

PROBLEMATIKA DALAM PENANGANAN CYBER CRIME

DI INDONESIA

OLEH

Boby Iskandar, S.iP.,M.H

Dosen Sekolah Tinggi Ilmu Hukum Umel Mandiri

E-mail : iskandarboby@gmail.com

Abstrak

Perkembangan teknologi saat ini merupakan pertanda bahwa era modernisasi dengan menggunakan perangkat-perangkat elektronik akan semakin membuat manusia semakin bergantung pada perangkat tersebut. Dalam situasi ini perangkat-perangkat elektronik yang digunakan oleh setiap orang seperti smartphone, pc, smartwatch hingga perangkat rumah tangga dan perangkat elektronik lainnya yang terhubung dengan internet, dapat mempermudah hubungan sosial antar individu namun disisi lain menyimpan sejumlah besar potensi sebagai korban kejahatan oleh orang yang tidak bertanggung jawab.

Tidak dapat dipungkiri bahwa teknologi modern saat ini menciptakan kejahatan jenis baru. Walaupun kejahatan ini mirip dengan apa yang terjadi di dunia nyata seperti, pencurian, pencemaran nama baik, peniruan label sebuah perusahaan dan lain sebagainya, namun teknologi modern membuat kejahatan ini dapat terjadi tanpa menghadirkan pelaku di tempat kejadian, seperti peretas yang meretas saldo bank nasabah dan lain sebagainya.

Kejahatan siber tentu membawa kekhawatiran tersendiri bagi penegak hukum di Indonesia karena karakteristiknya yang menurut penulis masih tergolong unik.

Kata Kunci : *Cyber Crime, Teknologi*

PENDAHULUAN

Istilah “cybercrime” merujuk pada suatu tindakan kejahatan yang berhubungan dengan dunia maya (cyberspace) dan tindakan kejahatan yang menggunakan computer dan perangkat elektronik yang mengakses internet.

Ada ahli yang menyamakan tindakan kejahatan cyber (cybercrime) dengan tindakan komputer, dan ada ahli yang membedakan di antara keduanya. Secara umum yang dimaksud kejahatan komputer atau kejahatan di dunia cyber (cybercrime) adalah upaya memasuki atau menggunakan fasilitas komputer atau jaringan komputer tanpa ijin dan dengan melawan hukum dengan atau tanpa menyebabkan perubahan dan atau kerusakan pada fasilitas komputer yang dimasuki atau digunakan tersebut. (Didik Mansyur; 11;2005)

Kejahatan dalam dunia maya (cybercrime) secara sederhana dapat diartikan sebagai jenis kejahatan yang dilakukan dengan mempergunakan media internet sebagai alat bantu.

Jenis-jenis kejahatan dalam kategori cybercrime diantaranya :

1. Cyber-terorisme ;
2. Cyber-pornography : penyebarluasan obscene materials termasuk pornography, indecent exposure, dan child pornography
3. Cyber-harassment : pelecehan seksual melalui e-mail, websites, atau chats programs ;
4. Cyber-stalking : crimes of stalking melalui penggunaan komputer dan internet ;
5. Hacking : penggunaan programming abilities dengan maksud yang bertentangan dengan hukum ;
6. Carding (credit-card fraud) ;

Ciri-ciri khusus cybercrime, yakni :

1. Non violence (tanpa kekerasan) ; Sedikit melibatkan kontak fisik (minimize of physical contact) ;
2. Menggunakan peralatan (equipment) dan teknologi ;
3. Memanfaatkan jaringan telematika (telekomunikasi, media dan informatika) global ; (Didik Mansyur; 11;2005)

Dari ciri-ciri cybercrime ketiga dan keempat tersebut Nampak jelas bahwa

cybercrime dapat dilakukan dimana saja, kapan saja serta berdampak kemana saja, seakan-akan tanpa batas (borderless). Keadaan ini mengakibatkan pelaku kejahatan, korban, tempat terjadinya perbuatan pidana (locus delicti) serta akibat yang ditimbulkannya dapat terjadi pada beberapa negara, disinilah salah satu aspek transnasional/internasional dari kejahatan ini.

Kemajuan teknologi yang dipergunakan oleh pelaku kejahatan dalam cybercrime mengakibatkan timbulnya berbagai masalah hukum tersendiri dalam penanggulangannya.

Hal ini sebagaimana yang dikemukakan oleh Mochtar Kusumaatmadja, bahwa “Perkembangan kedua yang mempunyai akibat yang besar sekali terhadap perkembangan masyarakat internasional dan hukum internasional yang mengaturnya ialah kemajuan teknologi. Kemajuan teknik dalam berbagai perhubungan menambah mudahnya perhubungan yang melintasi batas Negara.

Dengan potensi kejahatan yang bisa merebak luas dan menimbulkan dampak serius dalam kehidupan masyarakat modern, maka Tindakan tegas harus

diambil guna meredam perkembangan kejahatan yang berpotensi merusak dan massif ini dapat berkembang lebih jauh. Indonesia sendiri sudah mengantisipasi kejahatan ini dengan merancang dan mengesahkan UU ITE nomor 16 tahun 2009 untuk meredam aksi kejahatan dunia maya. Sayangnya jika kita melihat kasus-kasus yang terjadi di Indonesia, kebanyakan hanya kasus *hate speech*, *pornografi cyber*, *cyber bullying*, dan lain sebagainya. Menurut penulis ini sangat disayangkan, mengingat kejahatan dunia modern bukan hanya berkutat tentang masalah tersebut namun semestinya lebih besar dan lebih berbahaya. Hal ini seperti *cyber Terrorism* atau *Hacking* yang dilakukan oleh kelompok-kelompok tertentu.

Hal inilah yang seharusnya diwaspadai sejak awal. Ketika undang-undang ITE di resmikan dan berlaku sejak tahun 2008 lalu. Namun menjadi suatu keprihatinan tersendiri bagi penulis melihat bahwa keberadaan undang-undang ITE ini lebih menjurus ke arah penertiban sosial di dunia maya seperti yang sudah disebutkan diatas seperti: pencemaran nama baik atau Cyber Bullying hingga pornografi Cyber.

Masalah inilah yang ingin penulis kaji lebih dalam agar bisa menjadi kajian ilmiah tentang posisi undang-undang ITE itu sendiri dalam konteks penanganan cyber crime di Indonesia.

METODE

Metode penelitian yang digunakan penulis adalah metode penelitian normatif dengan model deskriptif yang mendalami aspek peraturan-peraturan hukum yang terkait dengan tindak pidana siber, sehingga hasil penelitian penulis diharapkan dapat memberikan kontribusi minimal bagi pihak-pihak yang ingin mendalami permasalahan hukum siber di Indonesia.

PEMBAHASAN

Kejahatan di dunia maya hingga saat ini masih terus berkembang ke arah yang lebih maju, orang-orang yang ahli menggunakan perangkat elektronik selalu mencari metode baru untuk mencari celah keamanan untuk dibobol/diretas.

Jika dilihat dari segi akibat kejahatan, maka kejahatan melalui dunia maya (internet) dapat berdampak di dalam maupun di luar dunia maya.

Ini merupakan sebuah ilustrasi menarik yang membuktikan bahwa kejahatan siber/cyber crime bukan merupakan jenis kejahatan yang ringan walaupun modusnya mirip dengan jenis kejahatan lama yang sudah teridentifikasi dalam jenis hukum pidana maupun perdata namun, kejahatan siber benar-benar yang dikemas dalam kemasan yang benar-benar baru dan memiliki dampak *impact* yang besar. Kejahatan siber tidak lagi memerlukan kehadiran pelaku kejahatan, pelaku kejahatan dapat melakukan kejahatan tanpa terbatas ruang dan waktu, selama target berada dalam jangkauan internet yang aktif. Cukup banyak kejadian yang melibatkan serangan hacker untuk melakukan kejahatan:

1. Kasus pembobolan bank

Merujuk pada berita liputan6.com, kasus pembobolan bank juga terjadi di Indonesia dengan total kerugian mencapai 130 Milyar. Sampai saat ini pun kasus tersebut belum terungkap pelaku kejahatan tersebut. Yang diketahui melalui konferensi pers oleh Mabes Polri bahwa pelaku belum diketahui identitasnya dan berasal dari ukraina.

(<https://www.liputan6.com/bisnis/read/2213243/dibobol-hacker-uang-nasabah-di-3-bank-terkurus-rp-130-miliar>)

Ini suatu malapetaka bagi perkembangan dunia maya di Indonesia, karena pelakunya berada di negara yang berbeda, dan salah satu karakteristik penanganan cyber crime adalah kemungkinan tumpang tindih dalam yurisdiksi antar negara.

Hal ini disebabkan pada sifat dari Informasi Elektronik yang dapat ditransmisikan dari mana saja dan dapat menimbulkan akibat di berbagai tempat, baik di dalam maupun di luar wilayah suatu negara.

2. Kasus pembobolan data Bansos warga AS di Indonesia.

Kasus ini diberitakan pada 17 April 2021, dimana kejahatan ini menimbulkan kerugian mencapai \$500 Juta, pelaku membuat scampage dan menyebarkan kepada penduduk di Amerika Serikat dan mendapatkan keuntungan dari dana Bansos tersebut. Kejadian ini terjadi di Indonesia, tepatnya di Jawa Timur

dua orang peretas dari Indonesia ini menyebarkan scampage dari Indonesia agar aksinya tidak terekam.

Dengan bantuan Mabes Polri dan FBI, kasus ini sudah terungkap sejak April 2021 dengan melakukan penyelidikan selama 3 bulan dan pelaku kejahatan tersebut mendapat dakwaan sesuai dengan Pasal 32 ayat (2) Jo pasal 48 ayat (2) UU RI nomor 19 tahun 2016 tentang perubahan atas UU nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik Jo pasal 55 ayat (1) KUHP, dengan ancaman hukuman 9 tahun penjara dan/atau denda paling banyak Rp3 miliar

(<https://www.youtube.com/watch?v=JAOkEDhCTF4>)

Berdasarkan asas teritorial, hukum pidana Indonesia berlaku bagi setiap orang, baik WNI maupun WNA yang melakukan tindak pidana di dalam wilayah Indonesia, baik wilayah darat maupun laut. Prinsip ini disebut prinsip teritorial. Ruang lingkup teritorial ini diperluas dengan mempersamakan

kendaraan air dan pesawat udara yang menggunakan bendera suatu negara sebagai bagian dari wilayah negara itu. Dalam KUHP, asas teritorial diatur dalam Pasal 2 KUHP, sedangkan perluasan dari asas ini diatur dalam Pasal 3 KUHP. Selengkapnya berbunyi sebagai berikut:

Pasal 2 KUHP

Ketentuan pidana dalam perundang-undangan Indonesia diterapkan bagi setiap orang yang melakukan sesuatu tindak pidana di Indonesia

Pasal 3 KUHP

Ketentuan pidana dalam perundang-undangan Indonesia berlaku bagi setiap orang yang di luar wilayah Indonesia melakukan tindak pidana di dalam kendaraan air atau pesawat udara Indonesia.

Tidak hanya itu saja, dalam Pasal 4 KUHP dan Pasal 5 KUHP juga terdapat asas-asas keberlakuan pidana. Pasal 4 KUHP memuat asas nasionalitas pasif. Maksudnya, hukum pidana Indonesia berlaku bagi setiap orang, baik WNI maupun WNA yang melakukan tindak pidana di luar wilayah Indonesia sepanjang perbuatan itu melanggar

kepentingan Indonesia. Sedangkan Pasal 5 KUHP mengandung asas nasionalitas aktif, yaitu hukum pidana Indonesia berlaku terhadap WNI di manapun ia berada.

Dalam perkembangan penerapannya, asas-asas tersebut memiliki keterbatasan dalam menjerat seseorang yang melakukan tindak pidana siber khususnya di luar wilayah suatu negara. Oleh karena itu, banyak negara menambahkan asas ekstrateritorial. Pasal 2 UU ITE menegaskan bahwa:

Undang-Undang ini berlaku untuk setiap Orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-Undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia.

Lebih lanjut lagi, dalam Penjelasan Pasal 2 UU ITE dijelaskan sebagai berikut:

Undang-Undang ini memiliki jangkauan yurisdiksi 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 di luar wilayah hukum (yurisdiksi) Indonesia baik oleh warga negara Indonesia maupun warga negara asing atau badan hukum Indonesia maupun badan hukum asing yang memiliki akibat hukum di Indonesia, mengingat pemanfaatan Teknologi Informasi untuk Informasi Elektronik dan Transaksi Elektronik dapat bersifat lintas teritorial atau universal.

Yang dimaksud dengan "merugikan kepentingan Indonesia" adalah meliputi tetapi tidak terbatas pada merugikan kepentingan ekonomi nasional, perlindungan data strategis, harkat dan martabat bangsa, pertahanan dan keamanan negara, kedaulatan negara, warga negara, serta badan hukum Indonesia.

Dari contoh kedua kasus tersebut diatas dapat ditarik kesimpulan bahwa kejahatan cyber sebenarnya memiliki dampak kerusakan yang luar biasa mengingat bahwa kejahatan dilakukan di negara lain sedangkan target dari pelaku juga di negara lain.

Hal ini cukup berbanding terbalik dengan penerapan UU ITE di Indonesia yang sudah kehilangan ruhnyanya (baca jurnal saya di jurnal hukum umel mandiri edisi 15) UU ITE di Indonesia saat ini pun dalam kondisi yang sama, tidak memiliki ruh atau sudah tidak sehat karena di Indonesia sendiri, pasal-pasal dalam UU ITE justru dijadikan ajang saling lapor terkait nama baik atau perbuatan tidak menyenangkan hingga kasus-kasus pornografi artis yang enurut hemat penulis, makin mengaburkan posisi UU ITE ini yang digunakan hanya untuk dijadikan dasar engenaan hukuman karena Tindakan pornografi padahal UU pornografi sudah ada dalam undang-undang nomor 44 tahun 2008.

Inilah problematika yang menurut hemat penulis belum mendapat titik terang karena sejak telah dilakukan kajian multitafsir dalam UU ITE sejak februari 2021 hingga April 2021 namun belum ada putusan dari pemerintah, namun meskipun demikian Keputusan Menkopolhukam No. 22 tahun 2021, Kita Patut mengapresiasi tim kajian UU ITE untuk memberikan payung hukum yang jelas dan tidak lagi menimbulkan multitafsir seperti yang sudah terjadi di masa lalu.

PENUTUP

Cyber Crime merupakan aktivitas kejahatan dengan menggunakan fasilitas computer atau jaringan computer tanpa ijin dan melawan hokum, baik cara mengubahnya atau tanpa perubahan (kerusakan) pada fasilitas komputer yang dimasuki atau digunakan, atau kejahatan yang dengan menggunakan sarana mediaelektronik internet karena dikategorikan sebagai kejahatan dunia maya, atau kejahatan di bidang komputer dengan cara illegal, Dapat pula dikategorikan sebagai kejahatan komputer yang ditujukan kepada sistem atau jaringan komputer, yang mencakup segala bentuk baru kejahatan yang menggunakan bantuan sarana media elektronik internet.

Sanksi bagi para pelaku cybercrime adalah melalui proses peradilan dengan vonis Hakim dengan ancaman hukuman berupa kurungan penjara, denda dan lainnya seperti yang diatur dalam UU ITE nomor 19 Tahun 2016.

.

DAFTAR PUSTAKA

Dikdik M. Arief Mansur, 2005, Elisatris Gultom, Cyber Law Aspek Hukum dan Teknologi Informasi, Bandung

Abdul Wahab (2002) Kriminologi dan Kejahatan Kontemporer, Malang: Lembaga Penerbitan Fakultas Hukum Unisma.

Abdul Wahid dan Mohammad Labib (2005) Kejahatan Mayantara (Cyber Crime), Jakarta: Refika Aditama.

Agus Raharjo (2002) Cybercrime, Bandung: PT Citra Aditya Bakti.

Andi Hamzah (1989) Aspek-Aspek Hukum Pidana di Bidang Komputer, Jakarta: Sinar Grafika.

Asril Sitompul (2001) Hukum Internet (Pengenalan Mengenai Masalah Hukum Di Cyberspace), Bandung: Citra Aditya Bakti.

Barda Nawawi Arief (2003) Kapitas elekta Hukum Pidana, Bandung: Citra Aditya Bakti.

----- (2006) Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime di Indonesia, Jakarta: Rajawali Grafindo Persada

----- (2007) Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan, Jakarta: Kencana Predana Media Group

Didik M. Arief dan Elisatris Gultom
(2005) Cyber Law (Aspek Hukum
Teknologi Informasi), Bandung: Refika
Aditama.

David I. Bainbrige (1993) Komputer dan
Hukum, terjemahan dari "Computer
and the Law", Cetakan I, Jakarta: Sinar
Grafika.