ISSN 2656-4041 (Media Online)

KRIMINOLOGY PADA BIDANG KEBIJAKAN "CYBER SECURTY"

Oleh :

Nurlely Darwis
Dosen Tetap Fakultas Hukum Universitas Dirgantara Marsekal Suryadarma Jakarta.
Email : (nurlely.darwis@gmail.com)

Abstrak :

Di era digital saat ini, praktik penipuan melalui layanan pesan singkat (SMS) palsu dan media sosial makin hari makin mencemaskan. Tindak kejahatan yang berkembang di masyarakat tidak lagi hanya kejahatan konvensional, tetapi juga kejahatan yang mendayagunakan teknologi informasi dan internet. Menurut Kepala Bidang Hubungan Masyarakat Polda Metro Jaya, tindak kejahatan cyber yang paling banyak dilaporkan masyarakat selama tiga tahun terakhir adalah penipuan lewat surat elektronik, pesan pendek, dan situs internet. Sedangkan pada urutan kedua adalah pencemaran nama baik melalui internet. Untuk mengantisipasi perkembangan kejahatan dunia maya ini ternyata belum di dukung oleh peraturan undang-undang yang memadai. Wakil Kepala Kepolisian RI Komisaris Jenderal Syafruddin mengatakan, bahwa Indonesia masuk dalam jajaran dua besar negara di dunia dengan kejahatan di dunia maya atau cyber-crime, tertinggi ke dua di dunia setelah Jepang, dengan total serangan cyber ini ada 90 juta. Menurut Identity Theft Resource Center (ITRC) sampai bulan Juli 2018 diketahui bahwa telah terjadi 668 kasus kejahatan cyber dengan total data hilang mencapai 22.408.258 sehingga perlu menginkripsi data. Metode penelitian yang penulis gunakan adalah "Penelitian hukum Normatif dengan studi dokumentasi di perpustakaan, hal ini menjadi penting karena seorang ahli digital forensik berperan langsung dengan barang bukti baik dari TKP saat penyidikan hingga laboratorium. Analisis data dilakukan secara kualitatif, Dan hasil penelitian ini melihat penerapan Undang-Undang ITE pada permasalahan Cyber-Crime, berikut kendala penerapan Undang-Undang ITE pada permasalahan Cyber-Crime, melalui peran dan kedudukan ahli digital forensik berkaitan dengan alat bukti digital sebagai alat bukti yang sah pada perkara cyber-crime sebagaimana diatur pada Pasal 184 ayat (1) KUHAP.

Kata kunci : Cyber-Crime; Cyber-Law; Peran Digital Forensik

A. PENDAHULUAN

Tentang Internet pada awalmula adalah suatu jaringan komunikasi digital yang sampai saat ini telah menghubungkan hampir seluruh dunia melalui jaringan, oleh karenanya terasa tidak ada jarak antara satu negara dengan negara lainnya. Internet yang dikenal masyarakat sekarang ini pada dasarnya berasal dari suatu jaringan (*Network*) yang diciptakan oleh Departemen Pertahanan Amerika Serikat pada awal tahun 1970-an. Network ini dinamakan *ARPAnet*, dibangun oleh *Advanced Research Projects Agency (ARPA)* dengan tujuan untuk menghubungkan berbagai lokasi militer dan lokasi riset, disamping juga merupakan proyek riset tersendiri yang bertujuan untuk

membangun sistem jaringan yang handal.[1]

Pada akhir tahun 1980-an, *National Science Foundation (NSF)*, yaitu Lembaga yang didirikan di Amerika Serikat, secara bertahap mulai mengembangkan jaringannya sendiri yang dinamakan *NSFnet* dengan menggunakan teknologi yang dikembangkan oleh ARPAnet, dan juga mengembangkan *High-speed backbone network* yang semula digunakan untuk memungkinkan kampus-kampus dan lembaga-lembaga riset untuk menggunakan network tersebut, dan penggunaan ini kemudian meningkat dengan diperkenalkannya E-Mail dan juga pengiriman data dan informasi antar lokasi. Dengan perkembangan ini muncul apa yang dikenal sekarang dengan "*Internet*".

Perkembangan teknologi informasi, internet, dan jejaring komputer telah membuat masyarakat bisa menciptakan ruang sosial baru di mana mereka satu dengan yang lain dapat bertemu dan saling berinteraksi satu sama lain didunia maya. Interaksi ini melintasi batas dan melampaui ruang serta waktu.

Di era digital saat ini, praktik penipuan melalui layanan pesan singkat (SMS) palsu dan media sosial makin hari makin mencemaskan, tindak kejahatan yang berkembang di masyarakat tidak lagi hanya kejahatan konvensional, seperti pencurian, perampokan, dan lain-lain, tetapi juga kejahatan yang mendayagunakan teknologi informasi dan internet. Menurut Kepala Bidang Hubungan Masyarakat Polda Metro Jaya, tindak kejahatan *cyber* yang paling banyak dilaporkan masyarakat selama tiga tahun terakhir adalah penipuan lewat surat elektronik, pesan pendek, dan situs internet. Sedangkan pada urutan kedua adalah pencemaran nama baik melalui internet. Di Jakarta, misalnya, jumlah kasus kejahatan di dunia maya ("*Cyber Crime*") yang ditangani Kepolisian Daerah Metro Jakarta Raya meningkat pesat. Jika pada tahun 2013 jumlah kejahatan yang dilaporkan hanya 541 kasus, dan pada tahun 2014 tercatat ada 785 laporan, maka hingga Agustus 2015 tercatat sudah ada 690 kasus.[2]

Tahun 2017, Polisi telah tangani 1.763 kasus kejahatan cyber,[3] yang dimaksud di antaranya penipuan lelang secara online, pemalsuan cek, penipuan kartu kredit atau *carding*, *confidence fraud* (penipuan kepercayaan), penipuan identitas, dan pornografi anak, dengan rincian antara lain, Polda Sumatera Utara (Sumut) menangani 95 kejahatan; Polda Sumatera Barat (Sumbar) menangani 125 kasus dengan penyelesaian 15 kasus. Polda Sumatera Selatan (Sumsel) menangani 21 kasus kejahatan cyber dan telah menyelesaikan 2 kasus; Polda Kepulauan Riau (Kepri) menangani 40 kasus; Polda Lampung menangani 28 kasus.

Wakil Kepala Kepolisian RI Komisaris Jenderal Syafruddin

[1] Asril Sitompul, *Hukum Internet Pengenalan Mengenai Masalah Hukum di Cyberspace*, Ctk Pertama, Citra Aditya Bhakti, Bandung, 2001

[2] https://geotimes.co.id/kolom/ancaman-kejahatan-di-era-digital/ diakses pada 9 Desember 2018 pukul 10.53 WIB.

[3] https://news.okezone.com/read/2017/12/21/337/1833784/tahun-2017-polisi-tangani-1-763-kasus-kejahatan-siber; diakses pada 15 Januari 2019

mengatakan, bahwa Indonesia masuk dalam jajaran dua besar negara di dunia dengan kejahatan di dunia maya atau cyber-crime,[4] tertinggi ke dua di dunia setelah Jepang, dengan total serangan cyber ini ada 90 juta. Hingga Juli 2018 sudah ada 668 kasus kejahatan cyber. Menurut *Identity Theft Resource Center* (*ITRC*) sampai bulan Juli 2018 diketahui bahwa telah terjadi 668 kasus kejahatan cyber dengan total data hilang mencapai 22.408.258 sehingga perlu menginkripsi data.[5]

B. Identifikasi Masalah

Berdasarkan latar belakang masalah yang telah diuraikan, dalam hal ini dapat dikemukakan beberapa masalah yang dapat diidentifikasi yaitu:

1. Sejalan dengan perkembangan masyarakat dibidang tehnologi ternyata berkembang juga bentuk kejahatan dunia maya (*Cyber-Crime*)
2. Fakta di masyarakat memperlihatkan bahwa belum sepenuhnya peraturan dapat mengatasi bentuk-bentuk kajahatan dunia maya yang terjadi.
3. Banyak masyarakat menjadi korban dari bentuk kejahatan dunia maya ini karena tidak mengerti permasalahan yang sesungguhnya berkaitan dengan teknologi.

C. Perumusan Masalah

1. Bagaimana penerapan Undang-Undang ITE pada permasalahan Cyber-Crime;
2. Apa kendala penerapan Undang-Undang ITE pada permasalahan Cyber-Crime;

D. Tujuan dan Manfaat Penelitian

Tujuan dilakukan kegiatan penelitian ini adalah untuk menjawab pertanyaan penelitian:

1. Mengetahui penerapan Undang-Undang ITE pada permasalahan Cyber-Crime;
2. Mengidentifikasi dan menganalisis kendala penerapan Undang-Undang ITE pada permasalahan Cyber-Crime.

Bahwa manfaat dari penelitian ini dapat dijadikan sebagai kemanfaatan secara akademis, dan praktis. Selanjutnya adalah untuk menambah literatur dan memperkaya ilmu pengetahuan di bidang Kriminologi.

E. Kerangka berfikir

1. Era globalisasi ternyata telah mempengaruhi kehidupan hampir seluruh lapisan kehidupan masyarakat, mulai dari lapisan masyarakat paling elit sampai pada lapisan masyarakat umum paling bawah;
2. Sejalan dengan perkembangan masyarakat, maka kebutuhan masyarakat juga mengalami peningkatan yang tentunya didukung oleh kekuatan tehnologi informasi yang diperlukan;
3. Bahwa fakta di masyarakat memperlihatkan telah terjadi bentuk-bentuk kejahatan di

[4] https://www.cnnindonesia.com/nasional/20180717140856-12-314780/polri-indonesia-tertinggi-kedua-kejahatan-siber-di-dunia; diakses pada 1 Februari 2019

[5] https://news.okezone.com/read/2018/08/12/337/1935417/hingga-juli-2018-sudah-ada-668-kasus-kejahatan-siber; diakses pada 1 Februari 2019

masyarakat juga didukung oleh tehnologi informasi yang pada akhirnya dikenal dengan bentuk kejahatan dunia maya (*Cyber-Crime*).

4. Bentuk Kejahatan Cyber di masyarakat ternyata sangat bervariatif, sedangkan untuk mengatasi bentuk kejahatan ini perangkat undang-undang yang ada belum sepenuhnya memadai, utamanya dalam hal pembuktian untuk mendukung proses acara formal dalam berperkara.

F. Metode Penelitian

1. Jenis Penelitian

Secara khusus menurut jenis, sifat dan tujuan suatu penelian hukum dibedakan menjadi 2 (dua) yaitu penelitian hukum Normatif dan penelitian hukum Empiris.[6] Maka dalam penelitian ini penulis menggunakan:

a. Penelitian hukum Normatif, disebut juga penelitian perpustakaan (studi dokumentasi), karena penelitian ini dilakukan atau ditujukan hanya pada peraturan - peraturan yang tertulis atau bahan-bahan hukum yang lain. Dan juga dikatakan sebagai penelitian kepustakaan karena penelitian banyak dilakukan terhadap data yang bersifat sekunder yang ada di perpustakaan.
b. Penelitian hukum Empiris, merupakan istilah lain yang digunakan dalam penelitian hukum sosiologis, dan dapat disebut juga dengan penelitian lapangan, karena didasarkan atas data primer yaitu data yang didapat secara langsung dari masyarakat sebagai sumber data utama, dalam hal ini keterangan ahli adalah merupakan peran sangat penting dalam proses pembuktian perkara pidana cyber-crime, karena seorang ahli digital forensik ini yang langsung berhubungan dengan barang bukti baik dari TKP saat penyidikan hingga laboratorium. Bahwa data primer ini adalah data yang nantinya akan menjadi pendukung data sekunder yang diperoleh melalui kepustakaan. Namun, kemudian muncul beberapa kendala seperti persoalan alat bukti yang sifatnya elektronik identik dengan situasi dunia maya sehingga sangat rentan untuk penyimpanannya dan pendataannya di kepustakaan.

2. Sumber Data

Dalam penelitian hukum normatif, data yang digunakan berupa data sekunder, yang bersumber dari kepustakaan, terdiri dari:

a. Undangan Undang-Undang Dasar 1945
b. Kitab Undang-Undang Hukum Pidana (KUHP)
c. Kitab Undang-Undang Hukum Acara Pidana (KUHAP)
d. Undang-Undang Nomor 48 Tahun 2009 Tentang Kekuasaan Kehakiman
e. Undang-Undang Nomor 11 Tahun 2008 Tentang

[6] Suratman; H. Philips Dilla; *Metode Penelitian Hukum;* Alfabeta Bandung; 2014, hlm. 51.

Informasi dan Transaksi Elektronik sebagaimana yang telah diubah oleh Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;

f. PP No. 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik;
g. Permenkominfo No. 36 Tahun 2016 tentang Tata Cara Pendaftaran Penyelenggara Sistem Elektronik (seperti dalam hal pelayanan publik harus ada kewajiban registrasi, yang diatur dalam Permen Nomor 36)

3. Analisis Data

Metode pengumpulan data dilakukan melalui penelitian kepustakaan, dengan menggunakan analisis data secara kualitatif yaitu mendiskripsikan suatu permasalahan dengan kata-kata tanpa angka.

Hasil penelitian ini melihat tentang penerapan Undang-Undang ITE pada permasalahan *Cyber-Crime*, berikut kendala penerapan Undang-Undang ITE pada permasalahan *Cyber-Crime*, melalui peran dan kedudukan ahli digital forensik berkaitan dengan alat bukti digital sebagai alat bukti yang sah pada perkara *cyber-crime* sebagaimana diatur pada Pasal 184 ayat (1) KUHAP.

Bahwa keterangan ahli adalah merupakan peran sangat penting dalam proses pembuktian perkara pidana *cyber-crime*, karena seorang ahli digital forensik ini yang langsung berhubungan dengan barang bukti baik dari TKP saat penyidikan hingga laboratorium. Namun, muncul beberapa kendala seperti persoalan alat bukti yang sifatnya elektronik identik dengan situasi dunia maya sehingga sangat rentan untuk penyimpanannya.

Selain itu persoalan lambatnya penanganan awal yang disebabkan karena masih ada keterbatasan SDM yang berkaitan dengan ahli digital forensik, serta keterbatasan alat-alat khusus untuk penanganan *cyber-crime* yang menunjang kelengkapan pembuktian perkara *cyber-crime* dalam hal melakukan *digital forensic investigation*.

G. Mengenal Kejahatan dunia maya.[7]

(Inggris: *cyber-crime*) adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. Termasuk ke dalam kejahatan dunia maya antara lain adalah penipuan lelang secara *daring* (dalam jaringan), pemalsuan cek, penipuan kartu kredit / carding, *confidence fraud*, penipuan identitas, pornografi anak, violence, dan lain-lain.

Walaupun kejahatan dunia maya atau *cyber-crime* umumnya mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer sebagai unsur utamanya, istilah ini juga digunakan untuk kegiatan kejahatan tradisional dimana komputer atau jaringan komputer digunakan untuk mempermudah atau memungkinkan kejahatan itu terjadi. Sebagai contoh kejahatan dunia maya

[7] https://id.wikipedia.org/wiki/Kejahatan_dunia_maya; diakses pada 15 Desember 2018

dimana komputer sebagai "alat" adalah *spamming* dan kejahatan terhadap hak cipta dan kekayaan intelektual. Berikut contoh kejahatan dunia maya di mana komputer sebagai "sasarannya" adalah akses illegal (mengelabui kontrol akses), *malware* dan serangan DoS.

Contoh kejahatan dunia maya dimana computer sebagai "tempatnya" adalah penipuan identitas. Sedangkan contoh kejahatan tradisional dengan komputer sebagai "alatnya" adalah pornografi anak dan judi daring.

Beberapa situs penipuan berkedok judi daring termasuk dalam sebuah situs yang merupakan situs kejahatan di dunia maya yang sedang dipantau oleh pihak kepolisian dengan pelanggaran pasal 303 KUHP tentang perjudian dan pasal 378 KUHP tentang penipuan berkedok permainan daring dengan cara memaksa pemilik website tersebut untuk menutup website melalui metode DDOS website yang bersangkutan. Begitupun penipuan identitas di permainan daring. Dengan hanya mengisi alamat identitas palsu, permainan daring tersebut bingung dengan alamat identitas palsu. Jika hal tersebut terus terjadi, maka permainan daring tersebut akan rugi atau pailit bahkan kemungkinan akan terjadinya kebangkrutan.

Seorang penjahat yang sudah ahli memanfaatkan ketidakjelasan identitas dan validitas informasi di dunia maya, biasanya melakukan aktivitas kejahatan dengan ponsel, atau jaringan komputer sebagai alat, sasaran atau tempat terjadinya kejahatan. Termasuk ke dalam kejahatan dunia maya ini antara lain adalah pemalsuan identitas, penipuan penjualan barang-barang, penipuan melalui SMS, pemalsuan kartu kredit, *confidence fraud*, judi *online*, pornografi anak, dan lain-lain. Berikut jenis jenis penipuan di dunia maya secara umum:

1. Iklan Jual Beli, pada situs daring, kemudian seseorang tertarik untuk membeli. Dengan modus transfer langsung, penipu meminta orang untuk menuju ATM dan secara tidak sadar orang dapat dipandu untuk melakukan transfer ke rekening penipu.
2. *Online Shop*, berbagai jenis penipuan toko daring, menjual barang apa saja yang sedang trend, harganya murah meriah, tergiur membeli, lalu tranfer uang, diperlihatkan foto bahwa barang siap dikirim, tetapi tak pernah sampai.
3. Modus Hadiah, dari Sido Muncul, Telkomsel, atau mengatas namakan perusahaan lain dengan menggunakan website gratisan yang serupa atau mirip dengan website asli. Pada akhirnya orang diminta mengirim uang administrasi.
4. Modus Bisnis, diajak berbisnis dan diminta menanamkan modal, bukannya untung yang ada adalah merugi. Jika pelaku orang Nigeria, biasanya mereka berpura-pura mau mengajak berbisnis tetapi sesungguhnya diajak membuat dolar palsu.
5. Modus Uang Dalam Paket, padahal nantinya anda akan diminta untuk membayar biaya kirim.
6. Komputer Terkena Virus, anda ditelepon orang yang mengaku

dari Microsoft dan mengatakan komputernya terkena virus lalu dipandu untuk melakukan sesuatu akhirnya diminta bayar jasa perbaikan.

7. *Scammer* Cinta, bahwa orang Indonesia banyak tertipu dengan cinta maya. Jika penipunya adalah wanita, dia akan memakai foto wanita bertubuh seksi. Kalau pelaku adalah pria, dia akan memakai foto tampan.
8. Perkenalan dari Dunia Maya, biasanya perkenalan dilakukan dari situs media sosial atau mungkin aplikasi untuk bertemu jodoh.

Mengenal perdagangan Elektronik (*E-Commerce*), dalam hal ini penggunaan internet untuk keperluan bisnis dan perdagangan mulai dikenal dengan cepat meluas terutama dinegara-negara maju. Dengan perdagangan melalui internet ini berkembang pula sistem binis *Virtual Store* dan *Virtual Company* dimana pelaku bisnis menjalankan bisnis dagangnya melalui media internet. Untuk Indonesia kendala yang menghambat perkembangan perdagangan melalui internet adalah pada sarana *settlement* yang belum memadai. Disamping sistem *delivery* dan pembayaran yang masih lemah, juga belum adanya perangkat hukum yang mendukung. Pada dasarnya perangkat hukum yang diperlukan di internet adalah dalam kaitan tentang Hak Cipta, Tentang Pornografi, Keabsahan Kontrak melalui Internet, Hukum Pembuktian dan lainnya.

Mengenal beberapa bentuk kejahatan yang mungkin terjadi melalui *cyber-space* antara lain:

1. Kejahatan yang berkaitan dengan data, seperti pemutusan transfer data, pengubahan perusakan dan penghapusan data dan pencurian data;
2. Kejahatan yang berhubungan dengan jaringan, penyadapan dan sabotase;
3. Kejahatan yang berkaitan dengan akses ke Internet yaitu *Hacking* dan Penyebaran virus;
4. Kejahatan yang berkaitan dengan komputer, membantu dan mendukung kejahatan di *Cyberspace*, pemalsuan data melalui komputer untuk mencari keuntungan, pemalsuan data melalui komputer digunakan sebagai data asli;
5. Kejahatan yang berhubungan dengan pasar modal;
6. Pornografi, penghinaan, pencemaran nama baik dan tindakan melanggar hukum lainnya.

Dalam hal ini "Hak Cipta" adalah merupakan pelanggaran hukum yang umumnya terjadi, dilakukan dengan cara yang relatif mudah oleh pengguna internet dan komputer. Pelanggaran hak cipta ini merupakan pelanggaran yang sangat merugikan.

Masih sulitnya penerapan hukum berkaitan dengan masalah perangkat hukum pendukung, dalam hal ini hukum pembuktian sebagai suatu aspek penyelesaian perkara bila terjadi persengketaan secara perdata maupun pidana. Pada dasarnya nya alat bukti alat yang diakui untuk Hukum Perdata adalah, "Bukti Tulisan, Bukti Kesaksian, Persangkaan, Pengakuan dan Sumpah". Kemudian untuk Hukum

Pidana sebagai mana terdapat dalam KUHAP adalah "Keterangan Saksi, Keterangan Ahli, Surat, Petunjuk, dan Keterangan Terdakwa".

Hal lain yang juga menjadi persoalan adalah masalah domisili menyangkut lokasi perusahaan, yang berhubungan dengan masalah pendirian, pendaftaran dan pembayaran pajak perusahaan penyedia internet dan penyelenggara Situs Web, selanjutnya juga masalah yurisdiksi berkaitan dengan wewenang pengadilan tempat kejadian perkara, tempat pengajuan gugatan, dan sebagainya, mengingat untuk pendirian perusahaan virtual ternyata tidak ada peraturan khusus yang mengaturnya. Dengan demikian Situs Web yang terbentuk tersebut belum dapat dikatakan sebagai sebuah "Bentuk Perusahaan" menurut hukum.

Dari uraian diatas tampak bahwa banyak masalah hukum yang mungkin terjadi pada media internet yang memerlukan adanya perangkat hukum untuk mengaturnya. Oleh karena belum ada hukum yang berlaku yang dapat melindungi para pengguna Internet, mengharuskan para pengguna untuk berhati-hati terhadap kejahatan yang dilakukan melalui internet.

Secara umum ada perbedaan antara *cyber-crime* dengan Kejahatan Konvesional yaitu: Pada *Cyber-Crime*; (1).Terdapat penggunaan technology informasi; (2).Alat bukti digital; (3).Pelaksanaan kejahatan non fisik (*cyberspace*); (4).Proses penyidikan melibatkan laboratorium forensik Komputer; (5).Sebagian proses penyidikan dilakukan dengan *virtual undercover;* (6).Penanganan komputer sebagai Tempat Kejadian Perkara /TKP; (7).Dalam proses persidangan, keterangan ahli menggunakan ahli Tehnologi Informasi/ TI.

Pada Kejahatan Konvensional; (1).Tidak ada penggunaan TI secara langsung; (2).Alat bukti adalah bukti fisik (terbatas menurut pasal 184 KUHAP); (3).Pelaku dan korban pada umumnya berada dalam satu tempat; (4).Pelaksanaan penyidikan melibatkan laboratorium computer; (5).Proses penyidikan memperlihatkan ada pada dunia nyata; (6).Tidak ada penanganan komputer sebagai TKP; (7).Proses persidangan, tidak menggunakan ahli TI.

Jadi dengan bantuan Sistem Elektronik, berarti semua tindak pidana konvensional dalam Kitab Undang – Undang Hukum Pidana sepanjang dengan menggunakan bantuan atau sarana Sistem Elektronik seperti pembunuhan, perdagangan orang, dapat termasuk dalam kategori tindak pidana Cyber dalam arti luas. Akan tetapi, dalam pengertian yang lebih sempit, pengaturan tindak pidana Cyber diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana yang telah diubah oleh Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik berikut PP No. 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik dan Permenkominfo No. 36 Tahun 2016 tentang Tata Cara Pendaftaran Penyelenggara Sistem Elektronik (seperti dalam hal pelayanan publik harus ada kewajiban registrasi, yang diatur dalam Permen Nomor 36)

H. Peraturan Pendukung pada Cyber-Space

1. UU- ITE Tahun 2016 tentang Perubahan UU No. 11 Tahun 2008.

UU ITE telah menetapkan perbuatan-perbuatan mana yang termasuk tindak pidana di bidang *cyber-crime* dan telah ditentukan unsur-unsur tindak pidana dan penyerangan terhadap berbagai kepentingan hukum dalam bentuk rumusan-rumusan tindak pidana tertentu. Menurut instrumen Perserikatan Bangsa Bangsa (PBB) dalam *Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders* yang diselenggarakan di Vienna, 10-17 April 2000, kategori *cyber-crime* dapat dilihat secara sempit maupun secara luas, yaitu:[8]

a. *Cyber crime in a narrow sense ("computer crime"): any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them;*
b. *Cyber crime in a broader sense ("computer-related crime"): any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession, offering or distributing information by means of a computer system or network.*

Convention on Cyber crime (Budapest, 23.XI.2001) tidak memberikan definisi *cyber-crimes*, tetapi memberikan ketentuan-ketentuan yang dapat diklasifikasikan menjadi:

a. *Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems*
b. *Title 2 – Computer-related offences*
c. *Title 3 – Content-related offences*
d. *Title 4 – Offences related to infringements of copyright and related rights*
e. *Title 5 – Ancillary liability and sanctions Corporate Liability*

Dalam **Black's Law Dictionary 9th Edition**, definisi *computer-crime* adalah sebagai berikut: "*A crime involving the use of a computer, such as sabotaging or stealing electronically stored data. - Also termed cyber-crime".*

2. Pengaturan Tindak Pidana Cyber Materil di Indonesia

Berdasarkan Instrumen PBB tersebut, maka pengaturan tindak pidana cyber di Indonesia juga dapat dilihat dalam arti luas dan arti sempit. Secara luas, tindak pidana cyber ialah semua tindak pidana yang **menggunakan sarana atau dengan bantuan** system elektronik. Itu artinya semua tindak pidana konvensional dalam Kitab Undang - Undang Hukum Pidana **("KUHP")** sepanjang dengan menggunakan bantuan atau sarana sistem elektronik seperti pembunuhan, perdagangan orang, dapat termasuk dalam kategori tindak pidana cyber

[8] https://www.hukumonline.com/klinik/detail/cl5960/landasan-hukum-penanganan-cyber-crime-di-indonesia; diakses pada 15 Desember 2019

dalam arti luas. Demikian juga tindak pidana dalam Undang-Undang Nomor 3 Tahun 2011 tentang Transfer Dana **(UU No. 3 tahun 2011)** maupun tindak pidana perbankan serta tindak pidana pencucian uang dalam Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang **(UU TPPU)**.

Akan tetapi, dalam pengertian yang lebih sempit, pengaturan tindak pidana cyber diatur dalam Undang – Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik **(UU ITE)** sebagaimana yang telah diubah oleh Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik **(UU 19 tahun 2016")** sama halnya seperti *Convention on Cyber-crimes*, UU ITE juga tidak memberikan definisi mengenai *cyber-crimes*, tetapi membaginya menjadi beberapa **pengelompokkan** yang mengacu pada *Convention on Cyber-crimes* (Sitompul, 2012):[9]

a. Tindak pidana yang berhubungan dengan aktivitas illegal, yaitu:
   1) Distribusi atau penyebaran, transmisi, dapat diaksesnya konten illegal, yang terdiri dari:
      a) Kesusilaan (**Pasal 27 ayat (1) UU ITE**);
      b) Perjudian (**Pasal 27 ayat (2) UU ITE**);
      c) penghinaan dan/atau pencemaran nama baik (**Pasal 27 ayat (3) UU ITE**);
      d) Pemerasan dan/atau pengancaman (**Pasal 27 ayat (4) UU ITE**);
      e) Berita bohong yang menyesatkan dan merugikan konsumen (**Pasal 28 ayat (1) UU ITE**);
      f) Menimbulkan rasa kebencian berdasarkan SARA (**Pasal 28 ayat (2) UU ITE**);
      g) Mengirimkan informasi yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi (**Pasal 29 UU ITE**);
   2) Dengan cara apapun melakukan akses illegal (**Pasal 30 UU ITE**);
   3) Intersepsi atau penyadapan illegal terhadap informasi atau dokumen elektronik dan Sistem Elektronik (**Pasal 31 UU 19/2016**);
b. Tindak pidana yang berhubungan dengan gangguan (interferensi), yaitu:
   1) Gangguan terhadap Informasi atau Dokumen Elektronik (*data interference* - **Pasal 32 UU ITE**);
   2) Gangguan terhadap Sistem Elektronik (*system interference* - **Pasal 33 UU ITE**);

[9] Sitompul, Josua. *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana,* PT. Tatanusa; 2012.

c. Tindak pidana memfasilitasi perbuatan yang dilarang (**Pasal 34 UU ITE**);
d. Tindak pidana pemalsuan informasi atau dokumen elektronik (**Pasal 35 UU ITE**);
e. Tindak pidana tambahan (*accessoir* **Pasal 36 UU ITE**); dan Perberatan-perberatan terhadap ancaman pidana (**Pasal 52 UU ITE**).
f. Tindak pidana memfasilitasi perbuatan yang dilarang (**Pasal 34 UU ITE**);
g. Tindak pidana pemalsuan informasi atau dokumen elektronik (**Pasal 35 UU ITE**);
h. Tindak pidana tambahan (*accessoir* **Pasal 36 UU ITE**); dan Perberatan-perberatan terhadap ancaman pidana (**Pasal 52 UU ITE**).

3. Pengaturan Tindak Pidana Cyber Formil di Indonesia

Selain mengatur tindak pidana cyber materil, UU ITE mengatur tindak pidana cyber formil, khususnya dalam bidang penyidikan.

Pasal 42 UU ITE mengatur bahwa penyidikan terhadap tindak pidana dalam UU ITE dilakukan berdasarkan ketentuan dalam Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana **(KUHAP)** dan ketentuan dalam UU ITE.

Artinya, ketentuan penyidikan dalam KUHAP tetap berlaku sepanjang tidak diatur lain dalam UU ITE. Kekhususan UU ITE dalam penyidikan antara lain:[10]

a. Penyidik yang menangani tindak pidana cyber ialah dari instansi Kepolisian Negara RI atau Pejabat Pegawai Negeri Sipil ("PPNS") Kementerian Komunikasi dan Informatika;
b. Penyidikan dilakukan dengan memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran layanan publik, integritas data, atau keutuhan data;
c. Penggeledahan dan / atau penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan sesuai dengan ketentuan hukum acara pidana;
d. Dalam melakukan penggeledahan dan / atau penyitaan sistem elektronik, penyidik wajib menjaga terpeliharanya kepentingan pelayanan umum.

Ketentuan penyidikan dalam UU ITE dan perubahannya berlaku pula terhadap penyidikan tindak pidana cyber dalam arti luas. Sebagai contoh, dalam tindak pidana perpajakan, sebelum dilakukan penggeledahan atau penyitaan terhadap server bank, penyidik harus memperhatikan kelancaran layanan publik, dan menjaga terpeliharanya kepentingan pelayanan umum sebagaimana diatur dalam UU ITE dan perubahannya. Apabila dengan mematikan server bank akan

[10] Pasal 43 ayat (1), ayat (2), ayat (3), ayat (4), dan ayat (5) UU 19/2016

mengganggu pelayanan publik, tindakan tersebut **tidak boleh** dilakukan.

Adapun prosedur untuk menuntut secara pidana terhadap perbuatan tindak pidana cyber, secara sederhana dapat dijelaskan sebagai berikut:[11]

a. Korban yang merasa haknya dilanggar atau melalui kuasa hukum, datang langsung membuat laporan kejadian kepada penyidik POLRI pada unit/bagian *Cyber-crime* atau kepada penyidik PPNS pada Sub Direktorat Penyidikan dan Penindakan, Kementerian Komunikasi dan Informatika. Selanjutnya, penyidik akan melakukan penyelidikan yang dapat dilanjutkan dengan proses penyidikan atas kasus bersangkutan Hukum Acara Pidana dan ketentuan dalam UU ITE.
b. Setelah proses penyidikan selesai, maka berkas perkara oleh penyidik akan dilimpahkan kepada penuntut umum untuk dilakukan penuntutan di muka pengadilan. Apabila yang melakukan penyidikan adalah PPNS, maka hasil penyidikannya disampaikan kepada penuntut umum melalui penyidik POLRI. Selain UU ITE, peraturan yang menjadi landasan dalam penanganan kasus *cyber-crime* di Indonesia ialah peraturan pelaksana UU ITE dan juga peraturan teknis dalam penyidikan di masing-masing instansi penyidik.

4. *Forensic Investigator* Dalam *Cyber-crime*.[12]

Walaupun terminologi *cyber-crime* termasuk sesuatu yang cukup populer, tapi hingga saat ini belum ada definisi yang disepakati bersama tentang apa itu sebenarnya *cyber-crime*. Namun demikian, setidaknya sejumlah organisasi sudah mulai memberikan *working definition* dari *cyber-crime*, diantaranya adalah dari *United Nation*, bahwa *cyber-crime* adalah :

a. *Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them";*
b. *Any illegal behavior committed by means of or in relation to a computer system or network including such crimes as illegal possession and offering or distributing information by means of computer system or network*.

Berbeda dengan di dunia nyata, kejahatan di dunia komputer dan internet variasinya begitu banyak, dan cenderung dipandang dari segi jenis dan kompleksitasnya meningkat secara eksponensial. Secara prinsip, kejahatan di dunia komputer dibagi menjadi tiga, yaitu:

[11] Pasal 42 UU ITE jo. Pasal 43 UU 19 tahun 2016 dan Pasal 102 s.d. Pasal 143 Undang -Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana.

[12] https://catatanforensikadigital.wordpress.com/2013/11/14/cybercrime-dan-forensic-investigator/; diakses pada 1 Januari 2019.

a. Aktivitas dimana komputer atau piranti digital dipergunakan sebagai alat bantu untuk melakukan tindakan kriminal;
b. Aktivitas dimana komputer atau piranti digital dijadikan target dari kejahatan itu sendiri; dan
c. Aktivitas dimana pada saat yang bersamaan komputer atau piranti digital dijadikan alat untuk melakukan kejahatan terhadap target yang merupakan komputer atau piranti digital juga.

Berdasarkan laporan yang dibuat oleh *Symantec* yang direlease pada bulan September 2012, setiap tahunnya terdapat sekitar 556 Juta korban dari aktivitas *cyber-crime*, 1,5 juta korban per hari dan 18 korban per detiknya. Sebagian besar korban adalah warga dari Uni Eropa. Dalam laporan *Symantec* tersebut di sebutkan bahwa hampir 2/3 pengguna aktif komputer pernah menjadi korban dari aktivitas *cyber-crime.*

Tiga Negara dilaporkan sebagai Negara dengan jumlah korban *cyber-crime* terbesar, yaitu: Rusia (92%), China (84%) dan Afrika Selatan (80%). Sementara itu penggunaan perangkat bergerak (mobile phone), perangkat wifi, email dan aplikasi jejaring sosial menjadi kecenderung utama pelaku *cyber-crime* dalam melakukan aksinya. Sementara itu berdasarkan laporan yang dibuat pada tahun 2011, *Symantec* juga menyebutkan bahwa target *cyber-crime* 50% adalah perusahaan besar dan menengah, 18 % perusahaan kecil sisanya adalah institusi pemerintah dan pendidikan.[13]

Setelah memahami jenis dan karakteristik dari *cyber-crime*, maka selanjutnya adalah bagaimana teknik untuk mendapatkan bukti-bukti terjadinya aktivitas *cyber-crime* tersebut untuk kemudian dijadikan sebagai alat bukti cukup untuk dilakukan penyidikan, penuntutan hukum serta pemaparan di persidangan. Dalam hal ini profesi forensika digital memegang peranan penting untuk proses penemuan alat bukti hingga pemaparan alat bukti tersebut di persidangan. Terkait dengan bukti, maka setidaknya harus memenuhi tiga hal, yaitu:

a. Bukti-bukti yang cukup untuk dapat dilakukan proses penyelidikan oleh pihak berwenang.
b. Bukti-bukti tersebut benar-benar berkualitas untuk dapat dijadikan alat bukti di pengadilan yang sah sesuai dengan hukum dan perundang-undangan yang berlaku; dan
c. Bukti dapat dipresentasikan dan / atau diperlihatkan keabsahannya sebagai alat bukti dalam proses persidangan.

Untuk itulah diperlukan peran ahli *forensic investigator*

[13] *Ibid;* https://catatanforensikadigital.wordpress.com. Diakses pada 15 Desember 2018

untuk pengungkapan bukti-bukti yang ada. Pemahaman Forensik adalah proses penggunaan pengetahuan ilmiah dalam mengumpulkan, menganalisa, dan mempresentasikan barang bukti ke pengadilan. Forensik pada dasarnya berhubungan dengan penyelamatan dan analisis barang bukti laten, dapat berbentuk banyak format, mulai dari sidik jari di jendela, DNA yang diperoleh dari noda darah sampai file-file di dalam hard disk komputer.

Khusus forensik digital (*Digital Forensic*), adalah sebuah disiplin ilmu yang relatif baru. Disiplin ilmu ini muncul dari interseksi berbagai bidang ilmu lainnya, diantara adalah: Ilmu Forensik umum (contoh yang sudah umum dikenal adalah kedokteran forensik, akuntansi forensik, psikologi forensik), ilmu komputer/ informatika/ teknologi informasi, kriminologi, hukum, statistik/ matematika, manajemen dan etika. Penanganan kasus-kasus *cyber-crime* membutuhkan perpaduan antara keahlian sebagai penyidik serta kemahiran dan dukungan teknologi computer yang modern. Namun hingga saat ini tenaga professional sebagai *forensic investigator* masih sangat terbatas.

Dikalangan penegak hukum, penyidik yang memiliki kemampuan sebagai *forensic investigator* masih dibawah 10%. Sedangkan di kalangan umumnya profesi sebagai *forensic investigator* belum dipandang sebagai profesi yang menjanjikan.[14] Padahal, sejalan dengan kesadaran para pelaku bisnis akan potensi besar *cyber-crime,* memperlihatkan kebutuhan profesi *forensic investigator* akan semakin meningkat, sebab aktivitas *cyber-crime* dapat menyerang siapa saja, baik individu, masyarakat ataupun institusi. Maka untuk itulah diperlukan ahli forensika digital, tidak hanya untuk kepentingan penegakan hukum saja, namun juga untuk berbagai keperluan lainnya, misalnya :

Organisasi atau perusahaan dapat selalu siap dan tanggap seandainya ada tuntutan hukum yang melanda dirinya, terutama dalam mempersiapkan bukti-bukti pendukung yang dibutuhkan;

Seandainya terjadi peristiwa kejahatan yang membutuhkan investigasi lebih lanjut, dampak gangguan terhadap operasional organisasi atau perusahaan dapat diminimalisir;

Para kriminal atau pelaku kejahatan akan bertimbang-timbang sebelum menjalankan aksi kejahatannya terhadap organisasi atau perusahaan tertentu yang memiliki kapabilitas forensik komputer; dan membantu organisasi atau perusahaan dalam melakukan mitigasi resiko teknologi informasi yang dimilikinya.

[14] *Ibid;* https://catatanforensikadigital.wordpress.com;

I. Analisis Penerapan UU- ITE Pada *Cyber-Crime*

Tindak Pidana *Cyber-crime* pada UU ITE diatur dalam 9 pasal, yaitu dari pasal 27 sampai dengan pasal 35. Pada 9 pasal tersebut dirumuskan 20 bentuk atau jenis tindak pidana. Pasal 36 tidak merumuskan bentuk tindak pidana ITE tertentu, melainkan merumuskan tentang dasar pemberatan pidana yang diletakkan pada akibat merugikan orang lain, dan ancaman pidananya ditentukan pada Pasal 45 sampai Pasal 52 dengan uraian sebagai berikut:

1. Tindak Pidana Distribusi, Penyebaran atau Transmisi Konten ilegal;
   a. Kesusilaan terdapat dalam Pasal 27 ayat (1).
   b. Perjudian terdapat dalam Pasal 27 ayat (2).
   c. Penghinaan atau pencemaran nama baik terdapat dalam Pasal 27 ayat (3).
   d. Pemerasan atau pengancaman dalam Pasal 27 ayat (4).
   e. Berita bohong yang menyesatkan dan merugikan konsumen/penipuan terdapat dalam Pasal 28 ayat (1).
   f. Menimbulkan rasa kebencian berdasarkan SARA terdapat dalam Pasal 28 ayat (2).
   g. Mengirimkan informasi yang berisi ancaman kekerasan atau menakut – nakuti yang ditujukan secara pribadi terdapat dalam Pasal 29.
   h. Dengan cara apapun melakukan akses ilegal pada Pasal 30.
   i. Intersepsi ilegal terhadap informasi atau dokumen elektronik dan sistem elektronik terdapat dalam Pasal 31.
2. Tindak pidana yang berhubungan dengan gangguan (interferensi)
   a. Gangguan terhadap Informasi atau Dokumen Elektronik (data interference) terdapat dalam Pasal 32.
   b. Gangguan terhadap Sistem Elektronik (system interference) terdapat dalam asal 33.
   c. Tindak pidana memfasilitasi perbuatan yang dilarang terdapat dalam Pasal 34.
   d. Tindak pidana pemalsuan informasi atau dokumen elektronik terdapat dalam Pasal 34.
   e. Tindak pidana tambahan terdapat dalam Pasal 36.
   f. Pemberatan-pemberatan terhadap ancaman pidana dalam Pasal 52.

Ada sejumlah catatan mengenai arah kebijakan penyelenggaraan teknologi informasi di Indonesia melalui revisi UU ITE ini.[15]

Pertama:

Revisi UU ITE ini sangat baik dalam hal memperjelas siapa saja yang termasuk sebagai penyelenggara sistem elektronik. Dalam UU ITE yang lama, cakupan penyelenggara sistem elektronik tidak diatur begitu jelas. "Ini jadi jelas siapa subjek hukum dari Revisi UU ITE ini."

Dalam revisi UU ITE dinyatakan bahwa penyelenggara sistem elektronik adalah "Setiap orang, penyelenggara negara, Badan Usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik, baik secara sendiri-

[15] https://www.hukumonline.com/berita/baca/lt58456c91c845b/penguatan-peraturan-pemerintah--kunci-perjelas-arah-uu-ite-terbaru; Diakses pada 15 Desember 2018

sendiri maupun bersama-sama kepada pengguna Sistem Elektronik untuk keperluan dirinya atau keperluan pihak lain."

Satu hal menarik dalam pasal yang ada adalah mengenai keikutsertaan negara sebagai penyelenggara sistem elektronik, seperti di Malaysia misalnya, regulasi di sana tidak mengikutsertakan negara sebagai pihak. Di sini, revisi UU ITE ini sedikit berbeda dimana regulasi terbaru bisa diaplikasikan buat negara, lembaga publik, hingga swasta. Namun, ada beberapa frasa yang mestinya diperjelas pada pasal tersebut seperti "menyediakan", "mengelola", dan "mengoperasikan". Jadi bagaimana sebetulnya sistem elektronik bisa terkena karena variasi tiga hal ini.

Bahwa mengingat ada semacam perluasan cakupan penyelenggara sistem elektronik, hal itu sejalan juga dengan kewajiban-kewajiban yang mungkin timbul bagi penyedia sistem elektronik terkait Peraturan Pemerintah/PP Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik dan Permenkominfo Nomor 36 Tahun 2016 tentang Tata Cara Pendaftaran Penyelenggara Sistem Elektronik. Misalnya sebagai pelayanan publik harus ada kewajiban registrasi pada Permen Nomor 36 yang diatur.

Kedua;

Mengenai bagaimana peranan pemerintah dalam revisi UU ITE, pasal 40 mengatur peran pemerintah dalam hal melakukan pencegahan penyebarluasan dan penggunaan informasi elektronik atau dokumen elektronik. Bahwa pertanyaan selanjutnya adalah terkait frasa pada Pasal 40 ayat (2a) yang menyebut frasa "muatan yang dilarang" dan Pasal 40 ayat (2b) yang menyebut frasa "muatan yang melanggar hukum". Jadi ini seperti ada dua rujukan, apakah keduanya atau salah satunya saja yang dilakukan pemerintah, untuk menjadi objek yang dilarang oleh pemerintah.

Selanjutnya merujuk ke Pasal 27 UU ITE, dinyatakan muatan yang dilarang atau melanggar hukum antara lain melanggar kesusilaan, perjudian, penghinaan, pencemaran nama baik, pemerasan, dan pengancaman. Selain itu, Pasal 28 dan Pasal 29 UU ITE diatur muatan yang dilarang seperti menyebarkan berita bohong, menimbulkan rasa kebencian, SARA, berisi ancaman kekerasan.

Bahwa Permenkominfo Nomor 19 Tahun 2014 tentang penanganan situs internet bermuatan negatif juga fokus melarang konten internet negatif terutama yang memuat pornografi dan kegiatan ilegal.

Hal yang sama juga diatur dalam SE Menkominfo Nomor 3 Tahun 2016 tentang Penyediaan Layanan Aplikasi dan/atau Konten Melalui Internet (*Over the Top*) yang melarang konten bertentangan dengan Pancasila dan UUD 1945, SARA, mendorong melakukan tindakan melawan hukum, narkotika, ujaran kebencian (*hate speech*).

"Permen itu terfokus pada internet, bila informasi elektronik tentu lebih dari sekedar situs internet apakah ini akan ada target yang dimonitor juga. Satu hal, dalam SE yaitu hal ini juga diatur muatan yang dilarang yang bertentangan.

Sebuah catatan penting adalah wewenang pemutusan akses dapat dilakukan sendiri atau melalui

penyelenggara, sebab pada praktiknya lazim dilakukan oleh *Internet Service Provider* (ISP). Untuk hal ini belum jelas, bagaimana sebetulnya mekanismenya karena akan muncul pertanyaan apakah ISP mempunyai hak untuk dapat informasi lebih lengkap atau hanya sekedar mengikuti perintah untuk memutus. Untuk hal ini kemungkinan akan diatur dalam Peraturan Pemerintah, dan semoga hal ini akan segera ada penjelasannya.

Ketiga,

Mengenai *Right to be Forgotten* dimana ada tiga tambahan ayat dalam revisi UU ITE ini, yang menjadi catatan adalah mengenai ketentuan dalam Pasal 26 ayat (3) yang menyebut penghapusan konten berdasarkan permintaan "orang yang bersangkutan" atau "penetapan pengadilan". Maka untuk hal ini ada permasalahan yang perlu mendapatkan kejelasan yaitu apakah permintaan tersebut saja, atau juga menyangkut harus dengan penetapan pengadilan untuk dapat dihapuskannya permintaan yang diajukan.

J. Kendala Penerapan UU ITE Pada *Cyber-Crime.*

Revisi UU Nomor 11 Tahun 2008 tentang Informasi Transaksi Elektronik (UU ITE)

Diakui menimbulkan pertanyaan dari banyak kalangan. Hal ini diutarakan oleh Direktur Penyidikan dan Penindakan Direktorat Keamanan Informasi Kementerian Komunikasi dan Informatika, pada acara diskusi Hukum Online bertajuk "Arah Kebijakan Penyelenggaraan Teknologi Informasi di Indonesia Pasca Revisi UU ITE".

Pada awal, revisi Undang-undang ITE permasalahan terfokus pada Pasal 27 ayat 3 yang mengatur tentang pencemaran nama baik, yang tujuan utama dari revisi UU ITE adalah penguatan peran pemerintah dan memperbaiki kesalahan dalam penerapan pasal 27 ayat (3) tersebut.

Poin utamanya adalah penegasan istilah "mendistribusikan", "mentransmisikan", dan "membuat dapat diaksesnya" informasi dan/atau dokumen elektronik. Melalui revisi UU ITE ini, Kominfo ingin menegaskan bahwa yang dimaksud dengan "Mendistribusikan" adalah mengirimkan dan/atau menyebarkan Informasi elektronik dan/atau dokumen elektronik kepada banyak orang atau berbagai pihak melalui sistem elektronik.

Sementara, maksud dari "mentransmisikan" adalah mengirimkan informasi elektronik dan/atau dokumen elektronik yang ditujukan kepada satu pihak lain melalui sistem elektronik. Kemudian maksud "Membuat dapat diakses" adalah semua perbuatan lain selain mendistribusikan dan mentransmisikan melalui sistem elektronik yang menyebabkan informasi elektronik dan/atau dokumen elektronik dapat diketahui pihak lain atau publik.

"Pemerasan dan/atau pencemaran pada Pasal 27 ayat (4) mengacu pada ketentuan pemerasan dan/atau pengancaman yang diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP). Kemudian Penghinaan dan/atau pencemaran nama baik Pasal 27 ayat (3) merupakan delik aduan. Selain itu, hal lain yang menjadi konsentrasi Kominfo dalam menyiapkan naskah

revisi UU ITE adalah upaya penguatan peran pemerintah. Dalam konteks ini, pemerintah wajib melakukan pencegahan penyebarluasan informasi elektronik yang memiliki muatan yang dilarang sesuai dengan ketentuan peraturan perundang-undangan.

Bahwa pemerintah berwenang melakukan pemutusan akses dan/atau memerintahkan kepada penyelengggara system elektronik untuk melakukan pemutusan akses terhadap Informasi elektronik yang memiliki muatan yang melanggar hukum. "Penegasan cakupan kewenangan pemerintah dalam memfasilitasi pemanfaatan Informasi Tekhnologi termasuk tata kelola tekonologi informasi yang aman, beretika, cerdas, kreatif, produktif, dan inovatif." Asumsinya, adalah karena ini terkait dengan informasi yang tidak relevan. Bahwa penentuannya ada di pengadilan. Artinya, harus ada permintaan dari seseorang dan penetapan pengadilan. Selain itu, bila terkait dengan data pribadi, bagaimana dengan definisi data pribadi dan termasuk dengan pengecualiannya, dalam rancangan RUU Perlindungan Data Pribadi, tercantum pengecualian mengenai apa yang bisa dihapus atau tidak. "Misalnya terkait dengan kegiatan jurnalistik itu tidak bisa dimintakan.

Menanggapi catatan yang ada, bahwa pihak Kominfo ada menjelaskan bahwa konsep *Right to be Forgotten* sebetulnya tidak pernah dipikirkan oleh Kominfo. Artinya, Kominfo belum pernah melakukan kajian detil dan mendalam tentang konsep tersebut. Sehingga, ada satu pasal yang mengamanatkan pembentukan Peraturan Pemerintah (PP) sebagai pedoman teknisnya yang lebih rinci.

Idealnya adalah sebuah norma dalam UU baru dapat dijalankan ketika mekanismenya sudah ada dalam peraturan di bawahnya. Tapi bukan berarti norma dan pasal tersebut tidak berlaku. Hal itu tetap berlaku, namun tentang bagaimana berlakunya, hal itu tentu perlu diatur secara internal.

K. Kendala Pada Peran Dan Kedudukan Ahli Digital Forensik Dalam Pembuktian Perkara Pidana Cyber-Crime.[16]

Proses pembuktian pada tindak pidana dalam kasus *cyber-crime* identik dengan penggunaan alat bukti elektronik. Bahwa permasalahan dalam penelitian ini adalah bagaimana kedudukan ahli digital forensik berkaitan dengan alat bukti digital dalam melakukan pembuktian perkara pidana *cyber-crime* dan bagaimana kendala yang dihadapi dalam pelaksanaan peradilan untuk proses pembuktian perkara pidana *cyber-crime.*

Hasil penelitian ini menunjukan bahwa kedudukan ahli digital forensik berkaitan dengan alat bukti digital pada perkara *cyber-crime* sebagaimana diatur pada Pasal 184 ayat (1) KUHAP berkedudukan sebagai alat bukti yang sah yaitu alat bukti keterangan ahli sehingga perannya sangat penting dalam proses pembuktian perkara pidana *cyber crime*, karena seorang ahli digital forensik ini lah yang langsung berhubungan dengan barang bukti

[16] http://repository.umy.ac.id/handle/123456789/15941

baik dari TKP saat penyidikan hingga laboratorium. Namun, muncul beberapa kendala seperti persoalan alat bukti yang sifatnya elektronik yang identik dengan situasi dunia maya, yang rentan untuk penyimpanan dokumen.

Selain itu persoalan lambatnya penanganan awal yang disebabkan masih kurangnya SDM yang berkaitan dengan ahli digital forensik, serta keterbatasan alat-alat khusus penanganan *cyber-crime* untuk menunjang melakukan pembuktian perkara tersebut sehingga terjadi kendala untuk melakukan *digital forensic investigation*.

Dapat disimpulkan bahwa, ahli digital forensik berkaitan dengan alat bukti digital berkedudukan sebagai salah satu alat bukti yang sah yaitu keterangan ahli sebagaimana diatur pada Pasal 184 ayat (1) KUHAP, seorang ahli digital forensik ini lah yang menjelaskan bagaimana terdakwa melakukan tindak pidana *cyber-crime* dan alat apa yang digunakan dengan kendala persoalan alat bukti yang bersifat elektronik sehingga sangat rentan untuk diubah, dihapus, atau disembunyikan oleh pelaku. Sehingga penanganannya seharusnya alat bukti elektronik tersebut di cetak dengan media kertas (*print out*) agar tidak terjadi manipulasi kemudian dianalisa oleh ahli digital forensik untuk disampaikan di persidangan. Hal ini tertuang dalam Pasal 5 Ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

L. Penerapan Beberapa Peraturan Perundang-Undangan

Pasal Pada Kitab Undang Undang Hukum Pidana

Pasal 362 KUHP yang dikenakan untuk kasus carding, Pasal 378 KUHP dapat dikenakan untuk penipuan. Pasal 335 KUHP dapat dikenakan untuk kasus pengancaman dan pemerasan yang dilakukan melalui e-mail yang dikirimkan oleh pelaku untuk memaksa korban melakukan sesuatu sesuai dengan apa yang diinginkannya. Pasal 311 KUHP dapat dikenakan untuk kasus pencemaran nama baik dengan menggunakan media Internet.

Pasal 303 KUHP dapat dikenakan untuk menjerat permainan judi yang dilakukan secara online di Internet dengan penyelenggara dari Indonesia.

Pasal 282 KUHP dapat dikenakan untuk penyebaran pornografi. Pasal 282 dan 311 KUHP dapat dikenakan untuk kasus penyebaran foto atau film pribadi seseorang.

Pasal 406 KUHP dapat dikenakan pada kasus *deface* atau *hacking* yang membuat sistem milik orang lain rusak.

Undang-Undang No 19 Tahun 2002 tentang Hak Cipta.

Menurut Pasal 1 angka (8) Undang-Undang No 19 Tahun 2002 tentang Hak Cipta, program komputer adalah sekumpulan intruksi yang diwujudkan dalam bentuk bahasa, kode, skema ataupun bentuk lain yang apabila digabungkan dengan media yang dapat dibaca dengan komputer akan mampu membuat komputer bekerja untuk melakukan fungsi-fungsi khusus atau untuk mencapai hasil yang khusus, termasuk persiapan dalam merancang intruksi-intruksi tersebut.

Undang-Undang No 36 Tahun 1999 tentang Telekomunikasi

Menurut Pasal 1 angka (1) Undang-Undang No 36 Tahun 1999, Telekomunikasi adalah setiap pemancaran, pengiriman, dan/atau penerimaan dan setiap informasi dalam bentuk tanda-tanda, isyarat, tulisan, gambar, suara, dan bunyi melalui sistem kawat, optik, radio, atau sistem elektromagnetik lainnya.

Undang-Undang No 8 Tahun 1997 tentang Dokumen Perusahaan

Undang-Undang No. 8 Tahun 1997 tanggal 24 Maret 1997 tentang Dokumen Perusahaan, pemerintah berusaha untuk mengatur pengakuan atas mikrofilm dan media lainnya (alat penyimpan informasi yang bukan kertas dan mempunyai tingkat pengamanan yang dapat menjamin keaslian dokumen yang dialihkan atau ditransformasikan. Misalnya *Compact Disk – Read Only Memory* (CD – ROM), dan *Write – Once -Read – Many* (*WORM*), yang diatur dalam Pasal 12 Undang-Undang tersebut sebagai alat bukti yang sah.

Undang-Undang No 25 Tahun 2003 tentang Perubahan atas Undang-Undang No. 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang

Jenis tindak pidana yang termasuk dalam pencucian uang (Pasal 2 Ayat (1) Huruf q). Penyidik dapat meminta kepada bank yang menerima transfer untuk memberikan identitas dan data perbankan yang dimiliki oleh tersangka tanpa harus mengikuti peraturan sesuai dengan yang diatur dalam Undang-Undang Perbankan.

UU No 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme

Undang-Undang ini mengatur mengenai alat bukti elektronik sesuai dengan Pasal 27 huruf b yaitu alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu. Digital evidence atau alat bukti elektronik sangatlah berperan dalam penyelidikan kasus terorisme. karena saat ini komunikasi antara para pelaku di lapangan dengan pimpinan atau aktor intelektualnya dilakukan dengan memanfaatkan fasilitas di Internet untuk menerima perintah atau menyampaikan kondisi di lapangan karena para pelaku mengetahui pelacakan terhadap Internet lebih sulit dibandingkan pelacakan melalui handphone. Fasilitas yang sering digunakan adalah e-mail dan chat room selain mencari informasi dengan menggunakan search engine serta melakukan propaganda melalui bulletin board atau mailing list.

Kesimpulan

Perkembangan *Cyber Law* di Indonesia umumnya belum bisa dikatakan maju, hal ini diakibatkan oleh belum meratanya pengguna internet di seluruh Indonesia. Bahwa kondisi yang berbeda dengan wilayah lainnya seperti Amerika Serikat yang telah menggunakan internet untuk memfasilitasi seluruh aspek kehidupan mereka. Oleh karena itu, perkembangan hukum dunia maya di Amerika Serikat sudah sangat maju. Landasan fundamental di dalam aspek yuridis yang mengatur lalu lintas internet sebagai hukum khusus, di mana terdapat komponen utama yang meng-cover persoalan yang ada di dalam dunia maya tersebut, yaitu :

a. Yurisdiksi hukum dan aspek-aspek terkait komponen ini menganalisa dan menentukan keberlakuan hukum yang berlaku dan diterapkan di dalam dunia maya itu.
b. Landasan penggunaan internet sebagai sarana untuk melakukan kebebasan berpendapat yang berhubungan dengan tanggung jawab pihak yang menyampaikan, aspek *accountability*, tangung jawab dalam memberikan jasa online dan penyedia jasa internet (*internet provider*), serta tanggung jawab hukum bagi penyedia jasa pendidikan melalui jaringan internet.
c. Aspek hak milik intelektual di mana ada aspek tentang patent, merek dagang rahasia yang diterapkan, serta berlaku di dalam dunia cyber.
d. Aspek kerahasiaan yang dijamin oleh ketentuan hukum yang berlaku di masing-masing yurisdiksi negara asal dari pihak yang mempergunakan atau memanfaatkan dunia maya sebagai bagian dari sistem atau mekanisme jasa yang mereka lakukan.
e. Aspek hukum yang menjamin keamanan dari setiap pengguna dari internet.
f. Ketentuan hukum yang memformulasikan aspek kepemilikan didalam internet sebagai bagian dari pada nilai investasi yang dapat dihitung sesuai dengan prinisip-prinsip keuangan atau akuntansi.
g. Aspek hukum yang memberikan legalisasi atas internet sebagai bagian dari perdagangan atau bisnis usaha.

Rekomendasi

a. Berdasarkan faktor-faktor diatas, akan dapat dilakukan penilaian untuk menjustifikasi sejauh mana perkembangan dari hukum yang mengatur sistem dan mekanisme internet di Indonesia. Walaupun belum dapat dikatakan merata, namun perkembangan internet di Indonesia mengalami percepatan yang sangat tinggi serta memiliki jumlah pelanggan atau pihak yang mempergunakan jaringan internet terus meningkat sejak paruh tahun 90′an.
b. Salah satu indikator untuk melihat bagaimana aplikasi hukum tentang internet diperlukan di Indonesia adalah dengan banyak perusahaan yang menjadi provider untuk pengguna jasa internet di Indonesia. Perusahaan-perusahaan yang memberikan jasa provider di Indonesian sadar atau tidak merupakan pihak yang berperan sangat penting dalam memajukan perkembangan *Cyber Law* di Indonesia dimana fungsi-fungsi yang mereka lakukan seperti, "Perjanjian aplikasi rekening pelanggan internet; Perjanjian pembuatan desain home page komersial; Perjanjian reseller penempatan data-data di internet server; Penawaran - penawaran penjualan produk-produk komersial melalui internet; Pemberian informasi yang di-update setiap hari oleh home page komersial; Pemberian pendapat atau polling online melalui internet." Pada dasar nya sudah harus disesuaikan peraturannya.

   Salah satu permasalahan yang dihadapi penegak hukum untuk menjerat pelaku tindak pidana cyber antara lain adalah masalah pembuktian tentang kesalahan terdakwa. Kenyataan tersebut menjadi suatu tantangan bagi kalangan penegak

hukum untuk menyelesaikan segala persoalan yang terjadi akibat perkembangan teknologi yang sangat pesat. Permasalahan penelitian adalah bagaimana proses pembuktian kejahatan cyber agar segera mendapat perhatian pada aplikasinya.

Pendekatan normatif yang digunakan untuk memperoleh data sekunder melalui studi pustaka, Analisis data dilakukan dengan cara kualitatif. Hasil penelitian menunjukkan dalam mengungkapkan suatu kasus kejahatan cyber, yang sangat rumit, kompleks, yang bersifat spesifik, keterangan ahli telematika sebagai alat bukti pada kejahatan cyber dalam proses peradilan pidana merupakan alat bukti yang sah menurut undang-undang. Berkaitan dengan permasalahan yang dibahas mengenai pembuktian tindak pidana *cyber crime* yang menggunakan sarana internet maka ketentuan hukum pembuktian yang dipakai tetap mengacu pada Kitab Undang-Undang Hukum Acara Pidana (KUHAP) dan Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.[17]

Untuk itu dapat disimpulkan bahwa, ahli digital forensik berkaitan dengan alat bukti digital berkedudukan sebagai salah satu alat bukti yang sah yaitu keterangan ahli sebagaimana diatur pada Pasal 184 ayat (1) KUHAP, dimana seorang ahli digital forensik ini yang menjelaskan bagaimana terdakwa melakukan tindak pidana *cyber-crime* dan alat apa yang digunakan dengan kendala persoalan alat bukti yang bersifat elektronik sehingga sangat rentan untuk diubah, dihapus, atau disembunyikan oleh pelaku. Sehingga penanganannya seharusnya alat bukti elektronik tersebut di cetak dengan media kertas (*print out*) agar tidak terjadi manipulasi, kemudian dianalisa oleh ahli digital forensik untuk disampaikan di persidangan. Hal ini tertuang dalam Pasal 5 Ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

[17] http://jurnal.ubl.ac.id/index.php/PH/article/view/144; diakses pada 15 November 2018

DAFTAR PUSTAKA

Buku:

Agus raharjo, Cyber Crime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi, Bandung: Citra Aditya Bakti, 2002

Ahmad M Ramli, Cyberlaw dan HAKI dalam Sistem Hukum Indonesia, Bandung: Refika Aditama, 2004

Al Wisnubroto, Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer, Yogyakarta: Universitas Widyatama, 1999

Andi Hamzah, Hukum Acara Pidana Indonesia, Jakarta: CV Sapta Arta Jaya, 1996

Andri Kristanto, Jaringan Komputer, Yogyakarta: Graha Ilmu, 2003

Budi Agus Riswandi, Hukum dan Internet di Indonesia, Yogyakarta: UII Press, 2003

Dikdik M Arief Mansur dan Elisatris Gultom, Cyber Law Aspek Hukum Teknologi Informasi, Bandung: Refika Aditama, 2005

Edmon Makarim, Pengantar Hukum Telematika, Jakarta: PT. Raja Grafindo Persada, 2005

_____, Kompilasi Hukum Telematika, Jakarta: PT. Raja Grafindo Persada, 2004

Irawan Budhi, Jaringan Komputer, Yogyakarta: Graha Ilmu, 2005

Jasmadi, Fasilitas Internet, Yogyakarta: CV Andi Offset, 2004

M Yahya harahap, Pembahasan Permasalahan dan penerapan KUHAP, Jakarta: Sinar Grafika, 2000

Otje Salman Soemadiningrat, Teori hukum Mengingat, Mengumpulkan dan Membuka Kembali, Bandung: Refika Aditama, 2004

PAF Lamintang, Dasar-Dasar Hukum Pidana Indonesia, Bandung: PT. Citra Aditya Bakti, 1997

PAF Lamintang dan Djisman Samosir, Delik-Delik Khusus, Bandung: Tarsito, 1995 Thor, Zero Knowledge Password, Jakarta: PT Elex Media Komputindo Gramedia Kelompok Gramedia, 2008

Wirjono Prodjodikoro, Tindak-Tindak Pidana Tertentu di Indonesia, Bandung: Refika Aditama, 2003 Yusuf Kurniawan, Kriptografi, Bandung: Informatika, 2004

Peraturan Perundang – Undangan

Undang-Undang Dasar 1945

Kitab Undang-Undang Hukum Pidana (KUHP)

Kitab Undang-Undang Hukum Acara Pidana (KUHAP)

Undang-Undang Nomor 48 Tahun 2009 Tentang Kekuasaan Kehakiman

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

PP Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Permenkominfo Nomor 36 Tahun 2016 tentang Tata Cara Pendaftaran Penyelenggara Sistem Elektronik.

Internet:

http://jurnal.ubl.ac.id/index.php/PH/article/view/144