YAYASAN AKRAB PEKANBARU
Jurnal AKRAB JUARA
Volume 9 Nomor 2 Edisi Mei 2024 (347-353)

2

PENGENDALIAN KASUS CYBER DI KOTA SURABAYA (STUDI PADA DISTRESKRIMSUS POLDA JAWA TIMUR)

Ika Octavia Vidianingrum H., Sinta Andhani Pou
Fakultas Hukum Universitas 17 Agustus Surabaya 1945
(Naskah diterima: 1 April 2024, disetujui: 25 April 2024)

Abstract

The scopes based on this observation are: 1) understanding the system of investigating cyber crime cases, 2) how to solve cyber crime cases and 3) the obstacles encountered in the course of investigating cyber crime cases carried out by the Ditreskrimsus Polda Jatim. This study uses a qualitative narrative technique using a case study approach. The location of the observation is the Ditreskrimsus Polda East Java and the data discovery method uses the interview and documentation method. The results of observations show that the prosecution of cyber crime cases in this case, the internal investigation system is usually the same as using normal case actions. The same applies to the accumulation of evidence, inspection & solving systems. While the difference is still in the system for catching criminals together with harmonization using exclusive aspects. it can be seen that the settlement of cyber crimes is more difficult than ordinary/general crimes, because it is mandatory to coordinate first using several exclusive parties, such as expert witnesses to receive certainty that this is indeed a criminal offense or not, the obstacle in the investigation process is the lack of good expert witnesses. Expert witnesses for images are also witnesses for language experts, and there is no unit that specifically handles cyber crime cases. Therefore, it is very necessary to take the role of expert witnesses in solving cyber crime cases and to introduce citizens to the dangers of cyber crime.
Keywords: *Case, Cyber Crime, Crime*

Abstrak

Cakupan berdasarkan observasi ini ialah: 1) memahami sistem penyidikan perkara cyber crime, 2) bagaimana pemecahan perkara cyber crime dan 3) hambatan-hambatan yang ditemui pada jalannya penyidikan perkara cyber crime yang dilakukan sang pihak Ditreskrimsus Polda Jatim. Penelitian ini memakai teknik naratif kualitatif menggunakan ancangan studi perkara. Letak observasi ialah Ditreskrimsus Polda Jatim & metode penemuan data memakai metode wawancara & dokumentasi. Hasil observasi menampakan penindakan perkara cyber crime pada perihal ini sitem penyidikan dalam biasanya sama menggunakan penindakan perkara normal biasanya. Sama pada hal akumulasi barang bukti, pemeriksaan & sistem pemecahan. Sesangkan bedanya masih ada dalam sistem penjeratan oknum kriminal bersama penyerasian menggunakan aspek-aspek eksklusif. dilihat bahwa penyelesaian perbuatan kriminal cyber crime lebih susah dibandingkan kejahatan biasa/umum, karena wajib berkoordinasi dulu menggunakan beberapa

pihak eksklusif misalnya saksi pakar agar menerima kepastian bahwa hal tadi memang adalah tindak kejahatan pidana atau bukan, hambatan pada proses penyidikan ini merupakan kurangnya saksi pakar baik saksi pakar gambar juga saksi pakar bahasa, dan nir adanya unit yg secara spesifik menangani perkara cyber crime. Karenanya sangat diperlukan kiprah saksi pakar pada penyelesaian perkara cyber crime & harus melakukan pengenalan pada warga mengenai bahaya cyber crime.
Kata Kunci: Kasus, Cyber Crime, Kejahatan

I. PENDAHULUAN

Jejaring sosial seperti Facebook, Instagram, Twitter, dan semacamnya adalah alat komunikasi yang menghubungkan satu orang ke orang lain. Bahkan dengan media sosial, kita bukan sekedar teman, kita bisa berteman dengan orang asing dan menjadi wahana bagi orang-orang untuk mengekspresikan diri melalui dunia maya. Seiring waktu, perusahaan telah mengembangkan alat media sosial untuk menjual dan memberikan layanan.

Kecepatan dan kemudahan dari apa yang sekarang dikenal sebagai media sosial telah memudahkan untuk mengakses sumber informasi. Namun, masih ada kelemahan di balik kepraktisan dan kejayaan teknologi.

Pada tataran politik, pemberantasan kejahatan dunia maya berbeda dengan pemberantasan kejahatan lainnya. Pemerintah biasanya dapat dengan mudah mengontrol dan menegakkan hukum di wilayahnya. Namun, ini tidak berlaku untuk aktivitas online, dan lokasi fisik atau lokasinya dapat berubah sewaktu-waktu, meskipun hanya dapat dibayangkan.

Berdasarkan obserfasi awal di Ditreskrimsus Polda Jawa Timur, Bahwa masih ada beberapa perkara cyber crime yang pernah ditangani, tentu hal ini sangat mengancam masyarakat. Oleh karenanya penulis berusaha melihat bagaimana proses penyelesaian berdasarkan perkara Cyber crime itu sendiri pada hal ini baik berdasarkan segi metode penyelesaian perkara sampai hingga dalam hambatan yang dihadapi sang pihak kepolisian pada penanganan perkara cyber crime (kejahatan global maya). Sehingga penulis merogoh judul "Pengendalian Kasus Cyber Di Kota Surabaya (Studi Pada Ditreskrimsus Polda Jawa Timur)" dengan memakai landasan yuridis UU ITE Nomor 11 tahun 2008 dan UU ITE 19 tahun 2006.

Perkembangan cyber crime dari berbagai muculnya beberapa istilah seperti *economic cyber crime; EFT (Electronic Funds Transfers) Crime, Cybank Crime; Internet*

Banking Crime; On-line Business Crime; Cyber / electronic Money Laundering; High Tech WWC (White Collar Crime); Cyber Terorism; Cyber Sex; Cyber Criminals dan lain-lain. Didalam back-ground paper lokakarya *Measures to Combat Computer-related Crime* Kongres XI PBB mengungkapkan dengan perkembangan teknologi yang mendunia di bidang communication and information mengacu pada pandangan gelap *(a dark shadow*), bahwa kemungkinan terjadinya wujud pendayagunaan baru, peluang hangat untuk perbuatan kriminal, dan gambaran baru atas perbuatan kriminal.

Dari perspektif hukum pidana, usaha pemberantasan kejahatan dunia maya khususnya di Indonesia bisa dipandang dari beberapa perspektif, diantaranya aspek politik pemidanaan (perumusan tindak pidana); aspek pertanggungjawaban pidana atau pemidanaan (termasuk pembuktian/alat bukti). Hal lain yang juga patut mendapat perhatian adalah investigasi kejahatan dunia maya untuk mengidentifikasi dan menghukum semua pelaku kejahatan dunia maya.

II. METODE PENELITIAN

Data primer dikumpulkan dari observasi yang dilakukan di Kepolisian Daerah Jawa Timur. Sumber lainnya adalah wawancara mendalam tentang studi kasus dan pencegahan kejahatan cybercrime. Data sekunder berasal dari literasi cybercrime

III. HASIL PENELITIAN

BENTUK-BENTUK KEJAHATAN CYBERCRIME

Sehubungan dengan perkembangan saat ini, telah banyak terjadi kejahatan yang ternyata merupakan kejahatan dunia maya. Mengenai cybercrime yang populer digunakan oleh masyarakat, dapat diartikan sebagai cybercrime atau tidak nyata. Oleh karena itu tampaknya tidak ada kejahatan atau kejahatan per tindakan. Penjahat harus memiliki objek tertentu dan subjek hukum tertentu, locus delicti dan tempus delicti Untuk menjelaskan kejahatan penulis menggunakan istilah cybercrime.

Perbuatan yg bisa mengkategorikan menjadi kejahatan pada bidang cyber crime bisa dibagi sebagai 2 (dua) kategori antara lain:

1. Tindak pidana umum yang menggunakan komputer sebagai alat atau sarana (bantuan) untuk melakukan tindak pidana, dalam hal ini komputer ikut campur, misalnya langsung atau tidak langsung, dalam proses terjadinya tindak pidana lain;

a. Carding / Credit Card Abuse or Fraud, ialah pemakaian kartu kredit dengan ilegal / ilegal memiliki tujuan atau pembelian suatu produk secara online dengan menggunakan nomor kartu kredit seseorang supaya membayar produk yang diminta.
b. Penipuan perbankan online/penipuan internet banking, yaitu melalui Internet, berarti transfer atau penarikan dana, atau transaksi bank menggunakan situs web bank dan dunia perbankan online.
c. Ancaman/terorisme, terutama melalui internet, dan memeras pihak lain untuk mencapai tujuannya.
d. Pornografi, ialah penyebaran gambar dan panggilan seksual eksplisit dari perempuan melalui Internet.

2. Kejahatan tersebut tertuju pada fasilitas komputer dan sistem teknologi informasi sehingga komputer yang bukan sasaran / korban atau biasa disebut kacking/cracing, menyerang program-program yang menguasai jaringan komputer, misalnya:

a. Dos Attack adalah serangan terhadap sistem operasi di setiap komputer.
b. Defacing/Kerusakan ilegal, perubahan (penambahan dan penghapusan) tampilan situs web / beranda tertentu secara tidak resmi / illegal
c. Fracking adalah serangan virus atau worm dan malware lainnya Robot atau Jaringan Bonet, yaitu jaringan pemilik mesin yang menyusup ke pusat komputer yang dikendalikan oleh penyerang.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengklasifikasikan berbagai kegiatan sebagai perbuatan kejahatan dunia maya. Perilaku ini meliputi:

a. Kejahatan terhadap nama domain (Pasal 16).
b. Kejahatan terhadap hak kekayaan intelektual dan hak atas informasi rahasia dalam kegiatan teknologi informasi (Pasal 19)
c. Kejahatan terhadap hak-hak pribadi (Pasal 22)
d. Kejahatan pornografi (Pasal 41)

PERTANGGUNGJAWABAN PIDANA ATAU PEMIDANAAN

Pertanggungjawaban pidana sebenarnya mengandaikan adanya celaan si pembuat (subyek hukum) atas kejahatan yang dilakukannya. Dengan demikian, pertanggungjawaban pidana mengandung pertanggungjawaban / pertanggungjawaban obyektif dan subyektif. Legitimasi), dan secara subyektif, pembuat patut dituntut atau dituduh/dijelaskan kejahatan-

nya. kewajiban (asas dosa/bersalah) yang untuknya ia patut dihukum.

Berdasarkan syarat objektif yang biasa, pertanggungjawaban pelaku kejahatan siber bahwa wajib berlandaskan terhadap asal hukum yang ada, baik dalam KUHP atau pada Undang-Undang Khusus, di samping KUHP. Selain itu, sistem Perundang-Undangan yang ada (baik KUHP maupun yang berada di luar lingkup KUHP) memiliki beberapa kekurangan dan kapasitas yang sangat terbatas untuk mengatasi bermacam permasalah kejahatan dunia maya.

Keterbatasan peraturan perundang-undangan yang ada, khususnya yang terkait dengan cybercrime, menjadikan prinsip common sense saat ini dihadapkan pada permasalahan yang timbul dari tumbuhnya cybercrime. Hal ini dapat dimengerti karena:

1. Kejahatan siber dalam lingkungan elektronik dan siber sulit didefinisikan secara pasti, sedangkan prinsip legitimasi normal berbeda dengan tindakan nyata dan keamanan hukum;
2. Cybercrime erat kaitannya oleh kemajuan teknologi maju yang berubah dengan pesat, sedangkan asas legitimasi normal jauh dari sumber hukum formal (hukum) yang statis;
3. Kejahatan dunia maya melewati batas-batas negara, sementara hukum suatu negara pada intinya cuma berfungsi di dalam wilayahnya.

Tanggung jawab pidana penjahat dunia maya juga harus berarti sensor subjektif. Ini berarti bahwa, secara subyektif, pelaku harus ditegur, didakwa, atau dibebaskan dari kejahatan untuk mendapatkan hukuman. Dengan demikian, sering dikatakan bahwa tidak ada kejahatan (criminal responsibility) tanpa kesalahan (criminal principle Prinsip keyakinan ini juga harus dipertimbangkan dalam hal pertanggungjawaban pidana penjahat dunia maya). Walaupun mungkin menghadapi permasalahan tersendiri dalam kasus cybercrime, namun tidak mudah untuk membuktikan adanya unsur kesalahan (dolus/culpa) dalam permasalahan cybercrime.

HUKUM ACARA DAN PENYIDIKAN

Pasal 42 UU ITE menyebutkan penyidikan terhadap tindak pidana sebagaimana dimaksud pada undang-undang ini, dilakukan menurut ketentuan pada aturan program pidana & ketentuan pada undang-undang ini. Hal ini berarti seluruh ketentuan pada KUHAP & undangundang lainnya yang bersangkutan menggunakan aturan program pidana, berfungsi pada maksud penyidikan pada upaya

mengungkapkan perbuatan pidana yang terjadi pada global cyber.

Selain penyidik Kepolisian Negara Republik Indonesia (Polri), sejumlah pejabat publik di pemerintahan yang ruang lingkup tugas dan tanggungjawabnya di bidang teknologi informasi dan transaksi elektronik diberi wewenang khusus, khususnya, sebagai pejabat. penyidik, sebagaimana diatur dalam hukum pidana. hukum acara penyidikan tindak pidana di bidang teknologi informasi dan transaksi elektronik, berwenang:

a. Mendapatkan pernyataan atau aduan;
b. Menginformasikan kepada seseorang atau pihak lainnya agar didengar dan/atau diperiksa menjadi tersangka atau saksi karena adanya sangkaan perbuatan pidana;
c. Mengadakan penyelidikan terhadap aduan atau penjelasan secara benar;
d. Mengadakan pengawasan kepada orang dan/atau badan usaha yang patut diduga melancarkan tindak pidana;
e. mengadakan inspeksi terhadap barang dan / atau sarana yang berhubungan atas kegiatan teknologi informasi yang diduga dipakai untuk mengadakan perbuatan pidana;
f. Mengadakaninspeksi kepada lokasi tertentu;
g. Mengadakan penutupan dan penyitaan;
h. Melibatkan prtolongan ahli untuk keperluan penyidikan;
i. Melaksanakan penyudahan penyidikan.

Dalam rangka mengungkap perbuatan pidana terkait penggunaan pemberitahuan elektronik dan transaksi elektronik, penyidik bisa bekerja sama terhadap penyidik di kota lain untuk bertukar informasi dan barang bukti. Alat bukti penyidikan, penuntutan, dan pemeriksaan di sidang pengadilan, berupa: (1) alat bukti sebagaimana dimaksud dalam ketentuan perundang-undangan, (2) alat bukti berupa informasi elektronik dan/atau dokumen elektronik.

Penyelidikan atas perampasan program elektronik berkaitan pada prediksi pelanggaran wajib dilaksanakan dengan perintah pimpinan pengadilan negeri setempat, yang memerlukan keputusan pimpinan pengadilan negeri setempat pada periode 24 jam.

IV. KESIMPULAN

Berdasarkan pembahasan diatas Pembuktian Cyber Crime Dalam Perspektif Hukum tersebut, bisa ditarik konklusi menjadi berikut: 1. Upaya – upaya yang dilakukan pada verifikasi tindak pidana pada global maya adalah :

a. Dalam rangka menanggulangi tindak pidana global maya, penyidik PoIda Jatim bisa

berkerja sama menggunakan penyidik kota lain guna mendapatkan indormasi dan barang bukti, dimana menggunakan barang bukti tersebut, bisa digunakan menjadi bahan verifikasi supaya menyebabkan keyakinan hakim terhadap kebenaran adanya suatu tindak pidana yang sudah dilakukan terdakwa.

b. Melakukan pendekatan teknologi kepada aparat penegak hukum dan masyarakat umum agar kasus cybercrime tidak berhadapan dengan teknologi dan dapat ditangani dengan menggunakan pendekatan teknologi.

Kendala yang dihadapi petugas Penegak hukum Saat menemukan bukti / pembuktian kejahatan Dunia Maya:

a. Masih kurangnya pada hal pengetahuannya mengenai teknologi digital, kode-kode digital sebagai akibatnya pada menangani tindak pidana global maya mengalami kendala pada pembuktian.
b. Undang-undang dan peraturan kejahatan dunia maya yang lemah masih ada, dan penjahat dunia maya dapat menggunakan ini untuk menemukan celah untuk menghindari jebakan hukum.

DAFTAR PUSTAKA

Barda Nawawi Arief, Tindak Pidana Mayantara, PT. Raja Grafindo, Jakarta, 2006

Budi Agus Riswandi, Hukum Cyberpace, Gita Nagari, Yogyakarta, 2006.

Undang-Undang Nomor 11 Tahun 2008

Undang-undang Nomor 36 Tahun 1999

Rancangan Undang-Undang KUHP

Kejahatan dalam Dunia Cyber.http://www.lkhtnet.com.LKHT FH UI

http://www.hukumonline.com, Hukum Online, 1 April 2010