KEJAHATAN *CYBER* DALAM PERKEMBANGAN TEKNOLOGI INFORMASI BERBASIS KOMPUTER

Oleh: Nani Widya Sari
Dosen Universitas Pamulang
Jl. Surya Kencana Satu Pamulang Tangerang Selatan
Email: 02124@unpam.ac.id

Abstrak

Penelitian ini bertujuan untuk mengetahui bentuk kejahatan yang berhubungan erat dengan penggunaan teknologi informasi yang berbasis utama komputer dan jaringan telekomunikasi. disamping itu juga ingin mengetahui pengaturan hukum mengenai *cyber crime* dalam pusaran teknologi informasi berbasis komputer yang dihubungkan dengan internet. Adapun metode yang penulis gunakan dalam peneltian ini adalah metode penelitian yuridis normatif dengan mengumpulkan bahan-bahan pustaka yang terhimpun dalam data sekunder. Data sekunder di dapat dari berbagai macam sumber referensi seperti bahan hukum primer, bahan hukum sekunder dan bahan hukum tersier. Hasil penelitian menunjukkan bahwa perkembangan teknologi informasi berbasis komputer telah memunculkan kejahatan *cyber* dengan menggunakan data atau informasi ke internet. Seperti misalnya kejahatan dengan memalsukan data pada dokumen-dokumen penting. Terdapat ketentuan hukum yang mengatur mengenai kejahatan dalam teknologi informasi. Dalam beberapa Pasalnya dijelaskan mengenai kejahatan dengan menggunakan teknologi informasi berbasis internet yang disambungkan melalui komputer.
Kata kunci: *Cyber,* teknologi informasi, komputer.

Abstract

This research is purposed to recognize the forms of crime that are closely related to the use of information technology based on computers and telecommunications networks, moreover, it also wants to know the legal arrangements regarding cyber crime in the whirlwind of computer-based information technology that is connected to the internet. While the method that I use in this research is a normative juridical research method by collecting library materials collected in secondary data. Secondary data can be obtained from various reference sources such as primary legal materials, secondary legal materials and tertiary legal materials. The results showed that the development of computer-based information technology has led to cyber crime by using data or information on the internet. Such as crime by falsifying data on important documents. There are legal provisions governing crime in information technology. In some cases it is explained about crime by using internet-based information technology that is connected through a computer.
Keywords: Cyber, information technology, computer.

A. Pendahuluan

Tidak dapat dipungkiri bahwa perkembangan teknologi informasi berbasis komputer berkembang sangat pesat di tengah masyarakat. Masyarakat kemudian dimanjakan dengan perkembangan teknologi ini. Betapa tidak, untuk berbelanja masyarakat tidak perlu harus pergi ke pasar-pasar atau ke pusat perbelanjaan untuk membeli sesuatu barang yang dibutuhkan. Tinggal klik barang langsung datang. Masyarakat sangat dimudahkan dan terbantu dengan kehadiran teknologi informasi berbasis komputer.

Perkembangan teknologi di bidang komputer dewasa ini melanda hampir seluruh belahan dunia, yang diakibatkan oleh pertumbuhan ekonomi yang tinggi di dunia dan menyebabkan perkembangan dalam dunia bisnis sudah makin mengglobal. Atas dasar tersebut, seiring dengan pesatnya perkembangan dibidang teknologi informatika, telah merubah paradigma dengan hadirnya *cyber space,* yang merupakan imbas dari jaringan komputer global, termasuk di dalamnya jaringan internet.[1]

Meskipun perkembangan teknologi informasi sangat pesat, namun perkembangan yang ada tidak selamanya digunakan untuk kepentingan yang positif, namun juga sering disalahgunakan untuk hal-hal yang negatif. Sejatinya, perkembangan teknologi informasi berbasis komputer yang terhubung melalui jaringan internet sering dijadikan sebagai sarana serta media untuk melakukan kejahatan. Misalnya melakukan pencemaran nama baik terhadap seseorang atau mungkin juga transaksi bisnis prostitusi *online* yang sekarang marak diberitakan.

Tingginya perkembangan informasi dan besarnya arus *cyber* media yang sangat cepat, maka setidaknya ada dua masalah krusial yang bisa dilihat dalam hal ini. *Pertama*, persoalan *cyber crime*. Jika dianalisis lebih jauh, istilah *cyber crime* merupakan tindakan pidana kriminal yang dilakukan pada teknologi internet melalui proses penyerangan atas fasilitas umum di dalam *cyber space* maupun data pribadi yang besifat penting maupun dirahasiakan. Ia serupa petir yang meruntuhkan gaya simentris dalam kebenaran sebuah data maupun informasi. Model kejahatan tindak pidana di atas dapat dibedakan menjadi *off-line crime*, semi *on-line*, dan *cyber crime.* Tindakan ini masing-masing memiliki karakteristik tersendiri yang khas. Potret kejahatan tersebut

[1]Dwidja Priyatno, *Bunga Rampai Pembaharuan Hukum Pidana Indonesia*, (Bandung: Pustaka Reka Cipta, 2018), hal. 13.

acapkali dilakukan atas dua hal yakni motif intelektual yakni kejahatan yang dilakukan hanya untuk kepuasan sendiri, dan telah mampu merekayasa dan mengimplementasikan bidang teknologi informasi, dan yang kedua adalah motif ekonomi dimana kejahatan-kejahatan tersebut digunakan untuk mencari keuntungan pribadi dan kelompok tertentu yang merugikan orang lain secara ekonomi. *Kedua*, adalah kejahatan *cyber sabotage.* Sebuah kejahatan baru yang mulai 'dikekalkan' dengan membuat gangguan, perusakan, atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.[2]

Dua kejahatan tersebut tentu merupakan ancaman nyata bagi keselamatan ekonomi, sistem sosial dan sebagainya. Sebab dunia maya adalah dunia dimana ruang-ruang diskursif hadir tanpa batas. *Cyber* media adalah perangkat yang menggunakan gugus *the free market of ideas.* Ketika semua orang berhak berkomentar dan menelurkan gagasan tanpa batas maka disanalah kejahatan akan lahir. Sebab kebebasan akan melahirkan gaya kejahatan yang baru, dan begitupun seterusnya.[3]

Secara umum yang dimaksud dengan kejahatan komputer atau kejahatan di dunia maya *(Cybercrime)* adalah: upaya memasuki dan atau menggunakan fasilitas komputer atau jaringan komputer tanpa ijin dan dengan melawan hukum dengan atau tanpa menyebabkan perubahan dan atau kerusakan pada fasilitas komputer yang dimasuki atau digunakan tersebut. Kejahatan komputer mencakup berbagai potensi kegiatan ilegal. Umumnya, kejahatan ini dibagi menjadi dua kategori: (1) kejahatan yang menjadikan jaringan komputer dan divais secara langsung menjadi target; (2) Kejahatan yang terfasilitasi jaringan komputer atau divais, dan target utamanya adalah jaringan komputer independen atau *device*.[4]

Kejahatan yang berhubungan dengan komputer merupakan keseluruhan bentuk kejahatan yang ditujukan terhadap komputer, jaringan komputer dan para penggunanya, dan bentuk-bentuk kejahatan tradisional yang menggunakan atau dengan bantuan peralatan komputer. Kejahatan tersebut dibedakan menjadi dua kategori yakni *cybercrime* dalam pengertian sempit dan dalam pengertian luas. *Cybercrime* dalam pengertian sempit merupakan kejahatan terhadap sistem komputer, sedangkan

[2] Linda Rahmawati, *Meminimalisir Kejahatan Cyber Crime dan Cyber Sabotage di Indonesia,* detikNews, Selasa 17 Juni 2014.

[3] *Ibid.*

[4]Hj Sri Sumarwani, *Tinjauan Yuridis Pemidanaan Cybercrime Dalam Perpektif Hukum Pidana Positif*, Jurnal Pembaharuan Hukum Volume I No. 3 September-Desember 2014, hal. 288.

cybercrime dalam pengertian luas mencakup kejahatan terhadap sistem atau jaringan komputer dan kejahatan yang menggunakan sarana komputer.[5]

Cybercrime sebagai suatu masalah bukanlah hal yang mudah untuk diselesaikan. Hal ini dikarenakan c*ybercrime* sebagai suatu jenis kejahatan merupakan suatu tindakan yang dilakukan di dalam dunia yang tidak mengenal batas wilayah hukum dan kejahatan tersebut dapat terjadi tanpa perlu adanya suatu interaksi langsung antara pelaku dengan korbannya. Sehingga dapat dikatakan, bahwa ketika suatu kejahatan *cyber* terjadi, maka semua orang dari berbagai negara yang dapat masuk ke dalam dunia *cyber* dapat terlibat di dalamnya, entah itu sebagai pelaku (secara langsung atau tidak langsung), korban, ataupun hanya sebagai saksi.[6]

Cybercrime, terjadi pertama kali di Amerika Serikat pada tahun 1960-an.[7] Pada tahun 1970 di Amerika Serikat terjadi kasus manipulasi data nilai akademik mahasiswa di Brooklyn College New York, kasus penyalahgunaan komputer perusahaan untuk kepentingan karyawan, kasus pengkopian data untuk sarana kejahatan penyelundupan narkotika, kasus penipuan melalui kartu kredit. Selain itu terjadi pula kasus akses tidak sah terhadap database *security pacific* national bank yang mengakibatkan kerugian sebesar $10.2 juta US pada tahun 1978. Selanjutnya kejahatan serupa terjadi pula disejumlah negara antara lain Jerman, Australia, Inggris, Finlandia, Swedia, Austria, Jepang, Kanada, Belanda, dan Indonesia. Kejahatan tersebut menyerang terhadap harta kekayaan, kehormatan sisitem dan jaringan komputer.[8]

Menurut Kamus Bahasa Inggris-Indonesia *cyber* berarti maya, sedangkan *crime* adalah *an offence which is punishable by law* (suatu kejahatan yang dihukum oleh hukum), *illegal activity in general* (kegiatan ilegal pada umumnya), atau *a bad,*

[5]*Ibid.*

[6]Bima Guntara, *Legitimasi Penyebaran Informasi Yang Memiliki Muatan Penghinaan Dan/Atau Pencemaran Nama Baik Dalam Pasal 310 Kuhp Dan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik,* Jurnal Surya Kencana Dua: Dinamika Masalah Hukum dan Keadilan, Volume 4 Nomor 2 Desember 2017, hal. 242.

[7]Edy Junaedi Karnasudirja, 1993, Jurisprudensi Kejahatan Komputer, (Jakarta: Tanjung Agung, 1993), hal. 3. Sebagaimana dikutip oleh Hj Sri Sumarwani, *Tinjauan Yuridis Pemidanaan Cybercrime Dalam Perpektif Hukum Pidana Positif,* Jurnal Pembaharuan Hukum Volume I No. 3 September – Desember 2014.

[8]Alexander Pattipeilohi, *"Di Balik Kecanggihan Sebuah Teknologi".* Majalah Komputer dan Elektronika, 1985, hal. 42. Sebagaimana dikutip oleh Hj Sri Sumarwani, *Tinjauan Yuridis Pemidanaan Cybercrime Dalam Perpektif Hukum Pidana Positif,* Jurnal Pembaharuan Hukum Volume I No. 3 September- Desember 2014.

immoral, or dishonourable act (tidak terhormat, tidak bermoral, atau tindakan yang buruk).[9]

Di Indonesia, masalah dari *cyber crime* juga bisa dikatakan mulai diperhatikan sebagai suatu masalah yang serius. Dengan masuknya Indonesia kedalam era globalisasi, khususnya dalam hal hubungannya dengan dunia *cyber*, berbagai bidang kehidupan masyarakat Indonesia mulai mendapatkan pengaruh dari dunia *cyber* tersebut. Oleh karenanya tidaklah mengherankan bila mulai bermunculan kasus-kasus kejahatan yang berhubungan pula dengan dunia *cyber* tersebut.[10]

Sebelum adanya Undang-Undang Informasi Transaksi Elektronik (ITE), tidak ada peraturan perundang-undangan di Indonesia yang mengatur secara khusus mengenai *cybercrime*. Oleh karenanya, dalam menangani kasus-kasus yang berkaitan dengan *cybercrime* pada masa sebelum adanya Undang-Undang ITE banyak digunakan peraturan perundang-undangan yang kiranya dapat dikaitkan dengan *cybercrime*, baik itu yang berasal dari Kitab Undang-Undang Hukum Pidana (KUHP) maupun dari luar KUHP.[11] Undang-Undang ITE dapat dikatakan sebagai *cyber law* di Indonesia.[12]

Meningkatnya perkembangan teknologi informasi sudah seharusnya dapat membawa manfaat yang besar bagi manusia. Perkembangan teknologi informasi harusnya dapat membawa kebaikan bagi seluruh masyarakat dalam menunjang keberlangsungan kehidupan, baik dalam pekerjaan, bisnis bahkan pendidikan. Untuk itu, seluruh kejahatan yang menggunakan sarana teknologi informasi berbasis internet yang dihubungkan lewat komputer sudah seharusnya diakhiri dengan menerapkan hukuman yang sesuai dengan prinsip keadilan dan kepastian hukum berdasarkan undang-undang yang ada.

Negara hukum berkewajiban untuk melindungi seluruh masyarakat dari berbagai macam bentuk kejahatan yang terjadi di dunia maya atau kejahatan yang lahir

[9]Longman Group, *Longman dictionary of Contemporary English,* (Ed. VIII; England: [t.tp], 1998), hal. 155.

[10]Bima Guntara *Op cit,* hal. 243.

[11] Petrus Reinhard Golose, *Seputar Kejahatan Hacking: Teori dan Studi Kasus,* (Jakarta: Dharmaputra, 2008), hal. 43. Sebagaimana dikutip oleh Bima Guntara, *Legitimasi Penyebaran Informasi Yang Memiliki Muatan Penghinaan Dan/Atau Pencemaran Nama Baik Dalam Pasal 310 Kuhp Dan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik,* Jurnal Surya Kencana Dua: Dinamika Masalah Hukum dan Keadilan, Volume 4 Nomor 2 Desember 2017, hal. 248.

[12]Bima Guntara, *Op cit,* hal. 248.

dari dampak negatif perkembangan teknologi informasi. Bahwa setiap manusia dimanapun berada harus dilindungi oleh negara sesuai dengan harkat dan martabatnya sebagai seorang manusia. Dari itu segala bentuk kejahatan atau perbuatan-perbuatan menyimpang lainnya yang dilakukan oleh masyarakat di dunia maya yang dapat merugikan masyarakat lainnya apalagi perbuatan tersebut dapat merusak tatanan kehidupan berbangsa dan bernegara tidak bisa dibiarkan terus merajalela.

B. Rumusan Masalah

Berdasarkan uraian latar belakang masalah diatas, maka penulis dapat membuat rumusan masalah sebagai berikut:

1. Bagaimana Bentuk Kejahatan Yang Berhubungan Erat Dengan Penggunaan Teknologi Informasi Yang Berbasis Utama Komputer Dan Jaringan Telekomunikasi?
2. Bagaimana Pengaturan Hukum Mengenai *Cyber Crime* Dalam Pusaran Teknologi Informasi Berbasis Komputer yang Dihubungkan dengan Internet?

C. Metode Penelitian

Dalam penulisan karya tulis ini metode penelitian yang penulis gunakan adalah metode penelitian yuridis normatif dengan mengumpulkan bahan-bahan pustaka yang terhimpun dalam data sekunder. Data sekunder yaitu bahan pustaka yang mencakup dokumen-dokumen resmi, buku-buku perpustakaan, peraturan perundang-undangan, karya ilmiah, artikel-artikel, serta dokumen yang berkaitan dengan materi penelitian. Data sekunder di dapat dari berbagai macam sumber seperti bahan hukum primer, bahan hukum sekunder dan bahan hukum tersier.[13] Data yang di dapat lalu diolah dan dianalisis untuk menjawab persoalan yang ada.

D. Pembahasan

1. Bentuk Kejahatan Yang Berhubungan Erat Dengan Penggunaan Teknologi Informasi Yang Berbasis Utama Komputer dan Jaringan Telekomunikasi

Perkembangan globalisasi dan teknologi informasi telah membawa perubahan

[13]Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif, Suatu Tinjauan Singkat*, (Jakarta: Raja Grafindo Persada, 2011), hal. 13.

besar dalam kehidupan manusia. Teknologi Informasi menjadikan hubungan komunikasi antar manusia dan antar bangsa semakin mudah dan cepat tanpa dipengaruhi oleh ruang dan waktu. Globalisasi adalah suatu proses perubahan dinamika lingkungan global sebagai kelanjutan dari situasi yang pernah ada sebelumnya yang ditandai dengan ciri kemajuan teknologi dan informasi, menimbulkan saling ketergantungan, pengaburan terhadap batas-batas negara *(borderless).*[14]

Teknologi informasi diyakini membawa keuntungan dan kepentingan yang besar bagi negara-negara di dunia. Setidaknya ada 2 (dua) hal yang menjadikan teknologi informasi dianggap penting dalam memacu pertumbuhan ekonomi dunia. *Pertama,* teknologi informasi mendorong permintaan atas produk-produk teknologi informasi itu, seperti komputer, modem, sarana untuk membangun jaringan internet dan sebagainya. *Kedua*, memudahkan transaksi bisnis terutama bisnis keuangan di samping bisnis-bisnis umum lainnya.[15]

Selain itu, teknologi internet dapat menjadi sebuah kemajuaan sekaligus kehancuran bagi siapapun yang tidak memahaminya. Internet membawa perubahan yang sangat cepat sehingga bagi masyarakat net *(netizen)* maupun masyarakat umum diperlukan pengetahuan dan sikap bijak dalam penggunaanya supaya efek negatif Internet dapat diminimalisir. Dalam perkembangannya, kejahatan siber juga menarget dan menyerang unit-unit vital negara secara efektif dan masif. Contoh kejahatan yang terkenal karena efek dashyatnya adalah Ransomware *WannaCry*. *WannaCry* adalah sebuah serangan siber yang menyerang seluruh dunia *(worldwide cyberattack)* mulai sejak bulan Mei 2017. *WannaCry* adalah sebuah *cryptoworm ransomare* yang menyerang komputer dengan sistem operasi *Windows* dengan cara mengenkripsi data vital suatu jaringan komputer dan meminta tebusan menggunakan *Bitcoin* untuk mengembalikan data yang telah dienkripsi. Dalam satu hari penyebarannya, *WannaCry* telah menyerang lebih dari 230.000 ribu komputer di lebih dari 150 negara. Hal yang paling merugikan adalah bahwa target dari *WannaCry* merupakan informasi vital institusi publik, maka dari itu insitusi publik benar-benar dibuat geger dengan infeksi dari *WannaCry*. Selain *WannaCry*, ada kejahatan siber lain yang lebih dulu beredar dan

[14]J.A. Scholte, Globalization: A Critical Introduction, (London: Palgrave, 2000). Dalam Ineu Rahmawati, *Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Peningkatan Cyber Defense*, Jurnal Pertahanan & Bela Negara | Agustus 2017, Volume 7 Nomor 2, hal. 52.

[15]Agus Raharjo, *Cyber Crime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Cet. I; (Bandung: PT Citra Aditya Bakti, 2002), hal. 1.

sama berbahayanya, yaitu *Malware Trojan*. *Trjoan* adalah salah satu malware yang paling banyak beredar dan berbahaya di dunia. Salah satu macam *Trojan* adalah *DDoS-Patty*. *DDos-Patty* adalah *Trojan* yang tersembunyi dalam malicious program. *DDoS-Patty* masuk ke komputer kita melalui malicious program yang membawa *Trojan* dan *terinstall* didalam komputer tanpa kita sadar. Dengan ini, *DDoS-Patty* memperoleh jalan masuk ke komputer kita.[16]

Beberapa bentuk kejahatan yang berhubungan erat dengan penggunaan teknologi informasi yang berbasis utama komputer dan jaringan telekomunikasi ini, dalam beberapa literatur dan praktiknya dikelompokkan dalam beberapa bentuk, antara lain:[17]

"a) *Unauthorized Acces Computer System and Service.* Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa ijin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya."

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

"c) Data *Forgery*. Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* melalui internet."

"d) *Cyber Espionage.* Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer pihak sasaran."

"e) *Cyber Sabotage and Extortion.* Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet."

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

[16] Savirna, *Kenali Kejahatan Cyber*, detikNew, Senin 24 Juli 2017.

[17] Dikdik M.Arif Mansur & Elisatris Gultom, *Cyber Law (Aspek Hukum Teknologi Informasi)*, (Bandung: PT Refika Aditama, 2005), hal. 9.

Dalam pandangan masyarakat, maka beberapa kejahatan *cyber* yang sering di dengar adalah seperti misalnya pembajakan (*copyright* atau hak cipta intelektual), pemalsuan dan pencurian kartu kredit, pornografi, penipuan lewat email, pembobolan rekening bank, perjudian *on line*, terorisme, situs menyesatkan, menyebarkan kebencian, transaksi narkotika.

Menurut Abdul Wahid dan Mohammad Labib, pembagian jenis *cyber crime* ada 2 (dua) jenis, yaitu: kejahatan yang menggunakan teknologi informasi (TI) sebagai fasilitas dan kejahatan yang menjadikan sistem dan fasilitas teknologi informasi (TI) sebagai sasaran. Contoh jenis pertama adalah *credit card fraud, banking fraud*, pornografi, dan peredaran obat terlarang melalui internet. Sedangkan *defecting* dan *hacking* bisa digolongkan pada jenis kedua. Dalam kasus jenis pertama ini, kedudukan internet sebagai media teknologi informasi sebagai media teknologi canggih telah disalahfungsikan sebagai alat kriminalitas yang tidak hanya membahayakan masyarakat regional, tetapi juga masyarakat global.[18]

Dengan munculnya beberapa kasus kejatan siber *(cyber crime)* di Indonesia telah menjadi ancaman stabilitas keamanan dan ketertiban nasional dengan eskalatif yang cukup tinggi. Perbuatan melawan hukum *cyber* sangat tidak mudah diatasi dengan mengandalkan hukum positif konvensional, karena berbicara mengenai kejahatan itu tidak dapat dilepaskan dari 5 (lima) faktor yang saling berkaitan, yaitu pelaku kejahatan, korban kejahatan, reaksi sosial atas kejahatan dan hukum. Hukum memang menjadi instrumen penting dalam pencegahan dan penanggulangan kejahatan. Akan tetapi, untuk membuat suatu ketentuan hukum terhadap bidang hukum yang berubah sangat cepat, seperti teknologi informasi ini bukanlah hal yang mudah. Disinilah sering kali hukum (peraturan) tampak cepat menjadi usang manakala mengatur bidang yang mengalami perubahan yang cepat, sehingga situasinya seperti mengalami kekosongan hukum *(vacuum recht).* Terhadap kejahatan di internet atau *cyber crime* ini tampaknya memang terjadi kekosongan hukum.[19]

Kejahatan dalam bidang teknologi informasi memerlukan keseriusan negara untuk mengatasinya. Institusi penegak hukum mempunyai kewenangan yang utama

[18]Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime),* (Jakarta: Refika Aditama, [t.th]), hal. 131.

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

untuk mengatasi kejahatan ini. Masalah ini sangat dibutuhkan dan ditunggu oleh masyarakat. Berbagai macam bentuk kejahatan yang berhubungan erat dengan penggunaan teknologi informasi yang berbasis utama komputer dan jaringan telekomunikasi ini tentunya jika dibiarkan akan dapat mengancam kedaulatan negara. Sebab tidak tertutup kemungkinan pelaku mencuri data-data yang berhubungan dengan rahasia negara. Para pelaku dalam kejahatan yang berhubungan dengan penggunaan teknologi informasi yang berbasis utama komputer dan jaringan telekomunikasi ini memiliki kemampuan yang canggih dalam mengendalikan komputer. Pelaku dapat menyimpan atau bahkan mengirimkan informasi dalam berbagai bentuk dan jumlah yang sangat banyak ke pihak-pihak lain. Pelakunya adalah orang-orang yang menguasai penggunaan internet beserta aplikasinya. Hal-hal inilah yang sekiranya perlu diwaspadai oleh negara. Agar segala macam bentuk kejahatan dalam pusaran teknologi informasi tidak semakin berkembang dan dapat diberantas atau minimal dikurangi.

2. Pengaturan Hukum Mengenai *Cyber Crime* dalam Pusaran Teknologi Informasi Berbasis Komputer yang Dihubungkan dengan Internet

Penegakan hukum tentang *cyber crime* terutama di Indonesia sangatlah dipengaruhi oleh lima faktor yaitu undang-undang, mentalitas aparat penegak hukum, perilaku masyarakat, sarana dan kultur. Hukum tidak bisa tegak dengan sendirinya, selalu melibatkan manusia di dalamnya dan juga melibatkan tingkah laku manusia di dalamnya. Hukum juga tidak bisa tegak dengan sendirinya tanpa adanya penegak hukum. Penegak hukum tidak hanya dituntut untuk professional dan pintar dalam menerapkan norma hukum tapi juga berhadapan dengan seseorang bahkan kelompok masyarakat yang diduga melakukan kejahatan.[20]

Dalam konteks kejahatan *cyber*, maka ada pelaku yang melakukan kejahatan tersebut dalam bentuk individu ataupun juga secara berkelompok. Pelaku yang melakukan kejahatan *cyber* akan berhadapan dengan aparat hukum yang ada. Aparat hukum bekerja sesuai dengan norma-norma yang ada secara profesional. Disinilah sebenarnya peran penegak hukum untuk maksimal dalam melakukan penyidikan atas kejahatan yang terjadi dalam dunia maya. Sehingga dapat memberantas kejahatan *cyber*

[20] Jurnalis J. Hius, Jummaidi Saputra, Anhar Nasution, *Mengenal Dan Mengantisipasi Kegiatan Cybercrime Pada Aktifitas Online Sehari-Hari Dalam Pendidikan, Pemerintahan Dan Industri Dan Aspek Hukum Yang Berlaku,* Prosiding Snikom 2014. Banda Aceh, 24 Mei 2014, hal. 6.

tersebut di masyarakat. Para pelaku yang melakukan kejahatan *cyber* dapat dicegah dalam upaya menciptakan tatanan kehidupan sosial yang lebih teratur dan penuh kedamaian.

Pada kejahatan *cyber*, biasanya pelakunya adalah orang-orang yang pastinya memiliki suatu pengetahuan dan kemampuan yang sangat mumpuni dalam bidang ilmu komputer. Mereka para pelaku biasanya memahami mengenai pemograman computer secara canggih dan ahli, bahkan para pelaku bisa menganalisis kerja sistem yang ada pada komputer. Mampu menelaah celah pada sistem yang ada dan kemudian melakukan tindak kejahatan.

Secara umum proses penyidikan kejahatan *cyber crime* sama dengan proses penyidikan kejahatan konvensional lainnya. Bedanya hanya dari segi proses penangkapan pelaku kejahatan beserta koordinasi dengan pihak-pihak tertentu. Terlihat bahwa penanganan tindak kejahatan *cyber crime* sedikit rumit dibandingkan kejahatan konvensional, sebab terlebih dahulu harus berkoordinasi dengan beberapa pihak tertentu untuk mendapatkan kepastian bahwa hal tersebut benar-benar merupakan tindak kejahatan pidana atau bukan. Sementara dalam menetapkan tersangka kejahatan *cyber crime*, memiliki tingkat kesulitan yang lebih rendah dibanding kejahatan konvensional, dengan melihat barang bukti berupa nomor handphone atau alamat sosial media yang dimiliki pelaku dan tentunya dengan barang bukti tersebut maka akan tertuju secara langsung kepada pihak yang melakukan tindakan kejahatan.[21]

Dalam mengantisipasi kejahatan dalam jaringan teknologi informasi berbasis internet, pemerintah telah mengeluarkan atau membuat peraturan yang mengatur tentang kejahatan dunia maya ini. Hal ini ditandai dengan lahirnya Undang-Undang tentang Informasi dan Transaksi Elektronik (UU ITE). UU ITE ini merupakan rujukan khusus apabila terjadi kasus kejahatan *cyber*.

Lahirnya hukum ITE *(Cyberlaw)* di negara kita disebabkan adanya aspek hukum yang dilakukan oleh subjek hukum yang memanfaatkan internet mulai pada saat "*online"* hingga memasuki dunia maya. Kemudian lahirlah hukum sistem informasi, hukum informasi, dan hukum telematika.[22]

[21] A. Aco Agus , *Penanganan Kasus Cyber Crime Di Kota Makassar (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar),* Jurnal Supremasi, Volume XI Nomor 1, April 2016, hal. 26.

[22] Jawade Hafidz, *Kajian Yuridis Dalam Antisipasi Kejahatan Cyber*, Jurnal Pembaharuan Hukum Volume I No.1 Januari-April 2014, hal. 33.

Dengan demikian, untuk mencegah dan menanggulangi kejahatan *cyber*, negara sudah mengundangkan suatu undang-undang. Hal ini dapat kita lihat dalam ketentuan hukum yaitu 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**.** Dengan demikian maka payung hukum kita untuk menangani *cyber crime* adalah UU ITE tersebut diatas.

Undang-Undang Informasi dan Transaksi Elektronik dipersepsikan sebagai *cyberlaw* hingga mampu menjadi harapan untuk dapat mengatur rotasi kegiatan dan segala urusan dunia teknologi dan internet termasuk di dalamnya memberi *punishment* terhadap pelaku *cybercrime.* Mengingat bahwa *cybercrime* bisa kita simpulkan sebagai kejahatan yang menggunakan teknologi informasi sebagai fasilitas: pembajakan, pornografi, pemalsuan/ pencurian kartu kredit, penipuan lewat email *(fraud),* email spam, perjudian *online,* pencurian *account internet,* terorisme, isu sara, situs yang menyesatkan, dan sebagainya.[23]

Beberapa ketentuan pasal yang mengatur mengenai kejahatan dalam teknologi informasi berbasis internet yang disambungkan melalui komputer seperti;

a) Distribusi atau penyebaran, transmisi, dapat diaksesnya konten illegal, yang terdiri dari: 1. kesusilaan (Pasal 27 ayat (1) UU ITE); 2. perjudian (Pasal 27 ayat (2) UU ITE); 3. penghinaan atau pencemaran nama baik (Pasal 27 ayat (3) UU ITE); 4. pemerasan atau pengancaman (Pasal 27 ayat (4) UU ITE); 5. berita bohong yang menyesatkan dan merugikan konsumen (Pasal 28 ayat (1) UU ITE); 6. menimbulkan rasa kebencian berdasarkan SARA (Pasal 28 ayat (2) UU ITE); 7. mengirimkan informasi yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi (Pasal 29 UU ITE);

b) Dengan cara apapun melakukan akses illegal (Pasal 30 UU ITE).

c) Intersepsi illegal terhadap informasi atau dokumen elektronik dan sistem elektronik (Pasal 31 UU ITE).

Kemudian ada juga tindak pidana yang berhubungan dengan gangguan (interferensi); yaitu: gangguan terhadap sistem elektronik (*system interference*–Pasal 33 UU ITE).

[23] *Ibid*, hal. 39.

Kemudian juga terdapat dalam Pasal 35 nya yaitu: Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik.

Selain mengatur tindak pidana siber materil, undang-undang ITE mengatur tindak pidana siber formil, khususnya dalam bidang penyidikan. Pasal 42 undang-undang ITE mengatur bahwa penyidikan terhadap tindak pidana dalam UU ITE dilakukan berdasarkan ketentuan dalam Undang-Undang No. 8 Tahun 1981 tentang Hukum Acara Pidana (KUHAP) dan ketentuan dalam undang-undang Informasi Transaksi Elektrronik.

Pengaturan hukum *cyber* sangat dibutuhkan dalam upaya penegakan hukum atas kejahatan yang terjadi dalam perkembangan teknologi informasi. Sebab bagaimanapun *cyber crime* merupakan suatu perbuatan melawan hukum, dimana perbuatan tersebut dilakukan dengan menggunakan sarana internet dengan kecanggihan teknologi komputer. Kejahatan dunia maya atau *cyber crime* lebih cenderung aktifitasnya dengan menggunakan komputer atau jaringan internet, sehingga mempermudah orang melakukan suatu kejahatan meskipun dengan jarak yang sangat jauh sekali.

Oleh sebab itulah, dengan kecanggihan teknologi komputer yang dihubungkan dengan internet, *cyber crime* tidak terhalang oleh ruang dan waktu. Dari itulah, dalam upaya penegakan hukum khususnya dalam wilayah hukum pidana, hukum *cyber* akan menjadi dasar hukum dalam semua proses penegakan hukum atas seluruh kejahatan teknologi informasi. Bagaimanapun masyarakat harus dapat hidup dengan baik dan jauh dari perbuatan-perbuatan yang merugikan orang lain.

Tinggal sekarang bagaimana pihak-pihak terkait bersama dengan masyarakat memberantas atau mencegah terjadinya kejahatan ini dalam kehidupan sosial masyarakat. Semua ini bertujuan agar tatanan kehidupan sosial masyarakat bisa lebih baik dan jauh dari segala macam kejahatan dalam pusaran perkembangan teknologi informasi.

Semuanya berpulang kepada seluruh elemen masyarakat, apakah kita sebagai masyarakat akan terus hidup dalam kekacauan. Padahal dengan berkembangannya

teknologi informasi hendaknya dapat membawa hal-hal yang positif bagi kehidupan umat manusia. Untuk itu, mari cerdas memanfaatkan perkembangan teknologi informasi dengan mematuhi berbagai etika,norma, aturan dan hukum yang berlaku.

E. Penutup

1. Kesimpulan

a**.** Beberapa bentuk kejahatan yang berhubungan erat dengan penggunaan teknologi informasi yang berbasis utama komputer dan jaringan telekomunikasi seperti misalnya pencemaran nama baik yang dilakukan melalui media sosial berbasis internet. Kejahatan yang dilakukan dengan menyusup ke dalam suatu sistem jaringan komputer secara ilegal tidak atas sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Atau kejahatan dengan menggunakan dan atau memalsukan data atau informasi ke internet tentang suatu hal yang tidak benar, tidak pantas dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Ada juga bentuk kejahatan dalam pusaran teknologi informasi dengan menyebarkan berita-berita bohong yang tidak jelas sumbernya namun diumumkan lewat media sosial. Tujuannya untuk menjatuhkan atau membuat seseorang menjadi terhina atau merendahkan martabat dan wibawa seseorang.

b. Pengaturan hukum mengenai kejahatan *cyber* dalam pusaran teknologi informasi berbasis komputer yang dihubungkan dengan internet dapat ditemui 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**.** Dalam beberapa Pasalnya dijelaskan mengenai kejahatan dengan menggunakan teknologi informasi berbasis internet yang disambungkan melalui komputer seperti; a) Distribusi atau penyebaran, transmisi, dapat diaksesnya konten illegal, yang terdiri dari: 1. kesusilaan (Pasal 27 ayat (1) UU ITE); 2. perjudian (Pasal 27 ayat (2) UU ITE); 3. penghinaan atau pencemaran nama baik (Pasal 27 ayat (3) UU ITE); 4. pemerasan atau pengancaman (Pasal 27 ayat (4) UU ITE); 5. berita bohong yang menyesatkan dan merugikan konsumen (Pasal 28 ayat (1) UUITE); 6. menimbulkan rasa kebencian berdasarkan SARA (Pasal 28 ayat (2) UU

ITE); 7. mengirimkan informasi yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi (Pasal 29 UU ITE).

2. Saran

1. Pemerintah harus terus mensosialisasikan penggunaan teknologi informasi secara baik dan benar. Kemudian pemerintah harus memberikan sanksi hukum bagi siapa saja yang melakukan kejahatan dalam dunia maya berbasis teknologi informasi. Sebab dengan perkembangan teknologi informasi, masyarakat mesti lebih bijak dalam menggunakannya untuk hal-hal yang positif, sehingga akan lebih bermanfaat dan dapat menunjang dan membantu dalam melaksanakan berbagai macam kegiatan yang positif.

2. Aparat terkait seperti misalnya, aparat hukum yang ada, harus lebih maksimal memahami hukum *cyber*. Karena kejahatan dalam pusaran teknologi informasi terus saja berkembang dengan berbagai modus dan bentuknya. Hal ini menjadi penting agar *cyber crime* tidak semakin merajalela dan tumbuh subur dalam kehidupan masyarakat.

Daftar Pustaka

Buku

Agus Raharjo, *Cyber Crime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi* (Cet. I; Bandung: PT Citra Aditya Bakti, 2002).

Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime),* (Jakarta: Refika Aditama, [t.th]).

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

Dwidja Priyatno, *Bunga Rampai Pembaharuan Hukum Pidana Indonesia*, (Bandung: Pustaka Reka Cipta, 2018).

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

Longman Group, *Longman dictionary of Contemporary English,* (Ed. VIII; England: [t.tp], 1998).

Petrus Reinhard Golose, *Seputar Kejahatan Hacking: Teori dan Studi Kasus,* (Jakarta: Dharmaputra, 2008).

Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif, Suatu Tinjauan Singkat*, (Jakarta: Raja Grafindo Persada, 2011).

Peraturan Perundang-undangan

Undang-Undang Nomor 11 tahun 2008 tentang Informasi Transaksi Elektronik

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 8 tahun 1981 tentang Kitab Undang-Undang Hukum Acara Pidana.

Undang-Undang Nomor 1 tahun 1946 tentang Peraturan Hukum Pidana.

Jurnal/Media Massa

A. Aco Agus , *Penanganan Kasus Cyber Crime Di Kota Makassar (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar),* Jurnal Supremasi, Volume XI Nomor 1, April 2016.

Alexander Pattipeilohi, *"Di Balik Kecanggihan Sebuah Teknologi".* Majalah Komputer dan Elektronika, 1985. Sebagaimana dikutip oleh Hj Sri Sumarwani, *Tinjauan Yuridis Pemidanaan Cybercrime Dalam Perpektif Hukum Pidana Positif,* Jurnal Pembaharuan Hukum Volume I No. 3 September – Desember 2014.

Bima Guntara, *Legitimasi Penyebaran Informasi Yang Memiliki Muatan Penghinaan Dan/Atau Pencemaran Nama Baik Dalam Pasal 310 Kuhp Dan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik*, Jurnal Surya Kencana Dua: Dinamika Masalah Hukum dan Keadilan, Volume 4 Nomor 2 Desember 2017.

Edy Junaedi Karnasudirja, *Jurisprudensi Kejahatan Komputer*, (Jakarta: Tanjung Agung, 1993). Sebagaimana dikutip oleh Hj Sri Sumarwani, *Tinjauan Yuridis Pemidanaan Cybercrime Dalam Perpektif Hukum Pidana Positif,* Jurnal Pembaharuan Hukum Volume I No. 3 September-Desember 2014.

Hj Sri Sumarwani, *Tinjauan Yuridis Pemidanaan Cybercrime Dalam Perpektif Hukum Pidana Positif,* Jurnal Pembaharuan Hukum Volume I No. 3 September-Desember 2014.

J.A. Scholte, Globalization: A Critical Introduction, (London: Palgrave, 2000). Dalam Ineu Rahmawati, *Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Peningkatan Cyber Defense*, Jurnal Pertahanan & Bela Negara | Agustus 2017, Volume 7 Nomor 2.

Jurnalis J. Hius, Jummaidi Saputra, Anhar Nasution, *Mengenal Dan Mengantisipasi Kegiatan Cybercrime Pada Aktifitas Online Sehari-Hari Dalam Pendidikan, Pemerintahan Dan Industri Dan Aspek Hukum Yang Berlaku,* Prosiding Snikom 2014. Banda Aceh, 24 Mei 2014.

Jawade Hafidz, *Kajian Yuridis Dalam Antisipasi Kejahatan Cyber,* Jurnal Pembaharuan Hukum Volume I No.1 Januari –April 2014.

Linda Rahmawati, *Meminimalisir Kejahatan Cyber Crime dan Cyber Sabotage di Indonesia,* detikNews, Selasa 17 Juni 2014.

Nandang Sutrisno, *Cyberlaw: Problem dan Prospek Pengaturan Aktivitas Internet*, Jurnal Hukum. Nomor 16 Volume 8 Maret 2001.

Savirna, *Kenali Kejahatan Cyber,* detikNew, Senin 24 Juli 2017.