PROSIDING SEMINAR NASIONAL LP2M UNM - 2019
"Peran Penelitian dalam Menunjang Percepatan Pembangunan Berkelanjutan di Indonesia"
ISBN: 978-623-7496-14-4

Penyelesaian Kasus Kejahatan Internet (Cybercrime) dalam Perspektif UU ITE No.11 TAHUN 2008 dan UU No.19 Tahun 2016

Hamsu Abdul Gani[1], Andika Wahyudi Gani[2]
[1]Fakultas Teknik, Universitas Negeri Makassar
[2]Fakultas Ilmu Sosial, Universitas Negeri Makassar
E-mail: hamsuabdulgani@yahoo.com

Abstrak. Penelitian ini mendeskripsikan tentang bagaimana penyelesaian kasus pidana tertentu yang terjadi internet atau cybercrime dalam perspektif Undang-Undang (UU) ITE no. 11 tahun 2008 dan UU ITE no. 19 tahun 2016 di Kota Makassar. Tujuannya adalah untuk menelaah sejauhmana efektifitas UU ini dalam penyelesaian kasus-kasus jehatan yang terjadi dalam internet atau cyberspace yang demikian kompleks dan beragam modus. Adapun metode yang digunakan dalam penelitian ini adalah empiris-kualitatif. Data-data dikumpulkan dari lapangan dengan teknik wawancara dan observasi. Dari data tersebut selanjutnya dianalisis dengan pendekatan sosiologi hukum (sosio-legal) dan undang-undang (constitutional statute). Sebagai hasilnya, peneliti menemukan bahwa anatara tahun 2015 sampai tahun 2017 setidaknya terdapat 26 kasus terkait pelanggaran pidana tertentu, cybercrime, dan selanjutnya dijerat hukum berdasarkan UU ITE tahun 2008 dan 2016. Adapun jenis kejahatannya beraneka ragam, mulai dari menghecking account media social orang lain hingga penipuan dan hoaks..Lebih jauh, penelitian ini melihat bahwa UU ITE yang dijadikan secagai perangkat hukum masih belum cukup memadai mengingat kompleksitas persoalan yang terjadi dalam cyberspace berikut modus kejahatan yang mengiringinya.

Kata Kunci: Cybercrime, cyberspace, UU ITE, Sosio-Legal, Kompleks.

Abstract. This research describes about how the constitution of electronic and technological Information (ETI) of the Republic of Indonesia in 2008 number 11 dan in 2016 number19 resolve cybercrimen in Makassar, South Sulawesi. The aim is to scrutinize the effectivity of the constitution have accomplished a planty of complex cases occuring in the internet or cyberpace and followed by various modes. The method of this research is empirical-qualiatative. The data were collected by interview technique and observation. Forthermore, the data are analysed by both approaches socio-legal and constitutional statute. In the result, researchers discovered that these are twenty six cases and reports deal with cybercrime in the official police of Makassar in from 2015 until 2017. Although the its cybercrimes were decided according by the ETI constitution (2008 and 2016), but it was inadequate to resolve a plenty of the cybercrime which are complex and rapid in cyberspace flourishing unpredictably.

Keywords: Cybercrime, Cyberspace, ETI Constitution, Socio-Legal, Complex

PENDAHULUAN

Peradaban manusia telah menciptakan perkembangan teknologi dan informasi yang semakin canggih dan kompleks dari hari ke hari. Tujuannya tentu saja untuk mempermudah aktivitas manusia menjadi lebih efektif dan efisien. Saat ini, perkembangan tersebut telah menembus batas-batas waktu dan teritoial. Teknologi baru yang bernama internet ini telah memperpendek jarak serta mempersingkat waktu. Akibatnya, pergaulan antara individu semakin cair dan tidak terbatas. Dengan kata lain, ruang dan waktu spasial menjadi semakin relatif, sehingga batas antar negara pun menjadi semakin kabur (*borderless*). Seseorang pada tempat dan waktu yang sama dapat berkomunikasi dan *sharing* dengan yang lain dari Negara dan Benua berbeda hanya dengan duduk manis di sofa rumahnya. Semua hal tersebut merupakan manfaat positif teknologi bagi kehidupan manusia.

Perkembangan teknologi informasi ini pada gilirannya merubah tatanan masyarakat dan laku sosial. Bahkan, tidak hanya sampai di situ, tapi juga merubah realitas perekonomi, kebudayaan, politik dan juga hukum. Oleh sebab itu, dibalik manfaatnya yang positif, teknologi internet juga pada sisi lain membawa dampak negatif yang sedikit. Salah satunya adalah dijadikannya sebagai sarana melakukan kejahatan, yang selanjutnya dikenal dengan istilah kejahatan internet atau *cybercrime* (Amirullah, 2011: 1).

Selain dikenal dengan istilah *cybercrime*, istilah ini juga disebut *computer-related crime*, yakni suatu jenis kejahatan manusia yang dilakukan di dunia mayantara atau internet melalui sarana komputer untuk meraup keuntungan sebanyak-banyaknya dari orang lain, baik dengan cara menipu, membohongi publik, membobol rekening orang lain, maupun dengan cara mengacak sistem informasi suatu negara. Menurut Enggarani (2012: 151) bahwa tindakan

ISBN: 978-623-7496-14-4

ini dilakukan oleh segelintir orang yang memanfaatkan untuk kepentingan dirinya sendiri namun merugikan orang lain. Bahkan, dalam beberapa kasus, kejahatan jenis ini memiliki potensi yang dapat menyebabkan kerugian besar bagi para korbanya di bandingkan jenis kejahatan konvensional atau tradisional. Seperti misalnya, pencurian melalaui modus *hacking*.

Fenomena kejahatan dunia maya (internet) semakin meningkat dari waktu ke waktu. Bahkan, modus kejahatannya pun semakin beragam, mulai kasus penipuan hingga pembolan rekening Bank. Bentuk penipuan pun bermacam-macam, mulai dari penggunaan akun palsu di media sosial, produk yang seolah-olah menjanjikan hadiah bagi konsumen, hingga situs website palsu yang mengiming-iming hadiah ratusan jutaan rupiah. Adapun pembobolan rekening Bank bisanya dalam bentuk modus *hacking* dengan mengacak jaringan pihak Bank, dan selanjutnya menyerap saldo nasabah, atau juga langsung membobol *password* orang-orang tertentu yang terkenal memiliki rekening "gendut".

Berdasarkan pengamatan peneliti, setidaknya terdapat sembilan jenis kejahatan dunia maya (*cyber crime*): *Pertama*, *Hacking*, yakni dengan modus membobol sistem keamanan Bank (*Bank secuty system*), atau dengan membobol password nasabah (*user*). Pelaku jenis kejahatan ini disebut juga *hacker*, yakni orang yang memiliki kemampuan komputerisasi yang baik, namun digunakan untuk kepentingan negative; *Kedua*, adalah *Cracking*, yakni kejahatan dengan mengintip simpanan nasabah Bank, yang selanjutnya menginformasikannya kepada *hacker*. Pelakunya ini disebut juga *cracker*. Orang ini tidak saja berasal dari luar institusi, namun juga biasanya dilakukan oleh pihak internal sendiri atau karyawan di suatu institusi keuangan. Modusnya dengan memberikan bocoran informasi nasabah yang memiliki saldo yang banyak; *ketiga*, *defacing*, yakni dengan membuat dan mengubah halaman website pihak lain. Modus ini semata-mata hanya untuk mengganggu dan unjuk kemampuan pelakunya; *keempat*, *Carding*, yakni modus penipuan dengan menggunakan nomor dan identitas orang lain yang diperoleh dengan cara yang illegal. Seperti misalnya, menjual barang melalui internet dengan harga murah, namun setelah konsumen melakukan pembayaran ia tidak kunjung mengirimkan barangnya, karena barang yang dijualnya hanya fiktif belakan. Pelaku kejahatan ini disebut juga carder.

Kelima, *Faud*, yakni suatu jenis kejahatan melalui memanipulasi informasi dengan tujuan memperoleh keuntungan dari pihak lain. Modusnya seperti situs lelang fiktif. *Keenam*, adalah *Spamming*, yakni pengiriman berita informasi atau iklan melalui email. Kata lain dari spam ini adalah sampah, karena pelaku sengaja mengirimkan informasi yang tidak dikehendaki dan mintah oleh pemiliki *account*, dan bahkan yang lebih dari itu hingga informasi tertentu baik berupa iklan maupun surat yang (seolah-olah) resmi, namun hanya dipergunakan untuk kepentingan penipuan. *Ketujuh*, adalah *Cyber Pornography*, yakni penyebaran video pernografi melalui internet. *Kedelapan*, *Online Bambing*, yakni bentuk kejahatan perjudian yang dilakukan secaran online. *Kesembilan*, adalah *hoax*, yakni menyeberkan informasi bohong dengan sengaja yang kemudian meresahkan masyarakat. Informasi ini biasanya produksi oleh seseorang, baik sengaja mapun tidak sengaja, di media soasial dan selanjutnya direproduksi oleh media.

Kejahatan melalui internet ini pada gilirannya melahirkan aspek hukum baru yang selanjutnya disebut rezim hukum *cyber* yang mencakup, yakni: hukum administrasi, perdata dan juga pidana. Ketiga bidang hukum *cyber* lazim dikenal dengan istilah *cyber law*. Dalam aspek hukum pidana, ruang lingkup *cyber* sangat luas, meliputi hukum pidana materil, hukum pidana formil dan hukum panentensir (Widodo, 2013: vi). Di Indonesia, rezim hukum *cyber* masih terbilang kajian yang baru sehingga perlu di sosialisasikan secera terus menerus, baik kepada para penegak hukum maupun kepada seluruh masyarakat.

Pada tahun 2002, berdasarkan data *clear commerce*, Indonesia menduduki peringkat terbesar kedua di dunia setelah Ukraina untuk jenis kejahatan *carder*. Menurut Anton Taba Staf Ahli Kapolri, pada tahun 2009 Indonesia sudah menduduki peringkat pertama sebagai negara asal *carder*, dan pada tahun 2011 Indonesia menduduki peringkat ke 11 sebagai negara paling banyak melakukan pembajakan hak cipta. Bahkan, pada tahun 2004 silam, kejahatan *defacing* (*dafacing crime*) menyerang website lembaga negara, Komisi Pemilihan Umum. Oleh sebab itu, untuk menangani persoalan jenis kejahatan ini, pemerintah membuat regulasi dalam bentuk undang-undang (UU) yakni Informasi dan Transaksi Elektronik (UU ITE) No. 11 Tahun 2008 dan diperbahui melalui UU No. 19 tahun 2016.

Alih-alih mengurangi angka kejahatan internet (*cybercrime*) di negeri ini, justru angka angkanya menunjukkan *trend* yang semakin meningkat dari tahun ke tahun. Seperti fenomena *hoax* misalnya, dapat menyerang siapa saja, baik itu person, perusahaan, maupun pemerintah itu sendiri. Peruhahan yang juga pernah menjadi korban *hoax*, salah satunya adalah PT. Sinar Sostro Joseph, perusahaan Teh Botol Sostro. Sebagaimana dilansir oleh detiknews.com (15/5/2009), telah beredar informasi yang tidak

ISBN: 978-623-7496-14-4

benar di Internet bahwa Teh Botol Sostro mengandung zat yang berbaya, yakni; *hydroxycil acid*. Meskipun istilah ini sebenarnya adalah nama kimia dari 'air', H20, namun masyarakat lebih menerimanya tanpa filter. Terlebih, pengguna Internet di Indonesia banyak tanpa kritis menerima informasi.

Fenomena kejahatan *hoax* dalam dua tahun terakhir di Indonesia bahkan menunjukkan grafik peningkatan dan paling banyak menyita perhatian publik. Pelakunya pun tidak mengenal usia, status dan kelas sosial. Apalagi saat ini Indonesia memasuki tahun politik, pemilihan umum – pemilihan Calon Anggota Legislatif (Pileg) dan Pemilihan Prisiden tahun 2019. Informasi *hoax* dijadikan sebagai senjata atau maneuver bagi para aktor politik berikut orang-orang yang memiliki interest (kepentingan) politik. Manuver ini dipandang sebagai salah satu alat ampuh untuk menggiring opini publik. Bagaimana tidak, dengan kemudahan membagi informasi lewat media sosial, satu berita dapat dibaca oleh jutaan orang dalam tempo yang relatif sangat singkat. Terlebih lagi informasi tersebut memiliki kemudahan untuk direproduksi secara terus menerus. Dalam konteks ini, dapat dilihat misalnya, pada pemilihan gubernur DKI Jakarta tahun 2016 silam, di mana Ahok sebagai petaha pada akhirnya harus menerima kekalahannya, meskipun masyarakat Jakarta pada survey kepuasan pelayanan dan pembangunan pada angka 70 persen.

Setidaknya terdapat dua contoh kasus yang sempat menghebohkan publik, bahkan melibatkan elit dan aktor-aktor politik di di negeri ini. Keduanya pun pada akhirnya berujung penjara. *Pertama*, adalah kasus Jonro, Jon Riah Umar Ginting, pada bulan Agustus 2017 yang dilaporkan Muannas Alaidin ke Mapolda Metro Jaya, karena menyebarkan berita bohong di *facebook*-nya. Sebagai akibatnya, majelis hakim Pengadilan Negeri Jakarta Timur, menjatuhkan 1,5 (satu setengah) tahun, kepada Jonro atas tidankannya yang terbukti menyebarkan berita bohong dalam tiga *upload* terakhirnya. Jonro pun pada akhirnya harus merasakan dingin penjara selama sembilan bulan, dua per tiga masa tahanannya (dalam cnnindonesia.com/23/11/2018). *Kedua*, peristiwa kebohongan yang disebar oleh Ratna Sarumpaet. Kebohongan yang dilakukan oleh Ratna pada bulan September 2018 mulanya hanya terbata dalam lingkungan keluarganya bahwa lebam pada wajahnya akibat penganiayaan suatu kelopok tertentu yag tidak dikenal. Kebohongan ini kemudian diceritaan kepada media, dan selanjutnya direproduksi secara terus menerus oleh media hingga seantero negeri menjadi riuh. Akibatnya, Ratna, seperti juga Jonro, pun harus menerima dingingnya lantai penjara. Dua kasus ini, baik oleh Jonru maupun oleh Ratna, dipandang telah melanggar UU No. 19 tahun 2016 pasal 1 dan 2 perubahan dari UU ITE No. 11 tahun 2008, karena menyebarkan berita kobohongan kepada publik yang menimbulkan kebencian.

Apabaila mengamati beberapa peristiwa di atas, maka dapata dikatakan bahwa kemudahan untuk mengakses internet, pada sisi lain dimanfaatkan oleh sekolompok orang yang tidak bertanggung jawab. Internet yang sejatinya menudahkan dan mengefektikan kerja-kerja manusia, justru digunakan untuk tujuan yang salah dan merugikan orang lain. Oleh sebab itu, untuk menangani persoalan kejahatan internet (*Cybercrime*) ini, pemerintah menerbitkan UU ITE yaitu undang-undang No. 11 Tahun 2008 dan merevisinya pada UU No. 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik. Harapannya, aturan ini dapat meredam dan mengatasi masalah kejahatan internet. Namun demikian, perlu diingat juga bahwa UU ITE ini bukanlah tindak pidana khusus, akan tetapi juga memuat tentang pengaturan pemerintah mengani pengolaan informasi dan transaksi elektronik, dengan tujuan pembangunan teknologi informasi yang optimal dan merata secara nasional (Ismoyo, 2014: 5).

Dari uraian persoalan ini, maka dalam hemat penulis memandang perlu untuk melakukan peneltian terkait kemberlakuan UU ITE sebagai aturan hukum yang digunakan dalam menindak pelaku kejahatan internet (*cybercrime*). Tidak hanya sampai di situ penelitian ini juga ingin melihat seberapa jauh undang-undang ini efektik digunakan, baik dalam konteks preventif maupun penindakan. Daripada itu, diharapkan persoalan ini dapat diurai secara lebih terang, sehingga memunkinkan lahirnya revisi atau pun penguatan atas undang-undang ini. Hanya dengan begitu, keadilan hukum dapat dirakan oleh seluruh warga masyarakat Indonesia.

METODE PENELITIAN

Metode yang digunakan dalam penelitian ini empiris-kualitatif. Data-data diperoleh melalui sumber-sumber primer di lapangan dengan cara melukukan wawancara kepada para penegak hukum, dalam hal ini kepolisian serta pelaku dan korban kejahatan *cybercrime*. Adapun data sekunder diperoleh melalui penelusuran di lapangan berupa laporan serta literature-literatu yang relevan dengan penelitian ini, baik daring maupun luring. Dari data tersebut selanjutnya dianalisis dengan pendekatan sosiologi hukum (*sosio-legal*) dan undang-undang (*constitutional statute)*.

ISBN: 978-623-7496-14-4

HASIL DAN PEMBAHASAN

Manusia, Kejahatan dan Teknologi

Sokrates, Filsuf Yunani Klasik, beberapa abad silam selah mengatakan bahwa manusia pada hakikatnya tidak bisa dipisahkan dengan manusia lainya dalam kehidupan bersama meski berangkat dari tujuan yang berbeda. Dalam kehidupan bersama terdapat standar normatif yang disepakati bersama. Kesepakatan tersebut tidak melulu bersifat konvensional semata tapi juga dibenarkan oleh akal budi. Dalam pada itu, tindakan dalam kehidupan bersama "terhukumi" menjadi normal dan tidak tidak normal. Disebut normal, karena sesuai dengan norma sosial serta akal budi dalam masyarakat itu, dan demikian sebaliknya dikatakan tidak normal karena menyimpan dari kaedah norma sosial masyarakat. Agustinus Dewantara (2017: 6) menjelaskan bahwa Disebut *normatif*, karena etika hendak mengantar *students of ethics* pada sikap-sikap bertanggung jawab, sikap yang mengedepankan pembelaan atas nilai-nilai etis, sikap yang menjunjung tinggi norma-norma/aturan-aturan kehidupan, sikap yang mempromosikan kepekaan akan prinsip-prinsip kemanusiaan. Pendek kata, menurutnya, karakter normatifnya etika *bukan* hanya melarang (untuk melakukan pelanggaran), melainkan juga mendesakkan kehendak, tekad, dan keputusan tindakan yang makin memanusiawikan hidup manusia.

Tindakan yang tidak sesuai dengan norma sosial dan akal budi tersebut pada gilirannya disebut sebagai kejahatan. Namun perlu dipahami di sini bahwa kejahatan pada aras yang subtil bukan hanya sekadar karena kelemahan akal budi seseorang atau berimplikasinya pada kerugian orang lain secara fisik, akan tetapi pada menyelewengan atas dirinya sebagai makhluk yang bebas. Dengan kata lain, kodratnya yang bebas digunakan pada tindakan-tindakan yang melawan akal budinya sendiri. Oleh sebab itu, kejahatan pertama-tama bukan karena tinkdakannya yang tidak bersesuaian dengan norma sosial, tetapi pengingkarannya atas akal budinya sendiri. Dewantara (2017; 11) menyebutnya, tindakan seperti ini karena manusia terjebak pada dirinya sebagai *actushominis*, yakni tindakan keseharian yang disebabkan oleh kekurangan serta mungkin himpitan ekonomi, bukan justru sebagai *actus humanus* yang bertindak sesuai nurani dan akal budi. Sementara itu, menurut Maurice Blondel sebagaimana dikutip dalam Agustinus (2017: 9) menjelaskan bahwa tindakan manusia adalah representasi dirinya yang paling umum. Selain yang paling umum, tindakan manusia juga merupakan representasi dirinya yang paling lengkap. Dengan tindakannya, manusia menghadirkan dirinya secara memesonakan.

Pada konteks ini, dapat dikatakan bahwa kejahatan merupakan sesuatu yang inheren pada menudia itu sendiri. Maksudnya, kebebasan yang merupakan sesuatu yang kodrati dalam diri manusia dapat sekaligus menjadi bencana baginya. Dengan kata lain, ia seperti belati bermata dua; pada satu sisi dapat digunakan pada kemanfaatan yang positif, namun pada sisi lain dapat melukai diri pemiliknya sendiri. Kebebasan yang sejatinya menjadi kendaraan yang mentarnya menjadi *actus humanus*, justru menjadi bencana memenjarakannya dalam kerangken a*ctus hominis*.

Sebagai sesuatu yang melekat pada manusia, kejahatan pun berubah seiring dengan berkembangnya teknologi kominukasi yang dikembangkan oleh manusia. Kejahatan melekas pada dunia manusia itu sendiri. Perkembangan teknologi pada gilirannya melahirkan dunia baru yag disebut *cyberspace*. Dunia ini dihidupi oleh manusia berikut dengan mengikutsertakan tindakan aktivitas kesehariannya. Dunia ini yang sejatinya menjadi alat dan dunia antara atau "mediator" yang menyambungkan antar individu di jarak yang jauh, justru menjadi ruang destruktif. Ia menjadi alat dan media baru lahirnya jenis kejahatan baru, yang selanjutnya disebut sebagai *cybercrime* – kejahatan yang dilakukan dalam jaringan internet. Meskipun esensial kejahatannya tetap sama, namun motif dan bentuknya berbeda. Karena berlangsung dalam jaringan internet maka modus dan bentuknya pun berbeda pula. Dengan kata lain, ia menyesuaikan dengan ruang berlansungnya kejahatan tersebut dilakukan.

Seperti yang telah dijelaskan sebelumnya bahwa kejahatan ini memiliiki jenis dan modud yang berbeda-beda. Karena demikian bervariasinya sehingga kerugian yang dihasilkan pun bervariasia, yakni mulai dari yang paling kecil hingga yang paling besar. Dengan kata lain, mulai dari yang paling sederhana hingga yang paling kompleks. Di Indonesia misalnya, kejahatan ini dilakukan mulai dari pencurian kartu kredit, *hacking* beberapa situs, menyadap transmisi data orang lain - misalnya melalui email, dan memanipulasi data dengan cara menyiapkan perintah yang tidak dikehendaki ke dalam program computer hingga pencurian uang orang lain. Pada tingkat tertentu, kejahatan *Cybercrime* ini dapat menjadi ancaman terhadap stabilitas negara di mana pemerintah sulit mengimbangi teknik kejahatan yang dilakukan dengan teknologi komputer, khususnya jaringan internet dan intranet (Abidin, 2015: 501).

Pada konteks inilah, maka Indonesia sebagai Negara dipandang penting untuk mengatur lalu lintas internet demi menghindari kerugian

ISBN: 978-623-7496-14-4

warga masyarakatnya. Sebagai negara hukum, pengaturan tersebut tentu saja harus mengacu pada ideologi pancasila dan konstitusi. Thomas Hobbes (1651) dalam bukunya, Leviathan, menawarkan konsep *state of nature* dalam masyarakat yang kacau akibat perubahan dan kebebasan individu. Karena bagaimana pun menurutnya, kebebasan individu selalu menjadi ancaman bagi kebabasan orang lain, sehingga praktis menghilangkan kebebasan itu sendiri. Dari konteks inilah, Hobbes menawarkan konsep kehidupan bersama, yakni setiap orang menyerahkan hak untuk melakukan segalanya kepada suatu pihak, *primus inter pares*, asalkan setiap orang lain juga menyerahkan yang sama kepadanya. Pihak itulah yang disebut negara. Melalui hukum, negara memaksa warga untuk mengendalikan diri dan memberikan respek satu sama lain (dalam Hardiman, kompas, 1/03/2017).

Pendapat serupa juga dikemukakan oleh Daniel S.Lev (2002), bahwa negara hukum merupakan *sine qua non*, yakni tanpa proses hukum yang efektf, tidak akan terwujud keadilan dan perbaikan ekonomi, politk, dan pendidikan. Hukum adalah sarana dalam menjaga ketertiban sekaligus menjadi ujung tombak bagi pembaruan sosial yang senantiasa bergerak dari waktu ke waktu, *tempora mutantur, nos et mutamur in Illis)*. Bukan justru sebaliknya, yakni menghambat lajur perkembangan dengan dalih hukum untuk kepentingan dirinya sendiri atau kelompoknya.

Lebih lanjut, fungsi hukum dalam hubungannya dengan kejahatan bisnis dijelaskan oleh Romli Atmasasmita adalah sebagai berikut:
(1) Hukum dipandang bukan sebagai perangkat yang harus dipatuhi oleh masyarakat saja melainkan juga harus dipandang sebagai sarana yang harus dapat membatasi perilaku aparat penegak hukum dan pejabat publik; (2)Hukum bukan hanya diakui sebagai *a tool of social engineering* semata-mata tetapi juga harus diakui sebagai *a tool of social control and beureucratc engineering;* (3) Kegunaan atau kemanfaatan hukum tdak lagi hanya dilihat dari kacamata kepentngan pemegang kekuasaan melainkan harus juga dikaji dari prospektf dan perspektf kepentngan *stakeholder;* (4) Fungsi hukum sebagai sarana pembaharuan sosial dan birokrasi dalam kondisi masyarakat yang bersifat *vulnerable* dan *transitonal*, tdak dapat dilaksanakan secara optimal hanya menggunakan pendekatan preventf dan represif semata-mata melainkan juga memerlukan pendekatan *restoratf*, dan *rehabilitatf;* (5) Agar fungsi dan peranan hukum dapat dilaksanakan secara optmal maka hukum tdak semata-mata dipandang sebagai wujud dari komitmen politk, melainkan harus dipandang sebagai sarana untuk merubah sikap (*attude*) dan perilaku (*behavior*) (Atmasmita, 2003: 20-21).

Kebutuhan suatu negara untuk mereformasi regulasi untuk menjawab tantangan zamannya adalah dijelaskan oleh Hallen Silver dalam tulisannya yang berjudul, *The National Reform Agenda: Origins And Objectives.* Meskipun Silver dalam artikelnya ini menjelaskan tentang agenda reformasi di Australia, namun tampaknya relevan dengan konteks Indonesia yang sedang mengalami gelombang perubahan menuju dunia baru, revolusi industri keempat. Menurut Silver (2008: 63), *all governments need to develop a new National Reform Agenda with regulatory reform and human capital at its heart*. Tujuannya, melihat dan merencanakan agenda nasional di era mendatang. Usaha ini selain tujuannya untuk pembangunan nasional juga menjawab tantangan serta memberikan *impact* terhadap peningkatan kompetisi negara di dunia internasional.

Membaca Persoalan *Cybercrime* di Indonesia

1. Pasar dan *Crybercrime* dalam *Cyberspace*

Mobilitas sosial dalam duniainternet dari hari ke ke hari semakin massif dan dramatik. Peningkatan ini beriringan pula dengan jumlah penyelah gunaan terhadap dunia baru ini. Buktinya, angka pelanggaran hukum dalam dunia internet ini atau *cyber crime* meningkat dari waktu ke waktu. Akibatnya, dunia baru ini menjadi ambivalen; pada satu sisi memberikan manfaat yang tidak sedikit, sementara pada sisi lain juga memberikan dampak negatif yang sulit diprediksi.

Jika ditilik lebih jauh, istilah *cyberspace* diperkenalkan tahun 1984 oleh William Gibson dalam novelnya *Neuromancer* (sebelumnya *cyberspace* disebut sebagai the Net, *the Web, the Cloud, the Matrix, the Metaverse, the Datasphere, the electronic frontier, the Information Superhighway,* dll.). *Cyberspace* menjadi *setting* utama novel-novel Gibson selanjutnya, *Count Zero* (1986), *Mona Lisa Overdrive* (1988), dan *Virtual Light* (1993). Belakangan karya fiksi yang memakai gaya Gibson disebut cyberpunk. Tokoh utama *cyberpunk*, selain Gibson, adalah Pat Cadigan yang menulis *Patterns* (1989), *Synners* (1991), dan *Fools* (1994). Dalam *Neuromancer* Gibson menjelaskan *cyberspace* sebagai "pamandangan yang dihasilkan oleh komputer-komputer yang 'ditancapkan langsung'—kadang juga dengan langsung memasukkan elektroda-elektroda ke dalam soket-soket yang ditanamkan di otak".

Apa yang paling penting dari *cyberspace* sebenarnya bukanlah kabel-kabel, telepon, atau komputer jaringan. Sebab semuanya itu hanyalah menunjuk pada kendaraan, hanya menunjuk jalan raya informasi, dan bukannya tujuan yang disebut Gibson: kecemerlangan kota cahaya di akhir jalan itu. Lebih dari sekedar "wiring system" ataupun internet, *cyberspace* adalah sebuah pengalaman,

ISBN: 978-623-7496-14-4

adalah tentang masyarakat yang memakai teknologi baru untuk melakukan sesuatu yang sebenarnya secara genetis sudah mereka programkan, yaitu berkomunikasi.

Dunia ini disambut gegap gempita oleh masyarakat dunia, tidak hanya sekadar sebagai budaya sebagaimana dijelaskan di atas, tapi juga sebagai pasar baru masyarakat. Buktinya, sejak ditemukannya internet telah memberikan kontribusi positif terhadap pertumbuhan ekonomi pada setiap Negara, baik itu di Negara maju mapupun berkembang. Ini dapat dilihat dari peningkatan inevestasi di negera-negara maju seperti Amerika Serikat, Inggris, Australia, dan Singapura. Investasi ini secara otomaris memberikan *impact* pada pertumbuhan Gross Domestic Product (GDP) di negara ini, yakni: sekitar 7.8% di USA, 8.0% di UK, 8.3 di Singapura, dan 8.4 di Australia (Bhatnagar, 2005).

Trend pertumbuhan ini di ikuti juga oleh negera-negera berkembang seperti Indonesia. Berdasarkan data dari kementerian Keuangan dalam periode fiscal tahun 2009-sampai 2010 transaksi melalui media Internet melampaui empat Negara maju yang disebutkan di atas, yakni meningkat sekitar 18.24% atau setara dengan USD 219 Juta. Bagaimana tidak, pengguna *mobile phone* di Negeri ini mencapai lebih dari seperdua populasi warganya, yakni sekitar 180 juta orang dari 260 juta jiwa. Oleh sebab itu, Indonesia menjadi pengguna social mendia terbesar di dunia dengan estimasi; pengguna facebook terbesar ketiga dunia, dan menjadi pengguna terbesar kelima untk twitter (Setiadi, dkk., 2012: 107).

Jika melihat perkembangan pengguna *mobile phone* sebagai sistem telekomunikasi di Indonesia sejak di adopsi pada tahun 1999, industry ini diakui meningkat secara cepat. Bahkan untuk kawasan Asia Tenggara, Indonesia menjadi pengguna internet terbesar. Terlebih lagi, hal ini di dorong oleh pemerintah sebagaimana diterangkan dalam *World Summit Information Society* pada tahun 2003untuk mendorong warganya mengakses Internet.

Sayangnya, keberadaan internet tidak hanya memberikan kontribusi positif pada sektor ekonomi sebagaimana dijelaskan di atas, tapi juga kontrubisi negative dengan meningkatnya angka kejahatan pada dunia baru ini, yang selanjutnya disebut sebagai *cybercrime*. Kejahatan ini tidak saja terjadi di Indonesia tapi juga di seluruh dunia. Bahkan, modus kejahatannya beriringan dengan peningkatan kualitas teknologi informasi ini. Lebih jauh, modus-modus yang beraneka ragam dan semakin cangkih ini beriringan dengan jumlahnya yang cera kuantitas meningkat dari hari ke hari pula.

Pada konteks inilah, diperlukan suatu perangkat hukum yang dapat menyelesaikan persoalan tersebut. Sebagaimana fungsi dari hukum pidana yakni memberikan perlindungan terhadap kepentingan masyarakat *(social defence)*. Tujuannya, tentu saja untuk dapat menyelesaikan perkara kejahatan di dunia *cyber* yang telah menyebabkan berlangsunya pembangunan kesejahteraan masyarakat *(social welfare)*. Upaya melalui kebijakan hukum pidana yang integral harus dimaksimalkan. Mulai dari substansi hukum, struktur hukum bahkan kultur hukumnya harus berjalan dengan maksimal. Hanya melalui penegakan hukum pidana yang terpadu diharapkan fungsionalisasi hukum pidana dalam penangulangan *cybercrime* dapat terealisasi.

Di Indonesia, penggunaan Internet ini di atur dalam UU sendiri yang disebut UU ITE No. 11 tahun 2008 dan No. 19 tahun 2016. Lahirnya baru UU-ITE setelah melalui perbincangan aalot di DPR dan selanjutnya diundang tepat pada tanggal 21 April tahun 2008 dapat dikatakan sebagai sebuah respon positif (Maskun,2010: 26). Istilah hukum telematika ini secara secara internasional disebut juga *cyber law*. Langkah ini merupakan perwujudan dari niat baik dan komitmen pemeritah untuk melahirkan suatu produk khusus dibidang informasi dan transaksi elektronik. Selain itu, ini juga merupakan jawaban atas keprihatinan yang timbul dalam praktik penegakan hukum dibidang telematika. Dengan kata lain, ini merupakan bentuk pertanggungjawaban moral pemerintah terhadap masyarakat untuk melindugi warganegaranya. Namun demikian, alilih menyelesaikan dan mengurangi, justru angka pelanggaran semakin meningkat seperti dijelaskan di atas. Bahkan dapat dikatakan bahwa, aturan ini selalu tertinggal selangkah dari perkembangan modus kejatan di dunia internet itu sendiri.

2. Implementasi Penyelesaian Kasus *Cybercrime* di Makassar

Meskipun UU ITE lahir untuk tujuan dapat mengatur dan menyelesaikan persoalan kejahatan dalam *cyberspace*, bukan berarti persoalan ini selesai. Sebeaimana disebutkan sebelumnya bahwa perkembangan teknologi maju demikian cepat dan pesat, menjadikan modus kejahatan dalam ruang ini pula semakin canggih. Akibatnya, penegak hukum dalam menangani persoalan ini tidak semudah membalikkan telapak tangan.

Hal ini diakui pula oleh para penegak hukum seperti yang ditemukan oleh peneliti di lapangan. Namun demikian menurut kepolisian, sebagai salah satu institusi penegak hukum, AKP. Ahmad Canggi, Kepala Unit Tindak Pidana Tertentu Polrestabes Makassar, menjelaskan bahwa setidaknya ada dua intrumen yang dijadikan sebagai dasar penyidikan untuk menemukan bukti-

ISBN: 978-623-7496-14-4

bukti yang kuat dan sah, yakni: *tempus* dan *locus delicti*. Kedua instrument ini ditelitisik dalam komputer sebagai sarana memperoleh bukti, serta melakuka uji forensik komputer sebagai cara lain. Adapun untuk *tempus delicti*, kepolisian pertama-tama akan menelusuri jejek-jeka pelaku (kapan dan di mana mengakses, membuat dan melakukan) tindakannya. Kedua, yakni kapan tempus data tersebut diterima dalam sistem internet. Sedangkan yang ketiga, yakni kapan waktu kejahatan itu dioperasikan dalam sistem jaringan internet. Untuk bagian terakhir ini, relatif lebih muda dari dua lainnya karena data dan dokumen tersebut secara otomatis tersimpan dalam jaringan. Jejek-jejaknya sangat mudah diperoleh.

Setelah alat-alat dan bukti-bukti yang perlukan di rasa cukup, maka selanjutnya berkas dan bukti tersebut diteruskan kepada kejaksaan dan akan akan ditindak lanjuti oleh jaksa penuntut umum. Daripada itu, kejaksaan selanjutnya akan menyerahkan pengadilan untuk disidangkan, berikut menerbitkan surat dakwaan kepada terdakwa dalam kasus tersebet. Namun demikian, kepolisian sebelum menyerahkan ke kejaksaan terlebih dahulu melakukan mediasi kepada kedua bela pihak, baik korban maupun pelaku. Jika langkah mediasi ini berhasil melalui proses damai maka berkas kasus tersebut di tidak dilimpahkan lagi ke kejaksaan. Dengan kata lain, kasus tesebut berakhir dikantor polisi. Namun sebaliknya, jika gagal maka kasus ini akan berlanjut hingga pengadilan.

Berdasarkan data yang diperoleh peneliti di Polrestabes Makassar bahwa kasus *cybercrime* antara tahun 2015 hingga 2017 setidaknya terdapat 26 kasus. Daftar laporan yang dimiliki oleh polrestabe Makassar ini, meskipun menujukkan ada pertumbuhan jumlah angka *crybercrime* setiap tahun, namun tidak demikian signifikan. Angka ini masih sangat juah dari kata rentang. Karena antara tahun 2015 ke 2016 hanya bertambah lima (dari lima menjadi 10), sedangkan pada tahun selanjutnya, 2017, hanya bertambah satu (dari 10 menjadi 11). Adapun mudus-mudur *cybercrime* tersebut, cenderung beragam. Mulai dari kasus penipuan melalui telpon seluler, dengan menelpon korban yang 'seolah-oleh' memenangkan undian di suatu perusahaan, permintaan pulsa, hingga berupa pengakuan dari suatu instansi rumah sakit dengan mengatasnakan dokter atau pihak apotik bahwa salah satu dari keluarga korban mengalami kecelakaan sehingga diperlukan *fresh money*. Korban pun tanpa piker, diakibatkan karena kepanikan langsung mentrasferkan sejumla uang ke pada pelaku (penelpon). Modus ini juga terjadi pada whatsapp dengan nama dan foro profil orang-orang tertentu dengan mengatasnamakan nama orang-orang yang cukup popular (biasanya: pejabat dan pengusaha), dan selanjutnya meminta sejumlah uang, baik dengan alasan pinjaman maupun lainnya.

Hal yang sama pun terjadi, lewat media sosial *facebook* dengan cara menghecker profil tersangka.adapun modusnya berupa dua hal di atas. Selain, modus ini hal lainnya yang terjadi di *facebook* adalah berupa komenter-komentar yang menyudutkan orang lain, menghina bahkan mencemarkan nama baik. Hal lainnya sempat menyita perhatian aparat hukum adalah penyebaran *kebencian* dan *hoax*. Modus ini justru terjadi dipenghujung tahun 2017 menjelang pesta demokrasi, Pilpres dan Pilek. Namun karena pelakunya, "samar" atau anomin sehingga polisi sulit untuk mencari pelakunya.

Selain itu, yang rentang terjadi lewat media sosial lainya, baik faceebook, line, whatsapp, dll., adalah foto-foto tak sennoh (bugil). Ini dibagiakan baik dengan cara sengaja dengan mengheck *account* orang lain maupun dengan sengaja karena motif dendam atau hanya sekadar iseng. Kesulitan yang dilakukan oleh kepolisian sebagaiamana diakui oleh Ahmad Canggi adalah pelaku yang menggunakan profil dan *account* yang anonim di media sosial. Akibatnya, masih banyak yang tidak dapat di singkapnya. Dari 26 kasus yang masuk, masing-masing memiliki modes yang berbeda-beda, meskipun antara satu sama lainnya masih terdapat kesamaan, seperti yang dijelaskan di atas. Yang mengcengangkan kejadian ini, tidak memangdang status sosial, latar belakang pendidikan, serta profesi. Semua orang seperti data yang tertera di atas memungkin melakukan *cybercrime*. Lebih jauh misalnya, hal ini pun menimpa dua aktivis kelas nasional, Eggy Sudjana dan Ratna Sarumpaet terkait kasus hoaks yang secara *background* pendidikan tidak teragukan lagi.

Kendati pihak penegak hukum dalam hal ini kepolisian dapat menjadikan UU ITE tahun 2008 dan 2016 sebagai acuan penindakan untuk pelaku tindak pidana tertentu (*cybercrime*), namun tampak jelas dari kasus yang ditangani dalam interval 2015-2017 masih sangat minim dari yang seharusnya jika kita melihat fenomena dalam *cyberspace*. Makassar dengan kepadatan yang hampir mencapai dua juta jiwa hanya memperoleh laporan secara rata-rata 8 kasus pertahun. Ini tampak kontras dengan kasus pidana biasa ("bukan-tertentu") yang hampir mencapai seribu pertahun. Oleh sebab itu, undang-undang ini menarik untuk ditelaah lebih jauh.

Telah Kritis Atas Penyelesaian Kasus Cyber Crime

Apabila ditelaah lebih jauh terkait penyelesaian kasus *cybercrime* di atas, tampat jelas masih banyak ditemukan kekurang di sana sini.

ISBN: 978-623-7496-14-4

Meskipun acuan UU ITE mengacu pada syaratan dan asas-asas pertanggungjawaban pidana yang dikemukakan di atas, namun acuan ini masih merupakan sesuatu yang umum dan konvensional dalam doktrin/teori maupun dalam peraturan perundang-undangan (hukum positif). Permasalahannya adalah dapatkah doktrin/teori dan asas-asas hukum positif yang konvensial tersebut diterapkan dalam masalah pertanggungjawaban pidana *cybercrime* yang demikian sanggih? Dari kasus Makassar di atas, maka jawabannya sebagaimana diterangkang sebelumnya bahwa UU ITE, baik tahun 2008 mapun 2016, tampak masih jauh dari yang diharapkan. Mengapa demikiaan, ini dikarenakan mudus-modus kejahatan di ruang ini demikian canggih seiring dengan perkembangan teknologi yang selalu baru dan berganri secara cepat. Merujuk pada pendapat Barda (2005) bahwa ini disebabkan oleh setidaknya tiga hal adalah sebagai berikut:1) *Cyber* crime berada di lingkungan elektronik dan dunia maya yang sulit diidentifikasikan secara pasti, sedangkan asas legalitas konvensional bertolak dari perbuatan riil dan kepastian hukum; 2) *Cybercrime* berkaitan erat dengan perkembangan teknologi canggih yang sangat cepat berubah sedangkan asas legalitas konvensional bertolak dari sumber hukum formal (UU) yang statis; 3) *Cybercrime* melampui batas-batas negara, sedangkan perundang-undangan suatu negara pada dasarnya/umummnya hanya berlaku di wilayah teritorialnya sendiri.

Oleh sebab itu, meskipun pemerintah telah mengatur dan mengundangkan persoalan ini, tetap saja tak cukup sebagai perangkat untuk menyelesaikan persoalan yang demikian kompleks. Bahkan dengan kenyataan tentang aturan dan struktur organisasi pemerintah yang berhubungan dengan Teknologi Komunikasi dan Informasi seperti dijelaskan oleh Setiadi, dkk, (2012: 110). Ini dapat dilihat dari lahirnya UU ITE ini pada tahun pada 2008 dan kemudian direvisi ulang melalui UU ITE tahun 2016. Dari perubahan ini, sudah mengidikasikan dua hal, yakni; *pertama*, ketidakcukupan UU ITE tahun 2008 ini menjadi acuan penyelesaian tindak pidana tertentu (*cybercrime*) sehingga diperlukan revisi (perbaikan dan penambaha) pada UU ITE tahun 2016; *kedua*, adalah lambatnya perubahan serta keterbatasan UU ini untuk mengatur dan mengakomodir kompleksitas kejahatan yang terjadi di dunia internet. Dengan kata lain, bahwa pengaturan dan pengundangan ini mengikuti jenis-jenis perubahan yang terjadi di ruang *cyberspace*.

Selain dua hal tersebut, persoalan yang lain yang tidak adapat diabaikan berangkat dari kasus Makassar di atas adalah UU ini tidak diikuti oleh perangkat yang canggih serta keterbetasan sumber daya untuk menindak dan menyelesaikan perkara *cybercrime*. Terlebih, aparat relative pasif dalam menerima laporan-laopran pelanggaran di Masyarakat. Meskipun kepolisian berkilah bahwa ada banyak kasus yang di selesaikan dengan cara mendiasi, tapi tampak terang acuan yang digunakan masih dalam standar hukum positif konvensional, yakni; "tempus" dan "locus delicti". Sementara itu, jika lihat secara lebih seksama, modus *cybercrime* dalam *cyberspace*, dapat direkayasa; waktu dapat rubah atau di*setting* dan tempat dapat diganti sesuai keinginan *hacker*-nya. Oleh sebab itu, kasus-kasus yang ditangani oleh pihak kepolisian di atas masih terbilang standar dan konvensional. Sementara kejahatan seperti *spontaneus information* yang terstruktus secara internasional, menganggu server pemerintah, *data diddling*, *Trojan horse*, dan lain-lain.

Dengan masih terbatasnya perundang-undangan yang ada, dalam konteks hukum pidana ini mengindikasikan asas legalitas konvensional saat ini menghadapi tantangan serius dari perkembangan *cybercrime*. Oleh sebab itu, diperlukan suatu gagasan hukum baru dan asas baru yang dapat menjadi acuan dalam pidana tertentu yang semakin hari semakin meningkat berikut modus-modusnya yang mengikutinya. Tentu ini bukan hanya persoalam niat baik *good will* dari para legislator untuk membuat UU baru, lebih dari itu ini persoalan yang fundamental karena terkait asas yang menjadi dasar dan rujukan hukum pidana

KESIMPULAN

Perkembangan teknologi informasi merupakan kenyataan yang tak terhindakan saat ini. Lebih jauh, perkembangan tertesebut telah menciptakaan dunia dan ruang baru yang disebut dengan *cyberspace*, atau yang lebih popular kenal "dunia maya". Dunia atau ruang imajiner baru dari kehidupan manusia. Buktinya, ruang ini berhasil memobilisir manusia masuk ke dalamnya, baik sadar maupun tidak. Dunia baru ini telah berhasil menyodot lautan kesadaran untuk bisa berselancar di dalamnya. Namun demikian, sebagai teknologi diciptakan manusia, ia tentu tidak pernah bisa dilepaskan dari *ultimum goal* yang tak lain adalah untuk mempermudah aktifitas manusia.

Tidak sedikit orang memperoleh manfaat darinya, baik dalam skala yang kecil, personal, mapun lebih jauh pada skala besar. Negara. Bagaimana tidak, sebagai dunia baru, *cyberspace* tidak hanya merobohkan dinding-dinding pemisah serta merapatkan jarak geo-spacial antar individu penggunanya, tapi juga menjadi arena baru pertukaran dan pasar yang secara ekonomi telah berkontribusi positif bagi mereka yang ada di

ISBN: 978-623-7496-14-4

dalamnya. Kendati dengan manfaat ekonimis yang besar tersebut, pada sisi lain juga memberikan sumbangan negatif yang tidek terbilang jumlahnya, yakni dengan lahirnya jenis kejahatan baru yang disebut *cybercrime*. Modusnya pun sangat beragam tergantung pada jenis dalam arena yang digunakannya. Dengan kata lain, arena ditentukan oleh alat yang digukannya. Alat ini selanjutnya mendeterminasi jenis dan modus kejahatan ini dilakukan.

Berangkat dari kenyataan ini, pemerintah Indonesia menyadari bahwa untuk menyelesaikan persoalan cybercrime dibutuhkan suatu perangkat hukum baru yang selanjutnya melahirkan UU ITE no. 11 tahun 2008 dan UU ITE no. 19 tahun 2016. Sayangnya, berdasarkan penelitian yang dilakukan di Makassar, tampak terang bahwa UU tidak cukup memadai untuk mengatur persoalan *cybercrime* dalam *cyberspace* yang demikian kompleks. Meskipun dalam beberapa kasus UU ini berhasil dijadikan sebagai acuan menyelesaikan perkara ini, namun pada hal-hal dan kasus tentu saja. Hal ini disebabkan oleh perkembangan teknologi informasi yang demikian cepat dan semakin canggih, sementara dipihak hukum pidana masih mengacu pada asas-asas hukum positif konvensional. Oleh sebab itu, diperlukan sebuah perangkat hukum baru berikut fondasi asasnya yang sesuai dengan arena kejahatan itu dilakukan. Hanya dengan begitu penyelesaian persoalan dapat teratasi.

DAFTAR PUSTAKA

Abidin, Zaenal, 2015. "Kejahatan Dalam Teknologi Informasi Dan Komunikasi", dalam Jurnal Ilmiah Media Processor, Vol. 10, No.2. (Hal. 509-516).

Amirulloh, M., 2011. *Eu Convention On Ciber Crime: Dikaitkan Denagan Upaya Regulasi Tindak Pidana Teknologi Informasi*, Jakarta; Badan Pembinaan Hukum Nasional.

Arief, Barda Nawawi, 2005. *Bunga Rampai Kebijakan Hukum Pidana*, (cetakan ketiga), Bandung: Citra Aditya Bakti.

_____, 2002. *Perbandingan Hukum Pidana*, Jakarta: PT Raja Grafindo Persada.

Barda, Nawawi, 2005. *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime Di Indonesia*. Jakarta: PT Raja Grafindo Persada.

Bhatnagar, S., 2005. "ICT Investments in Developing Countries: An Impact Assessment Study, Information Technology in Developing Countries," *Newsletter of the IFIP Working Group 9.4*., Vol. 15, No. 2, (Hal. 1-8).

Dewantara, Agustinus W., 2017. *Filsafat Moral: Pergumulan Etis Keseharian Hidup Manusia*, Yogyakarta, Kanisius.

Enggarani, Nuria Siswi, 2012. *Penanggulangan Kejahatan Di Indonesia*, Jurnal Ilmu Hukum, Vol. 15 No. 2. (Hal. 149-169).

Departemen Pendidikan dan Kebudayaan, *Kamus Besar Bahasa Indonesia*, Jakarta; Balai Pustaka.

Ismoyo, Denni Wahyuning, 2014. Kendala Penyidik Dalam Mengungkap Tindak Pidana Penipuan Online Melalui Media Elektronik Internet (Studi di Polres Malang Kota), (Skripsi), Fakultas Hukum Universitas Brawijaya Malang.

Maskun, 2010, *Kejahatan Siber Suatu Pengantar*, Jakarta: Kencana.

Setiadi, Farisya, dkk., 2012."An Overview of the Development Indonesia National Cyber Security", dalam *International Journal of Information Technology & Computer Science (IJITCS)*, Volume 6 : Issue on November /December, (Hal. 106-116).

Soekanto, Soerjono, 1982. *Pengantar Penelitian Hukum*, Jakarta: UII Press.

Widodo, 2009. *Sistem Pemidanaan Dalam Cybercrime, Alternatif Ancaman Pidana Kerja Sosial dan Pidana Bagi Pelaku Cybercrime*, Yogyakarta: Laksbang Mediatama.

_____, 2013. *Hukum Pidana Dibidang Teknologi dan Informasi, Cybercrime Law, Telaah Teoritik dan Bedah Kasus*, Yogyakarta; Aswaja Pressindo.