Regulasi Kejahatan *Cyber* Sebagai Upaya Pertanggungjawaban Pelaku Tindak Pidana *Cybersquatting*

Dewi Muti'ah[1] Firda Laily Mufid[2]

[1]*Fakultas Hukum, Universitas Trunojoyo Madura., Jl. Raya Telang PO. BOX 2 Kamal, Bangkalan-Madura, 69162*
E-mail: dewi.mutiah@trunojoyo.ac.id
2 Fakultas Hukum, Universitas Islam Jember, Jl. Tidar 19 Jember 68124
E-mail: firdalaily@uij.ac.id

Abstract—It's undeniable that the emergence of the internet is like a double-edged sword, on the one hand it has a positive impact and on the other it has a negative impact. The positive impact of the internet is that we can get various information around the world easily. Misuse of domain names has led to a new crime in the cyber world, namely cybersquatting. Criminals take advantage of well-known domain names by making duplicates of those domain names which then register them for resale to other parties at a higher price. This article uses normative legal research, meaning that the issues raised, discussed and described in this research are focused on applying the rules or norms in positive law. This type of normative juridical research is carried out by examining various kinds of formal legal rules such as laws, literatures that are theoretical concepts which are then related to the problems that are the subject of discussion. The results obtained from writing this article are that regulations regarding cyber regulation in Indonesia are not only regulated in KUHP but also regulated in Undang-undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik and that regulations regarding cyber in Indonesia have not yet reached cybersquatting crime.. The current ITE Law is in fact still unable to realize criminal responsibility for cybersquatting perpetrators.

***Keywords*—: cyber, cybersquatting, regulation**

I. PENDAHULUAN

Era globalisasi saat ini menyebabkan terjadinya perkemabngan di berbagai sector, salah satunya ialah sector teknologi. Perkembangan yang paling siginifikan dan pesat dalam sector teknologi ialah computer. Seiring berjalannya waktu, computer terus berkembangan dan melahirkan suatu hal baru yang kita kenal dengan nama *internet. Internet* adalah sebuah jaringan yang sangat besar yang saling terhubung satu sama lain diseluruh duni.[1] Tidak dapat dipungkiri bahwa munculnya *internet* diibaratkan pedang bermata dua, di satu sisi memberikan dampak positif dan di sisi lain menimbulkan dampak negative. Dampak posisitif dari adanya *internet i*alah kita dapat memperoleh berbagai informasi di seluruh dunia dengan mudah. Seiring dengan perkembangan *internet* yang semakin pesat, muncul kejahatan-kejahatan yang berkaitan dengan *internet* dan menyebabkan persoalan-persoala hukum baru yang terjadi dalam berbagai bidang.

Perkebangan *internet* selanjutnya ditandai dengan didirikannya suatu Lembaga yang mengurus tentang pengelolaan nama domain yang dikenal dengan *InterNIC* pada tahun 1993 dengan prinsip pelayanan *first-come-first-served*.[2] Undang-undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (untuk selanjutnya disebut dengan Undang-Undang ITE) Pasal 1 angka 20 menyatakan bahwa nama domain adalah alamat *internet* penyelenggara negara, orang, badan usaha, dan/atau masyarakat, yang dapat digunakan untuk berkomunikasi melalui internet, yang berupa kode atau susunan karakter yang bersifat unik untuk menunjukkan lokasi tertentu dalam *internet.* Kenyataannya, penggunaan nama domain berkaitan dengan fungsi nama domain itu sendiri yaitu sebagai alamat di *internet*. Selain itu, penamaan terhadap nama domain juga berkaitan dengan suatu perusahaan atau suatu produk yang sering kali dijadikan *trademark* dari perusahaan atau produk tersebut. Perusahaan atau produk tersebut biasanya telah mempunyai reputasi yang bagus dan dikenal masyarakat luas.

Penyalahgunaan terhadap nama domain telah menimbulkan suatu kejahatan baru dalam dunia *cyber*, yaitu *cybersquatting.* Para pelaku kejahatan memanfaatkan nama domain terkenal dengan membuat duplikat dari nama domain tersebut yang kemudian mendaftarkannya untuk dijual Kembali pada pihak lain dengan harga yang lebih tinggi. Dengan kata lain, *cybersquatting* adalah praktek-praktek oleh para pihak-pihak tertentu untuk mendahului mendaftarkan suatu nama domain tertentu yang terkait dengan perusahaan lain tertentu dengan tujuan memperoleh keuntungan dengan cara menjual nama domain

[1] Widodo, *Hukum Pidana di Bidang Teknologi Informasi, Cybercrime Law: Telaah Teoritik dan Bedah Kasus*, 1st ed (Yogyakarta: Aswaja Pressindo, 2013). Hlm.v
[2] Sabartua Tampubolon, *Aspek Hukum Nama Domain di Internet* (Jakarta: PT. Tatanusa, 2003). Hlm.4

tersebut kepada perusahaan yang seharusnya memiliki nama domain tersebut.[3] Sebagaimana ditulis dalam *International Ournal of Law dan Information Technology:*[4]

> *Cybersquatting is a particular type of domain name dispute which occurs when someone registers a domain which is associated with a famous firm with the sole intention of selling it on to them at a higher price.*

Cybersquatting sendiri dalam Peraturan dan organisasi Internasional telah diatur dalam *Anti-Cybersquatting Consumer Protection Act (ACPA)* dan *Uniform Dispute Resolution Policy (UDRP). ACPA* dikeluarkan pada pemerintahan Clinton dan 29 November 1999 yang bertujuan untuk *to extend the exisiting means of trademark protection to "non-famous" marks comes to fill an important legal gap.*[5] Organisasi internasional selanjutnya yang mengatur mengenai nama domain dan *cybersquatting* ialah *UDRP*. *UDRP* merupakan forum arbitrase yang disahkan pada tanggal 24 Oktober 1999. Ketentuan dalam *UDRP* hamper sama dengan *ACPA*, hanya saja prosedur dalam *UDRP* lebih fleksibel, lebih singkat, dan lebih murah.[6]Indonesia sendiri telah memiliki suatu Lembaga yang mengatur mengenai nama domain yaotu PANDI (Pengelola Nama Domain Internet Indonesia). PANDI dibentuk pada 29 Desember 2006 oleh pemerintah Indonesia yang tujuan utamanya adalah mengelola nama domain di Indonesia.[7]

Pada kenyataannya, meskipun terdapat organisasi dan peraturan yang mengatur mengenai. *Cybersquatting* dan nama domain, masih terdapat lejahatan yang berhubungan dengan nama domain, khususnya *cybersquatting*, baik di luar negeri maupun di Indonesia. Kejahatan *cybersquatting* yang terjadi di Indonesia ialah kasusu Traveloka, kasus mustikaratu.com, kasusu sengketa chanel5.com. kasus mustikaratu banyak mendapat perhatian di Indonesia dan sempat diproese ke Pengadilan Jakarta Pusat, meskipun pada akhirnya kasus tersebut ditolak oleh hakim karena tidak memenuhi unsur-unsur yang didakwakan Jaksa Penuntut Umum yang kemudian putusan tersebut dianulia oleh Mahkamah Agung.[8] Sedangkan untuk kasus yang terjadi pada Traveloka.com. Co-founder Traveloka menyatakan bahwa, meskipun mereka telah mendaftarkan merek dagang dengan nama "Traveloka", tetapi mereka tidak dapat melakukan apa-apa. Hal tersebut disebabkan karena privasi pemilik domain-domain tersebut dilindungi serta pihak travleoka tidak mengenatahui siapa pelakunya sebenarnya.[9] Berbeda dengan dua kasus diatas yang korban dan pelakunya merupakan WNI. Beberapa kasus ini melibatkan WNA baik sebagai korban maupun sebagai pelaku. Salah satunya ialah kasus sengketa channel5.com. kasus ini bermula dari *channel 5 broadcasting Ltd* yang mengajukan complain kepada *national arbitration forum* mengenai pedaftaran nama domain channel5.com oleh *respondent* dalam hal ini PT. Pancawana Indonesia, melalui *registrat* IARegistry.com.[10]

Tidak dapat dipungkiri bahwa aktifitas dalam dunai *cyber* mempunyai spesifik sendiri yang tidak lagi patuh pada Batasan-batasan territorial dan hukum yang berlaku saat ini dianggap masih belum memadai terhadap kasus-kasus *cyber* sekarang ini. Hal tersebut terjadi karena filosofi awal lahirnya Undang-undang ITE yang hanya mengatur mengenai transaksi elektronik saja dan tidak megatur mengenai kejahatan dalam dunia *cyber*. Sehingga Undang-undang ITE tidak dapat mengimbangi kejahatan-kejahatan *cyber* yang semakin meningkat. Munculnya segala perbuatan dalam dunia mayantara yang dapat merugikan orang lain, mendorong untuk dilakukannya kriminalisasi terhadap perbuatan-perbuatan tersebut. Hukum harus selalu berkembang agar dapat menjangkau perkembangan-perkembangan dalam teknologi. Akan tetapi, pada kenyataannyamhukum masih jauh tertinggal dari perkembangan teknologi khususnya perbuatan-perbuatan yang terjadi dalam dunia mayantara. Sehingga, hukum masih belum mampu mengatasi permasalahan-permasalahan yang timbul dari kegiatan mayantara tersebut.

Dalam perkembangan hukum positif di Indonesia yang berlaku saat ini, tidak ada norma yang menagtur secara khusus mengenai kejahatan-kejahatan yang berkaitan dengan nama domain khususnya *cybersquatting*. Bahkan, Undang-Undang ITE yang merupakan *lex specialis* juga tidak secara khusus mengatur mengenai kejahatan-kejahatan yang berkaitan dengan nama domain. Undang-Undang ITE hanya memberikan penjelasan mengenai pengertian, pendaftaran, dan pengelolaan nama domain. Undang-Undang ITE tidak mengatur secara khusus mengenai kejahatan *cybersquatting*. Sehingga jika terdapat kasus *cybersquatting* pihak penuntut umum memasukkan pasal-pasal KUHP dalam dakwaannya, dan penyelesaian seperti itu tidak berdasarkan hukum *lex specialis* yaitu Undnag-Undang ITE dan Undang-Undang di luar KUHP yang sifatnya lebih khusus. Berdasarkan hal tersebut, memunculkan keterkaitan untuk mengkaji dengan dua permasalahan. Permasalahan pertama bagaimana regulasi di Indonesia mengenai *cybercrime*. Permasalahan kedua adalah bagaimana penerapan regulasi tersebut terhadap *cyberxquatting*.

---

[3] *Ibid*. hlm.46

[4] M Moore, "Cybersquatting: Prevention better than cure?" (2009) 17:2 International Journal of Law and Information Technology 220–231.

[5] Tampubolon, *supra* note 2. Hlm.66

[6] *Ibid*.

[7] "Tentang Pandi", online: <https://pandi.id/profil/tentang-pandi/>.

[8] Tampubolon, *supra* note 2. Hlm.92

[9] Yoga Tri Prityanto, "'Kontroversi cybersquatting menyerang Indonesia dan Traveloka'", (13 November 2003), online: <https://www.merdeka.com/teknologi/kontroversi-cybersquatting-menyerang-indonesia-dan- traveloka.html>.

[10] Tampubolon, *supra* note 2. Hlm.99

II. TINJAUAN TEORITIS

A. *Konsep Cybercrime*

Kejahatan berbasis teknologi telematika dalam berbagai sumber sering disebut dengan istilah: penyalahgunaan computer atau kejahatan computer, kejahtaan mayantara, kejahtaan internet, tindak pidana teknologi informatika dan berbaga istila lainnya.[11] Menurut Barda Nawawi Arief sebagaimana dikutip oleh Widodo, pengertian *omputer Related Crime* sama dengan *cybercrime.*[12] *Cybercrime* merupakan keseluruhan bentuk kejahatan yang ditujukan terhadap komputer, jaringan komputer dan para penggunanya, dan bentuk-bentuk kejahatan konvensional yang menggunakan atau dengan bantuan peralatan komputer.[13] Draft Virginia Computers Crime Act menyatakan bahwa computer adalah *" an electronic, magnetic, optical, electrochemical, or other hight speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communication facility directly related to or operating in conjunction with such device, but such term doesn't includean authomated typerwriter or type-setter, a portable hand-held calculator, or other similar device"*.[14] Dalam Virginia Computers Crime Act yang diterjemahkan oleh Widodo, komputer adalah peralatan elektronik, magnetik, optikal, elektrokimia, atau alat pengolah data berkecepatan tinggi yang dapat melakukan penalaran, atau fungsi penyimpanan, yang meliputi fasilitas penyimpanan atau fasilitas komunikasi yang secara langsung berhubungan dengan pengoperasian peralatan secara terpadu, tetapi istilah tersebut tidak meliputi mesin ketik atau mesin ketik elektronik, kalkulator jinjing, atau alat serupa lainnya.[15]

Dengan demikian, dapat dipahami bahwa pengertian *cybercrime* adalah setiap aktivitas seseorang, sekelompok orang, badan hukum yang menggunakan komputer sebagai sarana melakukan kejahatan, atau menjadikan komputer sebagai sasaran kejahatan, dan semua kejahatan tersebut adalah bentuk-bentuk perbuatan yang bertentangan dengan peraturan perundang-undangan, baik dalam arti melawan hukum secara materiel maupun melawan hukum secara formil.[16] Dari pemaparan diatas mengenai konsep *cybercrime*, masih belum terjadi kesepakatan mengenai definisi dan konsep tentang *cybercrime*. Hal tersebut senada dengan yang diungkapkan oleh Agus Raharjo bahwa istilah *cybercrime* sampai saat ini belum terdapat satu kesatuan pendapat bahkan tidak ada pengakuan internasional mengenai istilah baku, tetapi ada yang menyamakan istilah *cybercrime* dengan *computer crime.*[17]

B. *Karakteristik dan jenis Cybercrime*

Terdapat dua pendapat mengenai kejahatan telematika sebagai kejahatan yang berteknologi tinggi. Pendapat pertama menyatakan bahwa kejahatan telematika merupakan kejahatan jenis baru yang berbeda dengan kejahatan konvensional. Pendapat yang kedua menyatakan bahwa kejahatan telematika sejatinya kejahatan konvensional dengan menggunakan teknologi canggih sebagai sarananya dan/atau sasarannya. [18] Pendapat pertama lebih mengedepankan pada perbedaan karakteristik antara kejahatan konvensional yang berbasis sistem manual dengan kejahatan modern yang berbasis *computerized/electronic/ digitalized*.[19] Pendapat kedua, tidak mengabaikan perbedaan-perbedaan antara sistem manual dan sistem elektronik yang mempengaruhi bentuk dan sifat kejahatan ekonomi yang berbasis teknologi, namun memandang bahwa perbedaan karakteristik kejahatan ekonomi berbasis teknologi tersebut hanya sebagai varian dari bentuk kejahatan konvensial, yakni: pencurian, penipuan, penggelapan, penyelundupan, dan berbagai perbuatan tidak jujur atau curang lainnya.[20] Namun demikian, baik pendapat pertama maupun pendapat kedua mengakui bahwa secara kriminologis kejahatan berbasis teknologi telematika mengarah pada jenis *white collar crime* dan *organized crime* yang memerlukan upaya penanggulan secara serius.[21]

The International *Handbook on Computer crime* mengklasifikasikan *cybercrime* kedalam tiga kategori. Kategori pertama, *cybercrime* adalah kejahatan ekonomi yang terkait dengan komputer, meliputi penipuan dengan manipulasi komputer, pembajakan perangkat lunak komputer, spionase komputer, sabotase, pencurian jasa, akses tidak sah ke dalam sistem atau jaringan komputer, komputer sebagai alat untuk menyerang bisnis tradisional. Kategori kedua, adalah pelanggaran terhadap keleluasaan pribadi, yaitu penggunaan data yang tidak benar, pengumpulan data secara tidak sah, penyalahgunaan data, pelanggaran rahasia perusahaan. Sedangkan, kategori ketiga, misalnya melakukan penyerangan terhadap negara dan kepentingan politk, dan penyerangan terhadap kebebasan pribadi orang per orang.[22]

---

[11] Al Wisnubroto, *Strategi Penanggulangan kejahatan Telematika*, 1st ed (Yogyakarta: Atma Jaya Yogyakarta, 2010). Hlm.1

[12] Widodo, *Sistem Pemidanaan dalam Cybercrime (alternatif ancaman pidana, kerja sosial dan pidana pengawasan bagi pelaku cybercrime)*, 1st ed (Yogyakarta: Laksbang Mediatama, 2009). Hlm.23

[13] *supra* note 1. Hlm.12

[14] *supra* note 12. Hlm.25

[15] *Ibid*.

[16] Widodo, *Aspek Hukum Pidana Kejahatan Mayantara*, 1st ed (Yogyakarta: Aswaja Pressindo, 2013). Hlm.7

[17] Agus Raharjo, *Cybercrime, Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi* (Bandung: Citra Aditya Bakti, 2002). Hlm.227

[18] Wisnubroto, *supra* note 11. Hlm.6-7

[19] *Ibid*. hlm.7

[20] *Ibid*.

[21] *Ibid*.

[22] *supra* note 16. Hlm.167

Berdasarkan uraian tentang bentuk-bentuk *cybercrime* di atas dapat disimpulkan bahaw sampai saat ini para ahli hukum belum menyepakati tentang bentuk-bentuk dari *cybercrime*. Tetapi secara umum bentuk *cybercrime* dapat dikategorikan menjadi dua, yaitu komputer sebagai alat melakukan kejahatan, dan sebagai sarana kejahatan.[23]

C. Konsep cybersqatting

Cybersquatting merupakan salah satu kejahatan dalam dunia siber *(cybercrime)* yang berhubungan dengan nama domain. Secara sederhana, nama domain dapat dikatakan seperti nomor telepon dan alamat rumah seseorang. Pada awalnya, nama domain *(domain name)* digunakan hanya untuk mengidentifikasi komputer. Penggunaannya kemudian menjadi lebih intensif dan nama domain menjadi bagian dari identitas seseorang (seperti misalnya alamat email atau alamat situs web).[24] Penggunaan nama domain sejatinya hanya untuk pemakain internet. Hal tersebut sesuai dengan yang dikemukan oleh Andrew R. Basile dalam jurnal Internasional. Beliau menyatakan bahwa:[25]

> *The internet is a network of computers interconnected for electronic communication. Every computer connected to the internet is assigned a numeric address, which the other computers on the network use to route messages to that computer. A typical numeric internet address is 200.98.102.23. these addresses are difficult for humans to remeber, so the internet authorities also assign alphanumeric addresses, or domain name. Example of domain name include "whitehouse.gov" or "microsoft.com".* (*Terjemahan Penulis: Internet adalah jaringan komputer yang saling terhubung untuk komunikasi elektronik. Setiap komputer yang terhubung ke internet diberi alamat numerik, yang digunakan komputer lain untuk digunakan dalam rute pesan ke komputer tersebut. Alamat internet numerik yang khas adalah 200.98.102.23. alamat ini sulit bagi manusia untuk mengingat, jadi pihak berwenang internet juga menetapkan alamat alfanumerik, atau nama domain. Contoh nama domain termasuk "whitehouse.gov" atau "microsoft.com").

Black Law Dictinionary memberikan penjelasan mengenai *cybersquatting*, yaitu:[26]

> *Cybersquatting: the act of reserving a domain name on the internet, esp. a name that would be associated with a company's trademark, and then seeking to profit by selling or licensing the name to the company that has an interest in being identified with it. The practice was banned by federal law in 1999.* (*Terjemahan penulis. *Cybersquatting:* tindakan memesan nama domain di internet, esp. nama yang akan dikaitkan dengan merek dagang perusahaan, dan kemudian mencari keuntungan dengan menjual atau memberi lisensi nama tersebut kepada perusahaan yang memiliki kepentingan untuk diidentifikasi dengannya. Praktek tersebut dilarang oleh undang-undang federal pada tahun 1999).

Jadi, *cybersquatting* pada dasarnya adalah praktek-praktek oleh para pihak-pihak tertentu untuk mendahului mendaftarkan suatu nama domain tertentu yang terkait dengan perusahaan lain tertentu dengan tujuan memperoleh keuntungan besar dengan cara menjual nama domain tersebut kepada perusahaan yang berhak memiliki nama domain tersebut.[27] Dalam hukum positif Indonesia, pengaturan mengenai kejahatan yang berkaitan dengan nama domain masih belum di atur secara jelas. Undang-undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik hanya mengatur mengenai penjelasan, prosedur, dan pengelolaan nama domain. Undang-undang ITE tidak mengatur mengenai kejahatan nama domain yang dalam hal ini *cybersquatting*.

III.METODE PENELITIAN

Artikel ini menggunakan penelitian hukum normative, artinya permasalahan yang diangkat, dibahas dan diuraikan dalam penelitian ini difokuskan dengan menerapkan kaidah-kaidah atau norma-norma dalam hukum positif. Tipe penelitian yuridis normative dilakukan dengan mengkaji berbagai macam aturan hukum yang bersifat formal seperti undang-undang, literatur-literatur yang bersifat konsep teoritis yang kemudian dihubugngkan dengan permasalahan yang menjadi pokok pembahasan.[28] Pendekatan yang digunakan ialah pendekatan perundang-undangan dan pendekatan konseptual. Sumber bahan bukum terdiri dari bahan hukum primer dan bahan hukum sekunder. Bahan hukum primer terdiri Undang-Undang Nomor 1 tahun 1946 tentang Peraturan Kitab Undang-Undang Hukum Pidana; Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE. Selain itu digunakan juga beberapa ketentuan peraturan perundang-perundangan atau peraturan lainnya yang berkaitan dengan permasalahan yang dikaji.

---

[23] *Ibid*. hlm.172

[24] Tampubolon, *supra* note 2. Hlm.7

[25] Andrew R Basile Jr, "Risghts to Domain Names" (1996) Online Las SPAsLeg Guide Doing Bus Internet 227.

[26] Bryan A Garner, *Black's Law Dictionary* (United States of Amerika: Thomson Reuters, 2014). Hlm.470

[27] Tampubolon, *supra* note 2. Hlm.46-47

[28] Peter Mahmud Marzuki, *Penelitian Hukum* (Jakarta: Prenadamedia Group, 2013). Hlm.194

Sedangkan bahan hukum sekunder yang digunakan adalah bahan-bahan hukum yang erat kaitannya dengan bahan hukum primer dan dapat membantu untuk menganalisis dan memahami bahan hukum primer yang telah ada.

IV. ANALISIS DAN PEMBAHASAN

A. Regulasi di Indonesia terhadap dunia *Cyber*

Jauh sebelum Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik diundangkan, di Indonesia untuk menjangkau *cybercrime* para penegak hukum menggunakan pasal-pasal KUHP dan peraturan-peraturan di luar KUHO untuk mengadili pelaku *cybercrime.* Namun, setela Undang-Undang ITE diundangkan, Indonesia telah mempunya undang-undnag khusus yang mengatur tentang kejahatan-kejahatan yang terjadi di dunia maya *(cybercrime),* sehingga tidak lagi menggunakan KUHP untuk mengadili para pelaku *cubercrime.* Ketentuan dalam KUHP yang digunakan untuk menangani *cybercrime* adalah ketentuan tentang pemalsuan (Pasal 263-276), pencurian (Pasal 362-367)[29], penipuan (Pasal378-395), perusakan barang (Pasal 407-412) dan peraturan perundang-undangan lain di luar KUHP.

Setelah Undang-undang Informasi dan Transaksi Elektronik, Indonesia mengklasifikasikan *cybercrime* dalam beberapa kategori sebagai berikut:[30]

1. Akses Tidak Sah *(Illegal Access)*

Perbuatan yang memenuhi unsur tindak pidana akses secara tidak sah terhadap komputer dan/atau sistem elektronik milik orang lain diatur dalam Pasal 30 Undang-undang Informasi dan Transaksi Elektronik.

(1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun.
(2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apa pun dengsn tujusn untuk memperoleh informasi elektronik dan/atau dokumen elektronik.
(3) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

2. Penyadapan atau Interepsi Tidah Sah *(Intercepting)*

Tindak pidana intersepsi diatur dalam Pasal 31 Undang-undang Informasi dan Transaksi Elektronik.

(1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas informasi elektronik dan/atau dokumen elektronik dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain.
(2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau transmisi informasi elektronik dan/atau dokumen elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain, baik yang tidak menyebabkan perubahan apa pun meupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian informasi elektronik dan/atau dokumen elektronik yang sedang ditransmisikan.
(3) Ketentuan sebagaimana dimaksud pada ayat (1) dan ayat (2) tidak berlaku terhadap intersepsi atau penyadapan yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, atau institusi lainnya yang kewenangannya ditetapkan berdasarkan undang-undang.
(4) Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan undang-undang.

Mahkamah Konstitusi (MK) melalui Putusan Nomor.5/PUU-VIII/2010 telah membatalkan ketentuan Pasal 31 ayat (4) Undang-undang Informasi Transaksi dan Elektronik yang berisi tata cara penyadapan yang hanya diatur oleh Peraturan Pemerintah. Karena itu, ketentuan pasal tersebut tidak berlaku. Hal ji dapat dipahami karena pembatasan melalui penyadapan harus diatur dengan undang-undang agar terhindar dari penyalahgunaan wewenang yang melanggar HAM. Pengaturan penyadapan di Indonesia hanya dapat dilakukan dengan Undang-undang, karena menyangkut pembatasan HAM yang mendasar, sebagaimana tersirat diatur Pasal 28 J ayat (2) UUD 1945.[31]

3. Gangguan Terhadap Data Komputer *(Data Interference)*

Tindak pidana perubahan data dan gangguan terhadap data komputer diatur dalam Pasal 32 Undang-undang Informasi dan Transaksi Elektronik, yaitu:

(1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu informasi elektronik dan/atau dokumen elektronik milik orang lain atau milik publik.
(2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer informasi elektronik dan/atau dokumen elektronik kepada sistem elektronik prang lain yang tidak berhak.
(3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu informasi elektronik dan/atau dokumen elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

[29] *supra* note 1. Hlm.32
[30] *supra* note 16. Hlm.107-113
[31] *Ibid*. hlm.109

4. Gangguan Terhadap Sistem Komputer *(Sistem Interference)*

Tindak pidana berupa gangguan sistem diatur dalam Pasal 33 Undang-undang Informasi dan Transaksi Elektronik berikut. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggnya sistem elektronik dan/atau mengakibatkan sistem elektronik menjadi tidak bekerja sebagaimana mestinya.

5. Penyalahgunaan Perangkat Lunak Komputer *(Misuse Of Device)*

Tindak pidana berupa penyalahgunaan perangkat komputer diatur dalam Pasal 34 Undang-undang Informasi dan Transaksi Elektronik, yaitu:

(1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki:
   a. Perangkat keras atau perangkat lunak komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33;
   b. Sandi lewat komputer, kode akses, atau hal yang sejenis dengan itu yang ditujukan agar sistem elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33.

(2) Tidakan sebagaimana dimaksud pada ayat (1) bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian sistem elektronik, untuk perlindungan sistem elektronik itu sendiri secara sah dan tidak melawan hukum.

6. Pemalsuan Melalui Komputer *(Computer-Related Forgery)*

Pemalsuan melalui komputer diatur dala Pasal 35 Undang-undang Informasi dan Transaksi Elektronik berikut, 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.

7. Pornografi Melalui Komputer *(Pornography)*

Perbuatan pidana pornografi diatur dalam Pasal 27 Undang-undang Informasi dan Transaksi Elektronik sebagai berikut.

(1) Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau dokumen elektronik yang meiliki muatan yang melanggar kesusilaan.

Berdasarkan uarian di atas dapat dipahami bahwa kriminalisasi terhadap tindak pidana pornografi di internet bukan hanya terhadap pornografi anak tetapi juga pornografi dewasa.[32]

8. Kejahatan "Tradisional" yang Menggunakan Komputer

Perbuatan pidana tradisonal juga diatur dalamPasal 27 ayat (2), (3), dan (4) Undang-undang Informasi dan Transaksi Elektronik sebagai berikut.

(2) Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan perjudian.

(3) Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatam pemghinaan dan/atau pencemaran nama baik.

(4) Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentrasmisikan dan/atau dokumen elektronik yang memiliki muatan pemerasan dan/atau pengancaman.

Selain itu, tindak pidana berupa penyebaran berita bohong melalui internet diatur dalam Pasal 28 Undang-undang Informasi dan Transaksi Elektronik sebagai berikut.[33]

(1) Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik.

(2) Setiap orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antar golongan (SARA).

Tindak pidana pengancaman melalui internet kepada seseorang diatur dalam Pasal 29 Undang-undang Informasi dan Transaksi Elektronik, yaitu setiap orang dengan sengaja dan tanpa hak mengirimkan informasi elektronik dan/atau dokumen elektronik yang berisi ancaman kekerasan atau menaku-nakuti yang ditujukan secara pribadi.[34]

B. Penerapan Regulasi Di Indonesia Terhadap *Cybersquatting*

Cybersquatting merupakan bagian dari kejahatan *cybercrime*. Kejahatan ini merupakan kejahatan yang berkaitan dengan nama domain. Seperti yang telah penulis paparkan di atas bahwa *cybersquatting* merupakan salah satu kejahatan dalam *cybercrime* yang berhubungan dengan nama domain. Nama domain secara sederhana dapat dikatakan seperti nomor telepon dan alamat rumah seseorang. Pada awalnya, nama domain digunakan untuk mengidentifikasi komputer, yang penggunaannya lama-lama menjadi lebih intesif dan akhirnya nama domain menjadi bagian dari identitas seseorang (seperti alamat email atau alamat

[32] *Ibid*. hlm.112
[33] *Ibid*. hlm.113
[34] *Ibid*.

situs web).[35] Penggunaan nama domain sejatinya hanya untuk pemakaian internet sesuai dengan yang dikemukakan oleh Andrew R Basile dalam jurnal Internasional yang menyatakan:[36]

> *The internet is a network of computers interconnected for electronic communication. Every computer connected to the internet is assigned a numeric address, which the other computers on the network use to route messages to that computer. A typical numeric internet address is 200.98.102.23. these addresses are difficult for humans to remeber, so the internet authorities also assign alphanumeric addresses, or domain name. Example of domain name include "whitehouse.gov" or "microsoft.com".* (*Terjemahan Penulis: Internet adalah jaringan komputer yang saling terhubung untuk komunikasi elektronik. Setiap komputer yang terhubung ke internet diberi alamat numerik, yang digunakan komputer lain untuk digunakan dalam rute pesan ke komputer tersebut. Alamat internet numerik yang khas adalah 200.98.102.23. alamat ini sulit bagi manusia untuk mengingat, jadi pihak berwenang internet juga menetapkan alamat alfanumerik, atau nama domain. Contoh nama domain termasuk "whitehouse.gov" atau "microsoft.com").

UU ITE sendiri memberikan penjelasan mengenai apa yang dimaksud dengan nama domain yang terdapat dalam Pasal 1 angka 20 yaitu nama domain adalah alamat *internet* penyelenggara negara, orang, badan usaha, dan/atau masyarakat, yang dapat digunakan untuk berkomunikasi melalui internet, yang berupa kode atau susunan karakter yang bersifat unik untuk menunjukkan lokasi tertentu dalam *internet*. Penggunaan nama domain yang begitu pesat telah menyebabkan nama domain memiliki nilai bisnis yang sangat menggiurkan sehingga mulai disalahgunakan oleh beberapa orang salah satunya ialah praktik jual beli nama domain untuk mengambil keuntungan dari nama domain tersebut yang dikenal dengan kejahatan *cybersquatting*. *International Jurnal of Law and Infromation* yang berjudul *"Cybersquatting: Prevention Better Than Cure?"* menyatakan bahwa *Of all of the cybercrimes, cybersquatting as a phenomenon, was the one that received the most attention as it rapidly increased as quickly as the commercialisation of the internet in the mid 1990's, as many entrepreneurial types quickly realised the money to be made from forcing big brands into buying such coveted sites as wallstrees.com which was bought for $70 and sold for $1 million*[37] (*Terjemahan Penulis. Dari semua *cybercrimes*, *cybersquatting* merupakan salah satu fenomena yang telah mendapat banyak perhatian karena peningkatannya yang sangat cepat seiring perkembangan internet di pertengahan tahun 1990-an, karena banyak jenis kewiraswastaan dengan cepat menyadari bahwa uang itu harus dibuat dari memaksa besar merek membeli situs yang didambakan seperti *wallstreet.com* yang dibeli seharga $ 70 dan dijual seharga $ 1 juta).

Organisasi kekayaan intelektual dunia (WPO), melaporkan bahwa kejahatan *cybersquatting* berkembang sangat pesat sejak tahun 2006. Metode baru telah dikembangkan untuk mendapatkan kendali atas alamat domain atau nama domain yang berpotensi memiliki keuntungan. Perbuatan tersebut telah mengakibatkan banyak pemilik merek dagang terhalangi pada saat mencoba untuk membawa produk mereka langsung ke konsumen melalui internet. Praktik *cybersquatting* sebenarnya berkaitan dengan nama domain, merek dagang, dan hak kekayaan intelektual. Lembaga yang mengatur mengenai nama domain di Indonesia ialah PANDI (Pengelola Nama Domain Internet Indonesia). PANDI sendiri dibentuk oleh pemerintah Indonesia pada tanggal 29 Desember 2006 yang tujuan utamanya adalah mengelola nama domain di Indonesia. Lahirnya lembaga-lembaga di atas merupakan akibat dari berkembangnya kejahatan mengenai nama domain khususnya *cybersquatting*. Kasus-kasus *cybersquatting* sendiri telah banyak terjadi baik di dunia internasional maupun di Indonesia. Beberapa kejahatan *cybersquatting* yang terjadi di Indonesia ialah kasus mustikaratu.com, kasus sengketa chanel5.com, dan kasus Traveloka seperti yang telah penulis sebutkan di atas.

Kasus-kasus *cybersquatting* yang terjadi di Indonesia seperti pada kasus mustikaratu.com dan kasus traveloka seharusnya dapat diterapkan Undang-Undang tentang Merek dan Undang-Undang ITE. Akan tetapi, jika kasus tersebut menggunakan Undang-Undang tentang Merek, dalam Undang-Undang tenta Merek tersebut tidak mencantumkan bahwa nama domain memiliki fungsi yang sama dengan merek. Kasus *cybersquatting* seharusnya dapat menggunakan Undang-Undang ITE, tetapi dalam Undang-Undang ITE juga tidak mengatur secara khusus mengenai kejahatan nama domain khusus nya *cybersquatting*. Akan tetapi pasal-pasal dalam Undang-Undang ITE masih memungkinkan untuk di terapkan dalam kejahatan *cybersquatting* ini.

Apabila melihat kasus *cybersquatting* yang terjadi pada PT. Mustika Ratu, yang mengakibatkan konsumen tidak dapat masuk ke situs PT. Mustika Ratu tetapi masuk ke website www.belia.com yang memasarkan produk Sari Ayu. Perbuatan tersebut dapat diartikan telah mengubah suatu informasi elektronik dan menyebabkan suatu sistem elektronik terganggu sehingga sejatinya dapat diterapkan Pasal 32 Ayat (1) Jo Pasal 48 Ayat (1) Undang-Undang ITE dan Pasal 33 Jo Pasal 49 Undang-Undang ITE. Penerapan Pasal 32 Ayat (1) Undang-Undang ITE pada kasus PT. Mustika Ratu karena pada laman *webesite* PT. Mustika Ratu telah diubah tampilannya dan produk yang dipasarkan dalam *website* bukan lagi produk dari PT. Mustika Ratu melainkan produk dari Sari Ayu. Sedangkan penerapan Pasal 33 Undang-Undang ITE pada kasus ini dikarenakan para konsumen tidak dapat masuk ke *website* PT. Mustika Ratu tetapi di arahkan pada *website* www.belia.com yang memasarkan produk-produk dari PT. Martina Berto. Akan tetapi, penerapan pasal-pasal diatas kurang efektif menjerat pelaku kejahatan *cybersquatting* mempertanggungjawabkan perbuatannya dan membuat pelaku memiliki peluang untuk lolos dari pasal tersebut.

---

[35] Tampubolon, *supra* note 2.
[36] Basile Jr, *supra* note 25.
[37] Moore, "Cybersquatting", *supra* note 4.

Berbeda dari kasus yang menimpa PT. Mustika Ratu, kasus traveloka.com diarahkan pada *website* porno yang bernama krucil2. Seseorang telah membeli beberapa nama domain yang berhubungan dengan traveloka kemudian menghubungkannya ke dalam situs porno yang bernama krucil2. Perbuatan tersebut dapat dikatakan bahwa pelaku telah membuat dapat diaksesnya informasi elektronik yang memiliki muatan kesusilaan dan dapat diterapkan Pasal 27 Ayat (1) Jo Pasal 45 Ayat (1) Undang-Undang ITE.

Pasal-pasal di atas, baik pasal yang dapat di terapkan pada kasus PT. Musti Ratu maupun pada kasus traveloka.com jika dikaitkan dengan pengertian kejahatan *cybersquatting* sudah pasti pasal-pasal tersebut tidak kuat untuk diterapkan pada kasus *cybersquatting*, sehingga akan menyebabkan pelaku kejahatan *cybersquatting* tidak dapat diminta pertanggungjawaban secara pidana. Sehingga sistem pertanggungjawaban pidana dalam Undang-Undang ITE tidak dapat diterapkan. Apabila sistem pertanggungjawaban pidana dalam Undang-Undang ITE dipaksakan terhadap kejahatan *cybersquatting*, maka perbuatan tersebut telah bertentangan dengan asas hukum pidana yaitu asas legalitas.

Asas legalitas sendiri dalam hukum Indonesia terdapat pada Pasal 1 Ayat (1) KUHP yang menyatakan bahwa tiada suatu perbuatan dapat dipidana, kecuali berdasarkan kekuatan ketentuan perundang-undangan pidana yang telah ada sebelumnya. Artinya, suatu perbuatan tidak dapat dikualifikasikan dalam perbuatan pidana apabila perbuatan tersebut tidak dilarang menurut undang-undang pidana.

Tuntutan pidana hanya ditujukan terhadap perbuatan yang telah dikualifikasikan sebagai perbuatan pidana. Tapi sebaliknya, tuntutan pidana tidak dapat ditujukan terhadap perbuatan yang belum atau tidak dilarang dalam hukum pidana meskipun perbuatan tersebut dikategorikan dalam perbuatan jahat dan telah menibulkan kerugian besar bagi korban atas perbuatan jahatnya tersebut hanya karena belum atau tidak diatur dalam undang-undang pidana.[38] Jadi, terhadap kasus *cybersquatting* apabila pasal-pasal dalam Undang-Undang ITE dipaksakan terhadap kasus ini, maka sejatinya hal tersebut telah melanggar asas legalitas karena *cybersquatting* sendiri masih belum diatur secara khusus dalam Undang-Undang ITE. Meskipun terdapat beberapa pasal yang masih dapat diterapkan tetapi pasal tersebut tidak cukup kuat untuk membawa pelaku mempertanggungjawabkan perbuatannya secara pidana.

Bedasarkan pemaparan di atas dapat digaris bawahi bahwa regulasi mengenai *cyber* di Indonesia masih belum menjangkau kejahatan *Cybersquatting*. Pelaku kejahatan *cybersquatting* masih belum dapat diminakan pertanggungjawaban pidana berdasarkan UU ITE. Pelaku kejahatan *cybersquatting* sangat mungkin untuk dimintakan pertanggungjawaban seacara pidana, mengingat kejahatan tersebut dapat menyebabkan kerugian secara materiil. Undang-Undang ITE yang ada saat ini kenyataannya masih belum dapat mewujudkan pertanggungjawaban pidana terhadap pelaku kejahatan *cybersquatting*. Hal tersebut terjadi karena kejahatan *cybersquatting* masih belum diatur secara dalam hukum positif Indonesia.

V. KESIMPULAN DAN SARAN

Hasil yang diperoleh dari penulisan artikel ini adalah bahwasanya regulasi mengenai pengaturan cyber di Indonesia selain diatur dalam KUHP juga diatur dalam Undang- Undang-undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan bahwa regulasi mengenai cyber di Indonesia masih belum menjangkau kejahatan Cybersquatting. Pelaku kejahatan cybersquatting sangat mungkin untuk dimintakan pertanggungjawaban seacara pidana, mengingat kejahatan tersebut dapat menyebabkan kerugian secara materiil. Undang-Undang ITE yang ada saat ini kenyataannya masih belum dapat mewujudkan pertanggungjawaban pidana terhadap pelaku kejahatan cybersquatting. Hal tersebut terjadi karena kejahatan *cybersquatting* masih belum diatur secara dalam hukum positif Indonesia.. Saran penulis adalah, pemerintah perlu membuat regulasi mengenai kejahatan *cybersquatting* agar kejahatan ini tidak terjadi lagi.

[38] Deni Setyo Bagus Yuherawan, *Dekonstruksi Asas Legalitas Hukum Pidana (sejarah asas legalitas dan gagasan pembaharuan filosofis hukum pidana)*, 1st ed (Malang: Setara Press, 2014). Hlm.3

VI.DAFTAR PUSTAKA

A. Buku

Garner, Bryan A, 2014, *Black's Law Dictionary* (United States of Amerika: Thomson Reuters).

Marzuki, Peter Mahmud, 2013, *Penelitian Hukum*,Jakarta: Prenadamedia Group.

Raharjo, Agus, 2002, *Cybercrime, Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Bandung: Citra Aditya Bakti, 2002..

Tampubolon, Sabartua, 2003, *Aspek Hukum Nama Domain di Internet* , Jakarta: PT. Tatanusa.

Widodo, 2013, *Aspek Hukum Pidana Kejahatan Mayantara*, 1st ed, Yogyakarta: Aswaja Pressindo.

———, 2013, *Hukum Pidana di Bidang Teknologi Informasi, Cybercrime Law: Telaah Teoritik dan Bedah Kasus*, 1st ed ,Yogyakarta: Aswaja Pressindo.

———, 2009, *Sistem Pemidanaan dalam Cybercrime (alternatif ancaman pidana, kerja sosial dan pidana pengawasan bagi pelaku cybercrime)*, 1st ed Yogyakarta: Laksbang Mediatama.

Wisnubroto, Al,2010, *Strategi Penanggulangan kejahatan Telematika*, 1st ed ,Yogyakarta: Atma Jaya Yogyakarta.

Yuherawan, Deni Setyo Bagus, 2014, *Dekonstruksi Asas Legalitas Hukum Pidana (sejarah asas legalitas dan gagasan pembaharuan filosofis hukum pidana)*, 1st ed Malang: Setara Press.

B. Jurnal dan Internet

Basile Jr, Andrew R, "Risghts to Domain Names" (1996) Online Las SPAsLeg Guide Doing Bus Internet 227.

Moore, M, "Cybersquatting: Prevention better than cure?" (2009) 17:2 International Journal of Law and Information Technology 220–231.

Prityanto, Yoga Tri, "'Kontroversi cybersquatting menyerang Indonesia dan Traveloka'", (13 November 2003), online: <https://www.merdeka.com/teknologi/kontroversi-cybersquatting-menyerang-indonesia-dan- traveloka.html>.

"Tentang Pandi", online: <https://pandi.id/profil/tentang-pandi/>.

B. Peraturan Perundang-Undangan

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

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