Jumadiyanto Eko. "Penerapan Yurisdiksi Pribadi Dalam Penegakan Hukum Di Internet Dan E-Commerce Law." *Pancasila Law Review* 1 no. 2 (2024): 116-130. DOI: xx.xxxxx/panclrev.xxxxxx

PancasilaLawReview

Volume 1 Issue 2, 2024
P-ISSN: 3064-2639, E-ISSN: 3064-1950

Penerapan Yurisdiksi Pribadi Dalam Penegakan Hukum Di Internet Dan E-Commerce Law

Eko Jumadiyanto

Universitas Al Azhar, Indonesia. E-mail: eko.jumadiyanto@gmail.com

Abstrak : Penegakan hukum tindak pidana siber tidak terlepas dengan yurisdiksi, terutama mengenai ruang berlakunya hukum pidana menurut tempat (yurisdiksi teritorial). Luas dan tersebarnya potensi locus delicti dalam tindak pidana siber akan menimbulkan masalah berkaitan dengan prinsip yurisdiksi atau terjadi konflik yurisdiksi. Pemberlakuan yurisdiksi universal, membutuhkan kerjasama dari negara-negara yang diawali dari adanya ratifikasi terhadap tindak pidana siber, dengan adanya kesamaan penegakan hukum, maka meminimalisir terjadinya pemanfaatan celah hukum dikarenakan yurisdiksi negara.

Kata Kunci : Yurisdiksi; Penegakan Hukum*; E-Commerce*

Abstract: *Law enforcement on cyber criminal act is not apart from jurisdiction, particularly space of validity of criminal law in a place (territorial jurisdiction). Widespread locus delicti potential in cyber criminal act will be give rising to problems in relation to principles of jurisdiction or the incidence of jurisdictional conflicts. The validity of universal jurisdiction requires states cooperation starting by any ratification of cyber criminal act. Given similarity of law enforcement, then minimize the use of legal loopholes due the state jurisdiction.*

Keywords : *Jurisdiction; Law Enforcement; E-commerce*

1. Pendahuluan

Diantara paling krusial yang dimunculkan oleh cybercrime adalah masalah yurisdiksi yang berkaitan dengan sejauh mana suatu negara dapat menerapkan kedaulatan hukumnya, atau dengan kata lain sejauhmana kemampuan suatu negara dalam persidangan suatu perkara bernuansa internasional. Permasalahan yurisdiksi di suatu negara terkait penerapan kedaulatan hukum atas suatu perkara bernuansa internasional.

Era globalisasi terbentuk karena adanya kecenderungan perkembangan teknologi negara-negara dunia. Arus informasi menyebabkan tidak adanya batas ruang dan waktu untuk mengetahui segala sesuatu yang berada di luar negaranya. Batasan negara sudah tidak ada lagi karena adanya teknologi informasi yang semakin canggih. Perlu diketahui dengan adanya era globalisasi ini menyebabkan perlu adanya pengaturan yang sifatnya universal terhadap tindak pidana yang ada di bidang siber.

Dunia yang sedang berada dalam abad informasi, keberadaan informasi mempunyai peranan penting di dalam kehidupan manusia. Melalui kemajuan informasi, komunikasi, dan teknologi (Information Communication Technology/ICT) dapat mendorong

perkembangan dan pertumbuhan ekonomi dunia.[1] Teknologi informasi dan komunikasi (TIK) telah mengubah perilaku masyarakat dan peradaban manusia secara global. Perkembangan teknologi informasi telah meyebabkan perubahan sosial yang secara signifikan berlangsung dengan cepat. Teknologi informasi saat ini menjadi "pedang bermata dua", karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum.[2]

Ketidakmampuan suatu negara untuk melacak dan mengungkap cybercrime pada akhirnya akan mempengaruhi penegakan hukum di negara lain, termasuk negara-negara maju yang memiliki kemampuan relatif tinggi baik sumber daya manusia maupun sarana prasarananya. Hal ini berkaitan dengan adanya prinsip double criminality untuk penegakan hukum terhadap tindak pidana transnasional.[3]

Menurut hukum internasional yang selama ini berlaku, suatu negara memiliki batasan-batasan tertentu dalam hal penerapan yurisdiksi terhadap kasus yang melibatkan kepentingan negara lain. Salah satu batasan yang dimaksud misalnya berupa kewajiban setiap negara untuk berhati-hati dan sedapat mungkin menghindari munculnya gangguan terhadap negara lain dalam upaya penerapan yurisdiksinya.

Meskipun demikian, pada praktiknya hukum internasional tidak dapat memaksakan suatu negara untuk menerapkan suatu konsep yurisdiksi tertentu, bahkan dalam konteks ini setiap negara cenderung diberikan kebebasan dalam menentukan konsep mana yang akan digunakan. Kebebasan tentu saja akan diberikan sepanjang tidak mengancam ketertiban internasional. Adapun secara umum yurisdiksi dibedakan menjadi tiga jenis, yaitu:

1.1. Yurisdiksi Legislatif

Secara umum yurisdiksi legislatif merupakan kemampuan suatu negara untuk menerapkan hukum nasionalnya terhadap individu dan peristiwa tertentu. Kemampuan ini pada prinsipnya dapat terwujud selama peristiwa yang dimaksud terjadi di wilayahnya atau peristiwa tersebut dilakukan oleh warga negara yang berada diluar batas wilayah negara tersebut. Selain itu jenis yurisdiksi ini juga dapat dikatakan sebagai titik tolak dalam menetukan penerapan jenis yurisdiksi lainnya. Artinya untuk menerapkan yurisdiksi yudikatif, maka harus diawali dengan menganalisa yurisdiksi legislatif terlebih dahulu, namun ini tidak perlu dilakukan jika pihak yang bertindak sebagai negara forum berkenan mempergunakan hukum asing. Persyaratan yang sama berlaku juga bila ingin menerapkan yurisdiksi eksekutif.

---

[1] Kofi A. Anan dalam UNCTAD *E-commerce and Development Report,* 2004, hlm 4

[2] Ahmad M. Ramli, Cyber Law dan HAKI dalam Sistem Hukum Indonesia, Refika Aditama, Bandung, 2004, hlm 1.

[3] Sigid Suseno, *Cybercrime, Pengaturan dan Penegakan Hukumnya di Indonesia dan Amerika Serikat,* Jurnal Ilmu Hukum Padjajaran Jilid XXXIII, 2009, hlm 41-42.

Dalam menentukan yurisdiksi legislatif, maka terhadap seseorang maupun suatu peristiwa, terdapat 6 (enam) prinsip lain yang dapat dijadikan acuan. Prinsip- prinsip tersebut antara lain :

a) Subjective territoriality (territorial subjektif)
b) Objective territoriality (territorial objektif)
c) Nationality (nasionalitas aktif)
d) Passive Nationality (nasionalitas pasif)
e) Protective Principle (prinsip perlindungan)
f) Universality (universalitas)

1.2. Yurisdiksi yudikatif

Yurisdiksi yudikatif merupakan kewenangan suatu negara untuk melakukan proses peradilan terhadap individu atau peristiwa yang mempunyai hubungan yang cukup dengan negara tersebut. Sebagaimana paparan sebelumnya, penerapan yurisdiksi yudikatif hampir selalu dengan penerapan yurisdiksi legislatif. Hal ini bisa dilihat dari praktik di seluruh dunia bahwa hampir tidak ada pengadilan yang sukarela memakai hukum pidana negara lain. Dalam kasus kejahatan internasional, penerapan yurisdiksi yudikatif secara normatif bergantung pada dimana pelaku kejahatan tersebut berada.

1.3. Yurisdiksi eksekutif

Yurisdiksi eksekutif mempunyai makna sebagai kewenangan negara untuk meningkatkan kepatuhan terhadap hukum dan kewenangan negara untuk menjatuhkan hukuman bagi yang melanggar hukum. Jenis yurisdiksi ini memiliki kaitan erat dengan yurisdiksi legislatif, maksudnya suatu negara tidak dapat menegakkan hukum nasionalnya begitu saja, kecuali negara tesebut memiliki yurisdiksi legislatif atas seseorang atau suatu peristiwa.

Yurisdiksi legislatif terkadang juga menjadi dasar pembenar bagi suatu negara untuk mengambil langkah-langkah yang dianggap perlu dalam rangka penerapan yurisdiksi eksekusinya di wilayah negara lain dengan syarat ada persetujuan dari negara tersebut. Persetujuan yang dimaksud disini adalah persetujuan yang diberikan oleh otoritas resmi dari negara yang bersangkutan, dan langkah-langkah yang dapat diambil antara lain : penahanan, pengiriman surat, pelayanan dokumen, dan penyelidikan.

Dalam penegakan hukum tindak pidana siber tidak akan terlepas dengan yurisdiksi, terutama mengenai ruang berlakunya hukum pidana menurut tempat (yurisdiksi teritorial). Luas dan tersebarnya potensi *locus delicti* dalam tindak pidana siber akan menimbulkan masalah berkaitan dengan prinsip yurisdiksi atau terjadi konflik yurisdiksi. Menurut Debra L. Shinder; *cybercrime cases, more than most others, often involve complex jurisdictional issues that can present both legal and practical obstacle to prosecution.*[4] Oleh karena itu upaya penegakan hukum terhadap pelaku *cybercrime* tidak hanya menjadi perhatian nasional saja tetapi juga regional dan internasional.

Lahirnya pemikiran untuk membentuk suatu aturan hukum yang dapat merespon persoalan-persoalan hukum yang muncul akibat dari pemanfaatan TIK terutama disebabkan oleh sistem hukum konvensional yang tidak dapat merespon persoalan-

[4] Ibid

persoalan tersebut dengan memuaskan. Hal ini pada gilirannya akan melemahkan atau bahkan mengusangkan konsep-konsep hukum yang sudah mapan seperti konsep-konsep kedaulatan dan yurisdiksi.[5]

Kedua konsep ini berada pada posisi yang dilematis ketika harus berhadapan dengan kenyataan bahwa dalam pemanfaatan internet tidak lagi menghiraukan batas-batas yurisdiksi negara. Dilema yang dihadapi oleh konsep- konsep hukum konvensional dalam menghadapi fenomena di *cyberspace* merupakan alasan utama perlunya membentuk regulasi yang akomodatif terhadap fenomena-fenomena yang muncul akibat pemanfaatan TIK, khususnya menyangkut yurisdiksi.

Prinsip-prinsip yurisdiksi dalam hukum internasional memiliki dasar yang sama, yaitu adanya penentuan wilayah yang jelas, apakah suatu peristiwa terjadi di wilayah suatu negara, ataukah di wilayah negara asing yang berdampak pada wilayahnya sendiri. Namun demikian yang menjadi kendala dalam penerapan yurisdiksi dalam hukum internasional adalah adanya suatu kondisi dalam teknologi informasi dan komunikasi yang tanpa batas.

Berdasar uraian latar belakang penelitian dan judul, permasalahan diidentifikasikan sebagai berikut:

a) Bagaimana penerapan prinsip yurisdiksi dalam penegakan hukum tentang di internet dan e-commerce law?
b) Bagaimana bentuk kerjasama internasional terkait dalam penegakan hukum tentang tindak pidana siber yang didasari prinsip yurisdiksi?

2. Metode

Metode yang digunakan dalam penulisan ini adalah deskriptif analitis, yaitu melalui pendekatan yuridis normatif serta menggunakan data berupa bahan primer, sekunder, dan tersier berupa peraturan perundang-undangan, literature hukum dan buku-buku. Teknik pengumpulan data yang digunakan adalah studi kepustakaan mengenai Hukum Internasional dan Hukum Siber.

3. Penerapan Yurisdiksi Pribadi dalam penegakan Hukumnya di internet dan di e-commerce Law.

Mengingat keberadaan yurisdiksi selalu dikaitkan dengan keberadaan suatu hukum, maka pendapat yang diuraikan pada paragraf diatas kurang lebih dapat diartikan bahwa di cyberspace pada dasarnya tidak ada hukum yang mengatur (lawless paradise). Munculnya pendapat tersebut dan jika di kaitkan karakteristik dari *cyberspace* yaitu *no boundaries*, maka dapat dikatakan bahwa keberadaan cyberspace bersama dengan karakteristiknya telah menyimpang dari konsep penerapan hukum yang umumnya didasarkan kondisi fisik dan wilayah.

[5] Dedi Feriandi, Tinjauan Hukum dan Etika Periklanan di Internet, Menegakkan Hukum Sistem Informasi, Institut Teknologi Bandung, Agustus 2000, hlm. 4

Yurisdiksi muncul karena perlu adanya penangan bersama mengenai tindak pidana internasional yang serius. Tetapi pada pelaksanaannya hal ini terbentur dengan kedaulatan suatu negara. Padahal masyarakat internasional harus memiliki keinginan bersama untuk menanggulangi tindak pidana yang efeknya besar. Masyarakat internasional pun dalam menanggapi yurisdiksi universal, kurang antusias, karena akan memunculkan dominasi negara kuat untuk serta merta memasuki kedaulatan negara lain.

Perkembangan teknologi yang begitu pesat terutama dalam bidang komputer melahirkan sebuah program yang akan menjadi sebuah fenomena dunia. Program ini disebut internet yang berasal dari penelitian yang dilakukan oleh Departemen Pertahanan dan Keamanan Amerika Serikat.

Ilmu pengetahuan dan teknologi telah menghasilkan prasarana yang memudahkan manusia. Salah satu produk dari ilmu pengetahuan dan teknologi adalah teknologi informasi atau yang lebih dikenal dengan teknologi telekomunikasi. Telekomunikasi telah membantu umat manusia berinteraksi dengan sesama umat manusia dengan mudah. Munculnya komputer dan internet membuat komunikasi tidak dibatasi dengan sekat-sekat teritori suatu negara.

Beberapa ahli telah mencoba mendefinisikan pengertian dari kejahatan komputer, baik dalam suatu literatur (pengertian kriminologis) atau dalam undang- undang/rancangan undang-undang (pengertian yuridis, sehingga muncul berbagai definisi tentang kejahatan komputer, sesuai dengan kepentingan dan sudut pandang masing-masing). Berikut ini penulis mencoba untuk menguraikan beberapa pengertian mengenai kejahatan komputer sebagai gambaran.

Perkembangan teknologi terutama internet membuat banyak dampak positif bagi kemajuan umat manusia, ini ditandai dengan munculnya berbagai layanan yang dilakukan via internet seperti e-commerce, e-banking, e-goverment dan e-learning. Selain dampak positif perkembangan teknologi juga memiliki dampak negatif, dalam hal ini dikaitkan dengan dunia kejahatan, para pelaku biasanya menggunakan intenet untuk melakukan kejahatan yang berhubungan dengan komputer seperti, penipuan kartu kredit dan bursa efek, pornografi anak dan terorisme, selain itu juga ada kejahatan yang menjadikan komputer sebagai targetnya seperti, *defacing, cracking* dan *phreaking*.

Tonggak awal dari adanya pengadilan pidana internasional, pada Statuta Roma Tentang Pengadilan Pidana Internasional (International Criminal Court/ICC) 17 Juli 1998 yang ditandatangani oleh 120 negara-negara di dunia. Tindak pidana pidana yang mengacam kehidupan umat manusia lain, dapat dijatuhi hukuman di Pengadilan Pidana Internasional yang saat ini beralamat Maanweg 174, 2516 AB The Hague, Belanda. Akan tetapi statuta tersebut memiliki kekurangan, yaitu tidak adanya aparatur yang melakukan penangkapan, penahanan, penyidikan, dan penuntutan.

Dampaknya secara hukum adalah dengan sifat fleksibilitas tersebut, pelaku kejahatan di cyberspace dapat saja lolos dari jeratan hukum hanya dengan memindahkan lokasi tempat aktifitas cybercrime berlangsung dari satu yurisdiksi ke yurisdiksi yang lain. Mereka dapat pula memilih yurisdiksi suatu negara yang kondisi penegakkan hukumnya lemah, sehingga semaikin membuka peluang untuk lolos dari jeratan hukum.

Penerapan yurisdiksi universal terhadap pelaku tindak pidana tidak mudah dilaksanakan, keterbatasan ini diakui juga oleh para ahli, yaitu sebagai berikut:

> *"Refers to jurisdiction established over a crime without reference to the place of perpetration, the nationality of the suspect or the victim or any other recognized linking point between the crime and the prosecuting State. It is a principle of jurisdiction limited to specific crimes."*[6]

Sehubungan dengan yurisdiksi Republik Indonesia di dalam ruang siber, UU ITE telah mengatur suatu yurisdiksi yang bersifat ekstrateritorial,[7] sebagaimana dimuat di dalam Pasal 2

UU ITE memiliki jangkauan yurisdiksi yang tidak semata-mata untuk perbuatan hukum yang berlaku di Indonesia dan/atau dilakukan oleh warga negara Indonesia, tetapi juga berlaku untuk perbuatan hukum yang dilakukan oleh warga negara Indonesia mupun warga negara asing yang memiliki akibat hukum di Indonesia mengingat pemanfaatan Teknologi Informasi untuk Informasi Elektronik dan Transaksi Elektronik dapat bersifat lintas territorial atau universal.[8]

Perkembangan teknologi informasi dan telekomunikasi yang sangat siginifikan menciptakan suatu "dunia baru" yang sering dikenal dengan istilah cyberspace. Cybercrime merupakan modus atau bentuk baru dari kejahatan yang terjadi di cyberspace akibat dari penyalahgunaan jaringan computer atau internet.

Cybercrime sebagai bentuk kejahatan jika di kaji dari aspek kriminologi dapat dilihat dari beberapa sudut pandang atau teori yaitu:

a) Teori Anomali :

   Teori ini berpijak dari adanya suatu keadaan "normless" yang terjadi di tengah masyarakat yaitu keadaan "total absence of norms" dalam terjemahan bebasnya terjadi kekosongan hukum ditengah-tengah masyarakat khususnya yang berhubungan dengan pengaturan tentang *Cybercrime*. Kekosongan hukum bukanlah dalam artian tidak ada sama sekali hukum yang mengaturnya, namun terjadi ketidakmampuan norma khusunya norma hukum termasuk perangkat hukum yang ada untuk mengatur dan mengontrol perilaku dari individu (inability of norms to control or regulate), hal ini disebabkan oleh ketidakmampuan hukum yang ada untuk menjangkau atau mengatur kejahatan yang terjadi di cyberspace.

   Hukum yang ada yang dibuat pada masa lampau khususnya KUHPidana sangat kurang memadai untuk menghadapi cybercrime, bahkan peraturan perundang-undangan yang dibuat juga tidak sepenuhnya merepresentasikan kebutuhan akan penegakan hukum dalam dunia cyber/telematika. Kekosongan hukum ini dimanfaatkan ataupun mendoroang serta menjadi celah bagi para pelaku untuk melakukan kejahatan di *cyberspace*.

---

[6] Cryer et al., Universal Jurisdiction: International and Municipal Legal Perspectives 220, supra note 9, See also Luc Reydams, 2003, hlm. 46.

[7] Danrivanto Budhijanto, Op.Cit, hlm. 136.

[8] Ibid

b) Teori Perbedaan Asosiasi (Differential Association)

Cybercrime adalah kejahatan yang memanfaatkan teknologi informatika dan telekomunikasi yang canggih, dan para pelaku biasanya adalah orang-orang yang mahir dalam bidang telematika, sehingga untuk dapat memasuki dunia cyber dan bahkan melakukan cybercrime, seseorang harus belajar terlebih dahulu. Oleh karena itu cybercrime dapat dikatakan sebagai kejahatan hasil proses belajar pelaku baik secara otodidak maupun belajar kepada para pakarnya. Pelaku harus belajar karena kejahatan ini dilakukan dengan memanfaatkan teknologi informatika dan telekomunikasi canggih yang tidak dapat dilakukan oleh orang sembarangan.

c) Teori Kontrol Sosial (*Control Social*)

Menurut teori ini setiap orang dapat melakukan kejahatan, dapat mencuri, membunuh, merampok, memakai narkoba, dan sebagainya, namun yang menjadi pertanyaan utama adalah mengapa masih ada orang yang mampu bertahan untuk menaati norma ketika banyak yang melanggar norma itu, banyak tekanan, kesempatan dan bujuk rayu untuk melakukan, ternyata masih ada orang yang mau melakukannya

Oleh karena itu masih ada yang bertahan berarti mereka yang melakukan kejahatan karena kurangnya kontrol atas diri mereka baik itu kontrol pribadi maupun kontrol sosial. Kontrol pribadi adalah bagaimana seseorang mampu mengontrol dirinya sendiri agar tidak melakukan perbuatan yang menyimpang dalam mencapai keinginannya sedangkan kontrol sosial adalah kemampuan kelompok sosial atau lembaga masyarakat untuk melaksanankan norma atau peraturan agar dapat berlaku secara efektif.

Pelaku *cybercrime* biasanya melakukan kejahatannya seorang diri atau bersifat tertutup hanya pribadi atau setidaknya kelompoknya saja yang tahu sehingga bersifat privat atau ekslusif, akibat yang timbul juga tidak seketika dan tidak menimbulkan ketakutan yang besar bahkan banyak kejahatan *cyber* yang tidak di sadari oleh korbannya. Sehingga kontrol pribadi pelaku sangat kurang karena respon korban terhadap *cybercrime* sangat lambat dan tidak menghebohkan. Dalam konsep negara sebagai suatu masyarakat, maka ketika hukum dan aparat penegaknya (negara) tidak mampu merespon *cybercrime,* maka kontrol sosial terhadap kejahatan tersebut makin lemah. Hal ini yang mendukung tumbuh kembangnya *cybercrime*.

Melalui perkembangan paradigma sistem komunikasi yang bersifat global menimbulkan suatu fenomena pemikiran yang dahulu bersifat lokal ataupun nasional menjadi bersifat internasional, sehingga dalam waktu seketika *cybercrime* menjelma sebagai kejahatan dunia maya yang memanfaatkan jaringan telematika global, kejahatan yang dapat dilakukan dimana saja dan kapan saja serta menimbulkan dampak negatif kepenjuru dunia internasional. Oleh karena itu *cybercrime* menjadi kejahatan dengan pelaku, korban, tempat terjadinya perbuatan pidana (*locus delictie*), serta akibat yang ditimbulkan dapat terjadi pada dan atau di beberapa negara.

Cybercrime sebagai kejahatan internasional memiliki beberapa karakteristik unik tertentu yaitu :

a) Perbuatan yang dilakukan secara illegal, tanpa hak atau tidak etis tersebut terjadi dalam ruang /wilayah siber (cyberspace), sehingga tidak dapat dipastikan yurisdiksi negara mana yang berlaku terhadapnya.
b) Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang terhubung dengan internet.
c) Perbuatan tersebut mengakibatkan kerugian materiil maupun immaterial (waktu, nilai, jasa, uang, barang , harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan kejahatan konvensional.
d) Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya.
e) Perbuatan tersebut sering dilakukan secara transnasional /melintasi batas negara.

Selain karena karakteristiknya cybercrime itu sendiri ada beberapa faktor pendukung perkembangan cybercrime yaitu :

a) Biaya pembelian komputer, telepon seluler dan penggunaan internet semakin murah dan terjangkau sehingga pengguna komputer dan internet sangat cepat pertumbuhannya.
b) Semakin mudahnya memperoleh akses jaringan informasi dan komunikasi termasuk internet seperti pemasangan Wi-fi (wireless fidelity) yang makin banyak dan tersebar di tempat-tempat umum serta banyaknya warung internet dengan biaya pemakaian yang murah.
c) Banyak informasi yang dapat diperoleh dari internet, baik itu informasi berita dari berbagai belahan dunia maupun informasi ilmu pengetahuan dari berbagai disiplin ilmu.
d) Mengakses internet dapat dilakukan dari manapun bahkan dari tempat yang tersembunyi dari penegak hukum dan korban, bahkan dari luar kota dan luar negeri.
e) Pengakses/pengguna internet bersifat anonym (tidak diketahui siapa yang menggunakan jasa internet tersebut), tidak mudah dilacak karena tidak ada kewajiban pengguaan identitas yang sebenarnya pasa saat memasuki cyberspace.

Kemudian mengenai perbuatan yang dilarang yang dapat menyebabkan seseorang terkena sanksi pidana akibat tindak pidana di bidang siber, diterangkan dalam Pasal 37 UU ITE, sebagai berikut:

> *"Setiap Orang dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada di wilayah yurisdiksi Indonesia."*

Keterbatasan dari undang-undang ini akibat belum adanya ratifikasi perjanjian internasional di bidang siber. Hal ini menyebabkan penegakan hukum siber terbatas pada perjanjian ekstradisi dan perjanjian timbal balik antar negara yang dituangkan ke dalam suatu undang-undang.

Di bidang tindak pidana siber, telah dibentuk suatu konvensi regional yang mengatur tentang kebutuhan adanya kebijakan kriminasilasi (legal policy) terhadap tindak pidana siber. Konvensi regional tersebut adalah Convention on Cybercrime tahun 2001 yang dihasilkan oleh Council of Europe. Konvensi ini lahir dengan pemikiran "global internet, global law" yang diartikan bahwa permasalahan internet yang bersifat global diselesaikan dengan hukum yang bersifat global pula (international regime). Hal ini dapat dilihat dari preamble dari konvensi tersebut yang berbunyi sebagai berikut:

> *"Convinced of the need to pursue, as a matter of prioriry, acommon criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation."*[9]

Dalam *preamble* di atas, dinyatakan secara tegas bahwa Negara Anggota Dewan Eropa dan Negara Penandatangan meyakini adanya kepentingan untuk mencapai, sebagai suatu prioritas, kebijakan kriminal bersama yang ditujukan pada perlindungan masyarakat terhadap tindak pidana siber, antara lain dengan mengadopsi peraturan perundang-undangan yang sesuai dan memajukan kerja sama internasional.

Convention on Cybercrime tahun 2001 dapat saja menjadi alternatif penyelesaian dilema yang ada dalam pengaturan hukum khususnya kebijakan kriminalisasi di internet, namun dalam perkembangannya terdapat beberapa masalah dalam hal penerimaan terhadap konvensi ini di komunitas internasional. Salah satu masalahnya adalah fakta bahwa konvensi ini lahir dalam tataran regional. Artinya banyak negara yang akan cenderung melakukan resistensi atau penolakan terhadap norma-norma, pengaturan, infrastuktur hukum, dan produk hukum yang lahir dalam lingkup regional dimana negara tersebut bukan merupakan anggota.

Sebagai contoh, pada tanggal 22 Juni 2001, *the European Committee on Crime Problems* memutuskan untuk membentuk suatu protokol tambahan (additional protocol) yang mengkriminalisasikan kejahatan terhadap penyebaran propaganda yang bersifat rasis dan xenophobic melalui jaringan komputer sebagai pelengkap dari *Convention on Cybercrime* tahun 2001. Terkait dengan hal ini, Amerika Serikat (AS) sebagai salah satu Negara yang meratifikasi konvensi, menolak secara tegas adanya protokol tambahan tersebut dengan alasan bahwa hal tersebut bertentangan dengan Amandemen pertama dari Konstitusi AS yang mengatur tentang kebebasan berekspresi.[10]

Masalah yurisdiksi di ruang siber juga erat kaitannya dengan masalah pembentukan hukum tiap-tiap negara. Sebagai dunia tanpa batas, pembentukan dan penentuan yurisdiksi di ruang siber bukan hal yang mudah. Perlu ada kepastian mengenai siapa yang berwenang dan hukum yang akan diterapkan di dunia tanpa batas tersebut.

Akan tetapi lain halnya apabila Rancangan Undang – Undang Tindak Pidana di Bidang Teknologi Informasi telah disahkan dan diundangkan, kasus penipuan ini dapat dipidanakan karena Bab III RUU ini menerangkan lingkup berlakunya yang dipertegas

[9] Preamble of Convention on Cybercrime, Budapest, 23.XL2001

[10] Cedric J. Magnin, The 2001 Council of Europe on Cyber-Crime: A Efficient Tool to Fight Crime in Cyber-Space, LLM Dissertation on Santa Clara University, hlm. 11.

dalam Pasal 4 ayat (2) b. ini dapat menjadi dasar bagi aparat penegak hukum untuk menjerat pelaku pencurian online tersebut.

4. Bentuk Kerjasama Internasional Terkait dalam Penegakan Hukum Tentang Tindak Pidana Siber yang Didasari Prinsip Yurisdiksi Universal.

Dalam tata krama pergaulan internasional dibutuhkan permohonan ekstradisi dari Requesting State kepada Requested State. Dengan demikian, keterbatasan kedaulatan territorial bisa dijembatani melalui kerja sama dengan negara-negara lainnya untuk proses penegakan hukum. Keberhasilan kerja sama penegakan hukum tersebut pada umumnya tidak akan menjadi kenyataan jika tidak ada perjanjian bilateral maupun multilateral dalam penyerahan pelaku tindak pidana atau dalam kerja sama penyidikan, penuntutan, dan peradilan. Prasyarat perjanjian tersebut tidak bersifat mutlak karena tanpa ada perjanjian itupun kerjasama penegakan hukum dapat dilaksanakan berlandaskan asas resiprositas (timbal balik).[11]

Dasar hukum untuk pelaksanaan pemidanaan yang melibatkan negara lain, Indonesia memiliki Undang-Undang Nomor 1 Tahun 1979 Tentang Ekstradisi, dan untuk kerja sama penyidikan dan penuntutan, termasuk pembekuan dan penyitaan asset, dengan Undang-Undang Nomor 1 Tahun 2006 Tentang Bantuan Timbal Balik dalam Masalah Pidana (mutual assistance in criminal matters). Perbedaan kedua bentuk perjanjian kerja sama penegakan hukum tersebut adalah, bahwa perjanjian ekstradisi untuk tujuan penyerahan orang (pelaku tindak pidana), sedangkan perjanjian MLAT's untuk tujuan perbantuan dalam proses penyidikan, penuntutan dan pemeriksaan di sidang peradilan pidana termasuk pengusutan, penyitaan dan pengembalian asset hasil tindak pidana.

Permintaan penyerahan pelaku tindak pidana (ekstradisi) tidak serta merta merupakan pengembalian asset hasil tindak pidana yang dibawa pelaku tindak pidana yang bersangkutan. Kedua bentuk perjanjian tersebut harus saling melengkapi dan bukan dilihat secara terpisah. Hal ini berarti permintaan ekstradisi wajib dilengkapi dengan permintaan bantuan timbal balik dalam masalah pidana terutama pengusutan dan pengembalian aset tindak pidana dari pelaku tindak pidana yang bersangkutan.[12]

Sejauh ini, ekstradisi membutuhkan kerjasama terlebih dahulu dari pimpinan para negara. Meskipun undang-undang ini direncanakan akan diganti dengan rancangan undang-undang yang belum disahkan, akan tetapi sampai saat ini belum ada undang-undang pengganti tersebut, maka untuk kerjasama dibuat undang-undang yang lebih spesifik membahas mengenai kerjasama Indonesia dengan negara yang ikut dalam perjanjian, contohnya: Undang-Undang Nomor 5 Tahun 2015 Tentang Pengesahan Perjanjian Ekstradisi Antara Republik Indonesia Dan Republik Sosialis Viet Nam (Extradition Treaty Between The Republic Of Indonesia And The Socialist Republic Of Vietnam).

Mengenai ekstradisi yang merupakan kerjasama antar negara, dilandasi prinsip diplomasi dalam menjalankan hubungan internasional. Maka, penerapan yurisdiksi

[11] Ibid

[12] Ibid

universal merupakan hubungan baik yang berkesinambungan, dengan kata lain bertimbal balik.

Di lintas regional (ASEAN) bentuk konkret dari kerjasama yang dilakukan guna menanggulangi tindak pidana pidana di bidang siber telah dilakukan pemerintah Indonesia, diantaranya:

a) ASEAN Plan Of Action To Combat Transnational Crimes

   Kerjasama tersebut, mencakup kerjasama pernberantasan terorisme, perdagangan obat terlarang, pencucian uang, penyelundupan dan perdagangan senjata ringan dan manusia, bajak laut, tindak pidana internet dan tindak pidana ekonomi intemasional.

b) Traktat Bantuan Hukum Timbal Balik di Bidang pidana (*Treaty on Mutual Legal Assistance in Criminal Matter*/MLAT), Perjanjian Bantuan Hukum

   Timbal Balik di bidang pidana (MLAT) telah ditandatangani oleh semua negara anggota ASEAN di Kuala Lumpur, Januari 2006. Traktat ini melandasi kerjasama ASEAN di bidang hukum pidana Indonesia telah meratifikasi MLAT melalui Undang-Undang Nomor l5 Tahun 2008. Perjanjian ini dibentuk oleh pemerintah Brunei Darussalam, Kamboja, Indonesia,Laos, Malaysia, Filipina, Singapura dan Vietnam.

Pada kedua bentuk kerjasama di atas merupakan hal konkret dari bentuk perjanjian yang dilakukan Pemerintah Indonesia untuk menanggulangi tindak pidana siber. Adapun pengelompokan tindak pidana siber ialah sebagai berikut:[13]

a) Unauthorized Access to Computer System and Service;
b) Illegal Contents;
c) DataForgery;
d) Cyber Espionage;
e) Cyber Sabotage and Extortion;
f) Offense against Inttectual Property:
g) Infringements of Privacy

Memperhatikan bentuk-bentuk tindak pidana siber di atas, menurut peneliti bentuk tindak pidana siber dapat dikelompok dalam dua kategori, yaitu:

a) Tindak pidana biasa (konvensional) memakai komputer dan internet sebagai sarana (alat);

b) Tindak pidana baru yang menjadikan komputer dan internet serta perangkatnya sebagai sasaran (objek).

Jadi dalam tindak pidana pertama, tetap merupakan tindak pidana yang sudah dikenal atau diatur dalam KUHP Indonesia, tetapi memakai jaringan komputer dan internet. Sedangkan jenis kedua, memang tindak pidana yang lahir seiring dengan pemakaian komputer dan internet serta perangkatnya.

[13] Ari Yuliano Gema., Cybercrime: sebtrah Fenomena di Dunia Maya., http/ Center For Law Information. Llhat juga dalam http://www.interpol.eo.id. Diakses tanggal 10 Juli 2024, jam 06.30 WIB.

Indonesia untuk menanggulangi tindak pidana siber yang sifatnya melintasi batas negara belumlah maksimal. Karena dari sisi legislator, belum mengesahkan Rancangan Undang-Undang Pengesahan European Union Convention On Cybercrime, 2001 (Konvensi Uni Eropa Tentang Tindak pidana Melalui Internet, 2001).

Perjanjian yang telah diteliti hanya sebatas dari penegakan hubungan ekstradisi semata, seperti dalam kasus penipuan yang dilakukan WNA tiongkok. Pada kasus tersebut tindak pidana yang dilakukan warga negara Tiongkok dan tindak pidana tersebut ditujukan untuk warga negara Tiongkok, tetapi dilakukan di Indonesia. Penerapan terhadap tindak pidana tersebut hanya sebatas pendeportasian. Tidak banyak yang dapat dilakukan oleh Pemerintah Indonesia.

Jika disahkan draft Rancangan Undang-Undang Pengesahan European Union Convention On Cybercrime, 2001 (Konvensi Uni Eropa Tentang Tindak pidana Melalui Internet, 2001). Pada penjelasan undang-undang tersebut, dalam Isi Pokok Konvensi pada Bab III Tentang Kerjasama internasional dimuat mengenai prinsip-prinsip umum, antara lain:

a) Prinsip-prinsip umum berkaitan dengan kerjasama internasional
b) Prinsip-prinsip yang berkaitan dengan ekstradisi
c) Prinsip-prinsip umum berkaitan dengan bantuan timbal balik dan Informasi spontan
d) Prosedur-prosedur tentang permintaan bantuan timbal balik dengan tidak adanya perjanjian-perjanjian internasional yang berlaku; dan Kerahasiaan dan pembatasan penggunaan

Negara-negara yang meratifikasi perjanjian tersebut, meskipun tidak adanya perjanjian timbal balik ataupun ektradisi, memiliki komitmen kuat untuk menaggulangi tindak pidana siber. Sebagaimana diterangkan dalam poin keempat tersebut, maka penanggulangan tindak pidana siber tidak perlu ada perjanjian timbal balik antar negara.

Hal ini menjadikan tindak pidana siber dapat diminimalisir, karena pelaku tindak pidana siber tidak dapat mengelak dari suatu tuntutan pidana, karena adanya unsur locus de licti, kewarganegaraan pelaku, kewarganegaraan korban, dan lokasi korban. Celah dari suatu penyidikan tindak pidana ialah adanya unsur yang tidak terpenuhi.

Pelaksanaan yurisdiksi atas tindak pidana siber tersebut ditempuh melalui kerjasama internasional agar hukum dan keadilan tetap ditegakkan tanpa melanggar kedaulatan negara lain. Kerjasama internasional yang dapat dilakukan adalah ekstradisi, bantuan hukum timbal balik, kerjasama antar penegak hukum, misalnya Kepolisian dengan Kepolisian; dan lain-lain.[14]

Jenis-jenis bantuan yang dapat dikerjasamakan tersebut membutuhkan kelengkapan perangkat teknologi informasi dan komunikasi yang sejajar dengan yang dimiliki negara lain. Oleh karena itu kerjasama internasional akan ditindaklanjuti dengan bantuan untuk meningkatkan sarana prasarana dan kemampuan aparat penegak hukum di bidang teknologi informasi dan komunikasi.[15]

[14] Ibid, hlm 246
[15] Idem

Atas dasar itulah peneliti menganggap pentingnya pengesahan draft Rancangan Undang-Undang Pengesahan *European Union Convention On Cybercrime*, 2001 (Konvensi Uni Eropa Tentang Tindak pidana Melalui Internet, 2001) sebagai dasar penerapan yurisdiksi internasional. Kesepahaman dengan negara-negara yang telah meratifikasinya menjadikan kejahatan siber dapat ditanggulangi. Untuk kasus Russian Computer Hacker jika kejahatan yang dilakukan lintas benua dapat ditanggulangi jika ada suatu kesepahaman dan juga ada rasa keadilan bagi pelaku yang melakukan tindak pidana. Karena jika tidak memberlakukan yurisdiksi universal, tidak menutup kemungkinan pelaku di hukum di negara operasional bertindak dan oleh negara yang yang menjadi korban kejahatannya. Hukuman yang diterima kedua kali untuk kasus sama merupakan hal yang tidak tepat dan bersinggungan dengan prinsip keadilan.

5. Simpulan

Berdasarkan analisis yang dilakukan, maka disimpulkan bahwa:

a) Penerapan yurisdiksi universal bagi tindak pidana siber belum sepenuhnya dilakukan. Indonesia sudah mempunyai instrumen hukum terkait penanganan tindak pidana siber, yaitu Undang-Undang Tentang Informasi dan Transaksi Elektronik. Yurisdiksi dalam penegakan hukum terhadap tindak pidana siber didasari UU tersebut sebatas yurisdiksi ekstrateritorial, bukan universal. Sedangkan dalam Rancangan Undang – Undang Tindak Pidana Di Bidang Teknologi Informasi sudah menerapkan yurisdiksi universal, hal ini dapat dilihat dari ruang lingkup berlakunya yang tertera dalam BAB III RUU tersebut. RUU ini dapat dijadikan dasar hukum untuk menjerat para pelaku pencurian online yang dilakukan warga Tiongkok.

b) Kerjasama di bidang penegakan hukum atas tindak pidana siber sejauh ini belum mampu memberlakukan yurisdiksi universal, padahal hal ini sangat diperlukan mengingat ruang siber yang tanpa batas sehingga pelaku tindak pidana dapat menjalankan tindak pidananya tanpa terikat oleh batas wilayah. Masyarakat internasional pada saat ini masih menghormati pacta sunt servanda, sehingga penegakan hukum masih bergantung pada perjanjian atau kerjasama yang dilakukan oleh negara bersangkutan. Sedangkan dalam yurisdiksi universal, tanpa adanya kerjasama internasional pun seharusnya dapat saja diterapkan. Asalkan negara tersebut melakukan berdasar untuk kepentingan masyarakat internasional dan mengancam nilai-nilai universal.

   Masukan untuk permasalahan pemberlakuan yurisdiksi internasional dalam tindak pidana siber di Indonesia dalam penelitian ini, sebagai berikut:

   1) Terkait penerapan prinsip yurisdiksi universal dalam tindak pidana siber, Pemerintah Indonesia harus segera mensahkan dan mengundangkan Rancangan Undang – Undang Tindak Pidana Di Bidang Teknologi Informasi sebagai bentuk peraturan pelaksana (implementing legislation) dari Undang – Undang Tentang Informasi dan Transaksi Elektronik. Sehingga dapat memperjelas yurisdiksi yang dapat diterapkan dalam upaya penegakan hukum terhadap tindak pidana siber di Indonesia. Aparatur penegak hukum di Indonesia diharapkan dapat meningkatkan kemampuan di bidang siber, sehingga dapat

melakukan pendeteksian dini terhadap tindak pidana transnasional ini. Selain itu aparatur mampu menelaah kasus yang dapat diadili oleh hukum nasional, yang hanya dapat diadili pemerintah asal pelaku tindak pidana, dan yang dapat diadili oleh masyarakat internasional. Tindak pidana siber memerlukan penanganan berbeda karena tidak terbatas ruang.

2) Pemerintah Indonesia diharapkan banyak melakukan kerjasama dengan negara-negara lain, karena potensi tindak pidana siber yang dapat terjadi dimanapun negaranya. Kerjasama di bidang keamanan dan pertahanan pun perlu ditingkatkan agar meningkatkan kemampuan pemerintah dalam upaya menciptakan kondisi dunia siber yang memiliki banyak hal positif, dibanding hal negatif yang dapat menimbulkan kerugian pada masyarakat nasional ataupun internasional.

Referensi

Ahmad M. Ramli, Cyber Law dan HAKI dalam Sistem Hukum Indonesia, Refika Aditama, Bandung, 2004.

Cryer et al., Universal Jurisdiction: International and Municipal Legal

Cedric J. Magnin, The 2001 Council of Europe on Cyber-Crime: A Efficient Tool to Fight Crime in Cyber-Space, LLM Dissertation on Santa Clara University.

Danrivanto Budhijanto, Hukum Telekomunikasi, Penyiaran, & Teknologi Informasi, Refika Aditama, Bandung, 2010.Dedi Feriandi, Tinjauan Hukum dan Etika Periklanan di Internet, Menegakkan Hukum Sistem Informasi, Institut Teknologi Bandung, Agustus 2000.

Kofi A. Anan dalam UNCTAD E-commerce and Development Report, 2004.

Peraturan Perundang-undangan:

Undang-Undang Dasar 1945

Undang-Undang Nomor 1 Tahun 1979 Tentang Ekstradisi, Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Undang-Undang Nomor 1 Tahun 2006 Tentang Bantuan Timbal Balik dalam Masalah Pidana (mutual assistance in criminal matters).

Undang-Undang Nomor 1 tahun 2024 Tentang Perubahan kedua atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor l5 Tahun 2008 Tentang Pengesahan MLAT Rancangan Undang – Undang Tindak Pidana Di Bidang Teknologi Informasi

Sumber lainnya:

Ari Yuliano Gema., Cybercrime: sebtrah Fenomena di Dunia Maya., http/ Center For Law Information. Lihat juga dalam http://www.interpol.eo.id. Diakses tanggal 10 Juli 2015, jam 06.30 WIB.

Sigid Suseno, Cybercrime, Pengaturan dan Penegakan Hukumnya di Indonesia dan Amerika Serikat, Jurnal Ilmu Hukum Padjajaran Jilid XXXIII, 2009.