

## TINJAUAN YURIDIS TINDAK PIDANA CYBERCRIME DALAM PERSPEKTIF HUKUM PIDANA

Oleh :

**Eliza Oktaliana Sari**  
STIEBBANK Yogyakarta

### Abstrak

Perkembangan teknologi informasi dan komunikasi membawa pengaruh besar dalam berbagai bidang kehidupan saat ini. Dimulai sejak abad ke 20, perkembangan ini membawa perubahan cepat dalam kehidupan manusia. Masyarakat telah banyak memanfaatkan kemajuan teknologi informasi dan komunikasi sebagai media untuk berbisnis, bahkan untuk kepentingan politik. Namunkarena adanya kemudahan untuk berkreaitivitas, banyak pihak tidak bertanggung jawab yang memanfaatkan kesempatan tersebut untuk hal-hal yang merugikan orang banyak. Tindak pidana yang sering terjadi saat ini adalah dalam bentuk *Cybercrime*, dengan cara memasuki, menggunakan fasilitas komputer atau jaringan komputer tanpa izin, dengan melawan hukum dengan atau tanpa menyebabkan perubahan, dan atau kerusakan pada fasilitas komputer yang dimasuki atau digunakan tersebut. Pelaku tindak pidana tersebut tidak terbatas pada usia, yang secara teritorial ini merupakan kejahatan lintas batas.

Tulisan ini bermaksud menganalisis tindak pidana *cybercrime* dalam perspektif hukumpidana, dan upaya-upaya yang dapat digunakan untuk menanggulangi kejahatan siber, dengan menggunakan metode pendekatan yuridis normatif yaitu penelitian yang menerangkan tentang ketentuan-ketentuan dalam peraturan perundang-undangan yang berlaku, dihubungkan dengan realita di lapangan. Kemudian dianalisis dengan membandingkan antara tuntutan nilai-nilai ideal yang ada dalam peraturan perundang-undangan dengan kenyataan yang ada di lapangan. Hasil penelitian yang diperoleh menunjukkan bahwa tinjauan yuridis tindak pidana *cybercrime* dalam hukum pidana yang ada di Indonesia,memiliki berbagai dampak positif maupun negatif, yang bersumber pada KUHP dan diluar KUHP, sesuai dengan pengaturan kejahatan konvensional, serta upaya-upaya yang dapat digunakan untuk menanggulangi tindak pidanacybercrime.

**Kata kunci:**Tinjauan Yuridis, Tindak Pidana *Cybercrime*, Hukum Pidana.

## A. Latar Belakang

Kemajuan teknologi informasi dan komunikasi saat ini telah menjadi pedang bermata dua, karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi sarana efektif terjadinya perbuatan melawan hukum. Dengan terjadinya perbuatan-perbuatan melawan hukum tersebut, maka ruang lingkup hukum harus diperluas untuk menjangkau perbuatan-perbuatan tersebut. Teknologi pada dirinya sendiri adalah tidak baik maupun tidak jahat, dan menyalahkannya seperti mencela gunung es karena telah menenggelamkan kapal Titanic. Kecanggihan teknologi dan perkembangan sistem transportasi dan komunikasi, yang menghasilkan ketergantungan antar bangsa telah mengakibatkan menciutnya dunia ini, sehingga menjelma menjadi suatu desa sejagat. Tidak ada satu pun bagian dari dunia ini yang terlepas dari pengamatan dan pemantauan. Kita telah dimanjakan oleh produk teknologi, karena kita dengan gampang bisa mengunjungi belahan bumi lain dari yang kita tempati dan menjalin komunikasi global, atau bercengkerama dengan orang lain, mencari pacar baru, dan bahkan belajar bagaimana menjadi teroris, menjadi anggota jaringan mafia, atau menjadi bagian dari kejahatan terorganisir.<sup>1</sup>

Munculnya kejahatan baru sebagai akibat dari perkembangan arus teknologi di dunia melalui globalisasi juga berkembang pesat, seperti pesatnya perkembangan teknologi itu sendiri, diantaranya kejahatan *manipulasi data, spionase, sabotase, provokasi, money laundering, hacking, pencurian software, penipuan on-line dan berbagai macamnya*. Bahkan pemerintah belum punya kemampuan yang cukup untuk mengimbangi kejahatan melalui internet ini sehingga sulit untuk mengendalikannya. Dengan munculnya beberapa kasus kejahatan siber (*cybercrime*) di Indonesia, telah menjadi ancaman stabilitas keamanan dan ketertiban nasional dengan eskalatif yang cukup tinggi. Pemerintah dan perangkatnya belum mampu mengimbangi teknik kejahatan yang dilakukan dengan teknologi komputer khususnya di jaringan internet dan internet (*internetwork*). Perbuatan melawan hukum *cyber* sangat tidak mudah diatasi dengan mengandalkan hukum positif konvensional, karena berbicara mengenai kejahatan itu tidak dapat dilepaskan dari 5 (lima) faktor yang saling berkaitan, yaitu pelaku kejahatan, korban kejahatan, reaksi sosial atas kejahatan dan hukum. Hukum memang menjadi instrumen penting dalam pencegahan dan penanggulangan kejahatan. Akan tetapi, untuk membuat suatu ketentuan hukum terhadap bidang hukum yang berubah sangat cepat,

---

<sup>1</sup> Abdul Wahid & Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)*, Bandung: PT Refika Aditama, 2005, hlm. 8.

seperti teknologi informasi ini bukanlah hal yang mudah. Disinilah sering kali hukum tampak cepat menjadi usang manakala mengatur bidang yang mengalami perubahan yang cepat, sehingga situasinya seperti mengalami kekosongan hukum (*vacuum recht*). Terhadap kejahatan di internet atau *cyber crime* ini tampaknya memang terjadi kekosongan hukum<sup>2</sup>.

Perkembangan yang pesat dari teknologi informasi dan komunikasi menghasilkan internet yang multifungsi. Perkembangan ini membawa kita ke ambang revolusi keempat dalam sejarah pemikiran manusia, bila ditinjau dari konstruksi pengetahuan umat manusia yang dicirikan dengan cara berfikir yang tanpa batas (*borderless way of thinking*). Percepatan teknologi semakin lama semakin meningkat yang menjadi sebab material perubahan yang terus menerus dalam semua interaksi dan aktivitas masyarakat informasi.<sup>3</sup>

Internet merupakan simbol material embrio masyarakat global. Internet membuat dunia seakan menjadi sempit. Era globalisasi ditandai dengan aksesibilitas informasi yang amat tinggi. Dimana informasi merupakan komoditi utama yang diperjualbelikan sehingga akan muncul berbagai *Network & Information Company* yang akan memperjualbelikan berbagai fasilitas bermacam jaringan dan berbagai basis data informasi tentang berbagai hal yang dapat diakses oleh pengguna dan pelanggan.

## B. Rumusan Masalah

Berdasarkan latar belakang tersebut, penulis tertarik dengan permasalahan yang ada sehingga mendorong penulis merumuskan permasalahan sebagai berikut:

1. Bagaimanakah tinjauan yuridis tindak pidana *cybercrime* dalam perspektif hukum pidana?
2. Upaya apa saja yang dapat digunakan untuk menanggulangi *cybercrime*?

## C. Metode Penelitian

Penelitian ini menggunakan metode pendekatan yuridis normatif yaitu penelitian yang menerangkan tentang ketentuan-ketentuan dalam peraturan perundang-undangan yang berlaku, dihubungkan dengan realita di lapangan. Kemudian dianalisis dengan membandingkan antara tuntutan nilai-nilai ideal yang ada dalam peraturan perundang-

---

<sup>2</sup> Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi Pengaturan dan Celah Hukumnya*, Jakarta: PT RajaGrafindo Persada, 2012, hlm. 3.

<sup>3</sup> Dikutip dari: <https://adrianestih.wordpress.com/2011/02/13/makalah-cyber-crime/> tanggal 12 September 2011.

undangan, dengan realita yang ada di lapangan, dan menganalisis upaya-upaya penanggulangannya.

#### D. Pembahasan

Kejahatan dunia maya (*Cybercrime*) merupakan kejahatan yang memanfaatkan perkembangan teknologi komputer khususnya internet.<sup>4</sup> Kejahatan dunia maya (*Cybercrime*) didefinisikan sebagai perbuatan melanggar hukum yang memanfaatkan teknologi komputer yang berbasis pada kecanggihan perkembangan teknologi internet.<sup>5</sup>

Indonesia sebagai negara hukum selalu mengutamakan semua kegiatan kenegaraan dan kemasyarakatan didasarkan pada ketentuan hukum. Karena hal itu, Indonesia selalu berusaha untuk melakukan pembaharuan Hukum Pidana, salah satunya dengan menerbitkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Karena penyelenggaraan kegiatan dalam bidang teknologi yang berbasis komputer sangat penting bagi masyarakat, dan rawan dalam melakukan pelanggaran hak asasi manusia.

Instrumen hukum memberikan landasan atau pedoman bagi para penegak hukum yang akan diterapkan kepada para pelaku *Cybercrime*. Sebagai hukum positif, pembuatannya tentu melalui mekanisme pembuatan perundang-undangan, dan sekaligus melekat sifat *Ius Constitutum*, yakni menjadi hukum positif yang memberikan sanksi bagi peristiwa atau perbuatan kriminal yang menggunakan komputer.

Dalam penerapan aturan pidana berdasarkan hukum pidana positif di Indonesia:

**1. Penerapan dalam Pasal-Pasal KUHP, dalam perkara yang menjadikan komputer sebagai sasaran kejahatan dan perkara yang menggunakan komputer sebagai sarana kejahatan.**

**a. Kategori perusakan barang yang digunakan untuk pembuktian dihadapan pihak berwajib.**

Dalam kasus *Unauthorized Transfer Payment* di Bank Negara Indonesia (BNI) Cabang New York Agency (Tahun 1986), Pengadilan Negeri Jakarta Pusat selain menjatuhkan pidana penjara terhadap terdakwa karena terbukti secara sah dan meyakinkan melanggar Pasal 363 KUHP, yaitu pencurian yang dilakukan oleh lebih

---

<sup>4</sup> Sitompul, Josua. *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana*, Jakarta.. Rajawali Pers. 2012. hlm.25

<sup>5</sup> Niniek Suparni. *Cyberspace Problematika & Antisipasi Pengaturannya*, Jakarta. Sinar Grafika, 2009. hlm.31

dari 2 orang atau lebih secara bersama-sama, juga membuktikan bahwa terdakwa terbukti secara sah dan meyakinkan melanggar Pasal 233 KUHP yaitu merusak barang yang digunakan untuk membuktikan sesuatu dihadapan pihak yang berwajib. Putusan itu dikuatkan Putusan Pengadilan Tinggi Jakarta, dan Putusan Mahkamah Agung.<sup>6</sup>

Pasal 233: Barang siapa dengan sengaja menghancurkan, merusak, membikin tidak dapat dipakai, menghilangkan barang-barang yang digunakan untuk meyakinkan atau membuktikan sesuatu di muka penguasa yang berwenang, akta-akta, surat-surat atau daftar-daftar yang atas perintah penguasa umum, terus-menerus atau untuk sementara waktu disimpan, diserahkan kepada seorang pejabat ataupun pada orang lain untuk kepentingan umum, diancam dengan pidana penjara paling lama empat tahun.

## b. Kategori Pencurian

Meliputi kasus-kasus :

- 1 Kasus *Anauthirized Transfer Payment* di Bank Negara Indonesia (BNI) Cabang New York *agency* (Tahun 1986).

Dalam kasustersebut, Pengadilan Negeri Jakarta Pusat menjatuhkan pidana penjara terhadap terdakwa karena terbukti secara sah dan meyakinkan melanggar Pasal 363 ayat (1) huruf di KUHP, yaitu pencurian yang dilakukan oleh lebih dari 2 orang secara bersama-sama. Putusan tersebut dikuatkan oleh putusan Pengadilan Tinggi Jakarta, dan Putusan Mahkamah Agung.<sup>7</sup>

- 2 Setoran Warkat Fiktif di PT Bank Bali Jakarta (Tahun 1989).

Dalam kasus tersebut, Pengadilan Negeri Jakarta Barat menjatuhkan pidana penjara kepada terdakwa karena terbukti secara sah dan meyakinkan melanggar Pasal 362 KUHP, yaitu pencurian biasa.<sup>8</sup>

Pasal 362 : Barang siapa mengambil barang sesuatu, yang seluruhnya atau sebagian kepunyaan orang lain, dengan maksud untuk dimiliki secara melawan hukum, diancam karena pencurian, dengan pidana penjara paling lama lima tahun atau pidana denda paling banyak sembilan ratus rupiah.

<sup>6</sup> Aloysius Wisnubroto, *Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer*, Universitas Atmajaya, Yogyakarta, 1999, hlm.131.

<sup>7</sup> *Ibid*

<sup>8</sup> *Ibid*

- 3 Kasus Manipulasi Data Saldo pada *Master File* Bank Danamon Cabang Glodok Plaza (Tahun 1990).

Pengadilan Negeri Jakarta Barat menjatuhkan pidana penjara kepada terdakwa karena terbukti secara sah dan meyakinkan melanggar Pasal 363 ayat (1) huruf e KUHP *juncto* Pasal 64 ayat (1) KUHP, yaitu melakukan pencurian dalam keadaan memberatkan yang dilakukan berulang kali sebagai perbuatan berlanjut. Putusan tersebut dikuatkan oleh putusan Pengadilan Tinggi, dan Putusan Mahkamah Agung.<sup>9</sup>

Ketentuan pasal 363 ayat (1) huruf e, diancam dengan pidana penjara paling lama tujuh tahun :Pencurian yang untuk masuk ke tempat melakukan kejahatan, atau untuk sampai pada barang yang diambil, dilakukan dengan merusak, memotong atau memanjat, atau dengan memakai anak kunci palsu, perintah palsu atau pakaian jabatan palsu.

#### c. Kategori Persaingan Curang

Dalam kasus "Domain Name" PT Mustika Ratu Mahkamah Agung melalui Putusan Mahkamah Agung No. 1082 K./Pid./2002, tanggal 24 Januari 2003, memutuskan bahwa domain name mustika-ratu.com memenuhi delik pemalsuan curang sebagaimana diatur dalam Pasal 382 bis KUHP. Untuk itu, terdakwa (Chandra Sugiono) dijatuhi penjara selama 4 (empat) bulan. Putusan Mahkamah Agung ini membatalkan Putusan Pengadilan Negeri Jakarta Pusat yang dalam putusannya membebaskan terdakwa dari segala tuntutan.<sup>16</sup>

Pasal 382 *bis* :Barang siapa untuk mendapatkan, melangsungkan atau memperluas hasil perdagangan atau perusahaan milik sendiri atau orang lain, melakukan perbuatan curang untuk menyesatkan khalayak umum atau seseorang tertentu, diancam, jika perbuatan itu dapat menimbulkan kerugian bagi konkuren-konkurennya atau konkuren-konkuren orang lain, karena persaingan curang, dipidana penjara paling lama satu tahunempat bulan, atau pidana denda paling banyak tiga belas ribu lima ratus rupiah.

#### d. Kategori Pemalsuan

<sup>9</sup> Widyopramono, 1994, *Kejahatan di Bidang Komputer*, Pustaka Sinar Harapan, Jakarta, hlm.67. 16 Sabartua Tampubolon, 2003, *Aspek Hukum Nama Domain di Internet*, Tata Nusa, Jakarta, hlm.92.

Terdakwa Petrus Pangkur dijatuhi pidana penjara selama 15 (lima belas) bulan oleh Pengadilan Negeri Sleman (Yogyakarta) karena terbukti secara sah dan meyakinkan melakukan tindak pidana pemalsuan melalui internet. Pelaku membeli barang dengan menggunakan kredit milik warga negara Amerika Serikat melalui perdagangan *online* (*e-commerce*). Ketentuan yang digunakan sebagai dasar mengadili terdakwa adalah Pasal 378 KUHP. Total harga barang yang dibeli adalah Rp.4.000.000,00 (empat juta rupiah). Waktu yang diperlukan untuk penyidikan kasus tersebut 8 (delapan) bulan.<sup>10</sup>

Pasal 378 :Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi hutang maupun menghapuskan piutang diancam karena penipuan dengan pidana penjara paling lama empat tahun.

## 2. Penerapan Ketentuan Undang-Undang di Luar KUHP untuk Mengadili Perkara yang menjadikan Komputer sebagai Sarana Kejahatan.

### a. Undang-Undang No. 28 Tahun 2014 tentang Hak Cipta.

Ketentuan Undang-Undang No. 28 Tahun 2014 tentang Hak Cipta diterapkan pada kasus pembajakan Program Komputer *Word Star* versi 5.0, pada tahun 1990. pengadilan negeri bandung menjatuhkan pidana penjara dan pidana denda kepada terdakwa, karena terbukti secara sah dan meyakinkan melanggar Pasal 11 ayat (1) huruf k, *juncto* Pasal 14 huruf g, *juncto* pasal 44 ayat (1) Undangundang No. 7 Tahun 1987 tentang hak cipta, *juncto* Keputusan Presiden (Kepres) RI Nomor 25 Tahun 1989, *Juncto* Pasal 55 ayat (1), *juncto* pasal 64 KUHP. Putusan ini dikuatkan oleh Putusan Pengadilan Tinggi Bandung.<sup>11</sup> Dalam pasal 11 ayat (1) huruf k, diatur tentang program komputer sebagai hak cipta khusus.

Pasal 44 ayat (1) : Barangsiapa dengan sengaja dan tanpa hak mengumumkan atau memperbanyak suatu ciptaan atau memberikan izin untuk itu, dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/ atau denda paling banyak Rp.100.000.000 (seratus juta rupiah).

<sup>10</sup> *Ibid.*

<sup>11</sup> Aloysius Wisnubroto. Cit., 1999, p. 162.

**b. Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi.**

Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi diterapkan dalam kasus pembobolan Situs Komisi Umum (KPU), pada tahun 2004. Pengadilan Negeri Jakarta Pusat menjatuhkan pidana penjara kepada Dani Firmansyah (usia 25 tahun), karena terbukti secara sah dan meyakinkan melanggar Pasal 22 huruf c, *juncto* pasal 50 Undang-undang Nomor 36 Tahun 1999 tentang telekomunikasi.<sup>12</sup>

Pasal 22 : Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi:

- 1) Akses ke jaringan telekomunikasi.
- 2) Akses ke jasa telekomunikasi, dan atau
- 3) Akses ke jaringan telekomunikasi khusus.

Pasal 50 : Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam pasal 22 dipidana dengan pidana penjara paling lama 6 (enam) tahun dan atau denda paling banyak Rp. 600.000.000 (enam ratus juta rupiah), dan semua tindak pidana dalam Undang-Undang Nomor 36 Tahun 1999 dinyatakan sebagai kejahatan.

**c. Undang-undang Nomor 32 Tahun 2002 tentang Penyiaran.**

- 1) Pasal 57 Jo. Pasal 36 ayat (5) mengancam pidana terhadap siaran yang :
  - ❖ Bersifat fitnah, menghasut, menyesatkan, dan/atau bohong ;
  - ❖ Menonjolkan unsur kekerasan, cabul, perjudian, penyalahgunaan narkotika dan obat terlarang; atau
  - ❖ Mempertentangkan suku, agama, ras, dan antar golongan.
- 2) Pasal 57 Jo. Pasal 36 ayat (6) mengancam pidana terhadap siaran yang memperolokkan, merendahkan dan/atau mengabaikan nilai-nilai agama, martabat manusia Indonesia, atau merusak hubungan internasional.
- 3) Pasal 58 jo. Pasal 46 ayat (3) mengancam pidana terhadap siaran iklan niaga yang di dalamnya memuat:
  - ❖ Promosi yang dihubungkan dengan ajaran suatu agama, ideologi, pribadi dan/atau kelompok, yang menyinggung perasaan dan/ atau merendahkan martabat agama lain, ideologi lain, pribadi lain, atau kelompok lain;
  - ❖ Promosi minuman keras atau sejenisnya dan bahan atau zat adiktif;
  - ❖ Promosi rokok yang memperagakan wujud rokok;

<sup>12</sup> Majalah Gatra, "Pembobol Situs KPU Divonis 6 Bulan 21 Hari ", Jakarta, 24 Desember 2006.

- ❖ Hal-hal yang bertentangan dengan kesusilaan masyarakat dan nilai-nilai agama; dan/atau
- ❖ Eksploitasi anak di bawah umur 18 tahun.

Catatan:

Berbeda dengan Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi, dalam Undang-Undang Penyiaran ini tidak ada penentuan kualifikasi delik sebagai kejahatan atau pelanggaran.

#### **d. Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.**

Sejak tanggal 21 April 2008, bangsa Indonesia memasuki babak baru dalam pengaturan penggunaan teknologi dan informasi dan transaksi elektronik, yaitu adanya pengesahan rancangan Undang-undang tentang informasi dan transaksi elektronik yang kemudian di Undangkan menjadi Undang-Undang Negara Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (LN Republik Indonesia Tahun 2008 Nomor 58; TLN Republik Indonesia Nomor 4842). Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disingkat UU-ITE) tersebut mutlak diperlukan bagi Negara Indonesia, karena saat ini Indonesia merupakan salah satu negara yang menggunakan dan memanfaatkan teknologi informasi secara luas dan efisien, dan secara faktual belum banyak memiliki ketentuan hukum, terutama dari aspek hukum pidana.

Cakupan materi UU-ITE secara umum antara lain berisi tentang Informasi dan dokumen elektronik, pengiriman dan penerimaan surat elektronik, tanda tangan elektronik, sertifikat elektronik, penyelenggaraan sistem elektronik.

Berdasarkan uraian kasus kejahatan dan penerapan hukum pidana diatas dapat disimpulkan sebagai berikut :

- 1) Ketentuan dalam hukum pidana diterapkan dengan cara melakukan penafsiran ekstensif.
- 2) Peraturan perundang-undangan yang mengatur secara eksplisit tentang kejahatan yang menyerang komputer hanya Undang-Undang telekomunikasi. Sedangkan Undang-Undang yang secara khusus mengatur tentang pembajakan program komputer hanya Undang-Undang Hak Cipta.
- 3) Jenis pidana yang dijatuhkan adalah pidana penjara dan pidana denda.

- 4) Jika dibandingkan dengan ketentuan dalam *Convention on Cybercrime*, bentuk-bentuk *Cybercrime* di Indonesia yang sudah diadili adalah data interference (yaitu kasus pembobolan situs KPU, *Computer Related Fraud* (yaitu kasus korupsi di beberapa Bank), *Computer Related Forgery* (yaitu kasus pemalsuan kartu kredit yang dilakukan oleh Petrus Pangkur), offences Related to infringement of copyright and related rights (yaitu kasus pembajakan program komputer *words star versi 5.0*).

Berdasarkan banyak kasus yang terjadi di Indonesia, maka menurut analisis penulis :bahwaperkembangan tindak pidana *cybercrime* di Indonesia sudah mencapai tingkat yang memprihatinkan. Hal ini ditandai dengan pesatnya perkembangan cara melakukan kejahatan (modus operandi) maupun alat yang digunakan. Akibatnya, Indonesia dijuluki dunia sebagai negara kriminal internet.

Pada tahun 2002, pihak Kepolisian Indonesia telah mengungkap 109 kasus tindak pidana Teknologi Informasi (TI) yang dilakukan oleh 124 orang tersangka yang merupakan warga negara Indonesia yang melakukan berbagai aksinya di berbagai kota di Indonesia. Secara garis besar, kejahatan yang berkaitan dengan teknologi informasi ini dibagi menjadi dua. Pertama, kejahatan yang bertujuan untuk merusak atau menyerang sistem atau jaringan komputer. Kedua, kejahatan yang menggunakan komputer atau internet sebagai alat bantu dalam melancarkan kejahatan. Dalam beberapa literatur dan situs-situs yang menyetengahkan kejahatan siber, berpuh jenis kejahatan siber yang terjadi. Yang termasuk dalam kategori kejahatan umum yang difasilitasi teknologi antara lain penipuan kartu kredit, penipuan bursa efek, penipuan perbankan, pornografi anak, perdagangan narkoba, serta terorisme. Sedangkan kejahatan yang menggunakan teknologi informasi adalah *defacing*, *cracking*, ataupun *phreaking*.

Menyikapi maraknya kasus tindak pidana *cybercrime* ini, maka dilakukan berbagai upaya penanggulangan tindak pidana sebagai berikut :

### 1. Sarana Penal (Kebijakan Penal)

Kebijakan Penal (kebijakan dalam hukum pidana) adalah salah satu kebijakan dalam penanggulangan kejahatan dengan menggunakan hukum pidana. Kebijakan tersebut dioperasikan dengan cara menerapkan hukum pidana, yaitu pidana materiil, hukum formil dan penitentier dalam masyarakat. Dalam Kongres PBB ke-4 yang berlangsung di Kyoto,

disepakati bahwa usaha pencegahan kejahatan termasuk penerapan hukum pidana merupakan bagian integral dari rencana pembangunan nasional<sup>13</sup>. Kebijakan hukum pidana pada hakikatnya merupakan usaha untuk mewujudkan peraturan perundang-undangan pidana agar sesuai dengan keadaan pada waktu tertentu (*ius constitutum*) dan masa yang akan datang (*ius constituendum*)<sup>14</sup>. Dalam upaya menanggulangi tindak pidana *cybercrime*, resolusi Kongres PBB VIII/1990 mengenai *computer related crimes* mengajukan beberapa kebijakan antara lain:

- a. Menghimbau negara-negara anggota untuk mengintensifkan upaya-upaya penanggulangan penyalahgunaan computer, lebih efektif dengan mempertimbangkan langkah-langkah berikut :
  - 1) Melakukan modernisasi hukum pidana materiil dan hukum acara pidana.
  - 2) Mengembangkan tindakan-tindakan pencegahan dan pengamanan komputer.
  - 3) Melakukan langkah-langkah untuk membuat peka warga masyarakat, aparat penegak hukum, dan pengadilan, terhadap pentingnya pencegahan kejahatan yang berhubungan dengan computer.
  - 4) Melakukan upaya-upaya pelatihan bagi para hakim, penegak hukum, dan pejabat, mengenai kejahatan dibidang ekonomi dan *cybercrime*.
  - 5) Memperluas *rules of ethics* dalam penggunaan computer, dan mengajarkannya melalui kurikulum informatika.
  - 6) Mengadopsi kebijakan perlindungan korban sesuai deklarasi PBB mengenai korban, dan mengambil langkah-langkah untuk mendorong korban melaporkan adanya kejahatan siber.
- b. Menghimbau agar negara-negara anggota meningkatkan kegiatan internasional dalam upaya penanggulangan tindak pidana *cybercrime*.
- c. Merekomendasikan kepada Komite Pengendalian dan Pencegahan Kejahatan PBB untuk:
  - 1) Menyebarkan pedoman dan standar untuk membantu negara anggota menghadapi *cybercrime* di tingkat nasional, regional, maupun internasional.
  - 2) Mengembangkan penelitian dan analisis lebih lanjut guna menemukan cara-cara baru menghadapi permasalahan *cybercrime* dimasa mendatang.

<sup>13</sup> Widodo, op.cit, hlm. 188.

<sup>14</sup> Lilik Mulyadi, *Bunga Rampai Hukum Pidana Prespektif, Teoritis dan Praktik*, Bandung: PT. Alumni, 2008, hlm. 390.

- 3) Mempertimbangkan *cybercrime* sewaktu meninjau pengimplementasian perjanjian ekstradisi, dan bantuan kerjasama dibidang penanggulangan kejahatan<sup>15</sup>.

## 2. Sarana Non Penal (Kebijakan Non Penal)

Kebijakan non penal dapat ditempuh dengan cara memperbaiki perekonomian nasional, melakukan pendidikan budi pekerti kepada setiap orang, baik secara formal maupun non formal, terutama kepada pihak yang rentan melakukan kejahatan, memperbaiki sistem kesehatan mental masyarakat, mengefektifkan kerjasama internasional dalam pemberantasan tindak pidana *cybercrime*, memperbaiki sistem pengamanan komputer, serta mengefektifkan hukum administrasi dan hukum perdata, yang berhubungan dengan penyelenggaraan sistem dan jaringan komputer. Hal ini senada dengan *Convention on Cyber Crime*, bahwa kerjasama internasional yang perlu dilakukan dalam rangka penanggulangan kejahatan siber adalah perjanjian ekstradisi, *mutual assistance in criminal matters*, pemberian informasi secara spontan, dan pembentukan jaringan yang dikelola oleh tenaga profesional dalam rangka menjamin terselenggaranya bantuan secepatnya untuk investigasi dan peradilan untuk mengumpulkan alat bukti elektronik. Bantuan-bantuan tersebut berupa fasilitas atau bantuan lain, dengan syarat dan izin oleh hukum nasional masing-masing Negara. Dalam hal ini diatur pula pertanggungjawaban korporasi, baik dalam hukum pidana, maupun dalam hukum perdata dan hukum administrasi.

## E. PENUTUP

Berdasarkan uraian dari pembahasan di atas, maka dapat dikemukakan **kesimpulan** sebagai berikut:

1. Bahwa tinjauan yuridis tindak pidana *Cybercrime* dalam perspektif hukum pidana yang terjadi selama ini, pengaturannya dibedakan menjadi 2 yaitu : didalam KUHP dan diluar KUHP.
  - a) Di dalam KUHP.
    - ❖ Kategori Pencurian diatur dalam pasal 362 KUHP.
    - ❖ Kategori Persaingan Curang diatur dalam pasal 382 KUHP.
    - ❖ Kategori Penipuan diatur dalam pasal 378 KUHP.

<sup>15</sup> Barda Nawawi Arief, *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia*, Jakarta: PT RajaGrafindo Persada, hlm. 3.

## b) Diluar KUHP

- ❖ Undang-Undang Nomor 14 tahun 2002 tentang Hak Cipta.
- ❖ Undang-Undang Nomor 28 tahun 2014 tentang Telekomunikasi.
- ❖ Undang-Undang Nomor 32 tahun 2002 tentang Penyiaran.
- ❖ Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik.

2. Berbagai upaya penanggulangan tindak pidana *cybercrime* dilakukan, meliputi atas:

- a) Sarana Penal (Kebijakan Penal)
- b) Sarana Non Penal (Kebijakan Non Penal)

Sarana dan kebijakan yang ada diharapkan dapat menanggulangi tindak pidana *cybercrime*, walaupun tidak bisa sepenuhnya bisa mengatasi tindak pidana tersebut. Peningkatan kualitas sarana dan kebijakan dalam menanggulangi kejahatan ini yang sangat dibutuhkan.

**Saran-saran** yang dapat penulis berikan berdasarkan pembahasan adalah :

1. Kebijakan kriminalisasi dan pemidanaan terhadap *cybercrime* dalam dunia maya harus terus diharmonisasikan, seiring maraknya kejahatan di dunia *cyber* yang semakin canggih. Hal ini disebabkan oleh tindak pidana teknologi informasi yang tidak mengenal batas-batas territorial, dan beroperasi secara maya. Oleh karena itu, Pemerintah harus selalu berupaya mengantisipasi aktivitas-aktivitas baru yang diatur, sesuai ketentuan hukum yang berlaku.
2. Perlu adanya aturan pemidanaan terhadap penyertaan, percobaan, dan pengulangan (*residive*) terhadap tindak pidana *cybercrime*. Pemidanaan yang sama terhadap penyertaan dan percobaan, serta ada pemberatan terhadap perbuatan pengulangan dimaksudkan untuk menghindari terjadinya ketidakadilan hokum, dan sebagai upaya untuk kesejahteraan sosial (*social welfare*) dan untuk perlindungan masyarakat (*social defence*).
3. Mengingat yurisdiksi *cybercrime* bersifat *transnational crime*, maka agar lebih efektif dan efisien, tindak pidana teknologi informasi dapat dipertimbangkan untuk memanfaatkan internet (melalui e-mail atau messenger) dan *digital signature* sebagai sarana pemeriksaan, sehingga dapat menghemat waktu, biaya dan jarak.

## DAFTAR PUSTAKA

### Literatur

- Abdul Wahid & Mohammad Labib, 2005, "*Kejahatan Mayantara (Cyber Crime)*", Bandung: PT Refika Aditama.
- Alexander Pattipeilohi, 1985, "*Di Balik Kecanggihan Sebuah Teknologi*". Majalah Komputer dan Elektronika.
- Aloysius Wisnusubroto, 1999, *Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer*, Universitas Atmajaya, Yogyakarta.
- Budi Suhariyanto, 2012, *Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi Pengaturan dan Celah Hukumnya*, Jakarta: PT Raja Grafindo Persada.
- Edy Junaedi Karnasudirja, 1993, *Jurisprudensi kejahatan Komputer*, Tanjung Agung, Jakarta.
- Hanny Kamarga, 2002, *Belajar Sejarah Melalui E-Learning : Alternatif Mengakses Sumber Informasi Kesejarahan*, Intimedia, Jakarta.
- Lilik Mulyadi, 2008, *Bunga Rampai Hukum Pidana Prespektif, Teoritis dan Praktik*, Bandung: PT. Alumni.
- Mardjono Reksodiputro, "*Kejahatan Komputer: Suatu Catatan Sementara dalam KUHP Nasional yang Akan Datang*", Prasaran dalam Lokakarya tentang Bab-Bab Kodifikasi Hukum Pidana, Diselenggarakan oleh BPHN-Departemen Kehakiman RI, Jakarta: 18-19 Januari 1988.
- Nawawi, Arief, Barda, 2006, *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia*, Jakarta: PT RajaGrafindo Persada.
- Niniek Suparni, 2009, *Cyberspace Problematika & Antisipasi Pengaturannya*, Jakarta. Sinar Grafika.
- Rachmat Rafiudin, 2009, *Internet Foeronsik*, CV Andi Offset, Yogyakarta.
- Sabartua Tampubolon, 2003, *Aspek Hukum Nama Domain di Internet*, Tata Nusa, Jakarta.
- Sitompul, Josua. 2012, *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana*, Jakarta.. Rajawali Pers.
- Widyopramono, 1994, *Kejahatan di Bidang Komputer*, Pustaka Sinar Harapan, Jakarta.

### Peraturan Perundang-Undangan

Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta.

Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.

Undang-Undang Nomor 32 Tahun 2002 tentang Penyiaran

Undang-undang Nomor 3 Tahun 1971 tentang pemberantasan Tindak Pidana Korupsi.  
(sekarang telah diganti dengan Undang-Undang Nomor 31 Tahun 1999 tentang  
Tindak Pidana Korupsi)

Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

### **Majalah**

Majalah Gatra, "*Pembobol Situs KPU Divonis 6 Bulan 21 Hari* ", Jakarta, 24 Desember 2006

### **Internet**

[https://adrianestih.wordpress.com/2011/02/13/makalah-cyber-crime/http://www.livinginternet.com/i/ii\\_ip.to.htm](https://adrianestih.wordpress.com/2011/02/13/makalah-cyber-crime/http://www.livinginternet.com/i/ii_ip.to.htm)<http://www.ugm.ac.id/files>