

# TINDAK PIDANA DUNIA MAYA DALAM PERSPEKTIF UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFOMARASI DAN TRANSAKSI ELEKTRONIK

Oleh:  
Dr. Sahuri Lasmadi, S.H., M.Hum<sup>1</sup>

## Abstrak

Dalam catatan beberapa literatur yang membahas mengenai tindak pidana dunia maya bahwa terdapat berpuluh jenis tindak pidana yang berkaitan dengan internet. Yang termasuk dalam kategori tindak pidana umum yang difasilitasi internet antara lain penipuan kartu kredit, penipuan perbankan, pornografi anak, perdagangan narkoba, serta terorisme. Sedangkan tindak pidana yang menjadikan fasilitas teknologi informasi sebagai sasaran di antaranya *denial of service attack*, *defacing*, *cracking* ataupun *phreaking*. Tindak pidana dunia maya ini merupakan perkembangan lebih lanjut dari tindak pidana yang dilakukan dengan memanfaatkan teknologi komputer. Dalam Undang-undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, secara limitatif mengatur tentang perbuatan bagaimanakah yang dikategorikan sebagai tindak pidana dunia maya sebagai suatu perumusan tindak pidana yang terdapat pada Pasal 27 sampai dengan Pasal 36, sedangkan untuk ketentuan pidana sebagai suatu kriminalisasi diatur dalam Pasal 45 sampai dengan Pasal 52 yang secara jelas tidak mengatur adanya ancaman staf minima khusus berarti berlaku ketentuan dalam KUHP, hanya mengatur ancaman straf maksima. Juga jenis ancaman pidana yang diatur hanya terbatas pada pidana pokok berupa pidana penjara dan denda. Hanya saja adanya penyimpangan dari KUHP mengenai stelsel ancaman pidana yang bersifat kumulasi relatif, karena dijumpai adanya kata dan/atau, ini menunjukkan bahwa hakim mempunyai pilihan untuk menjatuhkan pidana pokok apakah dua-duanya atau salah satunya. Hal ini merupakan penyimpangan penjatuhan pidana yang diatur pada Pasal 10 KUHP, terhadap pidana pokok penjatuhan pidananya bersifat alternatif.

**Keywords:** Tindak Pidana Dunia Maya, Undang-Undang Informasi dan Transaksi Elektronik.

## I. PENDAHULUAN

Pengesahan Undang-Undang tentang Informasi dan Transaksi Elektronik diyakini akan memperkuat kepercayaan internasional khususnya dalam hal transaksi bisnis. Undang-undang ini juga membuat

---

<sup>1</sup>Penulis adalah Dosen Fakultas Hukum Universitas Jambi

penipuan, *carding*, penipuan melalui elektronik, penyebarluasan informasi transaksi elektronik, pornografi, serta informasi elektronik yang merugikan untuk bisa diusut.

Undang-undang ini membentengi Indonesia dari tindak pidana di dunia maya yang dilakukan melalui teknologi informasi. Hukuman badan berupa kurungan mulai 6 (enam) bulan hingga 10 (sepuluh) tahun serta denda yang bervariasi antara ratusan juta hingga puluhan miliar rupiah menanti para pelanggarnya.

Oleh karena itu, tidak hanya polisi bahkan masyarakatpun menyambut baik kehadiran undang-undang yang khusus mengatur mengenai *cyber crime* ini. Terlebih lagi dengan adanya pengaturan yang khusus mengenai transaksi elektronik, yang diharapkan dapat mengatasi Bentuk-bentuk tindak pidana seperti *credit card fraud* (penipuan melalui kartu kredit), *hacking*, dan lain-lain.<sup>2</sup> Dahulu kasus-kasus semacam ini, yang mulai melanda Indonesia, boleh dikatakan hampir tidak tersentuh oleh hukum. Sehingga pihak yang berwenang tidak mempunyai dasar hukum yang pasti untuk menangani *cyber crime* yang masih samar.<sup>3</sup> Dengan demikian *cyber crime* ini kemungkinan besar tidak bisa diajukan ke meja hijau. Tetapi keadaan seperti itu sudah tidak berlaku lagi karena sekarang telah disahkan Undang-Undang tentang Informasi dan Transaksi Elektronik.

*Onno W. Purbo*, ahli TI dari Institut Teknologi Bandung, menjelaskan bahwa bentuk-bentuk *cyber crime*, antara lain penipuan kartu kredit (disebut juga dengan *carding*) dan merusak website milik orang lain.<sup>4</sup> Contoh *cyber crime* lainnya, menurut *Yuyun Mulyana* (Asisten Bimmas Polri), di antaranya adalah akses secara tidak sah, pelanggaran Hak Kekayaan Intelektual (HaKI), penghinaan dan sebagainya.<sup>5</sup> *Barda Nawawi Arief*, memberikan istilah lain mengenai *cyber crime* semacam ini dengan istilah tindak pidana dunia maya

Praktik tindak pidana dunia maya juga menyebabkan dunia bisnis nasional harus mengalami dampak kerugian besar, sebagai contoh adanya kasus-kasus seperti pemalsuan nama *website* layanan *internet banking* Bank BCA dan perebutan nama *domain website* milik perusahaan Mustika Ratu yang sempat mencuat menjadi kasus tindak pidana internet nasional beberapa waktu lalu.

---

<sup>2</sup>*Polisi Mengalami Future Shock dalam Kasus Cyber*, 12 November 2001. [www.google.com](http://www.google.com).

<sup>3</sup>*Sebagian Kejahatan Dunia maya Masih Samar*, 28 Agustus 2000, [www.google.com](http://www.google.com).

<sup>4</sup>*Ibid.*

<sup>5</sup>*Modus Operandi Cyber Crime Makin Canggih, Loc. Cit.*

Akan tetapi, menurut Judith M.S., ketua presidium Asosiasi Warnet Indonesia, *cyber crime* dalam bentuk *carding* atau *credit card fraud* (penipuan melalui kartu kredit) adalah Tindak pidana internet yang paling meresahkan di Indonesia sekarang ini.<sup>6</sup> Penipuan tersebut dilakukan dengan cara menggunakan nomor rekening kartu kredit milik orang lain untuk melakukan pembayaran dengan dana yang ada pada kartu kredit tersebut tanpa seizin pemilik sah kartu kredit atas transaksi melalui media internet.<sup>7</sup>

Pemecahannya yang paling utama diperlukan adalah adanya perangkat hukum atau peraturan perundang-undangan yang jelas. Perlunya perangkat hukum ini, diakui oleh aparat hukum sendiri. Dengan disahkannya Undang-Undang tentang Informasi dan Transaksi Elektronik, maka diharapkan undang-undang ini dapat menjadi solusi atas permasalahan yang selama ini dialami Indonesia mengenai penanganan tindak pidana dunia maya ini.

Kepolisian Republik Indonesia melihat bahwa undang-undang merupakan instrumen terakhir dalam menentukan hasil penyidikan.<sup>8</sup> Penerapan suatu tindak pidana yang salah akan mematahkan atau mementahkan penyidikan yang telah dilakukan.

Dalam penanganan kasus yang terjadi sebelum Undang-Undang tentang Informasi dan Transaksi Elektronik ini disahkan adalah dengan cara melakukan analogi terhadap pasal-pasal yang terdapat di dalam Kitab Undang-Undang Hukum Pidana yang paralel dengan tindak pidana yang terjadi. Sehingga para penjahat dunia mayapun dipidana dengan Kitab Undang-Undang Hukum Pidana (selanjutnya disebut KUHP).

Penyidik juga menyadari bahwa upaya analogi ini mengandung banyak kelemahan.<sup>9</sup> Karena cara tersebut selain bertentangan dengan asas legalitas yang berlaku di Indonesia, juga tidak dapat memenuhi kebutuhan dalam upaya memberantas praktik tindak pidana dunia maya. Misalkan saja di Bandung terdapat kasus dengan terdakwa Harry Parlindungan Samosir yang telah melakukan perbelanjaan/transaksi dengan memesan barang melalui internet dan membayarnya dengan menggunakan kartu kredit orang lain tanpa seizin pemilik kartu kredit dan membuat identitas palsu untuk mengambil barang pesannya tersebut. Terhadap kasus tersebut, Jaksa Penuntut Umum menganalogikan perbuatan terdakwa tersebut sebagai pemalsuan surat atau pencurian. Hal ini dapat dilihat dalam dakwaan dari Jaksa Penuntut Umum yaitu Kesatu Primair Pasal 263 Ayat (1) KUHP Subsidiar Pasal 263 Ayat (2)

---

<sup>6</sup>e-Law, Saatnya Ada Undang-Undang Cyber, 20 Februari 2003. [www.wartaekonomi.com](http://www.wartaekonomi.com).

<sup>7</sup>Santosa Raharjanto, *Carder*, [www.google.com](http://www.google.com).

<sup>8</sup>*Polisi Mengalami Future Shock dalam Kasus Cyber*, Loc. Cit.

<sup>9</sup>*Ibid.*

KUHP dan Kedua Pasal 362 KUHP jo. Pasal 55 Ayat (1) ke-1e KUHP. Setelah melalui proses pemeriksaan di persidangan, pada tingkat pertama majelis hakim Pengadilan Negeri Bandung dalam Putusan Nomor: 162/Pid.B/2004/PN.BDG memutuskan bahwa terdakwa terbukti melakukan tindak pidana pemalsuan surat dan pencurian dengan pidana selama 3 (tiga) bulan. Selanjutnya pada tingkat banding, majelis hakim Pengadilan Tinggi Bandung dalam Putusan Nomor: 181/PID/2004/PT.Bdg memutuskan untuk menguatkan putusan Pengadilan Negeri Bandung dengan perbaikan mengenai lamanya pidana yang dijatuhkan dari 3 (tiga) bulan menjadi 5 (lima) bulan penjara.

Berdasarkan contoh kasus-kasus di atas dapat dilihat bahwa perkembangan teknologi canggih, khususnya internet sebagai suatu dunia maya, melahirkan modus operandi baru terhadap perbuatan-perbuatan yang melawan hukum.<sup>10</sup> Karena praktik tindak pidana dunia maya, sebelumnya tidak dikenal sama sekali dalam perundang-undangan di Indonesia, sampai akhirnya Undang-Undang tentang Informasi dan Transaksi Elektronik disahkan baru-baru ini. Untuk itu perlu kajian tentang Tindak Pidana Dunia Maya Dalam perspektif Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

## **II. Rumusan Masalah**

Berdasarkan pemikiran tersebut di atas, maka yang mejandi masalah dalam tulisan adalah:

1. Bagaimana kategori Tindak pidana dunia maya sebagai bentuk tindak pidana baru?
2. Bagaimana kriminalisasi Tindak pidana dunia maya dalam Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik?

## **III. PEMBAHASAN**

### **A. Kategori Tindak Pidana Dunia Maya Sebagai Tindak pidana Baru.**

Terdapat dua hal yang menyebabkan timbulnya *cyber crime* (tindak pidana dunia maya) yaitu teknis dan sosio ekonomi (kemasyarakatan).<sup>11</sup> Pertama, dalam hal teknis. Tidak dapat dipungkiri bahwa kemajuan teknologi (teknologi informasi) dapat berdampak negatif bagi perkembangan masyarakat. Berhasilnya teknologi tersebut menghilangkan batas wilayah negara menjadikan dunia ini begitu sempit. Keterhubungan antara jaringan yang satu dengan jaringan yang lain memudahkan pelaku tindak pidana untuk melakukan aksinya. Kemudian, tidak meratanya penyebaran teknologi menjadikan yang satu lebih kuat

---

<sup>10</sup>*Modus Operandi Cyber Crime Makin Canggih, Loc. Cit.*

<sup>11</sup>*Telekomunikasi & Teknologi Tindak pidana Cyber Crime, www.hukumonline.com.*

daripada yang lain. Kelemahan tersebut dimanfaatkan oleh mereka yang tidak bertanggung jawab untuk melakukan tindak pidana.

Kedua, dalam hal sosio ekonomi. Tindak pidana dunia maya merupakan produk ekonomi. Isu global yang kemudian dihubungkan dengan tindak pidana tersebut adalah keamanan jaringan (*security network*). Keamanan jaringan merupakan isu global yang digulirkan berbarengan dengan internet. Sebagai komoditi ekonomi, banyak negara yang tentunya sangat membutuhkan perangkat keamanan jaringan. Tindak pidana dunia maya berada dalam skenario besar dari kegiatan ekonomi dunia.

Jika dipandang dari sudut alat komunikasi, maka internet memiliki karakteristik khusus dibandingkan dengan alat komunikasi lainnya seperti telepon atau fax. Melalui internet, pertukaran informasi dapat dilakukan secara cepat, tepat, serta dengan biaya yang relatif murah. Dengan memperhatikan karakteristik internet yang demikian khusus, maka internet dapat menjadi media yang memudahkan seseorang untuk melakukan tindak pidana yang berbasis teknologi informasi (tindak pidana dunia maya).

Secara garis besar, tindak pidana yang berkaitan dengan teknologi informasi dapat dibagi menjadi dua bagian besar.<sup>12</sup> Pertama, tindak pidana yang bertujuan merusak atau menyerang sistem atau jaringan komputer. Kedua, tindak pidana yang menggunakan komputer atau internet sebagai alat bantu dalam melancarkan kejahatan. Namun demikian, mengingat teknologi merupakan konvergensi telekomunikasi, komputer, dan media, maka tindak pidana jenis ini terus berkembang menjadi lebih luas.

Dalam catatan beberapa literatur yang membahas mengenai tindak pidana dunia maya bahwa terdapat berpuluh jenis tindak pidana yang berkaitan dengan internet. Yang termasuk dalam kategori tindak pidana umum yang difasilitasi internet antara lain penipuan kartu kredit, penipuan perbankan, pornografi anak, perdagangan narkoba, serta terorisme. Sedangkan tindak pidana yang menjadikan fasilitas teknologi informasi sebagai sasaran di antaranya *denial of service attack*, *defacing*, *cracking* ataupun *phreaking*.<sup>13</sup> Tindak pidana dunia maya ini merupakan perkembangan lebih lanjut dari tindak pidana yang dilakukan dengan memanfaatkan teknologi komputer.

---

<sup>12</sup>Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)*, 2005, Bandung, Refika Aditama, hal. 26.

<sup>13</sup>*Ibid.*, hal. 27.

Ade Maman Suherman menyatakan bahwa manifestasi dari tindak pidana *cyber crime* muncul dalam berbagai macam atau varian seperti berikut ini:<sup>14</sup>

- a. *Reactional Hackers*. Tindak pidana ini dilakukan oleh *netter* tingkat pemula untuk sekedar mencoba kekuranghandalan sistem sekuritas suatu perusahaan;
- b. *Crackers* atau *criminal minded hackers*, pelaku tindak pidana ini biasanya memiliki motivasi untuk mendapatkan keuntungan finansial, sabotase dan pengrusakan data. Tipe tindak pidana ini dapat dilakukan dengan bantuan orang dalam, biasanya staf yang sakit hati atau datang dari kompetitor dalam bisnis sejenis;
- c. *Political hackerks*. Aktifis politis atau lebih populer dengan sebutan *hacktivis* melakukan perusakan terhadap ratusan situs *web* untuk mengkampanyekan programnya, bahkan tidak jarang dipergunakan untuk menempelkan pesan untuk mendiskreditkan lawannya. Usaha tersebut pernah dilakukan secara aktif dan efisien untuk kampanye anti-Indonesia dalam masalah Timor Timur yang dipelopori oleh Ramos Horta;
- d. *Denial of service attack*. Serangan ini adalah untuk memacetkan sistem dengan mengganggu akses dari pengguna yang *legitimated*. Taktik yang digunakan adalah dengan membanjiri situs *web* dengan data yang tidak penting. Pemilik situs akan banyak menderita kerugian karena untuk mengendalikan atau mengontrol kembali situs *web* memakan waktu lama;
- e. *Insider* atau *internal hackers*. Tindak pidana ini bisa dilakukan oleh orang dalam perusahaan sendiri. Modusnya dengan menggunakan karyawan yang kecewa atau bermasalah dengan perusahaan;
- f. *Viruses*. Program pengganggu dengan penyebaran virus dewasa ini dapat menular melalui aplikasi internet. Sebelumnya pola penularan virus hanya melalui *floopy disk*. Virus dapat bersembunyi dalam *file* dan *ter-down load* oleh *user* bahkan bisa menyebar kiriman *e-mail*;
- g. *Piracy*. Pembajakan *software* merupakan trend dewasa ini. Pihak produsen *software* dapat kehilangan profit karena karyanya dapat dibajak melalui *down load* dari internet dan dikopi ke dalam *CD-room* yang selanjutnya diperbanyak secara *illegal* tanpa seizing pemiliknnya;
- h. *Fraud*. Adalah sejenis manipulasi informasi keuangan dengan tujuan mengeruk keuntungan sebesar-besarnya;
- i. *Gambling*. Perjudian di dunia *cyber* yang berskala global. Dari kegiatan ini dapat diputar kembali di negara yang merupakan

---

<sup>14</sup>Abdul Wahid dan Mohammad Labib, *Op.Cit.* ,hal. 70-72.

- tax heaven*, seperti Indonesia yang sering dijadikan sebagai negara tujuan *money laundering*;
- j. *Pornographahy and Paeddophilia*. Dunia *cyber* selain mendatangkan berbagai kemudahan dengan mengatasi kendala ruang dan waktu, juga telah menghadirkan dunia pornografi. Melalui *news group*, *chat rooms* mengeksploitasi pornografi anak di bawah umur;
  - k. *Cyber-stalking*. Adalah segala bentuk kiriman *e-mail* yang tidak dikehendaki *user*;
  - l. *Hate sites*. Situs ini sering digunakan untuk saling menyerang dan melontarkan kata-kata tidak sopan dan vulgar yang dikelola oleh para ekstrimis. Penyerangan terhadap lawan sering menggunakan isu rasial, perang program dan promosi kebijakan atau suatu pandangan;
  - m. *Criminal communication*. Internet telah menjadikan segalanya handal dan modern untuk melakukan komunikasi antar gangster, anggota sindikat obat bius dan komunikasi antar *hooligan* di dunia sepak bola.

Berdasarkan hal tersebut, dapat dilihat bahwa *cyber crime* adalah tindak pidana yang dilakukan dengan memanfaatkan teknologi informasi.<sup>15</sup> Berbagai definisi pernah dikemukakan oleh para ahli, namun belum terdapat keseragaman.

Dalam Kongres Perserikatan Bangsa-Bangsa X tentang *The Prevention of Crime and the Treatment of Offenders* di Vienna, 10-17 April 2000, memberi pengertian tentang *cybercrime* dalam dua kategori, yaitu:<sup>16</sup>

- a. *Cyber crime in narrow sense (computer crime): any illegal behavior directed by means of electronic operations that targets the security of computer system and the data processed by them:*  
Artinya:  
Cyber crime dalam pengertian sempit (tindak pidana komputer): perilaku apapun yang tidak sah yang diarahkan atas bantuan operasi elektronik dengan sasaran keamanan sistem komputer dan data yang diprosesnya;
- b. *Cyber crime in a broader sense (computer related crime): any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of computer system or network.*  
Artinya:  
Cyber crime dalam pengertian luas (tindak pidana yang terkait dengan komputer): perilaku apapun yang tidak sah yang

---

<sup>15</sup>Telekomunikasi & Teknologi Tindak Pidana Cyber Crime. Loc. Cit.

<sup>16</sup>Johannes Ibrahim, *Kartu Kredit*, 2004, Bandung, Refika Aditama, hal. 90-93.

dilakukan atas bantuan, atau dalam hubungan dengan suatu sistem komputer atau jaringan, mencakup tindak pidana pemilikan tidak sah dan menawarkan atau membagi-bagikan informasi atas bantuan suatu sistem komputer atau jaringan.

*Cyber crime* (tindak pidana dunia maya) ini merupakan pola tindak pidana dengan memanfaatkan jaringan internet telah menciptakan dunia baru yang dinamakan *cyber space*. *Cyber space* merupakan sebuah dunia komunikasi berbasis komputer (*computer mediated communication*) dengan menawarkan realitas baru, yaitu realitas virtual (*virtual reality*). Internet merupakan sarana untuk melakukan tindak pidana dengan menembus batas-batas yurisdiksi suatu negara dan dapat dilakukan di rumah, ataupun tempat-tempat pelayanan publik, misalnya warung internet dan sebagainya.

Pemanfaatan teknologi telekomunikasi dan komputer sebagai bentuk komunikasi berbasis komputer (*computer mediated communication*) ini meliputi jaringan komputer, *electronic mail*, *Electronic Bulletin Board Service*, dan pertemuan dengan menggunakan komputer ini dalam menghubungkan komunikasi diantara mereka dinamakan *Net*. Penggunaan *cyber space* dalam pola tindak pidana *cyber crime* memungkinkan tindak pidana dilakukan tanpa mempermasalahkan jarak, waktu, dan ruang.

*Cyber crime* adalah suatu tindak pidana baru yang sangat berbeda dengan dua jenis tindak pidana yang sudah ada sebelumnya, yaitu *blue collar crime* dan *white collar crime*.<sup>17</sup> *Blue collar crime* adalah tindak pidana konvensional seperti pencurian, pembunuhan. Sedangkan *white collar crime*, menurut Jo Ann Miler, umumnya dibagi ke dalam empat jenis yaitu tindak pidana korporasi, tindak pidana birokrat, malpraktek, dan tindak pidana individu.

Berdasarkan hal-hal tersebut di atas, maka dapat disimpulkan bahwa *cyber crime* merupakan kategori tindak pidana yang benar-benar baru dan memiliki karakteristik yang khas dibandingkan dengan tindak pidana konvensional yang lain. Adapun karakteristik khas tersebut diantaranya:

- a. Perbuatan yang dilakukan secara illegal, tanpa hak atau tidak etis yang terjadi dalam ruang/wilayah siber (*cyber space*), sehingga tidak dapat dipastikan yurisdiksi negara mana yang berlaku terhadap tindak pidana tersebut;
- b. Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang terhubung dengan internet;

---

<sup>17</sup>Sutarman, *Cyber Crime (Modus Operandi dan Penanggulangannya)*, 2007, Yogyakarta, Laks Bang, hal.33.

- c. Perbuatan tersebut mengakibatkan kerugian material maupun immaterial (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan dengan tindak pidana konvensional;
- d. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya;
- e. Perbuatan tersebut sering digunakan secara transnasional/melintasi batas negara.

Dalam perspektif hukum, *cyber crime* (tindak pidana dunia maya) merupakan jenis tindak pidana baru. Karena meskipun dengan konsep tindak pidana konvensional, tetapi dalam pelaksanaannya menggunakan media dan cara baru yang kemudian dikembangkan oleh para pelaku.

### **B. Kriminalisasi Tindak Pidana Dunia Maya Dalam Undang-undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik**

Kebijakan kriminalisasi merupakan suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana menjadi suatu tindak pidana (perbuatan yang dapat dipidana).<sup>18</sup>

Persoalan-persoalan yang menentukan suatu perbuatan sebagai tindak pidana atau bukan (kriminalisasi dan dekriminalisasi) antara lain:<sup>19</sup>

1. Masalah kriminalisasi dan dekriminalisasi suatu perbuatan harus sesuai dengan politik kriminal yang dianut oleh bangsa Indonesia, yaitu sejauh mana suatu perbuatan bertentangan dengan atau tidak dengan nilai-nilai fundamental yang berlaku dalam masyarakat dan oleh masyarakat dianggap patut atau tidak patut dihukum dalam rangka menyelenggarakan kesejahteraan masyarakat;
2. Untuk menetapkan suatu perbuatan sebagai tindak pidana, perlu diperhatikan kriteria umum sebagai berikut:
  - a. Apakah perbuatan itu tidak disukai atau dibenci oleh masyarakat karena kerugian, atau dapat merugikan, mendatangkan korban atau dapat mendatangkan korban;
  - b. Apabila biaya mengkriminalisasikan seimbang dengan hasil yang akan dicapai. Artinya biaya pembuatan undang-undang, pengawasan, dan penegakkan hukum, beban yang dipikul korban dan pelaku tindak pidana itu sendiri harus seimbang dengan situasi tertib hukum yang dicapai;
  - c. Apakah akan makin menambah beban aparat penegak hukum sehingga terjadi ketidak seimbangan kemampuan dan beban tugas,

---

<sup>18</sup>Abdul Wahid dan Mohammad Labib, *Op.Cit.* ,hal. 54.

<sup>19</sup>Muladi, *Pelaksana Pidana di Bidang Hukum Ekonomi*, F.H.UNKRIS, Jakarta 1989, hal. 8.

atau nyata-nyata tidak dapat diemban oleh kemampuan yang dimiliki penegak hukum;

- d. Apakah perbuatan itu menghambat atau menghalangi cita-cita bangsa, yakni terwujudnya masyarakat adil dan makmur, sehingga merupakan bahaya bagi keselamatan masyarakat.

Menurut TB. Ronny R. Nitibaskoro, suatu perbuatan dijadikan perbuatan pidana (diskriminalisasikan) karena alasan-alasan:<sup>20</sup>

1. Perbuatan itu merugikan masyarakat;
2. Sudah berulang-ulang dilakukan;
3. Ada reaksi sosial atas perbuatan itu;
4. Ada unsur bukti.

Berdasarkan hal-hal di atas, maka tidak serta merta setiap perbuatan yang merugikan dapat dirumuskan secara formal sebagai perbuatan pidana. Oleh karena itu, di dalam dunia maya perlu dipilah dengan seksama, mana saja perbuatan-perbuatan yang layak dikategorikan sebagai tindak pidana dunia maya.

Dalam melakukan kriminalisasi masih diperlukan kriteria lain untuk menyatakan suatu perbuatan patut dicela atau tidak dicela. Untuk itu perlu dilakukan penelitian mengenai pendapat, sikap, dan pandangan masyarakat terhadap suatu perbuatan. Hal ini dikarenakan sulitnya menentukan suatu perbuatan sebagai tindak pidana atau bukan tindak pidana sebagai akibat perubahan sosial dan pandangan yang berbeda di antara golongan dan suku bangsa Indonesia, maka kecenderungan melakukan kriminalisasi dan dekriminalisasi suatu perbuatan perlu memperhatikan akibat-akibat kemajuan zaman yang diiringi dengan kemajuan teknologi dalam masyarakat.

Masalah penetapan perbuatan yang dilarang (tindak pidana) dalam hukum pidana untuk dipandang sebagai tindak pidana harus bersifat asusila dan immoral, hal sebagaimana dikemukakan Roeslan Saleh dengan mensitir pendapat J.M. Van Bemmelen dalam buku *Criminologie, Leerboek der Misdaadkunde*, berpendapat pada umumnya harus dipandang sebagai tindak pidana adalah segala kelakuan yang bersifat merusak dan tidak susila atau immoral.<sup>21</sup>

Hal yang sama juga dikemukakan oleh Packer, bahwa *only conduct generally considered immoral should be treated as criminal*.<sup>22</sup> Dijelaskan lebih lanjut, bahwa ancaman pidana harus terbatas pada bentuk tingkah laku yang dipandang oleh masyarakat pada umumnya sebagai perbuatan

---

<sup>20</sup>Sutarman, *Op. Cit.*, hal. 60.

<sup>21</sup>Sahuri L., Disertasi, *Pertanggungjawaban Korporasi dalam Perspektif Kebijakan Hukum Pidana Indonesia*, 2003, hal. 82.

<sup>22</sup>*Ibid.*

yang immoral, tanpa adanya perbedaan paham kemasyarakatan yang berarti.

Sehubungan dengan kriteria untuk menentukan suatu perbuatan sebagai tindak pidana tersebut di atas, Roeslan Saleh menjelaskan dengan mensitir pendapat van Bemmelen yaitu:<sup>23</sup>

Tiap-tiap kriteria hanya mempunyai arti yang relatif. Penentuan sifat merusak (merugikan) maupun sifat immoralitas suatu kelakuan memainkan peranan. Pada suatu kejadian sifat merusak dan kemungkinan adanya kerusakan atau kerugian yang memainkan peranan utama, sedangkan pada kejadian lain sifat immoralitasnya pula yang utama. Hal ini mengakibatkan bahwa tidak ada suatu kriteria mempunyai arti yang mutlak.

Berdasarkan hal-hal tersebut di atas, maka penting bagi Indonesia untuk membentuk suatu aturan yang secara jelas mengatur mengenai tindak pidana dunia maya. Upaya perumusan hukum pidana secara lebih baik dapat dilakukan dengan cara mencakup di dalamnya mengenai kebijakan merubah atau membuat aturan khusus (hukum pidana) yang berkaitan dengan tindak pidana dunia maya. Artinya, walaupun mungkin secara esensial tindak pidana dunia maya dapat dianalogikan dengan tindak pidana yang diatur dalam Kitab Undang-Undang Hukum Pidana, namun hukum pidana tetap tidak menerima analogi.

Dalam pelaksanaannya tindak pidana dunia maya dijerat dengan hukum pidana dengan cara penafsiran, mengingat bahwa tindak pidana dunia maya merupakan tindak pidana yang sama sekali baru. Sementara umumnya hukum pidana hanya menerima penafsiran otentik saja. Selain itu juga karena karakteristik tindak pidana tersebut yang berbeda maka dimungkinkan untuk dijadikan sebagai tindak pidana tersendiri dengan aturan tersendiri juga dalam rangka mewujudkan rumusan hukum pidana yang lebih baik.

Hal ini tentu saja berkaitan dengan asas legalitas. Asas legalitas ini sangat fundamental dalam hukum pidana Indonesia. Pengaturan asas legalitas terdapat dalam Pasal 1 Ayat (1) Kitab Undang-undang Hukum Pidana yang menentukan bahwa tiada suatu perbuatan boleh dipidana, melainkan atas kekuatan ketentuan pidana dalam undang-undang yang mengatur atas perbuatan itu terlebih dahulu daripada perbuatan tersebut.

Asas legalitas (*nullum delictum nulla poena sine praevia lege*) dimaksudkan agar larangan dan ancaman pidana ditentukan terlebih dahulu secara tegas, sehingga orang mengetahui sesuatu perbuatan adalah terlarang.<sup>24</sup> Jika perbuatan itu dilakukan, maka telah diketahui

---

<sup>23</sup>*Ibid.*

<sup>24</sup>*Ibid.*, hal. 109.

dengan jelas mengenai sanksi pidana yang akan dikenakan terhadap pelakunya.<sup>25</sup>

Asas legalitas di sini mengandung tiga pengertian, yaitu:<sup>26</sup>

1. Tidak ada perbuatan yang dilarang dan diancam dengan pidana jika hal itu terlebih dahulu belum dinyatakan dalam suatu peraturan perundang-undangan;
2. Untuk menentukan adanya perbuatan pidana tidak boleh menggunakan analogi;
3. Aturan-aturan hukum pidana tidak boleh berlaku surut.  
Berkaitan dengan asas legalitas ini, maka hal utama yang harus dilakukan adalah mengkriminalisasikan *cyber crime* sebagai suatu tindak pidana dalam hukum nasional Indonesia.

Berdasarkan hal-hal tersebut di atas, maka Indonesia membentuk dan mengesahkan Undang-Undang Informasi dan Transaksi Elektronik. Undang-undang ini mengatur mengenai perbuatan yang dilarang untuk dilakukan di dalam dunia maya. Adapun bentuk perbuatan/Tindak pidana yang dimaksud adalah sebagai berikut:

1. Pasal 27 pada pokoknya menentukan bahwa:

Ayat (1)

Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.

Ayat (2)

Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian.

Ayat (3)

Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.

Ayat (4)

Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.

---

<sup>25</sup> *Ibid.*, hal. 82.

<sup>26</sup> Abdul Wahid dan Mohammad Labib, *Op.Cit.*, hal. 50-51.

2. Pasal 28 pada pokoknya menentukan bahwa:

Ayat (1)

Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.

Ayat (2)

Setiap Orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA).

3. Pasal 29 pada pokoknya menentukan bahwa:

Setiap Orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakutkan yang ditujukan secara pribadi.

4. Pasal 30 pada pokoknya menentukan bahwa:

Ayat (1)

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.

Ayat (2)

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.

Ayat (3)

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

5. Pasal 31 pada pokoknya menentukan bahwa:

Ayat (1)

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain.

Ayat (2)

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.

Ayat (3)

Kecuali intersepsi sebagaimana dimaksud pada ayat (1) dan ayat (2), intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang.

Ayat (4)

Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.

6. Pasal 32 pada pokoknya menentukan bahwa:

Ayat (1)

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.

Ayat (2)

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.

Ayat (3)

Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

7. Pasal 33 pada pokoknya menentukan bahwa:

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.

8. Pasal 34 pada pokoknya menentukan bahwa:

Ayat (1)

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki:

- a. perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33;
- b. sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33.

Ayat (2)

Tindakan sebagaimana dimaksud pada ayat (1) bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian Sistem Elektronik, untuk perlindungan Sistem Elektronik itu sendiri secara sah dan tidak melawan hukum.

9. Pasal 35 pada pokoknya menentukan bahwa:

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.

10. Pasal 36 pada pokoknya menentukan bahwa:

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi Orang lain.

Ketentuan pasal-pasal tersebut di atas jelas secara limitatif mengatur tentang perbuatan bagaimanakah yang dikategorikan sebagai tindak pidana dunia maya sebagai suatu perumusan tindak pidana, sedangkan untuk ketentuan pidana sebagai suatu kriminalisasi diatur dalam beberapa pasal dibawah ini:

1. Pasal 45 pada pokoknya menentukan bahwa:

Ayat (1)

Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3), atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 1.000.000.000., (satu miliar rupiah).

52 *Tindak Pidana Dunia Maya, Undang-Undang Informasi dan Transaksi Elektronik.*

Ayat (2)

Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 28 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 1.000.000.000,00 (satu miliar rupiah).

Ayat (3)

Setiap orang yang memenuhi unsur yang sebagaimana dimaksud dalam Pasal 29 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun/denda paling banyak Rp. 2.000.000.000,00 (dua miliar rupiah).

2. Pasal 46 pada pokoknya menentukan bahwa:

Ayat (1)

Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling lama banyak Rp. 6.000.000.000,00 (enam ratus juta rupiah).

Ayat (2)

Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp. 7.000.000.000,00 (tujuh ratus juta rupiah).

Ayat (3)

Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp. 800.000.000,00 (delapan ratus juta rupiah).

3. Pasal 47 pada pokoknya menentukan bahwa:

Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 31 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp. 800.000.000,00 (delapan ratus juta rupiah).

4. Pasal 48 pada pokoknya menentukan bahwa:

Ayat (1)

Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp. 2.000.000.000,00 (dua miliar rupiah).

Ayat (2)

Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9

(sembilan) tahun dan/atau denda paling banyak Rp. 3000.000.000,00 (tiga miliar rupiah)

Ayat (3)

Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (3) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp. 5000.000.000,00 (lima miliar rupiah).

5. Pasal 49 pada pokoknya menentukan bahwa:

Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 33 dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp. 10.000.000.000,00 (sepuluh miliar rupiah).

6. Pasal 50 pada pokoknya menentukan bahwa:

Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 34 ayat (1) dipidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp. 10.000.000.000,00 (sepuluh miliar rupiah).

7. Pasal 51 pada pokoknya menentukan bahwa:

Ayat (1)

Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp. 12.000.000.000,00 (dua belas miliar rupiah).

Ayat (2)

Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 36 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp. 12.000.000.000,00 (dua belas miliar rupiah)

8. Pasal 52 pada pokoknya menentukan bahwa:

Ayat (1)

Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 ayat (1) menyangkut kesusilaan atau eksploitasi seksual terhadap anak dikenakan pemberatan sepertiga dari pidana pokok.

Ayat (2)

Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau yang digunakan untuk layanan publik dipidana dengan pidana pokok ditambah sepertiga.

Ayat (3)

Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem

Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan diancam dengan pidana maksimal ancaman pidana pokok masing-masing Pasal ditambah sepertiga.

Ayat (4)

Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 dilakukan korporasi dipidana dengan pidana pokok ditambah dua pertiga.

Berdasarkan ketentuan pidana sebagaimana diatur dalam Undang-undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik yang terdapat pada Pasal 45 sampai dengan Pasal 52 tersebut di atas, jelas tidak mengatur adanya ancaman staf minima khusus berarti berlaku ketentuan dalam KUHP, hanya mengatur ancaman straf maksima. Juga jenis ancaman pidana yang diatur hanya terbatas pada pidana pokok berupa pidana penjara dan denda. Hanya saja adanya penyimpangan dari KUHP mengenai stelsel ancaman pidana yang diatur dalam Undang-undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diatur pada Pasal 45 sampai dengan Pasal 52 bersifat kumulasi relatif, karena dijumpai adanya kata dan/atau, ini menunjukkan bahwa hakim mempunyai pilihan untuk manjatuhkan pidana pidana pokok apakah dua-duanya atau salah satunya. Hal ini merupakan penyimpangan penjatuhan pidana yang diatur pada Pasal 10 KUHP, terhadap pidana pokok penjatuhan pidananya bersifat alternatif

#### **IV. PENUTUP**

##### **A. Kesimpulan**

Berdasarkan pembahasan tersebut di atas, maka penulis dapat menyimpulkan beberapa hal yaitu:

1. Bahwa tindak pidana dunia maya merupakan kategori tindak pidana yang baru mempunyai bentuk-bentuk sebagai berikut:
  - a. Perbuatan yang dilakukan secara illegal, tanpa hak atau tidak etis yang terjadi dalam ruang/wilayah siber (*cyber space*), sehingga tidak dapat dipastikan yurisdiksi negara mana yang berlaku terhadap tindak pidana tersebut;
  - b. Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang terhubung dengan internet;
  - c. Perbuatan tersebut mengakibatkan kerugian material maupun immaterial (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan dengan tindak pidana konvensional;
  - d. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya;

- e. Perbuatan tersebut sering digunakan secara transnasional/melintasi batas negara.
2. Dalam Undang-undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik sebagai suatu kriminalisasi terhadap bentuk tindak pidana telah diatur mengenai perbuatan yang dilarang untuk dilakukan di dalam dunia maya, sebagaimana diatur dalam Pasal 27 sampai dengan Pasal 37. Undang-Undang Informasi dan Transaksi Elektronik telah secara jelas memasukkan aspek penting terkait dunia maya. Hal ini dapat dilihat dari adanya pengakuan terhadap Informasi Elektronik, Dokumen Elektronik, Transaksi Elektronik, dan Sistem Elektronik dalam setiap pengaturan perbuatan yang dilarang.

## **B. Saran**

Berdasarkan kesimpulan tersebut di atas, maka penulis dapat memberikan saran sebagai berikut:

1. Hendaknya perlu dipahami secara mendalam tentang bentuk-bentuk tindak pidana dunia maya yang berhubungan dengan perumusan perbuatan yang dilarang maupun akibat yang ditimbulkan, mengingat dimensi tindak pidana dunia maya sangat luas.
2. Hendaknya rumusan tindak pidana yang terdapat pada Pasal 27 sampai dengan Pasal 37 yang diatur dalam Undang-undang No. 11 tahun 2008 tentang Informasi dan Elektronik perlu dipahami dalam penegakkannya mengingat sangat terkait dengan pertanggungjawaban pidana. Terutama Pasal 27 Undang-Undang Informasi dan Transaksi Elektronik pada pokoknya menentukan bahwa salah satu perbuatan yang dilarang adalah mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan, perjudian, penghinaan dan/atau pencemaran nama baik, pemerasan dan/atau pengancaman. Mengingat bahwa tindak pidana dunia maya merupakan tindak pidana transnasional artinya melewati batas yurisdiksi suatu Negara. Karena perbuatan kesusilaan di setiap negara berbeda-beda. Oleh sebab itu, perlu dibuatkan Peraturan Pelaksana yang lebih mempertegas batasan tentang kesusilaan. Sehingga terciptalah suatu kepastian hukum;

## **DAFTAR PUSTAKA**

- Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)*, Bandung, Refika Aditama, 2005.
- Alfon, *Pengamanan Aplikasi Komputer Dalam Sistem Perbankan dan Aspek Penyidikan Tindak Pidana*, 2006, [www.google.com](http://www.google.com).
- Barda Nawawi Arief, *Tindak Pidana Dunia Maya (Perkembangan Kajian Cyber Crime di Indonesia)*, Jakarta, Raja Grafindo Persada, 2006.

56 *Tindak Pidana Dunia Maya, Undang-Undang Informasi dan Transaksi Elektronik.*

Didik M. Arif Mansur dan Elisatris Gultom, *Cyber Law Aspek Hukum Teknologi Informasi*. Jakarta, Refika Aditama, 2005.

*e-Law: Saatnya Ada Undang-Undang Cyber*, 20 Februari 2003, WWW. Warta ekonomi Com.

Johannes Ibrahim, *Kartu Kridit*, Bandung, Refika Aditama, 2004.

*Modus Operandi Cyber Crime Makin Canggih*, 01 Agustus 2000, [www.google.com](http://www.google.com).

Muladi, *Pelaksana Pemidanaan di Bidang Hukum Ekonomi*, F.H.UNKRIS, Jakarta, 1989.

*Polisi Mengalami Future Shock dalam Kasus Cyber*, 12 November 2001. [www.google.com](http://www.google.com).

Sahuri L., Disertasi, *Pertanggungjawaban Korporasi dalam Perspektif Kebijakan Hukum Pidana Indonesia*, 2003.

Santosa Raharjanto, *Carder*, [www.google.com](http://www.google.com).

*Sebagian Kejahatan Dunia Maya Masih Samar*, 28 Agustus 2000, [www.google.com](http://www.google.com).

Sutarman, *Cyber Crime (Modus Operandi dan Penanggulangannya)*, Yogyakarta, Laks Bang, 2007.

*Telekomunikasi & Teknologi Tindak Pidana Cyber Crime*, [www.hukumonline.com](http://www.hukumonline.com).

### **Peraturan Perundang-undangan**

Republik Indonesia, Kitab Undang-undang Hukum Pidana.

Republik Indonesia, Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 154, Tambahan Lembaran Negara Republik Indonesia Nomor 3881).

Republik Indonesia, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2009 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843).