**PERKEMBANGAN ETIKA SIBER DAN PENGATURAN CYBERLAW DI INDONESIA**

**Luna Safitri Salsabil**

[lsafitri@unis.ac.id](mailto:lsafitri@unis.ac.id)

***Abstraksi***

*Dalam perkembangan teknologi informasi saat ini, membawa dampak perubahan struktur komunikasi yang terjadi dalam dan hal ini dapat menimbulkan dampak positif dan negatif dalam kehidupan masyarakat. Terdapat etika dalam melakukan komunikasi antar manusia begitu juga yang terjadi dalam dunia siber. Terdapat perbedaan antara etika dunia siber hal ini karena adanya perbedaan sruktur komunikasi dalam dunia siber. Selain itu juga dalam dunia siber rentan akan terjadi suatu kejahatan yang berbeda pada umumnya. Terdapat bentuk kejahatan baru yang menggunakan instrument komputer dan jaringannya dalam dunia siber, baik sebagai target kejahatan maupun sebagai alat atau sarana kejahatan (cyber crime). Pemerintah Indonesia dalam hal ini telah mengeluarkan regulasi yaitu Undang-Undang Informasi dan Transaksi Elektronik nomor 11 Tahun 2008 sebagai bentuk upaya untuk menanggulangi kejahatan tersebut. Salah satu bentuk kejahatan dunia siber adalah pencurian data atau informasi. Kasus Cambridge analytica merupakan kejahatan dunia siber. Oleh sebab perlu diteliti atau ditelaah kembali bagaimana etika dan peraturan dalam UU ITE dapat melindungi pengguna dunia siber.*

*.*

***Keywords****: Dunia Siber, Etika Siber, Kejahatan Siber*

***Abstract***

*Today, we are already In the development of information technology, the impact of changes in communication structure that occurs in and this can lead to positive and negative impacts in society. There is has an ethics in communication between people as well as in the cyberspace. There is have a difference between this cyberspace ethic because of the difference in culture in the cyberspace. In addition also in the cyberspace vulnerable will occur a crime. There is a new form of crime that using a computer as instruments and networks in the cyberspace, either as a target of crime or as a tool or means of crime (cybercrime). The Government of Indonesia in this matter has issued a regulation that is the Law of Information and Electronic Transactions number 11 of 2008 as a form of effort to prevent the crime* *One form of cyber crime types is the theft of data or information. The case of Cambridge analytica is a cyber-world crime. It needs to be examined or reviewed again how the ethics and regulations in the Law on ITE can protect the world of cyber users.*

***Keywords****: cyberspace, cyberethics, cybercrime*

**Pendahuluan**

Etika merupakan salah satu cabang dari ilmu filsafat yang berhubungan dengan apa yang dianggap benar atau salah. Definisi etika telah banyak diusulkan, seperti "kode moral profesi tertentu", "standar perilaku profesi tertentu", "kesepakatan di antara orang-orang untuk melakukan yang benar dan untuk menghindari kesalahan". Berdasarkan Kamus Collegiate Webster, bahwa etika merupakan “disiplin yang berurusan dengan apa yang baik dan buruk dan dengan kewajiban dan kewajiban moral”. Selain itu juga menurut Dengan kata yang lebih sederhana, itu adalah studi tentang apa yang benar untuk dilakukan dalam situasi tertentu, dan apa yang harus kita lakukan.

Penting untuk dicatat bahwa apa yang tidak etis belum tentu ilegal. Dalam kehidupan kita sehari-hari, banyak individu dan organisasi menghadapi masalah etika yang umum. Misalnya, masalah perusahaan yang secara sah memantau e-mail karyawan adalah masalah yang sangat kontroversial. Secara sederhana, etika adalah studi tentang apa yang benar untuk dilakukan dalam situasi tertentu, dan apa yang harus kita lakukan. Perlu diperhatikan adalah bahwa etika tidak sama dengan aturan. Terkadang apa yang tidak etis belum tentu melanggar hukum, begitu juga sebaliknya. Dalam hukum, bahwa etika merupakan salah satu sumber hukum materiil. Berarti, bahwa etika yang berlaku dalam masyarakat dapat dijadikan suatu hukum yang berlaku bagi masyarakat secara luas.

Dalam perkembangan teknologi komunikasi dan informasi, salah satu adanya ditemukan dan dikembangkanya Internet. Adanya internet saat ini membawa dampak tidak hanya berdampak di bidang komunikasi akan tetapi berdampak ke berbagai aspek kehidupan dalam masyarakat. Adanya internet tersebut telah mengubah cara kita melakukan bisnis, berkomunikasi, menghibur, mengambil informasi, dan bahkan mendidik diri kita sendiri. Dalam internet kita terhubung dalam suatu dunia siber. Di dalam dunia siber tersebut memungkinkan setiap orang dapat melakukan interaksi dengan berbagai orang tanpa memperhatikan lokasi geografis dan waktu serta dapat melakukan suatu pertukaran besar dan sumber data, informasi dan perangkat lunak.

Dalam kehidupan bermasyarakat pada umumnya, bahwa etika mempunyai peranan sebagai pengatur tingkah laku manusia untuk bersosialisasi. Begitupun dalam melakukan kegiatan dalam dunia siber. Terdapat etika-etika tertentu apa yang boleh dan tidak boleh dilakukan dalam dunia siber. Hal ini tidak terlepas bahwa dunia siber merupakan dunia luas tanpa batas. Semua orang dapat dengan mudah untuk mengakses keluar masuk dalam dunia siber. Selain itu juga dalam dunia siber tidak ada halangan ataupun batasan untuk setiap orang dapat berkomunikasi dan berinteraksi kapan saja dan dimana saja.

Dunia siber merupakan dunia virtual, sehingga dapat menghubungkan setiap orang dimana saja dan kapan saja dalam satu wadah dunia siber. Oleh sebab itu diperlukan suatu etika siber dalam melakukan kegiatan di dunia siber. Terdapat suatu pokok permasalahan dari etika siber yaitu adanya perilaku manusia yang tidak berfungsi. Dalam dunia siber permasalahan etika dan hukum seperti pencurian, pembajakan, peretasan, pelecehan, kesalahan informasi, pencabulan, plagiarisme, dan virus. Dalam etika siber yang dibahas adalah mengenai perilaku pihak pengguna dunia siber. Bagaimana seorang pengguna bertingkah laku dalam dunia siber.

Pada awal tahun 2018, bahwa sempat heboh mengenai kasus Cambridge analytica. Dalam kasus tersebut telah terjadi pencurian data pribadi melalui facebook dengan menggunakan kuis atau kuisoner yang berkedok akademis. Tindakan pengambilan data pribadi tersebut tidak diketahui oleh pengguna dan tentu saja hal ini dapat merugikan pengguna dunia siber. Tindakan pencurian data tersebut merupakan tindakan yang dilaran dalam etika siber. Tindakan tersebut juga dapat dikategorikan sebagai bentuk kejahatan dalam dunia siber (*cyber crime*). Oleh sebab itu perlu ditelaah mengenai bagaimana suatu pendekatan atau teori mengenai hubungan antara hukum dan teknologi. Hal ini agar suatu hukum dapat mengatur tata cara seseorang dalam hal penggunaan teknologi dalam dunia siber.

**Tinjauan Pustaka**

**Pendekatan dan Teori**

1. Teori Instrumental

Dalam teori instrumental, bahwa ““teori ini melihat bahwa suatu teknologi adalah teknologi (*technology is technology*), yaitu alat atau instrumen yang dikembangkan secara rasional untuk memenuhi kebutuhan tertentu. Teknologi dikembangkan dengan prinsip-prinsip itu, teknologi menghadirkan atau memberikan pilihan-pilihan dan kebutuhan- kebutuhan yang rasional bagi masyarakat. Oleh karena itu, teknologi bersifat netral (tidak bersifat baik atau buruk) dan terpisah dari proses ekonomi, politik, sosial dan budaya. Produktifitasnya dapat diukur secara objektif, terlepas dari budaya, sehingga teknologi dapat dialihkan dari suatu masyarakat lain, atau dengan kata lain teknologi dapat diterapkan secara universal. Dalam hal ini terjadi suatu penyalahgunaan teknologi, teori istrumental melihat bahwa *guns don’t kill people-people kill people*. Pihak yang harus dipersalahkan ialah orang yang menyalahgunakan teknologi, dan bukan teknologi itu sendiri”. pendapat ini memperlihatkan bahwa teknologi adalah suatu benda yang tidak memiliki kesadaran dan stagnan.

1. Teori Substantif

Berbeda dengan teori instrumental, ““teori substansif menjelaskan bahwa teknologi adalah sesuatu yang tidak netral karena teknologi berkaitan erat dengan kepentingan dan kesadaran dari subjek yang membuat teknologi yang dimaksud””,”“sejarah perkembangan teknologi komputer dan internet dimaksudkan untuk memenuhi kebutuhan perang. Oleh karena itu teknologi dapat menjadi sesuatu alat yang berbahaya karena pembuat teknologi dapat mengontrol atau mendominasi orang tau masyarakat yang mengunakan teknologi tersebut melalui teknologi yang dibuatnya. Lebih dari itu, teknologi memberi dampak bagi masyarakat baik yang sesuai dengan maupun diluar tujuan pembuatan teknologi. Teknologi telah membatasi kebebasan manusia karena manusia sesemakin tergantung dengan teknologi, dan teknologi bukanlah manusia yang memiliki kebebasan atau makhluk otonom. Penganut teori substansif juga melihat bahwa dibalik rantai produksi, distribusi, dan konsumsi teknologi, ada struktural sosial yang kompleks. Kekompleksan struktural sosial ini tidak dilihat oleh teori instrumental. Kedua teori tersebut dapat diterapkan dalam pembuatan kebijakan dan regulasi. Teori instrumentalis memberikan pendekatan yang konservatif, kaku dan melihat ke belakang (*backward-looking*) dalam pembentukan kebijakan atau regulasi. Pendekatan ini disebut sebagai pendekatan teknologi adalah hukum (*technology is law*)”. Teori “substantif memberikan pendekatan yang fleksibel, liberal, dan melihat ke depan (*forward-looking*) dalam pembentukan kebijakan atau regulasi. Pendakatan ini disebut sebagai pendekatan hukum adalah teknologi (*law is technology*).

1. Pendekatan Sintesa Teori Hukum dan Teknologi

Pada tahun 2007”, seorang peneliti yaitu Cockfiled dan Pridmore mengajukan suatu sintesa terhadap teori *mainstream* hukum dan teknologi yang berkembang pada saat itu (teori substansif dan teori teori instrumental). Mereka menyadari bahwa baik teori substansif maupun “teori instrumental memiliki kelebihan dan kekuranganya masing-masing. Oleh sebab itu mereka mengajukan suatu kerangka berpikir yang dapat digunakan oleh regulator dalam menbentuk regulasi atau hukum dengan mengunakan kedua teori tersebut melalui 2 tahapan analisa sebagai berikut:”

“Tahap pertama, bahwa pembuat regulasi harus menentukan apakah perkembangan suatu teknologi telah menggangu atau merusak kepentingan atau nilai yang telah diatur oleh hukum yang ada. Hal ini dilakukan dengan mengidentifikasi kepentingan yang terkena dampak perkembangan teknologi tersebut dengan menggunakan hukum serta doktrin-doktrin hukum yang telah ada dan menilai apakah kepentingan tersebut telah benar terganggu akibat perkembangan teknologi yang dimaksud.”" “Dalam tahap ini digunakan teori instrumentalis yang menggunakan pendekatan *backward looking* yaitu melihat bahwa hukum yang telah ada cukup untuk menyesuaikan dirinya dengan perkembangan teknologi. Apabila dari hasil analisa di atas pembuat regulasi meyakini bahwa kepentingan atau nilai yang telah dilindungi hukum yang tidak terngangu maka pembuat regulasi tidak perlu membentuk regulasi yang baru untuk menanggapi perkembangan teknologi yang dikhawartikan itu. Akan tetapi, apabila dari hasil analisa regulator meyakini bahwa kepentingan yang dimaksud ternggangu akibat perkembangan teknologi itu, pembuat regulasi perlu melakukan tahap kedua yaitu memeriksa dengan cermat ruang lingkup teknologi yang berubah itu dan dampak yang mungkin ditimbulkan oleh teknologi tesebut terhadap kepentingan atau nilai yang telah diatur hukum yang ada dan membentuk regulasi untuk melindungi kepentingan atau nilai itu, dengan tetap diusahakan sedapat mungkin selaras dengan hukum yang telah ada.”

“Pada tahap kedua diterapkan teori substansif dengan pendekatan “melihat kedepan (*looking forward*) artinya pembuat regulasi harus membentuk regulasi yang baru untuk melindungi kepentingan yang terganggu akibat perkembangn teknologi. Pembentukan regulasi dilakukan dengan cermat dengan mempertimbangkan” teknologi yang berkembang, hukum yang telah ada, kepentingan atau nilai yang telah dan akan dilindungi; dan hukum yang akan diperlukan.

**Pembahasan**

**Dunia Siber**

Dunia siber merupakan dunia virtual yang berbeda dengan dunia nyata yang kita berada saat ini. Dunia siber terbentuk dari hasil penyatuan antara manusia sebagai user dengan komputer sebagai sarana dan jaringan sebagai penghubung. Perkembangan dunia siber merupakan perkembangan dari dunia teknologi informasi dan komunikasi. Menurut koops (2006), bahwa gabungan dari teknologi komputer, telekomunikasi, serta jaringan komputer dan telekomunikasi akan membentuk suatu teknologi informasi dan komunikasi.”

“Dalam perkembangan teknologi informasi dan komunikasi, bahwa internet tersendiri memiliki arti yang luas. Ada banyak kemungkinan untuk membagi internet sendiri menjadi berbagai "subdivisi". Bagi kebanyakan orang internet adalah sinonim untuk World Wide Web (WWW), yang mereka lihat di browser mereka. Untuk waktu yang lama, WWW hanya berbasis teks tetapi pada tahun-tahun terakhir juga elemen audio dan video biasanya ada di banyak situs web. Pengguna dapat menjelajah dari satu situs ke situs lain, dengan kata lain dia "berselancar" di web dan dapat mengkonsumsi banyak sekali animasi, video, aliran audio yang membuat dunia siber lebih realistis.”

Penggunaan internet lainnya yang lengkap adalah game online. Tidak ada penggunaan lain dari dunia maya yang lebih akurat dalam memenuhi metafora dunia siber. Orang-orang diwakili atau membuat kepribadian yang baru dalam game online oleh avatar dan dapat berkomunikasi dan berinteraksi dengan pemain lain dan "hidup" di dunia online buatan. Realisasi yang lebih abstrak dari dunia siber tetapi yang paling rentan adalah komunikasi mesin-mesin eksklusif. Contohnya adalah bagaimana komunikasi server yang dimiliki oleh perusahaan kartu kredit dan lembaga perbankan, yang mentransfer setiap hari informasi akun pelanggan yang tak terhitung jumlahnya. Penanganan data sensitif seperti itu membutuhkan upaya keamanan yang tinggi.

“Dunia siber ini mempunyai karakteristik yang berbeda dengan dunia riil. Karekteristik tersebut dijelaskan oleh Dysson (1994 sebagai berikut:

1. Beroperasi secara virtual
2. Dunia siber (dunia maya) selalu berubah dengan cepat
3. Dunia siber tidak mengenal batas teritorial (borderless)
4. Orang yang hidup dalam dunia siber dapat melakukan aktivitasnya tanpa harus  menunjukkan identitas aslinya (anonim).
5. Informasi di dalamnya bersifat publik.”

Berdasarkan hal tersebut bahwa terdapat dua bentuk dari dunia maya. Bentuk pertama adalah dunia maya sebagai realitas virtual. Dimana suatu lingkungan dunia maya 3-D manusia (avatar) dapat 'masuk' dan 'bergerak melalui', berinteraksi dengan komputer dan manusia lainnya, seperti yang digambarkan dalam film seperti *The Lawmower Man* dan *Disclosure*. Bentuk lain, kita memiliki dunia jaringan komputer, tetapi lebih bermanfaat, terhubung melalui kabel dan router (mirip dengan koneksi telepon) yang memungkinkan kita untuk berkomunikasi, menyimpan dan mengambil informasi. Sejauh ini yang terbesar dan paling terkenal adalah Internet yang awalnya digunakan untuk email, ftp (transfer file), papan buletin dan newsgroup, dan telepon internet (akses komputer jarak jauh), dan sekarang bahkan lebih dari nama rumah tangga milik Dunia Wide Web, yang memungkinkan navigasi jaringan bebas hambatan dan sederhana. Memacu dunia maya kedua ini meliputi tidak hanya koneksi antar komputer, tetapi juga peramban dan perangkat lunak email yang mentransmisikan informasi, ditambah ruang internal microchip dan teknologi penyimpanan elektronik lainnya, yaitu tempat di mana informasi sebenarnya berada.

**Etika Siber**

Etika adalah bidang studi yang berkaitan dengan mempelajari apa yang benar dan salah, dan baik dari yang buruk. Etika dapat menganalisis moralitas perilaku manusia, kebijakan, hukum dan struktur sosial. Para ahli etika mencoba untuk membenarkan penilaian moral mereka dengan mengacu pada prinsip-prinsip etika dari teori-teori yang mencoba untuk menangkap intuisi moral kita tentang apa yang benar dan salah. Dua pendekatan teoritis yang paling umum dalam etika konsukuensialisme dan deontologi. Pendekatan konsekuensialisme mengasumsikan bahwa tindakan yang salah sejauh bahwa mereka memiliki konsekuensi buruk, sedangkan pendekatan deontologis menganggap bahwa orang memiliki kewajiban moral yang ada secara independen dari setiap konsekuensi baik atau buruk yang mungkin memiliki tindakan mereka.

“Seiring dengan kehadiran internet dan layanannya, maka terbentuk satu komunitas dunia siber yang berdiri secara bebas, menembus batasan ruang dan waktu yang ada, sehingga dengan kata lain, internet adalah jalan terbukanya penyatuan komunikasi manusia di dunia. Ruang lingkup internet yang tak terbatas, membuat masing-masing pihak yang terlibat di dalamnya harus ekstra hati-hati dalam berinteraksi. Hingga saat ini, belum ada aturan tertulis universal yang berlaku untuk pengguna dunia siber di seluruh belahan dunia. Kecuali adanya netiket, maka saat ini semua netter bebas berinteraksi dengan segala implikasinya di dalam internet, salah satu implikasi negatifnya adalah kemunculan kejahatan cyber yang bermula dari diabaikannya nilai-nilai etik dalam dunia maya (*cyber ethic*)”.”

Etika siber merupakan suatu aturan yang “tidak tertulis yang menjadi aturan main bagi pengguna dunia siber di seluruh dunia. Filosofi berinteraksi dalam dunia maya adalah berinteraksi dengan kemungkinan terbesar tanpa pernah bertemu fisik secara langsung.” Hal ini karena dalam dunia siber komunikasi dan interaksi dilakukan secara virtual semata. Dalam suatu “interaksi itu tentu ada nilai-nilai yang harus dihargai menyangkut karya cipta orang lain yang dipublikasikan melalui internet. Untuk itulah maka cyber ethic menjadi hal yang penting untuk dikembangkan.”

Permasalahan-permasalahan menyangkut etika yang timbul dalam dunia siber diantaranya adalah menyangkut:

1. Privasi;
2. Akurasi;
3. Properti (Kepemilikan); dan
4. Akses.

Masalah privasi adalah sebagai area terpenting di mana kepentingan mereka perlu dilindungi. Privasi telah lama dianggap "hak untuk dibiarkan sendiri". Privasi pada dasarnya adalah tentang perlindungan dari intrusi dan pengumpulan informasi oleh orang lain. Biasanya, itu telah didefinisikan dalam hal kemampuan individu untuk secara pribadi mengendalikan informasi tentang diri mereka sendiri. Tetapi membutuhkan individu untuk mengendalikan informasi mereka sendiri akan sangat membatasi apa yang bersifat pribadi.

Akurasi atau keakuratan adalah mengenai kebenaran informasi sangat penting bagi masyarakat karena komputer mendominasi dalam aktivitas pencatatan perusahaan. Ketika catatan dimasukkan secara salah, siapa yang harus bertanggung jawab. Salah satu masalah paling kompleks yang kita hadapi sebagai masyarakat adalah masalah hak kekayaan intelektual. Ada kekhawatiran ekonomi dan etika yang besar seputar hak-hak ini; kekhawatiran seputar atribut-atribut khusus dari informasi itu sendiri dan sarana-sarana yang dengannya ia ditransmisikan. Setiap barang informasi bisa sangat mahal untuk diproduksi dalam contoh pertama. Namun, begitu diproduksi, informasi itu memiliki kualitas ilusif yang mudah untuk direproduksi dan dibagikan kepada orang lain. Selain itu, replikasi ini dapat terjadi tanpa merusak yang asli. Hal ini membuat informasi sulit dijaga karena, tidak seperti properti nyata, ia menjadi komunikatif dan sulit untuk menyimpannya untuk diri sendiri. Bahkan sulit untuk mendapatkan penggantian yang sesuai ketika orang lain menggunakan informasi Anda.

Aksesbilitas adalah menyangkut informasi atau kemampuan untuk memperoleh data, menjadi semakin penting. Apakah pengguna informasi harus terlebih dahulu mendapatkan kemampuan fisik untuk mengakses sumber informasi online, yang secara luas berarti mereka harus mengakses sistem komputasi. Kedua dan yang lebih penting, mereka kemudian harus mendapatkan akses ke informasi itu sendiri. Dalam pengertian ini, masalah akses terkait erat dengan properti.

**Pembahasan**

**Hukum Siber (*Cyberlaw*) dan Kejahatan Siber (*Cybercrime*)**

Penggunaan internet saat ini sudah mempengaruhi berbagai aspek kehidupan manusia. Tidak dapat dipungkiri bahwa teknologi informasi dan komunikasi menjadi hal yang penting di era globalisasi. Kondisi tersebut dapat menjadikannya bahwa saat ini kita sudah memasuki dusun global (*global village*) atau dunia siber yang dalam hal ini diisi oleh berbagai warga jaringan (netizen). Kemajuan dan perkembangan teknologi informasi dan komunikasi pada akhirnya mengubah tatanan organisasi dan hubungan sosial kemasyarakatan. Perkembangan tersebut disatu sisi membawa kemudahan bagi manusia untuk menggunakannya tapi disisi lain ada berbagai masalah yang muncul dari perkembangan tersebut. Dalam hal ini perlu adanya suatu aturan atau hukum yang dapat mengatur atau mengontrol tindakan pengguna internet.

Hukum siber adalah istilah umum yang mengacu pada semua aspek hukum dan peraturan yang berlaku dalam dunia siber atau internet. “Cyberlaw adalah aspek hukum yang ruang lingkupnya meliputi setiap aspek yang berhubungan dengan orang perorangan atau subyek hukum yang menggunakan dan memanfaatkan teknologi internet yang dimulai pada saat mulai online dan memasuki dunia cyber atau maya. Cyberlaw sendiri merupakan istilah yang berasal dari Cyberspace Law.”

Dalam masyarakat hukum dapat dijadikan sebagai alat untuk memantau, mengendalikan dan mengatur masyarakat (*law is a tool of social engineering*). Fungsi dari hukum selain sebagai sarana mengatur dapat juga sebagai sarana mencegah. Hukum siber akan menjadi dasar hukum dari penegakan hukum dari kejahatan yang terjadi didunia siber. Selain itu juga sebagai alat pengontrol dari tindakan pengguna internet.

Secara umum istilah kejahatan siber dapat dianalisis menjadi dua kategori dan didefinisikan sebagai berikut:

1. “Kejahatan dunia siber dalam arti sempit (kejahatan komputer): Perilaku ilegal apa pun yang diarahkan melalui operasi elektronik yang menargetkan keamanan sistem komputer dan data yang diproses oleh pengguna.”
2. “Kejahatan dunia maya dalam arti yang lebih luas (kejahatan yang berhubungan dengan komputer): Setiap perilaku ilegal yang dilakukan melalui, atau terkait dengan, sistem komputer atau jaringan, termasuk kejahatan seperti kepemilikan ilegal dan/atau menawarkan atau mendistribusikan informasi melalui sistem komputer atau jaringan.”

“Kejahatan di dunia siber “memiliki karakter yang khusus dibandingkan kejahatan konvensional, yaitu antara lain:

1. Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis tersebut terjadi di ruang/wilayah siber (cyberspace), sehingga tidak dapat dipastikan yurisdiksi hukum negara mana yang berlaku terhadapnya;
2. Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang bisa terhubung dengan jaringan telekomunikasi dan/atau internet;
3. Perbuatan tersebut mengakibatkan kerugian materil maupun immateril (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan kejahatan konvensional;
4. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya; dan
5. Perbuatan tersebut seringkali dilakukan secara transnasional/melintasi batas negara”.”

Dalam dunia siber kejahatan yang terjadi sangat berhubungan erat dengan penggunaan teknologi yang berbasis utama komputer dan jaringan telekomunikasi ini dalam beberapa literatur dan prakteknya dikelompokan dalam beberapa bentuk, antara lain:

1. Unauthorized Access to Computer System and Service  
   Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan (cracker) melakukannya dengan maksud untuk menyabotase ataupun pencurian informasi penting dan rahasia. Namun begitu, ada juga yang melakukan hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Kejahatan ini semakin marak dengan berkembangnya teknologi internet/intranet.
2. Ilegal Contents

Merupakan kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Sebagai contohnya adalah pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau harga diri pihak lain, hal-hal yang berhubungan dengan pornografi atau pemuatan suatu informasi yang merupakan rahasia negara, agitasi dan propaganda untuk melawan pemerintahan yang sah, dan sebagainya.

1. Data Forgery

Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai scriptless document melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen e-commerce dengan membuat seolah-olah terjadi "salah ketik" yang pada akhirnya akan menguntungkan pelaku.

1. Cyber Espionage

Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (computer network system) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu sistem yang computerized.

1. 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. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu logic bomb, virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku. Dalam beberapa kasus setelah hal tersebut terjadi, maka pelaku kejahatan tersebut menawarkan diri kepada korban untuk memperbaiki data, program komputer atau sistem jaringan komputer yang telah disabotase tersebut, tentunya dengan bayaran tertentu. Kejahatan ini sering disebut sebagai cyber-terrorism.

1. Offense against Intellectual Property

Kejahatan ini ditujukan terhadap Hak atas Kekayaan Intelektual yang dimiliki pihak lain di internet. Sebagai contoh adalah peniruan tampilan pada web page suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.

1. Infringements of Privacy

Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara computerized, yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materil maupun immateril, seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.

Menurut Ari Juliano Gema (2013) ada beberapa langkah yang dapat dilakukan oleh setiap negara dalam menanggulangi atau mencegah kejahatan dunia siber diantaranya adalah:

1. Melakukan modernisasi hukum pidana nasional beserta hukum acaranya, yang diselaraskan dengan konvensi internasional yang terkait dengan kejahatan tersebut;
2. Meningkatkan sistem pengamanan jaringan komputer nasional sesuai standar internasional
3. Meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yang berhubungan dengan cybercrime;
4. Meningkatkan kesadaran warga negara mengenai masalah cybercrime serta pentingnya mencegah kejahatan tersebut terjadi; dan
5. Meningkatkan kerjasama antar negara, baik bilateral, regional maupun multilateral, dalam upaya penanganan cybercrime, antara lain melalui perjanjian ekstradisi dan mutual assistance treaties.

Terdapat tiga pendekatan untuk mempertahankan keamanan di cyberspace, pertama adalah pendekatan teknologi, kedua pendekatan sosial budaya-etika, dan ketiga pendekatan hukum. Untuk mengatasi keamanan gangguan pendekatan teknologi sifatnya mutlak dilakukan, sebab tanpa suatu pengamanan jaringan akan sangat mudah disusupi, diintersepsi, atau diakses secara ilegal dan tanpa hak Dalam ruang cyber pelaku pelanggaran seringkali menjadi sulit dijerat karena hukum dan pengadilan Indonesia. Hal ini disebabkan karena karakteristik dunia siber yang luas. Oleh sebab itu Indonesia tidak memiliki yurisdiksi terhadap pelaku dan perbuatan hukum yang terjadi, mengingat pelanggaran hukum bersifat transnasional.

Kegiatan melalui ruang siber (cyber space), meskipun bersifat virtual dapat dikategorikan sebagai tindakan atau perbuatan hukum yang nyata. Secara yuridis kegiatan pada ruang siber tidak dapat didekati dengan ukuran dan kualifikasi hukum konvensional atau pada umumnya. Hal ini disebabkan akan terlalu banyak kesulitan dan hal yang lolos dari pemberlakuan hukum. Kegiatan dalam ruang siber adalah kegiatan virtual yang berdampak sangat nyata meskipun alat buktinya bersifat elektronik. Untuk mengatasi gangguan keamanan dalam penyelenggaraan sistem secara elektronik, pendekatan hukum bersifat mutlak, karena tanpa kepastian hukum, persoalan pemanfaatan teknologi informasi menjadi tidak optimal

**Pengaturan atau Regulasi Hukum Siber di Indonesia**

Kehadiran undang-undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Ekonomi (UU ITE) merupakan usaha pemerintah Indonesia untuk melindungi baik masyarakat selaku konsumen jasa maupun pelaku industri dalam mengembangkan inovasi produk layanannya, selain itu diharapkan dapat lebih mendorong pengembangan penggunaan teknologi secara lebih meluas serta sekaligus dapat memberikan keamanan serta kepastian hukum dalam seluruh kegiatan transaksi. Dalam kaitannya dengan transaksi keuangan perbankan, sebagai undang- undang yang menjadi payung bagi kegiatan- kegiatan bank terkait dengan media elektronik termasuk mengenai kegiatan transfer dana secara elektronik, maka keberadaan UU ITE dalam menunjang sistem kelancaran pembayaran menjadi sangat penting dan sangat besar kontribusinya.

Dalam Undang-Undang Informasi dan Transaksi Elektronik materi yang mangatur dapat dikelompokkan menjadi dua bagian besar yaitu pengaturan mengenai informasi dan transaksi elektronik dan pengaturan mengenai perbuatan yang dilarang (*cybercrime*). Ketentuan *cybercrime* dalam Undang-Undang Informasi dan Transaksi Elektronik mengacu kepada *European Union Convention on Cybercrime* (CoC) yang merupakan instrumen internasional yang digunakan oleh banyak Negara.

Beberapa aspek penting yang terkait dengan aspek pidana yang perlu diatur secara jelas antara lain :

1. Tanggung jawab penyelenggara sistem elektronik, perlu dilakukan pembatasan atau limitasi atas tanggung kawab sehingga tanggung jawab peneyelenggara tidak melampau kewajaran;
2. Informasi elektronik dan tanda tangan yang dihasil oleh suatu sistem informasi, termasuk print out-nya harus dapat menjadi alat bukti dipengadilan;
3. Perlindungan hukum terhadap bank sentral dan lembaga perbankan/keungan, penerbit kartu kredit/kartu pembayaran dan lembaga keungan lainnya dari kemungkinan adanya gangguan dan ancaman kejahatan elektronik;
4. Ancaman pidana yang bersifat deteren terhadap tindak kejahatan elektronik (Cybercime), sehingga dapat memberikan perlindungan terhadap integritas sistem dan nilai investasi yang telah dibangun dengan alokasi sumber daya yang cukup besar.

**Kesimpulan**

Dunia siber memiliki karakteristik yang berbeda dengan dunia nyata. Akan tetapi bentuk dan kegiatan saat ini semakin menyatu dan tidak terpisahkan antara kegiatan dalam dunia nyata atau dunia siber. Perkembangan teknologi informasi dan komunikasi saat ini memudahkan setiap orang untuk mengakses dunia siber kapan saja dan dimana saja. Hal ini menyebabkan bahwa dunia siber semakin menjadi bagian kehidupan manusia dalam berbagai hal.

Dunia siber merupakan bentuk virtual dari dunia nyata. Dalam dunia siber perlu ada suatu satu cara untuk pengaturan seorang pengguna internet agar dapat menjalankan aktifitasnya dengan baik di dunia siber. Dalam hal ini adalah perlu adanya suatu etika siber. Etika siber berbeda dengan Hukum siber. Etika siber tidak perlu diatur secara tertulis melainkan sudah menjadi kebiasaan berbeda dengan hukum siber yang berbentuk tertulis dan mengatur dalam dunia siber.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Ekonomi (UU ITE) merupakan payung hukum Negara kita untuk mengantisipasi *cybercrime* yang dipersepsikan sebagai *cyberlaw* dan menjadi tonggak untuk dapat mengatur kebijakan dan kegiatan serta segala urusan dunia teknologi dan internet termasuk di dalamnya memberi *punishment* terhadap pelaku *cybercrime*.

Penegakan hukum *cybercrime* cukup menyulitkan yurisdiksi hukum tapi bukan berarti tidak bisa ditangani ketika bukti itu ada. Alasan sulitnya adalah; pertama, kegiatan dunia cyber tidak dibatasi oleh teritorial Negara, Kedua, Kegiatan dunia cyber relatif tidak berwujud hingga secara hukum tradisional kadang sulit untuk menemukan bukti yang dapat disebut pembuktian karena data elektronik relatif mudah untuk diubah, disadap, dipalsukan dan dikirimkan ke seluruh belahan dunia dalam hitungan detik.

Demikian juga dengan apabila ada kejahatan dunia siber, pencurian *bandwidth, carding, typosit*, dan sebagainya apakah memungkinkan menghadirkan alat bukti dalam konteks *cyberspace. Hardware* hanya alat yang belum tentu bisa menjamin kepastian yurisdis dan ketetapan bukti hukum yang pasti.

**Daftar Pustaka**

Budhijanto, Danrivanto. 2017. Revolusi Cyberlaw Indonesia (Pembaruan dan Revisi UU ITE 2016), Bandung: Refika Aditama,

Hafidz, Jaweda. 2014. Kajian Yuridis dalam antisipasi kejahatan Cyber, Jurnal Pembaharuan Hukum, Volume I No. 1, April, 2014

Mansur, M Arief. 2009. *Cyberlaw,* aspek hukum teknologi informasi*,* Bandung: Refika Aditama.

Koloay, Renny N.S. Perkembangan hukum Indonesia berkenaan dengan teknologi informasi dan komunikasi, Jurnal Hukum Unsrat Vol 22, No. 5, Januari 2016.

Koops, Bert-Jaap. 2009. *Should ICT Regulation be Technology-Netral,* IT-Law Series Vol 9. The Hague. T.M.C Accer Press.

Senjaya, Sasa Djuarsa. 2007. Teori Komunikasi. Jakarta: Universitas Terbuka.

Sitompul, Josua. 2012. *Cyberspace, Cybercrimes, Cyberlaw,* Tinjauan Aspek hukum pidana, Jakarta: Tatanusa.

Sobur, Alex. 2014. *Komunikasi Naratif: Paradigma, Analisis, dan Aplikasi*, Bandung: Rosda.