ha dan dengan sengaja:)*
2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm. (*2. Pihak Negara perlu mensyaratkan bahwa perilaku yang dimaksudkan pada ayat (1) merupakan kejahatan yang dapat menimbulkan masalah yang berbahaya dan sangat serius).*

d). Pasal 5 tentang Pelanggaran Melakukan Gangguan Sistem (*System*

Interference);

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data; *(Pihak Negara harus*

menerapkan undang-undang dan mengambil tindakan-tindakan lain

yang diperlukan untuk ditetapkan sebagai tindak pidana: secara serius merintangi fungsi dari sebuah sistem komputer dengan tnpa hak, melalui memasukkan, memindahkan, merusak, menghapus, memperburuk, mengubah atau menahan data komputer:)

e). Pasal 6 tentang Penyalahgunaan Perangkat *(Misuse of Device*);

1. Each Party adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: *(1. Pihak Negara harus menerapkan undang- undang dan mengambil tindakan-tindakan lain yang diperlukan untuk ditetapkan sebagai tindak pidana jika dilakukan secara sadar dan tanpa hak:)*

a. the production, sale, procurement for use, import distribution or otherwise making available of: *(memproduksi, menjual, impor, distribusi dan pengadaan untuk:)*

i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences establish in accordance with Article 2 through:5; *(alat atau perangkat, termasuk program komputer yang dirancang atau didesain untuk tujuan melakukan salah satu tindak pidana yang ditetapkan sesuai dengan Pasal 1 sampai 5;)*

ii. a computer password, acces code, or similar data by which the whole or any part of computer system is capable of being accessed; *(sandi, kode akses atau data yang sama dalam komputer baik seluruhnya atau sebagian dari sebuah sistem komputer yang bisa diakses.)*

b. with intent that it be used for the purpose of committing any of offences establish in Article 2 throug 5: and *(dengan maksud yang digunakan untuk tujuan melakukan salah satu*

tindak pidana yang ditetapkan dalam Pasal 2 sampai 5, dan;)

c. the possession of an item referred to in paragraphs I or ii above, with intent that it be used for the purpose of committing any of the offences establish in Article 2 through 5; A Party may require by law that a number of such item be possessed before criminal liability attaches; (*kepemilikan bperangkat sebagaimana dimaksud dalam ayat (i) atau (ii) di atas, dengan maksud bahwa perangkat tersebut digunakan untuk tujuan melakukan salah satu tindak pidana yang ditetapkan dalam Pasal 2 sampai 5. Pihak Negara dapat meminta berdasarkan hukum bahwa sejumlah perangkat tersebut dimiliki sebelum tanggung jawab pidana muncul;)*

2. This Article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence establish in accordance with Article 2 through 5 of this Convention, sech as for the authorized testing or protection of a computer system; *(2. Pasal ini tidak boleh diinterpretasikan sebagai penetapan kewajiban pidana di mana produksi, penjualan, pengadaan untuk penggunaan, impor, distribusi kepemilikan sebagaimana*

   dimaksud pada ayat (1) pasal ini tidak untuk tujuan melakukan sesuatu kejahatan menurut Pasal 2 dsampai 5 Konvemnsi ini, seperti untuk pengujian resmi atau perlindungan dari sebuah sistem komputer;)

3. Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article; *(3.* Pihak *Negara berhak untuk tidak menerapkan ayat (1) pasal ini, jika memang tidak ada*

hubungannya dengan penjualan, distribusi atau membuat persediaan dan item yang dimaksud di dalam ayat (1) pasal ini poin ii).

f). Pasal 7 tentang Pemalsuan (*Computer-Related Forgery*);

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in authentic data with the intent that it be considered or acted upon for legal purpose as if it were authentic, regardless whether or not the data is directly readable and intelligible; *(Pihak Negara harus menerapkan undang-undang dan mengambil tindakan- tindakan lain yang diperlukan untuk ditetapkan sebagai tindak pidana: jika melakukan secara sengaja dan tanpa hak, memasukkan, merubah, menghapus, atau menahan data komputer, sehingga data menjadi tidak seperti aslinya dengan maksud bahwa hal itu dianggap atau dimaksudkan untuk sebuah tujuan hukum tertentu seolah-olah asli, tanpa mempertimbangkan apakah data itu dapat dibaca dan dapat dimengerti secara langsung;)*
A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches; *(Pihak Negara dapat mensyaratkan kejadian tersebut untuk maksud menipu atau maksud tidak jujur lainnya, sebelum konsekuensi hukum mengikatnya).*

g). Pasal 8 tentang Penipuan (*ComputerRrelated Fraud*);

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to snother person by: (*Pihak Negara harus menerapkan undang-undang dan* mengambil *tindakan-tindakan lain yang diperlukan untuk ditetapkan sebagai tindak pidana: jika melakukan secara sengaja dan tanpa hak, menyebabkab kerugian seseorang yang*

dilakukan dengan cara:)

a. any input alteration, deletion or suppression of computer data; *(memasukkan, penghapusan, mengubah, atau penahanan data komputer:)*

b. any interference with the functioning of a computer system; *(mengganggu sistem komputer);* with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person; *(dengan maksud menipu atau niat tidak jujur dalam hal pengadaan, tanpa hak, untuk keuntungan ekonomi untuk diri sendiri atau orang lain).*

h). Pasal 9 tentang Pornografi Anak *(Offences Related to Child Pornography);*

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct; *(1. Pihak Negara harus menerapkan undang-undang dan mengambil tindakan-tindakan lain yang diperlukan untuk ditetapkan sebagai tindak pidana: jika melakukan secara sengaja dan tanpa hak, tindakan berikut :)*
   a. producing child pornoghrapy for the purpose of its distribution through a computer system; *(memproduksi pornografi anak untuk tujuan distribusi melalui sistem komputer;)*
   b. offering or making available child pornoghrapy throught a computer system; *(menawarkan atau membuat pornografi anak yang tersedia melalui sistem komputer;)*
   c. distributing or transmitting child pornography through a computer system; *(mendistibusikan atau mengirimkan pornografi anak melalui sistem komputer;)*
   d. producing child pornography through a computer system for oneself

or for another person; *(pengadaan pornografi anak melalui sistem komputer untuk diri sendiri atau untuk orang lain;)*

e. possessing child pornography in a computer system or on a computer- data storage medium*; (*memiliki *pornografi anak di sistem komputer atau pada suatu media penyimpanan data komputer.)*

2. For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts; *(2. Untuk tujuan ayat (1) di atas, istilah " pornografi anak " mencakup materi pornografi yang menggambarkan secara visual:)*

a. a minor engaged in sexually explicit conduct; *(a. anak di bawah umur melakukan hubungan seksual secara jelas;)*

b. a person appearing to be a minor engaged in sexually explicit conducr*;(b. seseorang seperti anak di bawah umur yang melakukan hubungan seksual secara amat jelas);*

c. realistic images representing a minor engaged in sexually explicit conduct *;(c. gambar realistis mewakili anak di bawah umur yang melakukan hubungan seksual secara sangat jelas).*

3. For the purpose of paragraph 2 above, the term"minor" shall include all persons under 18 years of age.; *(3. Untuk tujuan ayat (2) di atas, istilah "di bawah umur" harus mencakup semua orang di bawah usia 18 tahun.)* A Party may, however, require a lower age-limit,which shall be not less than 16 years.(*Pihak Negara, bagaimanapun, membutuhkan batas umur yang lebih rendah, yang harus tidak kurang dari 16 tahun.)*

4. Each Party may reserve the right not to apply, in whole or in part paragraph 1, sub-paragraph d, and e and paragraph 2; sub-paragraph b and c (*4. Pihak Negara berhak untuk tidak*

menerapkan, secara keseluruhan atau sebagian, paragraph 1, sub-paragraf d, dan e, dan paragraf 2, sub-paragraf b. dan c.)

i). Pasal 10 tentang Pelanggaran Hak Cipta *(Offences Related to Copyright and Related right);*

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligation it has undertaken unter the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspect of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventiom, where such acts are commited wifully, on a commercial scale and by means of a computer system; *(1. Pihak Negara harus menerapkan undang-undang dan mengambil tindakan-tindakan lain yang diperlukan untuk ditetapkan sebagai tindak pidana pelanggaran hak cipta, sebagaimana didefinisikan dalam hukum Hak Cipta, sesuai dengan kewajiban yang telah dituangkan berdasarkan Undang-Undang Paris 24 Juli 1971 yang merevisi Konvensi Bern tentang perlindungan Karya Seni dan Sastra , perjanjian tentang Perdagangan yang berhubungan dengan Aspek Hak Kekayaan Intelektual dan Traktat Hak Cipta WIPO, dengan pengecualian dari setiap hak moral yang diberikan oleh Konvensi tersebut, di mana tindakan tersebut dilakukan sengaja, pada skala komersial dan melalui suatu sistem komputer.)*
2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined as under the law of that party, pursuant to the obligation it has

undertaken under the international convention for the protection of performers, producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspect of Intellectual Property Rights and the WIPO performances and phonograms treaty, with the exception of any moral rights conferred by such conventions, where such acts are commited willfully, on a commercial scale and by means of a computer system; *(2. Pihak Negara harus menerapkan undang-undang dan mengambil tindakan-tindakan lain yang diperlukan untuk ditetapkan sebagai tindak pidana atas pelanggaran hak-hak istimewa, sebagaimana didefinisikan dalam hukum para pihak, sesuai dengan kewajiban yang telah dilaksanakan di bawah konvensi internasional untuk perlindungan terhadap pelaku pertunjukan, organisasi produser rekaman dan penyiaran (Konvensi Roma), Perjanjian Perdagangan yang berhubungan dengan Aspek Hak Kekayaan Intelektual dan performa WIPO serta traktat rekaman, dengan pengecualian dari setiap hak moral yang diberikan oleh konvensi tersebut, dimana seperti tindakan sengaja berkomitmen, dalam skala komersial dan melalui suatu sistem komputer.)*

3. A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumtances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligation set forth in the international instrument referred to in paragraphs 1 and 2 of this article*; (3.Pihak Negara berhak untuk tidak menerapkan tanggung jawab pidana berdasarkan ayat (1) dan (2) pasal ini dalam keadaan terbatas, asalkan pemulihan yang efektif lain yang tersedia dan reservasi tersebut tidak menyimpang dari kewajiban internasional ditetapkan dalam instrumen internasional sebagaimana dimaksud pada ayat 1 dan 2 pasal ini.)*

j). Pasal 11 tentang Membantu Pemupakatan Jahat *(Attempt and Aiding or Abetting);*

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present convention with intent that such offence be committed.; (*1. Pihak Negara harus menerapkan undang-undang dan mengambil tindakan-tindakan lain yang diperlukan untuk ditetapkan sebagai tindak pidana, jika dilakukan dengan sengaja, membantu atau bersekongkol untuk melakukan tindak pidana seperti tersebut dalam Pasal 2 sampai 10 dari konvensi ini dengan maksud berkomitmen untul melakukan pelanggaran.)*
2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences establish in accordance with articles 3 through 5, 7, 8 and 9.1a and c of this convention*:(2. Pihak Negara harus menerapkan undang-undang dan mengambil tindakan-tindakan lain yang diperlukan untuk ditetapkan sebagai tindak pidana jika dilakukan dengan sengaja, upaya untuk melakukan salah satu tindak pidana yang ditetapkan sesuai dengan Pasal 3 sampai 5,7 ,8 dan 9.1.a dan c. konvensi ini.)*
3. Each Party may reserve the right not to apply, in whole or in part, paraghraph 2 of this article. *(3.Pihak Negara berhak untuk tidak menerapkan, secara keseluruhan atau sebagian, ayat (2) pasal ini.)*

k). Pasal 12 tentang Tanggung Jawab Perusahaan (*Corporate Liability).*

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this convention,

committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on*:*

(1. Pihak Negara harus menerapkan undang-undang dan mengambil tindakan-tindakan lain yang diperlukan untuk memastikan bahwa semua pelaku hukum dapat dimintai pertanggungjawabannya atas tindak pidana yang dilakukan berdasarkan Konvensi ini, yang dilakukan untuk keuntungan pribad seseorang, baik dilakukan secara pribadi atau sebaga pegawai sebuah badan hukum dimana dia bertindak sebagai pimpinan, dengan berdasarkan kepada:)

a. a power of representation of the legal person;
(wewenang mewakili dari badan hukum;)

b. an authority to take decisions on behalf of the legal person; (*kewenangan untuk mewakili badan hukum;)*

c. an authority to exercise control within the legal person.;
(wewenang unuk melakukan kontrol dalam badan hukum.)

2. In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 2 has made possible the commission of a criminal offence established in accordance with this convention for the benefit of that legal person by a natural person acting under its authority: *(2. Selain kasus-kasus yang sudah disebutkan dalam ayat (1) pasal ini, Pihak Negara wajib mengambil langkah-langkah yang diperlukan untuk menjamim bahwa badan hukum dapat dimintai perbertanggungjawaban akibat kurangnya pengawasan atau kontrol sebagaimana dimaksud pada ayat (1) dimungkinkan komisi tindak pidana yang ditetapkan sesuai dengan konvensi ini*

untuk kepentingan hukum bagi yang bertindak tidak di bawah kekuasaannya.)

3. Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative: *(3. Sesuai dengan prinsip-prinsip hukum seseorang atau Pihak Negara, tanggung jawab suatu badan hukum dapat berupa pidana, perdata atau administratif.)*

4. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence; (*4. Tanggung jawab tersebut tanpa mengabaikan tanggung jawab pidana badan hukum yang telah melakukan pelanggaran.)*

Ada 11 (sebelas) pasal yang masuk dalam kategori *cybercrime* dalam Konvensi Dewan Eropa 2001 atau Konvensi Budapest. Bila dilihat dari tindak pidana mayantara yang dilakukan, sudah mengarah pada spesifiksi kejahatan yang memanfaatkan komputer sebagai media penyampaiannya dan melalui jaringan internet yang tersedia. Diperlukan penanganan khusus agar *cybercrime* ini dapat dikriminalisasai, sehingga dapat dipidana, baik penjara maupun denda..

Sementara itu, sanksi atas tindak pidana mayantara *(cybercrime)* dalam Konvensi Budapest hanya memuat satu pasal saja, yakni Pasal 13 tentang Sanksi dan Tindakan *(Sanction and Measures)*, yang bunyinya:

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences establish in accordance with Article 2 trough 11 are punishable by effective, proportionate and dissuasive sanction, which include depriviation of liberty; *(1. Pihak Negara wajib menerapkan undang-undang dan pendekatan-pendekatan lain yang diperlukan untuk memastikan bahwa pelanggaranyang dilakukan berdasrkan Pasal 2 sampai dengan 11 dapat dipidana sanksi yang efektif, proporsional, dan membuat jera, juga mencakup perampasan hak kemerdekaan);*

2. Each Party shall ensure that legal persons held liable in

accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanction. *(2. Pihak Negara harus menjamin bahwa individu-individu yang bertanggung jawab sesuai dengan Pasal 12 dikenakan sanksi pidana atau non-pidana yang*

efektif, proporsional dan bersifat larangan atau tindakan, termasuk sanksi moneter).

Konvensi Budapest cenderung mengetengahkan kriminalisasi terhadap pelaku kejahatan mayantara *(cybercrime)* ketimbang menyediakan hukuman atau sanksi yang berat. Sungguhpun demikian, pendefenisian sanksi dan hukuman akan diterapkan sesuai hukum nasionalnya masing-masing negara. Dengan demikian, bisa jadi hukuman yang diberikan lebih berat dari sanksi yang dicantumkan dalam Konvensi Budapest ini.

E. Dasar Hukum Pemanfaatan Media Internet

Peraturan perundang-undangan tentang pemanfaatan internet di Indonesia telah diatur dalam beberapa perangkat hukum yaitu:

1. Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

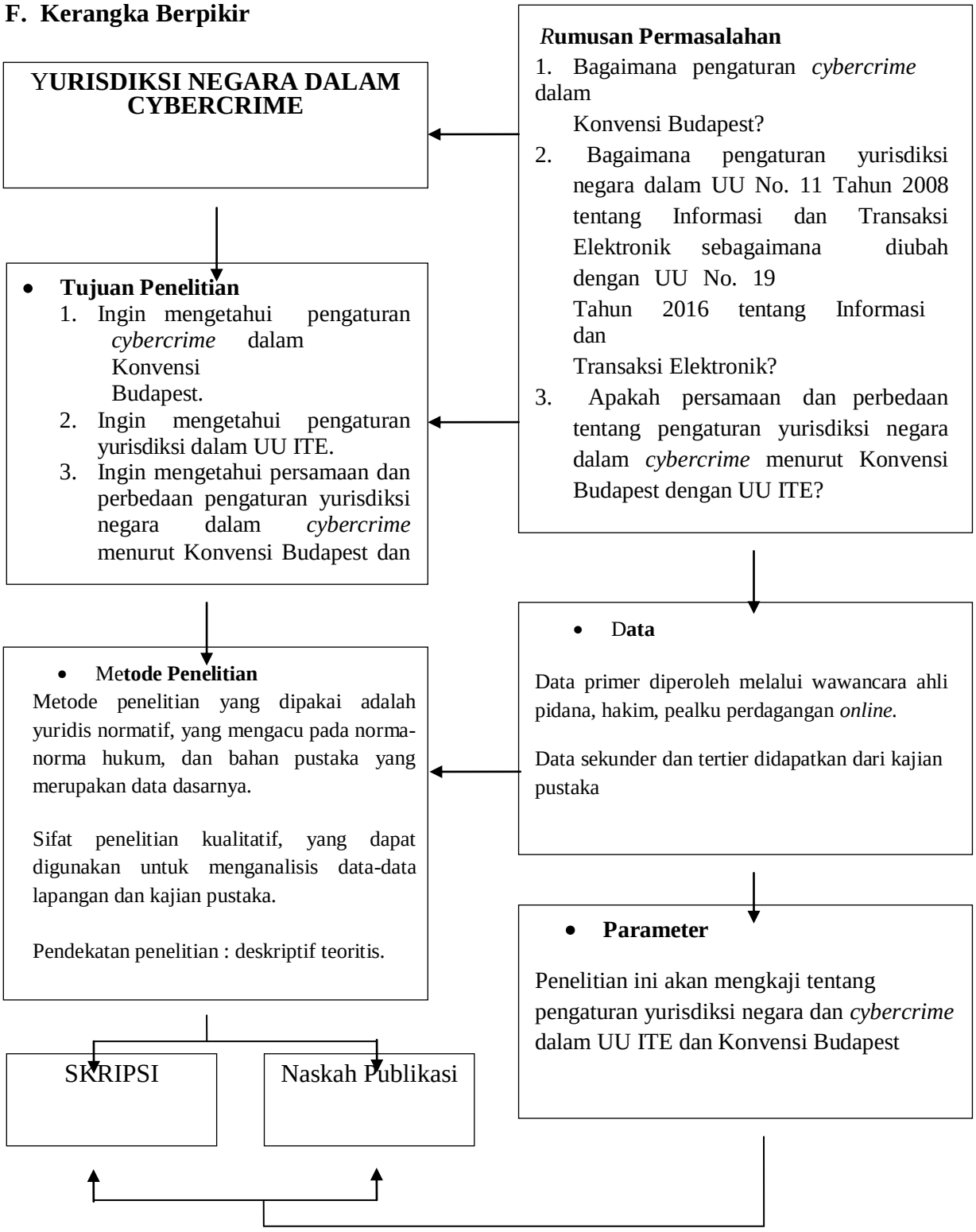
2. Undang-Undang No. 19 Tahun 2016 tentang Perubahan atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

3. Undang-Undang No. 8 Tahun 1999 tentang Perlindungan Konsumen (UUK).

4. Undang-Undang No. 7 Tahun 2014 tentang Perdagangan (UUP),

5. Undang-Undang No. 8 Tahun 1997 tentang Dokumen Perusahaan (UUDP)

F. Kerangka Berpikir



BAB III

METODE PENELITIAN

Menurut Peter Mahmud Marzuki (2005: 35) penelitian hukum merupakan suatu proses untuk menemukan aturan hukum, prinsip–prinsip hukum, maupun doktrin-doktrin hukum guna menjawab isu hukum yang dihadapi. Hal tersebut sesuai dengan karakter perspektif ilmu hukum.

Pada dasarnya, penelitian merupakan suatu upaya pencarian, bukan sekedar mengamati secara teliti terhadap suatu obyek yang mudah terpegang di tangan. Penelitian dalam bahasa Inggrisnya yaitu *research*, yang berasal dari kata "*re*" (kembali) dan "*search*" adalah penelitian. Jadi *research* adalah suatu upaya untuk mencari kembali/meneliti kembali mengenai suatu obyek (Bambang Sunggono, 2003: 27).

Metode penelitian ini digunakan untuk memberikan gambaran bahwa penelitian yang dilakukan berdasarkan suatu kerangka berpikir yang logis dengan mengetengahkan teori, metode serta pendekatan yang berkembang dalam ilmu hukum secara doktrinal (ajaran-ajaran ilmu pengetahuan). Metode penelitian ini juga diharapkan dapat menjadi rujukan dasar-dasar pembuatan usulan penelitian, dasar-dasar teknik pengumpulan data, teknik analisis data dan penyusunan laporan akhir. Untuk memperoleh hasil penelitian yang dapat dipertanggung jawabkan kebenarannya, maka perlu didukung suatu metodologi yang baik. Dengan demikian, dapat dikatakan bahwa metodologi merupakan suatu unsur mutlak

dalam suatu penelitian. Oleh karena itu, dalam penelitian ini penulis menggunakan prosedur atau tata cara penelitian sebagai berikut:

2.1. Jenis Penelitian

Penelitian ini adalah penelitian yuridis normatif, yakni suatu metode penelitian yang meneliti sistematika hukum, asal hukum, dan bahan pustaka yang merupakan data sekunder dan disebut juga penelitian kepustakaan (Soerjono Soekanto, 2005: 264).

Penelitian yang dilakukan untuk pembuatan skripsi ini adalah penelitian hukum normatif, dititikberatkan pada asas-asas hukum (asas-asas tanggung jawab hukum), norma-norma hukum, yang berkaitan dengan konsep yurisdiksi negara, hukum pidana, dan tentang kewenangan dalam menjalankan yurisdiksi negara tersebut terhadap pelaku tindak pidana mayantara *(cybercrime).*

2.2. Metode Pendekatan

Peter Mahmud Marzuki (2005: 141) menyebutkan bahwa metode penelitian yuridis normatif pada umumnya dilakukan pada lima jenis pendekatan hukum, yakni pendekatan undang-undang (*statute approach*), pendekatan kasus (*case approach*), pendekatan historis (*historical approach*), pendekatan komparatif (*comparative approach*), dan pendekatan konseptual (*conceptual approach).* Dalam penelitian skripsi ini, penulis menggunakan pendekatan undang-undang (*statute approach*), karena penelitiannya berdasarkan telaahan undang-undang, yakni UU ITE dan Konvensi Budapest untuk menentukan kewenangan suatu negara dalam menangani kasus kejahatan mayantara *(cybercrime*) berdasarkan yurisdiksi negaranya masing-masing. Hal ini juga

berarti, dalam pendekatan undang-undang ini, baik UU ITE maupun Konvensi Budapest, dikaji secara cermat dan mendalam untuk mengetahui kebenaran dari isu hukum yang sedang dipermasalahkan, sehingga didapatkan kebenarannya.

2.3. Spesifikasi Penelitian

Untuk meneliti pokok permasalahan serta memahami kebenaran obyektif dan dapat dipertanggungjawabkan, maka dipakai spesifikasi penelitian bersifat terapan. Menurut Kun Maryati (1989: 103), penelitian terapan adalah salah satu jenis penelitian yang bertujuan untuk memberikan solusi atas permasalahan tertentu secara praktis. Penelitian ini tidak berfokus pada pengembangan sebuah ide, teori, atau gagasan, tetapi lebih berfokus kepada penerapan penelitian tersebut dalam kehidupan sehari-hari. Ciri utama dari penelitian ini adalah tingkat abstraksi yang rendah, dan manfaat atau dampaknya dapat dirasakan secara langsung.

Menurut Fristina Irina (2017: 4-5), penelitian penerapan (*applied research*) adalah penelitian untuk alasan praktis, yakni pengembangan ilmu pengetahuan berkaitan dengan kenyataan-kenyataan di lapangan, sehingga dapat diterapkan dalam kehidupan nyata. Penelitian terapan dilakukan berkenaan dengan kenyataan-kenyataan praktis, penerapan, dan pengembangan ilmu pengetahuan yang dihasilkan oleh penelitian dasar dalam kehidupan nyata. Penelitian terapan berfungsi untuk mencari solusi tentang masalah-masalah tertentu. Tujuan utamanya adalah pemecahan masalah sehingga hasil penelitian dapat dimanfaatkan untuk kepentingan manusia baik secara individu atau

kelompok maupun keperluan industri atau politik dan bukan untuk wawasasan keimuan semata.

Penelitian terapan dilakukan untuk mencari pemecahan masalah-masalah nyata (riil) dalam kehidupan secara ilmiah. Hasil penelitian untuk onjektif mengenai latar belakang dan sebab-sebab suatu masalah merupakan petunjuk yang dapat dipergunakan dalam menyusun implementasi dan alternatif saran-saran tindakan dalam menyelesaikan permasalahan tersebut (Hadari Nawawi dan Mimin Martani, 2005: 5-6).

Spesifikasi penelitian ini bersifat terapan dengan maksud dapat memberikan solusi dan manfaat secara langsung atas kajian tentang kewenangan suatu negara dalam menentukan yurisdiksi negaranya terhadap kejahatan mayantara (*cybercrime*) yang dilakukan, baik di dalam batas teritorian negaranya maupun di luar batas territorial negara lain. Kewenangan untuk melaksanakan pemeriksaan terhadap pelaku tindak pidana mayantara yang dilakukan lintas negara ini dapat diperjelas dengan menggunakan metode penelitian terapan ini.

2.4. Bahan Penelitian

Menurut Soerjono Soekanto dan Sri Mamuji (2001: 24), pada penelitian hukum normatif, bahan pustaka merupakan data dasar yang dalam penelitian hukum digolongkan sebagai data sekunder.

Penelitian ini juga disebut sebagai penelitian deskriptif karena bertujuan untuk mendeskripsikan mengenai upaya penegakan hukum di dalam wilayah Negara Kesatuan Republik Indonesia (NKRI), kewenangan untuk melakukan tindakan hukum terhadap pelaku kejahatan mayantara yang dilakukan di dalam

yurisdiksi negara Indonesia. Dari deskripsi ini diharapkan dapat diperoleh suatu formulasi yang tepat dalam menerapkan hukum maupun upaya melakukan penegakan hukum yang sesuai dengan kaidah maupun norma hukum yang berlaku.

Adapun bahan hukum yang dipergunakan dalam penelitian ini adalah berasal dari bahan hukum primer dan bahan hukum sekunder. Jika dibutuhkan juga akan mempergunakan bahan non hukum.

1. Bahan Hukum Primer

   Yaitu bahan hukum yang bersifat autoritatif artinya memilki otoritas. Bahan hukum primer terdiri dari perundang-undangan, catatan-catatan resmi atau risalah dalam pembuatan perundang-undangan yang disesuaikan dengan pokok permasalahan yang dikaji. Bahan hukum primer meliputi:

   a. UU No. 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
   b. Konvensi Budapest.

2. Bahan Hukum Sekunder

   Bahan Hukum sekunder adalah bahan yang diperoleh dari berbagai bahan kepustakaan dengan cara mempelajari buku-buku atau literatur dan peraturan perundang-undangan yang terkait dengan penelitian. Bahan hukum sekunder meliputi: makalah, buku – buku, koran, internet, dan publikasi lainnya.

3. Bahan Non Hukum

Bahan Non Hukum yaitu bahan yang memberikan pentunjuk maupun penjelasan terhadap bahan hukum primer dan sekunder, meliputi:

a. Kamus Hukum.
b. Kamus Bahasa Indonesia (KBBI).
c. *Black's Law Dictionary.*

2.5. Tahapan Penelitian

Untuk mendapatkan hasil penelitian yang baik, maka perlu dilakukan persiapan yang matang. Oleh karena itu, penulis membuat perencanaan penelitian ini lewat beberapa tahapan, yaitu:

a. Tahap Pendahuluan

   Tahap ini, peneliti melaksanakan pengajuan usulan mengenai penelitian yang akan dilaksanakan dengan menyusun suatu proposal yang mengidentifikasi fakta hukum dan mengeliminir hal-hal yang tidak relevan untuk menetapkan isu hukum yang hendak dipecahkan.

b. Tahap Pelaksanaan

   Pada tahap ini peneliti melakukan pengumpulan bahan-bahan hukum dan sekiranya memiliki relevansi yang peneliti akan coba dapatkan dari interview/wawancara dan melakukan observasi lapangan tentang tindak pidana mayantara (*cybercrime)* ini serta berusaha mencari tahu lebih jauh lagi tentang kewenangan negara untuk mengadili atau menghukum pelaku tindak pidana mayantara ini melalui kajian pustaka yang terdapat di Perpustakaan Universitas Muhammadiyah Magelang, Perpustakaan Daerah maupun toko-toko buku yang memiliki bahan-bahan hukum yang dicari.

c. Tahap Akhir

Pada tahap ini peneliti melakukan telaah atas isu hukum dan memberikan preskripsi berdasarkan argumentasi yang telah dibangun dalam kesimpulan

2.6. Fokus Penelitian

Penelitian ini difokuskan pada penjabaran Konvensi Budapest dan UU No. 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Kedua regulasi tersebut memiliki kesamaan dalam hal mengulas tentang yurisdiksi negara, sehingga dibutuhkan suatu pemahaman tentang batas teritorial masing-masing negara ketika terjadi kejahatan mayantara (*cybercrime*). Hal ini perlu dikaji agar ada persamaan persepsi tentang negara-negara mana saja yang berwenang dan melaksanakan kewenangan tersebut untuk memeriksa tersangka *cybercrime.*

2.7. Lokasi Penelitian

Penelitian ini sebahagian besar mengacu pada bahan pustaka, sehingga penelitian ini lebih banyak berada di dalam Perpustakaan Universitas Muhammadiyah Magelang.

2.8. Metode Analisis Data

Gambaran umum mengenai data yang sudah terkumpul dari objek penelitian akan dianalisi menggunakan metode kuantitatif. Menurut Burhan Ashsopa (2000: 58), metode kuantitatif ini digunakan karena tipe penelitian ini adalah sebuah penelitian yang dikategorikan sebagai penelitian hukum normatif, yang pendekatannya deskriptif teoritis. Setelah data yang diperoleh dari lapangan dikategorisasi menjadi masalah atau temuan, dengan menggunakan pola pikir

yang kontekstual, kemudian ditelaah dan dibahas sesuai dengan urutan yang telah ditentukan.

Menurut Soerjono Soekanto (1986: 229), setelah semua data terkumpul baik data primer maupun data sekunder atau data lapangan, data tersebut akan dianalisa secara kualitatif, yaitu dengan cara menjabarkan data-data yang diperoleh kemudian mencari korelasinya dengan literatur yang digunakan sebagai landasan dalam penulisan

Penelitian ini menggunakan metode analisis induktif, yakni metode analisa data yang berangkat dari faktor-faktor yang bersifat khusus untuk ditarik kesimpulann yang bersifat umum. Metode induktif ini digunakan untuk mengungkap fakta-fakta atau fenomena-fenomena dari lapangan, kemudian menganalisisnya hingga menemukan solusinya. Proses berpikir induktif dimulai dari data yang terkumpul, kemudian disimpulkan.

Metode induktif dimulai dari fakta-fakta yang ada di lapangan lalu dikaji dan diruimuskan hingga sampai pada suatu kesimpulan. Metode induktif ini lebih banyak mengungkapkan fakta-fakta yang ada dan kompleks sehingga dalam mengkaji dan merumuskan suatu penelitian akan menghasilkan kesimpulan yang mendekati kebenaran (Hadari Nawawi dan Mimin Martani, 2005: 11-12).

Setelah semua data terkumpul baik data primer maupun data sekunder, data tersebut dianalisa secara kuantitatif dengan pendekatan indukttif, yaitu prosedur yang berpangkal pada suatu peristiwa umum yang kebenarannya telah diketahui atau diyakini dan berakhir pada suatu kesimpulan atau pengetahuan baru yang bersifat lebih khusus. Metode ini diawali dari pembentukan teori, hipotesis,

definisi operasional, instrumen dan operasionalisasi. Dengan kata lain, untuk memahami suatu gejala terlebih dahulu harus memiliki konsep dan teori tentang gejala tersebut dan selanjutnya dilakukan penelitian lapangan (Sugiyono, 2012: 335). Jadi, analisis data pada penelitian kuantitatif ini bersifat induktif, yakni suatu analisis berdasarkan data yang diperoleh baik data pustaka maupun data observasi.

BAB V
P E N U T U P

A. Kesimpulan

1. Dalam Konvensi Budapest atau Konvensi Dewan Eropa 2001, kejahatan mayantara *(cybercrime)* umumnya berkaitan dengan teknologi tingkat tinggi *(high technology*), baik menyangkut perangkat, jaringan maupun sistem yang mengendalikannya. Oleh karena itu, berkaitan dengan tindak pidana yang dilakukan oleh pelaku kejahatan, umumnya juga menggunakan sarana teknologi untuk menjalankan aksinya, dan komputer sebagai sarana kejahatan yang dilakukannya. Sehubungan dengan hal tersebut, maka untuk mengatur kejahatan mayantara ini, komputer merupakan salah satu perangkat yang harus masuk dalam pengaturan kejahatan mayantara ini. Dan berdasarkan kesepakatan Konvensi Budapest, maka pengaturan *cybercrime* dibuat menjadi 9 (sembilan) kategori perbuatan yang pelanggaran atapun yang dilarang dilakukan dengan sengaja atau tanpa hak, yaitu:

    a. Tindak pidana terhadap kerahasiaan *(confidentiality*), integritas *(integrity*), dan ketersediaan *(availability*) data dan sistem komputer, yang terdiri dari: *illegal acces* (Pasal 2), *illegal intercepcion* (Pasal 3), *data interference* (Pasal 4), *system interference* (Pasal 5), dan *misuse of device* (Pasal 6).

b. Tindak pidana yang berkaitan dengan komputer, terdiri dari *computer related forgery* (Pasal 7) dan *computer related fraud* (Pasal 8).

c. Tindak Pidana yang berkaitan dengan pornografi anak, yaitu *offences related to child pornography* (Pasal 9).

d. Tindak pidana yang berkaitan dengan pelanggaran hak cipta dan hak- hak terkait atau *offence to infringerments of copyright and related right* (Pasal 10). Dalam UU No. 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) pada Pasal 2 menyebutkan bahwa yurisdiksi menyangkut setiap orang yang melakukan perbuatan huku m sebagaimana yang diatur UU ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/ atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia.

2. Pengaturan yurisdiksi kriminal dalam Pasal 2 UU ITE relatif singkat dan padat, sehingga dalam implementasinya diperlukan penafsiran-penafsiran dan pengembangan terhadap prinsip-prinsip yurisdiksi dalam hukum internasional. Berdasarkan ketentuan Pasal 2 UU ITE prinsip yurisdiksi yang menjadi dasar berlakunya hukum pidana terhadap tindak pidana mayantara adalah:

a. Prinsip Teritorial

Prinsip territorial dalam Pasal 2 UU ITE terkandung dalam rumusan "yang berada di wilayah hukum Indonesia." Dalam rumusan selanjutnya juga ditegaskan prinsip teritorial objektif, yaitu dalam rumusan "di luar wilayah hukum Indonesia." Di lain pihak dalam ketentuan ini tidak ada penegasan berlakunya prinsip teritorial subjektif, yang sangat penting dalam pemberantasan tindak pidana mayantara yang seringkali perbuatannya dimulai di suatu wilayah negara dan penyelesaiannya atau efeknya ada di wilayah negara lain. Sungguhpun demikian, prinsip teritorial subjektif dapat digunakan dengan melakukan penafsiran

b. Prinsip Perlindungan

Prinsip perlindungan dalam Pasal 2 UU ITE terkandung dalam rumusan "di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia." Prinsip perlindungan dalam ketentuan ini lebih luas dari yurisdiksi perlindungan dalam KUHPidana dan prinsip perlindungan pada umumnya, yaitu untuk melindungi kepentingan vital suatu negara.

3. Persamaan dan perbedaan tentang pengaturan yurisdiksi dalam Konvensi Budapest dan UU ITE adalah sebagai berikut:

Yurisdiksi menurut Konvensi Budapest, menganut prinsip:

a. Prinsip Teritorial

b. Prinsip Nasional

c. Prinsip Bendera Kapal

d. Prinsip Pesawat Terdaftar

Sedangkan Yurisdiksi menurut UU ITE, memuat:

a. Prinsip Teritorial, dan

b. Prinsip Perlindungan.

1. Persamaan antara UU ITE dan Konvensi Budapest dalam menentukan batasan yurisdiksi adalah Prinsip Teritorial.
2. Perbedaannya, dalam UU ITE diterapkan Prinsip Perlindungan, sementara dalam Konvensi Budapaest tidak ada Prinsip Perlindungan, tetapi Prinsip Nasional.
3. Perbedaan lainnya, UU ITE tidak memuat Prinsip Bendera Kapal dan Prinsip Pesawat Terdaftar.

B. Saran

1. Sebaiknya Indonesia membuat definisi yang lebih terperinci lagi tentang kajahatan mayantara *(cybercrime)*, mengingat masih banyak kejahatan mayantara yang harus dimasukkan dalam tindak pidana mayantara, seperti perbudakan *(slavery)*, penjualan manusia (*human trafficking*), dengan menggunakan sarana internet yang belum termasuk dalam UU ITE,Karna dalam perkembanagannya kejahatan yang sangat masih serti di era globalisasi seperti sekarang ini

kerugian yang di dapat tidaklah hanya kerugian yangbersifat materiil saja melainkan kerugian yang juga berupa imateriil yang berdapak pada sisi sikologi pada korban kejahatan tsb .Dimana undang undang yang jelas dan memberi effek jera kepada pelaku tidan kejahatan tsb. Pada juridiksi inilaah masalah intergritas penegakan hokum suatu Negara dipertaruhkan.Didalam yuridiksi neagara harus juga diatur batasan_batasan Negara dalam menegakkan supremasi hukumnya .Dimana uu ite di Indonesia mengadopsi elemen elemen dari konvensi Budapest.

2. Yurisdiksi negara menjadi penting, ketika ada warga negara yang mengalami kasus hukum karena ketidaktahuannya mengakses, menghapus, memasukkan, menyimpan data komputer orang lain dari negara lain, sehingga harus berurusan dengan hukum, sehingga perlu sosialisasi tentang permasalahan ini. Dimana penegakan hukumnya juga harus selaras dengan maksud memberi pemahaman tentang persatuan dan kesatuan kita sebagai sebuah rebublik yang berdaulat secara hokum. Karna pada UU ITE mencakup pinsip teritori dan juga perlindungan,saya mengartikan bahwa kita Hrus menindak tegas siapapunn yang melakukan kejahatan diwilayah hokum Indonesia.

   Dalam prinsip perlindungan kita juga harus tegas menjaga warga Negara kita yang melanggar hokum di luar yuridiksi kita dengan tujuan menjaga harkat dan martabat bangsa. Sebagai pelaksnaan

atas UUD1945.

3. Indonesia harus memiliki UU ITE yang lengkap sesuai standar Hukum Internasional, jangan hanya mengadopsi Kovensi Budapest,sebagai acuan atas kejahatan mayantara yang ada di Indonesia. UU ITE Menjadi hal yang spesifik dari konvensi Budapest itu sendiri memuat banyak hal yang memberikan segala aturan hukum tentang kejahatan cybercrme di indoesia akan tetapi masih saja UU ite menjadi hal yang sulit ditegakkan karna aparat penegak hukum di ndonesia memang masih memandang tindak kejahatan yang ter katagori berat ini sulit di selesaikan. Maka harus ada peran pemerintah ang kuat di sini.

DAFTAR PUSTAKA

A. BUKU.

Adam Chazawi.2003.*Pelajaran Hukum Pidana* l.jakarta ; RajawaliGrafindo Persada.

Arsayad Sanusi. 2010 ‘’Efektifvitas UU ITE Dalam Pengaturan Perdagangan.

Elektronik *(E-commerce)’’ dalam jurnal Bisnis* vol.29,No.1.

Barda Nawawi Arief.2005.*Bunga Rampai kebijakan Hukum Pidana*.Bandung: citra Bakti.

Burhan Ashopa 2000.*Metode penelitian Hukum*.Jakarta;Rieneka Cipta.

CFG. Sunaryati Hartono 1994.*Penelitian Hukum Indonesia*.Bandung. Alumni.

Edmon Makarim.2003.*Kompilasi Hukum Telematika*.Jakarta.RajaGrafindo persada.

Efa Laila Fakhriah.*Bukti Elektronik Dalam Sistem Pembuktian Perdata*.

Bandung;Refika Aditama.

Hikmanto juwana .2006.*Yuridiksi Negara;Hukum Internasional*.jakarta;UI Press.

Hilman Haidikusuma.1995.*Metode Pembuatan Kertas Kerja atau skripsi Ilmu Hukum*.Bandung;Mandar Maju.

Hilman Hadikusuma .2013.*Bahasa Hukum Indonesia.*Bandung Alumni.

Maskun.2013.Kejahatan Siber (Cybercrime);Suatu Pengantar;Jakarta;Kencana Prenada Media.

Maskun dan Wiwik Meilarati.2016.*Hukum Internet.Aspek Penipuan Berbasis Internet*.Bandung; Keni Media.

Muladi dan Barda Nawawi Arief.1992.*Bunga Rampai Hukum Pidana*.Bandung;

Alumni.

Moeljanto.1983.*Aza- azas Hukum Pidana*.Jakarta;Bina Aksara.

Onno W Purbo dan Aang Arif Wahyudi.2001.Mengenal e-Commerce.Jakarta;Elex

Media.

Peter Mahmud Marzuki.Penelitian Hukum.Jakarta;Kencana.

Sigid Suseno.2012.Yuridiksi Tindak Pidana Siber.Bandung;Refika Aditama.

Siswanto Sumarno.2009.Hukum Informasi dan Transaksi Elektronik(Studi Kasus; Prita Mulyasari)jakata.Rineka Cipta.

Soerjono Soekamto dan Sri Mamuji.2001.Penelitian Hukum Normatif.Jakarta; Radjawal Pers.

Wiryono Prodjodikoro.1981.Azas_azas Hukum Pidana di Indonesia.Bandung; Penerbit Eresco.

B. PERATURAN PERUNDANG –UNDANGAN.

Kitab Undang Undang Hukum Pidana (KUHP)

UU No.19 tahun 2016tentang Perubahan Atas UU No, 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

UU No. 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik.

UU No.8 Tahun 1997 Tentang dokumen Perusahaan.

PP No.82 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

PPres No.74 Tahun 2017 tentang Peta Jalan system Perdgangan Nasional Berbasis Elektronik.

Konvensi Budapest atau Konvensi Dewan Eropa 2001.

C. Internet

www.Wikipedia.com

www.artikelsiana.com