

# PEMIDANAAN CYBERCRIME DALAM PERSPEKTIF HUKUM PIDANA POSITIF

Andri Winjaya Laksana  
Fakultas Hukum Unissula  
[andriwinjaya@gmail.com](mailto:andriwinjaya@gmail.com)

## **Abstract**

*Cybercrime is a crime that uses computers as a tool and crimes that target computers. With the enactment of Law Number 11 of 2008, which includes and regulates everything about cybercrime, it has made it easier for efforts to combat cybercrime in Indonesia. In this Law, imprisonment is still dominant in imposing crimes against cybercriminals. Due to the characteristics of cybercrime perpetrators that are unique and different from the characteristics of conventional criminals, including perpetrators who are relatively young, educated, respectable people, skilled in operating computers and their application programs like technological, creative, and resilient challenges, it is necessary to deal with them separately. which is different from other criminal offenders. This is based on the concept of individualization of punishment, that the crime must be in accordance with the convict's condition by observing the principle of mono dualistic balance. Supervision punishment, or social work punishment, and criminal fines, compensation, and certain actions can be used as an alternative to short-term imprisonment against cybercrime offenders.*

**Keyword:** *Cybercrime, positive criminal law, punishment,*

## **A. PENDAHULUAN**

Perkembangan teknologi informasi juga membentuk masyarakat dunia baru yang tidak lagi dihalangi oleh batas-batas teritorial dan telah membalikkan segalanya yang jauh jadi dekat yang khayal jadi nyata. Namun di balik kemajuan itu, juga telah melahirkan keresahan-keresahan baru dengan munculnya kejahatan yang canggih dalam bentuk *cybercrime*.

Developments in information technology have transformed almost all facets of life. In one side of the computer technology has the advantage of an opportunity to get information, work, participate in

politics and democratic life and other advantages, but on the other hand, information technology will "bite" real life which we have long struggled with all existing heritage. Netizens can see this as a problem to be solved before it moves further down the road and alleys of cyberspace.<sup>1</sup>

Kejahatan dengan menggunakan teknologi, yaitu teknologi informasi khususnya komputer dan internet (*cybercrime*) telah sampai pada tahap mencemaskan. Kemajuan teknologi informasi, selain membawa ke dunia bisnis yang revolusioner (*digital revolution era*) yang serba praktis, ternyata memiliki sisi gelap yang mengerikan, seperti pornografi, kejahatan komputer, bahkan terorisme digital, perang informasi sampah, dan *hacker*.

Problem pelanggaran hukum atau dengan nama lain kejahatan merupakan tanggung jawab setiap unsur masyarakat. Karena selain kejahatan itu setua usia sejarah kehidupan masyarakat juga embrio dan konstruksi masyarakat itu sendiri. Namanya saja kerawanan sosial dan penyakit membahayakan, tentulah logis jika masyarakat menunjukkan sikapnya.<sup>2</sup>

Internet dan teknologi informasi merupakan inovasi baru pada dekade terakhir ini dan sangat mempengaruhi kehidupan manusia. Beberapa aktifitas manusia berubah secara signifikan dengan mengambil keuntungan dari efisiensi, efektifitas, dan mobilitas. Sayangnya, kemajuan teknologi ini juga memperkenalkan permasalahan-permasalahan baru saat digunakan secara tidak tepat atau menyalahi dari yang semestinya. Kejahatan *cyber* (*cybercrime*) adalah bentuk ancaman baru yang belum pernah ada sebelumnya pada masyarakat dunia. *Hacking, cracking, defacing, sniffing, carding, phishing, spamming*, ataupun *scam* adalah sederet kejahatan internet

---

<sup>1</sup> Andri Winjaya Laksana, *Cybercrime Comparison Under Criminal Law In Some Countries*, *Jurnal Pembaharuan Hukum*, Vol V No.2 April – Agustus 2018, hlm.217-226

<sup>2</sup> Achmad Sodiki dalam Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cybercrime)*, Cetakan Kesatu, Refika Aditama, Bandung, 2005, hlm. vii.

yang cukup berbahaya dan telah menimbulkan kerugian nyata pada banyak pihak.

*Cybercrime* di Indonesia terjadi sejak tahun 1983, terutama terjadi di bidang perbankan.<sup>3</sup> Dalam tahun-tahun berikutnya sampai saat ini, di Indonesia banyak terjadi *cybercrime*, misalnya pembajakan program komputer, *cracking*, penggunaan kartu kredit pihak lain secara tidak sah (*carding*), pembobolan bank (*banking fraud*), pornografi, termasuk kejahatan terhadap nama domain (*domain name*). Selain itu, kasus kejahatan lain yang menggunakan komputer di Indonesia antara lain penyelundupan gambar-gambar porno melalui internet (*cyber smuggling*), *pagejacking* (*moustrapping*), *spam* (*junk mail*), *intercepting*, *cybersquatting*, *typosquatting*. Sedangkan kasus kejahatan terhadap sistem atau jaringan komputer antara lain *cracking*, *defacing*, *denial of service attack* (*DoS*), *distributed denial of service attack* (*DDoS*), penyebaran virus (*worm*), dan pemasangan *logic bomb*.

Memerangi kejahatan internet telah menjadi porsi utama bagi agen-agen penegak hukum dan intelejen baik nasional maupun internasional tak terkecuali praktisi-praktisi bisnis, *merchant*, para pelanggan, sampai kepada *end-user*. Pada kebanyakan kasus, kejahatan internet dimulai dengan mengeksploitasi *host-host* dan jaringan komputer. Oleh karena itu, para penipu dan *entruder* datang melintasi jaringan, terutama sekali jaringan-jaringan yang berbasis protokol TCP/IP.<sup>4</sup>

Saat ini, meskipun hukum pidana konvensional sebagaimana yang berlaku di Indonesia dapat digunakan hakim sebagai dasar

---

<sup>3</sup> 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, hlm. 2

<sup>4</sup> Rachmat Rafiudin, *Internet Forensik*, Andi Offset, Yogyakarta, 2009, hlm. 1.

hukum untuk mengadili pelaku *cybercrime*, tapi dalam praktik banyak sekali keterbatasannya, baik dari sisi unsur tindak pidana maupun pertanggung jawaban pidananya. Akibatnya, banyak pelaku yang lolos dari jeratan hukum, atau kalaupun dijatuhi pidana berdasarkan hasil penelitian semua pelaku dijatuhi pidana penjara. Dalam tataran filosofis, teori teoritis, normatif, maupun empiris, pidana penjara merupakan suatu jenis pidana yang mempunyai banyak kelemahan, karena pelaksanaan pidana penjara, khususnya di Indonesia kurang memadai.

Bank Dunia (*World Bank*) beranggapan bahwa lemahnya penegakan hukum dalam penanggulangan *cybercrime* di Indonesia karena belum memiliki peraturan perundang-undangan tentang pengembangan aplikasi informatika generasi baru. Bahwa sampai saat ini belum adanya peraturan perundang-undangan yang secara khusus disebabkan fakta bahwa peraturan *cyberspace* memerlukan kajian-kajian yang cermat dan mendalam agar dapat benar-benar tepat sasaran sesuai dengan tingkat perkembangan perilaku kehidupan masyarakat agar implementasinya tidak menimbulkan *stagnasi*.<sup>5</sup> Selain itu, sifat dari *cyber* adalah *global crimes*, yaitu kejahatan yang melampaui batas-batas negara atau kejahatan tanpa batas wilayah teritorial.<sup>6</sup>

Indonesia ketinggalan dengan negara-negara lain dalam bidang pengaturan *cybercrime*, misalkan dibandingkan dengan Singapura, Malaysia, Amerika Serikat, dan Jerman. Meskipun demikian, berkaitan dengan upaya pembaharuan hukum yang mengatur *cybercrime*, negara-negara anggota ASEAN (termasuk Indonesia) menyepakati bahwa *Convention on Cybercrime* adalah satu-satunya instrumen

---

<sup>5</sup> Yusril Ihza Mahendra, *Regulasi Cyberspace di Indonesia*, Makalah Pada Seminar Tentang *Cyberlaw*, Bandung, 2000, hlm. 3.

<sup>6</sup> Barda Nawawi Arief, *Bunga Rampai Hukum Pidana*, Cipta Aditya Bakti, Bandung, 2003, hlm. 114.

internasional yang digunakan sebagai acuan untuk penyusunan hukum domestik tentang *cybercrime* dan upaya penanggulangan secara internasional.<sup>7</sup> Dalam rangka menanggulangi kejahatan di bidang *cyber*, Majelis Umum Perserikatan Bangsa-Bangsa (PBB) juga sudah menyelenggarakan beberapa kongres dan menerbitkan beberapa resolusi yang berisi pedoman penanggulangan *cybercrime*.<sup>8</sup> Begitu pula dengan negara-negara yang telah meratifikasi *Convention on Cybercrime*,<sup>9</sup>

Kegiatan *cyber* meskipun bersifat *virtual* dapat dikategorikan sebagai tindakan dan perbuatan hukum yang nyata. Secara yuridis dalam hal ruang *cyber* sudah tidak pada tempatnya lagi untuk dikategorikan sesuatu dengan ukuran dalam kualifikasi hukum konvensional untuk dijadikan obyek dan perbuatan, sebab jika cara ini yang ditempuh akan terlalu banyak kesulitan dan hal-hal yang lolos dari jerat hukum. Kegiatan *cyber* adalah kegiatan virtual yang berdampak sangat nyata, meskipun alat buktinya bersifat elektronik. Dengan demikian, subyek pelaku harus di kualifikasikan pula sebagai orang yang telah melakukan perbuatan hukum secara nyata.<sup>10</sup>

Berkaitan dengan pelaku *cybercrime* yang berkarakter unik, penulis berpendapat bahwa penjatuhan pidana penjara kepada pelaku *cybercrime* sebagaimana yang dipraktikkan di Indonesia selama ini merupakan langkah yang tidak bijak. Hal ini di sebabkan oleh adanya ketidaksesuaian antara karakteristik pelaku tindak pidana dengan sistem pembinaan narapidana di Lembaga Pemasyarakatan, sehingga

---

<sup>7</sup> *Convention on Cybercrime* dalam [http: www.cybercrimelaw.net/tekster](http://www.cybercrimelaw.net/tekster), diakses tanggal 27 September 2010, pukul 01.27 WIB.

<sup>8</sup> *Internasional Review of Criminal Policy-United Nation Manual on The Prevention and Control of Computer-Related Crime* dalam <http://www.Uncjin.Org/Documents/Eidhthcongress.Html>, di akses, pada tanggal 27 September 2010, pukul 01.30 WIB.

<sup>9</sup> *Convention on Cybercrime* dalam <http://conventions.Coe.Int/Treaty/commun/chercheSig>, diakses tanggal 27 September 2010, pukul 01.35 WIB.

<sup>10</sup> Pasal 5 Undang-Undang Nomor 11 Tahun 2008 *Tentang Informasi dan Transaksi Elektronik* (UU ITE), Kementerian Komunikasi dan Informasi RI.

tujuan pemidanaan bagaimana diatur dalam undang-undang kemasyarakatan tidak akan tercapai. Penulis berpendapat jenis pidana penjara dapat diganti dengan pidana kerja sosial atau pidana pengawasan, karena ada kesesuaian antara karakteristik pelaku *cybercrime* dengan paradigma pemidanaan dalam pidana kerja sosial dan pidana pengawasan, sehingga tujuan pemidanaan dapat dicapai. Pidana kerja sosial dan pidana pengawasan lebih manusiawi dan prospektif dibanding dengan pidana penjara. Hasil penelitian di beberapa negara, pidana kerja sosial dan pidana pengawasan cukup efektif diterapkan kepada pelaku kejahatan, termasuk *cybercrime*. Di delapan negara di dunia mengancam pelaku *cybercrime* dengan pidana kerja sosial, dan hal ini tidak bertentangan dengan ketentuan *convention on cybercrime*.

Ancaman pidana terhadap pelaku tindak pidana harus dituangkan dalam peraturan perundang-undangan agar dapat mencerminkan asas legalitas dan kepastian hukum mengingat di Indonesia belum ada undang-undang yang secara khusus mengatur pemidanaan bagi pelaku *cybercrime*, maka dalam RUU KUHP perlu dimuat tentang ancaman pidana kerja sosial dan pidana pengawasan sebagai alternatif pengganti pidana penjara. Penulis berpendapat, RUU KUHP tahun 2008 cukup progresif dalam mengatur *cybercrime*, namun dalam pengaturan pemidanaan (kebijakan penalisasi) masih perlu disempurnakan agar lebih prospektif dan responsif

## **B. METODE PENELITIAN**

Metode yang digunakan adalah metode pendekatan yuridis normatif. metode pendekatan *yuridis normatif*. Yaitu penelitian yang menerangkan tentang ketentuan-ketentuan dalam peraturan perundang-undangan yang berlaku, dihubungkan dengan kenyataan yang ada di lapangan, kemudian dianalisis dengan membandingkan

antara tuntutan nilai-nilai ideal yang ada dalam peraturan perundang-undangan dengan kenyataan yang ada di lapangan. Disamping itu penelitian yuridis normatif dilengkapi pula dengan penelitian empiris, yaitu penelitian langsung di lapangan mengenai alasan para inventor yang enggan mendaftarkan invensinya.

## **C. HASIL PENELITIAN DAN PEMBAHASAN**

### **1. Proses pemidanaan pelaku *cybercrime* dalam perspektif hukum pidana positif;**

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.

Pembentukan peraturan perundang-undangan di dunia *cyber* pun, berpangkal pada keinginan masyarakat untuk mendapatkan jaminan keamanan, keadilan, dan kepastian hukum. Sebagai norma hukum *cyber* atau *cyber law* akan bersifat mengikat bagi tiap-tiap individu-individu untuk tunduk dan mengikuti segala kaidah-kaidah yang terkandung didalamnya. Ada empat komponen dalam sistem peradilan pidana, yaitu kepolisian, kejaksaan, pengadilan, dan lembaga pemasyarakatan. Keempat komponen sistem peradilan pidana ini harus dapat bekerjasama dan dapat membentuk suatu *integrated criminal justice system*. Tahap pemeriksaan diatur sangat rinci dalam KUHAP, yang pada prinsipnya memberikan kewenangan tertentu kepada lembaga (administratif-birokratis) untuk melaksanakan sistem, mekanisme aturan, serta menjamin

hak tersangka dalam proses pemeriksaan.

Berkaitan dengan pengaturan pemidanaan *cybercrime* di Indonesia, sampai saat ini mayoritas tindakan *cybercrime* di Indonesia belum diatur dalam norma hukum yang jelas dalam peraturan perundang-undangan, karena itu di dalam mengadili *cybercrime* diterapkan ketentuan KUHP dan ketentuan dalam undang-undang di luar KUHP. Ketentuan dalam KUHP yang dapat digunakan untuk mengadili *cybercrime* dengan cara melakukan penafsiran *extensif* adalah ketentuan tentang tindak pidana pemalsuan (sebagaimana diatur dalam Pasal 263 sampai dengan Pasal 276), tindak pidana pencurian (sebagaimana diatur dalam Pasal 362 sampai dengan 367), tindak pidana penipuan (bagaimana diatur dalam Pasal 378 sampai dengan Pasal 395), dan tindak pidana perusakan barang (sebagaimana diatur dalam Pasal 407 sampai dengan Pasal 412).

Berikut diuraikan tentang penerapan ketentuan hukum pidana untuk mengadili pelaku *cybercrime* di Indonesia

- a. Penerapan pasal-pasal KUHP dalam perkara yang menjadikan komputer sebagai sasaran kejahatan dan perkara yang menggunakan komputer sebagai sarana kejahatan;
  - 1) 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 dari dua 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.

2) Kategori pencurian;

Dalam kasus *anauthirized Transfer Payment* di Bank Negara Indonesia (BNI) Cabang New York *agency* (Tahun 1986), Pengadilan Negeri Jakarta Pusat menjatuhkan pidana penjara terhadap terdakwa karena terbukti secara sah dan meyakinkan melanggar Pasal 363 ayat (1) 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.

3) 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>11</sup>

4) Kategori pemalsuan;

Terdakwa Petrus Pangkur dijatuhi pidana penjara selama 15 bulan oleh Pengadilan Negeri Sleman

---

<sup>11</sup> Sabartua Tampubolon, *Aspek Hukum Nama Domain di Internet*, Tata Nusa, Jakarta, 2003, hlm. 92.

(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 delapan bulan.<sup>12</sup>

- b. Penerapan ketentuan undang-undang di luar KUHP untuk mengadili perkara yang menjadikan komputer sebagai sarana kejahatan.

Dalam mengadili perkara kejahatan terhadap data ataupun sistem komputer sampai dengan tanggal 31 Januari 2005 didasarkan pada ketentuan peraturan perundang-undangan di luar KUHP. Undang-Undang tersebut adalah Undang-Undang Nomor 7 Tahun 1987 Tentang Hak Cipta, dan Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi.

- 1) Undang-Undang Nomor 7 Tahun 1987 Tentang Hak Cipta;

Ketentuan Undang-Undang Nomor 7 Tahun 1987 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 *jo.* Pasal 14 huruf g *jo.* Pasal 44 ayat (1) Undang-Undang Nomor 7 Tahun 1987 Tentang Hak Cipta *jo.* Keputusan

---

<sup>12</sup> *Pelaku Cybercrime Dihukum Penjara 15 Bulan*, Harian Pikiran Rakyat, Sabtu Tanggal 31 Agustus 2002.

Presiden RI Nomor 25 Tahun 1989 *jo.* Pasal 55 ayat (1) *jo.* Pasal 64 KUHP. Putusan ini dikuatkan oleh Putusan Pengadilan Tinggi Bandung. Dalam Pasal 11 ayat (1) huruf k, diatur tentang program komputer sebagai hak cipta khusus.

2) 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, karena terbukti secara sah dan meyakinkan melanggar Pasal 22 huruf c *jo.* Pasal 50 Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi.<sup>13</sup>

3) Undang-Undang Nomor 32 Tahun 2002 Tentang Penyiaran Mengatur tindak pidana sebagai berikut :

- a) 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.
- b) 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.

---

<sup>13</sup> Majalah Gatra, *Pembobol Situs KPU Divonis 6 Bulan 21 Hari*, Jakarta, 24 Desember 2004.

- c) Pasal 58 *jo.* Pasal 46 ayat (3) mengancam pidana terhadap siaran iklan niaga yang didalamnya 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; hal-hal yang bertentangan dengan kesusilaan masyarakat dan nilai-nilai agama; dan/atau eksploitasi anak di bawah umur 18 tahun.
- 4) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE).

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

Ditinjau dari sisi jenis pidana (*strafsoort*), dalam UU ITE, jenis pidana pokok yang diancamkan hanya ada dua, yaitu pidana penjara dan pidana denda yang diancamkan secara campuran, yaitu menggabungkan antara sistem alternatif dan kumulatif.

Berdasarkan sistem tersebut, maka hakim tidak mempunyai pilihan lain untuk menjatuhkan jenis pidana penjara dan pidana denda, baik salah satu maupun keduanya. Hakim hanya mempunyai peluang untuk dapat menentukan berat atau ringannya kedua jenis pidana tersebut, yaitu menentukan berapa tahun lamanya dan jumlah pidana dendanya berapa rupiah.

Ditinjau dari sistem lamanya ancaman pidana (*strafmaat*), dalam UU ITE menggunakan stelsel ancaman pidana maksimum sebagai-mana digunakan dalam KUHP. Buktinya dalam semua pasal dalam UU ITE yang mengatur ancaman pidana, hanya menyebutkan ancaman pidana penjara dalam jangka waktu paling lama, dan/atau jumlah pidana denda paling banyak. UU ITE tidak menganut sistem ancaman pidana minimum khusus.

Berdasarkan pengkajian secara ilmiah alasan pembenar secara filosofis, teoritis, yuridis, dan empiris bahwa dalam bentuk *cybercrime* kategori tertentu, dan terhadap pelaku dengan karakteristik tertentu dapat dijatuhi pidana sosial (sebagai pengganti pidana penjara) bersamaan dengan pidana denda belum terakomodasi secara tersurat dalam UU ITE.

- c. Penerapan pasal-pasal dalam undang-undang di luar KUHP untuk mengadili kasus yang menggunakan komputer sebagai sarana kejahatan.

Dalam perkembangannya, saat ini telah ada perundang-undangan yang berkaitan dengan kejahatan teknologi canggih di bidang informasi dan telekomunikasi. Ketentuan undang-undang diluar KUHP yang digunakan sebagai dasar untuk mengadili kejahatan yang menggunakan komputer adalah Undang-Undang Nomor 3 Tahun 1971 Tentang Pemberantasan Tindak Pidana Korupsi dan Undang-Undang Nomor 14 Tahun 1967 Tentang Perbankan.

- 1) Undang-Undang Nomor 3 Tahun 1971 Tentang Pemberantasan Tindak Pidana Korupsi;

Dalam kasus korupsi di Bank Rakyat Indonesia (BRI)

Cabang Yogyakarta Tahun (1983), Pengadilan Negeri Yogyakarta menjatuhkan pidana penjara terhadap terdakwa karena terbukti secara sah meyakinkan melanggar Pasal 1 ayat (1) huruf a Undang-Undang Nomor 3 Tahun 1971 *jo.* Pasal 64 ayat (1) KUHP. Putusan ini dikuatkan oleh putusan pengadilan Tinggi Yogyakarta, dan putusan Mahkamah Agung.<sup>14</sup>

2) Undang-Undang Nomor 14 Tahun 1967 Tentang Perbankan.

Dalam kasus PT. MAI Wanita Mataram Yogyakarta (tahun 1985), Pengadilan Negeri Yogyakarta menjatuhkan pidana penjara dan pidana denda kepada terdakwa karena terbukti secara sah dan meyakinkan melanggar Pasal 8 *jo.* Pasal 38 Undang-Undang Nomor 14 Tahun 1967 *jo.* Pasal 55 ayat (1) sub 1 *jo.* Pasal 64 *jo.* Pasal 65 KUHP dan Pasal 1 ayat (1) huruf a *jo.* Pasal 28 Undang-Undang Nomor 3 Tahun 1971 *jo.* Pasal 55 KUHP.

Berdasarkan uraian kasus kejahatan dan penerapan hukum pidana di atas, maka dapat disimpulkan sebagai berikut :

- a. Ketentuan dalam hukum pidana diterapkan dengan cara melakukan penafsiran ekstensif;
- b. 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;
- c. Jenis pidana yang dijatuhkan adalah pidana penjara dan pidana denda;

---

<sup>14</sup> Widyopramono, *Kejahatan di Bidang Komputer*, Pustaka Sinar Harapan, Jakarta, 1994, hlm. 54-55.

d. 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 realeded fraud* (yaitu kasus korupsi di beberapa bank), *computer realeded forgery* (yaitu kasus pemalsuan kartu kredit yang dilakukan oleh Petrus Pangkur), *offences realeded to infrigement of copyright and related rights* (yaitu kasus pembajakan program komputer *Words Star versi 5.0*).

Contoh lain kasus *cybercrime*, yakni pada kasus Dani Firmansyah yang merupakan tersangka pelaku *hacking* situs <http://tnp.kpu.go.id> milik KPU pada tanggal 17 April 2004. Pengadilan menyatakan terdakwa Dani Firmansyah telah terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana “tanpa hak, tidak sah, atau memanipulasi akses ke jaringan telekomunikasi khusus” dan menjatuhkan pidana terhadap terdakwa dengan pidana penjara selama 6 (enam) bulan dan 1 (satu) hari.

Dengan putusan Majelis Hakim Pengadilan Negeri Jakarta Pusat ini, Majelis Hakim telah melakukan terobosan hukum dengan mengakui bukti-bukti elektronik (*electronic evidence*) yang diajukan ke muka persidangan sebagai alat bukti sah yang menjadi sumber keyakinan hakim atas kesalahan terdakwa Dani Firmansyah. Alat bukti elektronik memang belum secara tegas diatur di dalam peraturan perundang-undangan, namun secara yuridis Dani Firmansyah telah melanggar ketentuan yang telah diatur dalam delik formil Undang-Undang Telekomunikasi, yaitu melakukan suatu tindakan tanpa hak dan tanpa otoritas secara tidak sah.

Barda Nawawi Arief menyatakan bahwa ancaman pidana yang sangat dominan tersebut juga terjadi dalam KUHP Indonesia,

bahkan sejak dahulu sampai saat ini.<sup>15</sup> Ancaman pidana penjara terhadap pelaku *cybercrime* dalam RUU KUHP juga sangat dominan, bahkan tidak ada satupun jenis kejahatan yang tidak diancam dengan pidana penjara. Berdasarkan perbandingan antara hasil studi terhadap 56 hukum pidana negara asing dengan ketentuan dalam hukum pidana Indonesia dan RUU KUHP dapat diketahui bahwa jenis pidana penjara menjadi pidana pokok yang paling diandalkan dalam kebijakan kriminal disebagian besar negara.

Meskipun pidana penjara merupakan pidana utama yang diancamkan dan dilaksanakan oleh mayoritas negara, sejak dahulu sampai saat ini efektifitas pidana penjara diragukan. Penelitian Djisman Samosir di Lembaga Pemasyarakatan Cipinang pada tahun 1990 menemukan bahwa 85 orang dari 100 narapidana yang diteliti menyatakan, bahwa pidana penjara bukan sesuatu yang menakutkan, karena sebelum melakukan tindak pidana sudah mengetahui tentang risiko dari perbuatannya yaitu dijatuhi pidana penjara.<sup>16</sup> Karena itu, pidana penjara makin banyak mendapat sorotan tajam dari para ahli penologi. Bahkan berdasarkan hasil penelitian Roger Hood di Inggris tentang "*reasearch of the effectiveness of punishment and treatment*" menunjukkan bahwa jenis pidana yang paling kurang efektif adalah pidana penjara. Efektifitas pidana penjara yang rendah tersebut terjadi pada semua umur narapidana.

Hasil penelitian tersebut mengindikasikan bahwa pidana denda lebih sukses dibanding pidana percobaan atau pidana

---

<sup>15</sup> Barda Nawawi Arief, *Kebijakan Legislatif Dalam Penanggulangan Kejahatan Dengan Pidana Penjara*, Badan Penerbit Universitas Diponegoro, Semarang, 1994, hlm. 201.

<sup>16</sup> Djisman Samosir, *Fungsi Pidana Penjara Dalam Sistem Pemidanaan di Indonesia*, Bina Cipta Bandung, 1992, hlm. 56.

penjara pada pelanggar yang pertama kali melakukan kejahatan dan keberhasilan ini meliputi semua umur. Kebanyakan studi menunjukkan bahwa pidana penjara jangka panjang tidak sukses, dibandingkan dengan pidana penjara yang lebih pendek sebagai pidana alternatif. Pembinaan narapidana dalam institusi yang terbuka, lebih efektif daripada dalam institusi yang tertutup. Hasil penelitian ini selaras dengan kesimpulan juga Leslie T. Wilkins, bahwa berdasarkan hasil survey tentang pelaksanaan hasil pidana dan tindakan, ternyata sistem perawatan yang berperikemanusiaan (misalnya pidana percobaan) adalah sedikit lebih efektif untuk mengurangi kemungkinan pengulangan tindak pidana (*residivisme*) dibandingkan dengan beberapa bentuk pidana lainnya.

Menurut Barda Nawawi Arief, bahwa pidana penjara bukan hanya mengakibatkan perampasan kemerdekaan, melainkan juga menimbulkan akibat-akibat negatif, bahkan narapidana akan menjadi lebih jahat setelah keluar dari penjara.<sup>17</sup> Muladi berpendapat, bahwa pidana penjara menyebabkan dehumanisasi, berisiko terjadi prisonisasi, menimbulkan "cap jahat" (*stigma*). Meskipun demikian, secara teoretik pidana penjara dapat berpengaruh positif dalam segi prevensi umum, tetapi banyaknya jumlah pidana penjara yang dijatuhkan oleh pengadilan tidak menurunkan frekuensi kejahatan. Sedangkan dalam rangka prevensi khusus, residivis (sebagai indikator dari prevensi khusus) di seluruh Indonesia sangat kecil, setelah mereka dijatuhi pidana penjara.<sup>18</sup>

Dalam pidana penjara selalu melekat kerugian-kerugian yang sulit diselesaikan. Kerugian-kerugian tersebut dapat bersifat filosofis maupun praktis. Ditinjau dari segi filosofis, maka terdapat hal-hal

---

<sup>17</sup> Barda Nawawi Arief, *Kebijakan Legislatif... op.cit.*, hlm. 245.

<sup>18</sup> *Ibid.*, hlm. 198.

yang saling ambivalen (*ambivalence*), antara lain sebagai berikut :

- a. Tujuan dari pidana penjara adalah menjamin pengamanan narapidana, dan memberikan kesernpatan-kesempatan kepada narapidana untuk direhabilitasi;
- b. Hakikat fungsi penjara tersebut seringkali mengakibatkan dehumanisasi pelaku tindak pidana dan akhirnya dapat menimbulkan kerugian bagi narapidana karena terlalu lama di dalam lembaga, misalnya berupa ketidakmampuan narapidana untuk melanjutkan kehidupan yang produktif dimasyarakat.

Selama ini bukan jenis pidana penjara yang dipersoalkan atau disangsikan, melainkan bagaimana pelaksanaan pidana penjara di LAPAS mengenai penanganan narapidana di dalam dan di luar LAPAS, serta bagaimana cara menyadarkan masyarakat agar mantan narapidana tidak selalu dianggap sebagai penjahat. Efektivitas pidana pencabutan kemerdekaan tidak tergantung pada jenis pidana itu sendiri, melainkan berhubungan erat dengan aspek-aspek yang lain, yaitu :

- a. Pembinaan narapidana, baik di dalam lembaga maupun di luar Lembaga Pemasyarakatan, misalnya *after care*;
- b. Rasio perbandingan antara jumlah pembimbing pemasyarakatan di dalam maupun di luar Lembaga pemasyarakatan dengan jumlah narapidana;
- c. Faktor-faktor kepribadian masing-masing narapidana;
- d. Jenis tindak pidana yang dilakukan;
- e. Faktor lingkungan dan pengaruh pergaulan narapidana; dan
- f. Stigma sosial yang menempatkan mantan narapidana dalam kedudukan terpojok, sehingga karena sulit mendapatkan mata pencaharian yang halal, terpaksa mantan narapidana mengulangi lagi tindak pidana lagi.

Berdasarkan uraian tentang pendapat pro dan kontra terhadap penerapan pidana penjara, pidana penjara masih diperlukan dalam sistem pemidanaan dan layak diancamkan terhadap pelaku *cybercrime* di Indonesia, tetapi penjatuhannya perlu dibatasi berdasarkan prinsip-prinsip dan persyaratan tertentu serta ditunjang oleh konsepsi individualisasi pemidanaan. Menurut Barda Nawawi Arief, eksistensi dan dasar pembenaran pidana penjara di Indonesia selama ini tidak pernah dipersoalkan.<sup>19</sup> Pada umumnya, yang dipersoalkan adalah mengenai berat atau ringannya ancaman penjara dan sistem perumusannya di dalam undang-undang. Kelayakan ancaman pidana terhadap pelaku *cybercrime* juga didasari pertimbangan sebagaimana dikemukakan oleh Barda Nawawi Arief, bahwa perbuatan tersebut bertentangan dengan kesusilaan, agama, dan moral Pancasila; membahayakan atau merugikan kehidupan masyarakat, bangsa dan negara; serta menghambat tercapainya pembangunan nasional.

## **2. Kebijakan formulasi hukum pidana dalam penanggulangan *cybercrime* di masa yang akan datang.**

Menjawab tuntutan dan tantangan komunikasi global lewat internet, undang-undang yang diharapkan (*ius constituendum*) adalah perangkat hukum yang akomodatif terhadap perkembangan serta antisipatif terhadap permasalahan, termasuk dampak negatif penyalahgunaan internet dengan berbagai motivasi yang dapat menimbulkan korban-korban seperti kerugian materi dan non materi.

Penanggulangan terhadap tindak pidana teknologi informasi perlu diimbangi dengan pembenahan dan pembangunan sistem

---

<sup>19</sup> *Ibid.*, hlm. 196.

hukum pidana secara menyeluruh, yakni meliputi pembangunan kultur, struktur, dan substansi hukum pidana. Dalam hal ini kebijakan hukum pidana menduduki posisi yang strategis dalam pengembangan hukum pidana modern.

Barda Nawawi Arief menyatakan bahwa upaya melakukan pembaharuan hukum pidana pada hakikatnya termasuk bidang "*penal policy*" yang merupakan bagian dan terkait dengan "*law enforcement policy*", "*criminal policy*", dan "*social policy*". Ini berarti pembaharuan hukum pidana pada hakikatnya :<sup>20</sup>

- a. Merupakan bagian dari kebijakan (upaya rasional) untuk memperbaharui substansi hukum (*legal substansi*) dalam rangka lebih mengefektifkan penegakan hukum;
- b. Merupakan bagian dari kebijakan (upaya rasional) untuk memberantas/ menanggulangi kejahatan dalam rangka perlindungan masyarakat;
- c. Merupakan bagian dari kebijakan (upaya rasional) untuk mengatasi masalah sosial dan masalah kemanusiaan dalam rangka mencapai/menunjang tujuan nasional (yaitu *social defence* dan *social welfare*);
- d. Merupakan upaya peninjauan dan penilaian kembali (reorientasi dan re-evaluasi) pokok-pokok pemikiran, ide-ide dasar, atau nilai sosio-filosofik, sosio politik dan sosio kultural yang melandasi kebijakan kriminal dan kebijakan (penegakan) hukum pidana selama ini. Bukanlah pembaharuan (reformasi) hukum pidana, apabila orientasi nilai dari hukum pidana yang dicitakan sama saja dengan orientasi nilai dari hukum pidana lama warisan penjajah (KUHP lama atau WvS).

Bertolak dari kebijakan tersebut di atas, usaha dan kebijakan

---

<sup>20</sup> Barda Nawawi Arief, *Bunga Rampai...*, *op.cit.*, hlm. 28.

untuk membuat peraturan hukum pidana yang pada hakikatnya tidak dapat dilepaskan dari tujuan penanggulangan kejahatan. Dengan demikian penentuan kebijakan hukum pidana menanggulangi *cybercrime* harus dilakukan dengan pendekatan kebijakan dan di dalam setiap kebijakan (*policy*) terkandung pula pertimbangan nilai. Oleh karena itu, pembaharuan hukum pidana dalam penanggulangan tindak pidana teknologi informasi harus pula berorientasi pada pendekatan nilai.

a. Kebijakan formulasi tindak pidana;

Hukum pidana merupakan salah satu sarana kebijakan kriminal untuk menanggulangi *cybercrime*. Dalam kebijakan hukum pidana, maka akan bersentuhan dengan persoalan kriminalisasi (*criminalization*), baik itu perbuatan yang melawan hukum (*actus reus*), pertanggungjawaban pidana (*mensrea*), maupun sanksi yang dijatuhkan berupa pidana (*punishment*) maupun tindakan (*treatment*).

b. Kebijakan kriminalisasi;

Kriminalisasi harus memenuhi pelbagai syarat antara lain bahwa perbuatan tersebut benar-benar menampakkan korban (*victimizing*), baik aktual maupun potensial, kemudian konsistensi penerapan asas *ultimum remedium*, dukungan publik yang kuat, bersifat komprehensif dan tidak bersifat *ad-hoc*.<sup>21</sup>

Kebijakan kriminalisasi merupakan suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana (tidak dipidana) menjadi suatu tindak pidana (perbuatan yang dapat dipidana). Jadi pada hakikatnya, kebijakan kriminalisasi merupakan bagian dari kebijakan kriminal (*criminal policy*)

---

<sup>21</sup> Muladi, *Kebijakan Kriminal Terhadap Cybercrime*, Majalah Media Hukum Volume I No.3, tanggal 23 Agustus 2003, hlm. 2.

dengan menggunakan sarana hukum pidana (*penal*), dan oleh karena itu termasuk bagian dari “kebijakan hukum pidana” (*penal policy*), khususnya kebijakan formulasinya.<sup>22</sup>

## D. PENUTUP

### 1. Kesimpulan

Undang-Undang Negara Republik Indonesia Nomor 11 Tahun 2008 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. Dalam perspektif yuridis, khususnya dalam ruang lingkup hukum pidana Penerapan pidana penjara masih diperlukan dalam sistem pemidanaan dan layak diancamkan terhadap pelaku *cybercrime* di Indonesia, tetapi penjatuhannya perlu dibatasi berdasarkan prinsip-prinsip dan persyaratan tertentu serta ditunjang oleh konsepsi individualisasi pemidanaan., Dalam rangka mencari alternatif pengganti pidana penjara (*alternative to custodial sentence*), seyogyanya didasarkan pada pertimbangan-pertimbangan yang realistis dalam masyarakat. Jenis pidana yang layak menggantikan pidana penjara terhadap pelaku *cybercrime* di Indonesia adalah pidana kerja sosial dan pidana pengawasan. Meskipun demikian, bukan berarti setiap pelaku *cybercrime* di Indonesia dapat dijatuhi pidana kerja sosial atau pidana pengawasan. Dalam perkara tertentu, pidana penjara masih relevan dijatuhkan. Penentuan jenis pidana yang dijatuhkan tergantung dari kondisi pelaku kejahatan, kerugian yang ditimbulkan, dan perasaan hukum dalam masyarakat.

---

<sup>22</sup> Barda Nawawi Arief, *Tindak Pidana Mayantara, Perkembangan Kajian Cybercrime di Indonesia*, Raja Grafindo Persada, Jakarta, 2006, hlm. 90.

## 2. Saran

Diperlukan aturan pemidanaan terhadap penyertaan, percobaan, dan pengulangan (*residive*) terhadap tindak pidana teknologi informasi. Pemidanaan yang sama terhadap penyertaan dan percobaan serta ada pemberatan terhadap perbuatan pengulangan dimaksudkan untuk menghindari terjadinya ketidakadilan hukum dan sebagai upaya untuk kesejahteraan sosial (*social welfare*) dan untuk perlindungan masyarakat (*social defence*).

## DAFTAR PUSTAKA

### A. Buku

- Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cybercrime)*, Cetakan Kesatu, Refika Aditama, Bandung, 2005.
- Andri Winjaya Laksana, Cybercrime Comparison Under Criminal Law In Some Countries, *Jurnal Pembaharuan Hukum*, Vol V No.2 April-Agustus 2018;
- Bambang Sunggono, *Metode Penelitian Hukum*, Raja Grafindo Persada, Jakarta, 1998.
- Barda Nawawi Arief, *Kapita Selekta Hukum Pidana*, Citra Aditya Bakti, Bandung, 2003. Barda Nawawi Arief, *Sari Kuliah : Perbandingan Hukum Pidana*, Raja Grafindo Persada, Jakarta, 2006.
- Barda Nawawi Arief, *Kebijakan Legislatif Dalam Penanggulangan Kejahatan Dengan Pidana Penjara*, Badan Penerbit Universitas Diponegoro, Semarang, 1994.
- Barda Nawawi Arief, *Tindak Pidana Mayantara, Perkembangan Kajian Cybercrime di Indonesia*, Raja Grafindo Persada, Jakarta, 2006.
- Buletin Litbang Dephan, *Kejahatan Mayantara (Cybercrime), Dampak Perkembangan Teknologi Informasi "Dunia Maya"*, STT No. 2289 Volume VII Nomor 12 Tahun 2004.
- Djisman Samosir, *Fungsi Pidana Penjara Dalam Sistem Pidanaan di Indonesia*, Bina Cipta Bandung, 1992.
- Djisman Samosir, *Fungsi Pidana Penjara Dalam Sistem Pidanaan di Indonesia*, Bina Cipta, Bandung, 1992.
- Donny Budi Utomo, *Komunitas Internet Indonesia Terkena Embargo*, Kompas, tanggal 29 November 2002.
- Eddy Djunaedi Kamasudirdja, *Beberapa Pidanaan dan Pengamatan*
- Hermawan Sulisty Sutanto dan Tjuk Sugiarto, *Cybercrime Motif dan Penindakan*, Pensil 324, Jakarta, 2009.

Indriyanto Seno Adji, *Korupsi Sistematis dan Kendala Penegakan Hukum di Indonesia*, Jurnal Studi Kepolisian Perguruan Tinggi Ilmu Kepolisian, Restu Agung, 2005.

*Internasional Review of Criminal Policy-United Nation Manual on The Prevention and Control of Computer-Related Crime* dalam <http://www.Uncjin.Org/Documents/Eidhthcongress.Html>, di akses, pada tanggal 27 September 2010, pukul 01.30 WIB.

Marjono Reksodiputro, *Kemajuan Pembangunan Ekonomi dan Kejahatan*, Kumpulan Karangan Buku Kesatu, Pusat Pelayanan Keadilan dan Pengabdian Hukum, Jakarta, 1994.

Muladi, *Kebijakan Kriminal Terhadap Cybercrime*, Majalah Media Hukum Volume I No.3, tanggal 23 Agustus 2003.

Rachmat Rafiudin, *Internet Forensik*, Andi Offset, Yogyakarta, 2009.

Romli Atmasasmita, *Ruang Lingkup Berlakunya Hukum Pidana Terhadap Kejahatan Transnasional Terorganisasi*, Artikel dalam Padjajaran Jilid XXIV No. 2 Tahun 1996.

Soedjono Dirdjosisworo, *Sejarah dan Azas-Azas Penologi (Pemasyarakatan)*, Armico, Bandung, 1984.

Widodo, *Sistem Pidanaan Dalam Cybercrime*, Laksbang Mediatama, Yogyakarta, 2009.

Widyopramono, *Kejahatan di Bidang Komputer*, Pustaka Sinar Harapan, Jakarta, 1994.

Yusril Ihza Mahendra, *Regulasi Cyberspace di Indonesia*, Makalah Pada Seminar Tentang *Cyberlaw*, Bandung, 2000.

## **B. Perundang – Undangan**

KUHP

Undang – Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik