II. TINJAUAN PUSTAKA

A. Tugas Pokok Kepolisian Negara Republik Indonesia

Kepolisian Negara Republik Indonesia telah mempunyai seperangkat aturan mengenai tugas dan wewenang yang diatur secara tegas dalam Undang-Undang Nomor 2 Tahun 2002 Tentang Kepolisian Negara Republik Indonesia. Tugas dan wewenang Kepolisian Negara Republik Indonesia diatur dalam Pasal 13 sampai dengan Pasal 19 Undang-Undang Nomor 2 Tahun 2002 Tentang Kepolisian Negara Republik Indonesia sebagai berikut:

1. Pasal 13 Undang-Undang Nomor 2 Tahun 2002 Tentang Kepolisian Negara Republik Indonesia

   Tugas pokok Kepolisian Negara Republik Indonesia adalah:

   a. memelihara keamanan dan ketertiban masyarakat;
   b. menegakan hukum; dan
   c. memberikan perlindungan, pengayoman, dan pelayanan kepada masyarakat.

2. Pasal 14 Undang-Undang Nomor 2 Tahun 2002 Tentang Kepolisian Negara Republik Indonesia

   (1) Dalam melaksanakan tugas pokok sebagaimana dimaksud dalam Pasal 13, Kepolisian Negara Republik Indonesia bertugas:

a. melaksanakan pengaturan, penjagaan, pengawalan, dan patroli terhadap kegiatan masyarakat dan pemerintah sesuai kebutuhan;
b. menyelenggarakan segala kegiatan dalam menjamin keamanan, ketertiban, dan kelancaran lalu lintas di jalan;
c. membina masyarakat untuk meningkatkan partisipasi masyarakat, kesadaran hukum masyarakat serta ketaatan warga masyarakat terhadap hukum dan peraturan perundang-undangan;
d. turut serta dalam pembinaan hukum nasional;
e. memelihara ketertiban dan menjamin keamanan umum;
f. melakukan koordinasi, pengawasan, dan pembinaan teknis terhadap kepolisian khusus, penyidik pegawai negeri sipil, dan bentuk-bentuk pengamanan swakarsa;
g. melakukan penyelidikan dan penyidikan terhadap semua tindak pidana sesuai dengan hukum acara pidana dan peraturan perundang-undangan lainnya;
h. menyelenggarakan identifikasi keplolisian, kedokteran kepolisian, laboratorium forensik dan psikologi kepolisian untuk kepentingan tugas kepolisian;
i. melindungi keselamatan jiwa raga, harta benda, masyarakat, dan lingkungan hidup dari gangguan ketertiban dan/atau bencana termasuk memberikan bantuan dan pertolongan dengan menjunjung tinggi hak asasi manusia;
j. melayani kepentingan warga masyarakat untuk sementara sebelum ditangani oleh instansi dan/atau pihak yang berwenang;
k. memberikan pelayanan kepada masyarakat sesuai dengan kepentingannya dalam lingkup tugas kepolisian; serta
l. melaksanakan tugas lain sesuai dengan peraturan-perundang-undangan.

(2) Tata cara pelaksanaan ketentuan sebagaiman dimaksud dalam Ayat (1) huruf f diatur lebih lanjut dengan Peraturan Pemerintah.

3. Pasal 15 Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia

(1) Dalam rangka menyelenggarakan tugas sebagaimana dimaksud dalam Pasal 13 dan 14 Kepolisian Negara Republik Indonesia secara umum berwenang:
a. menerima laporan dan/atau pengaduan;
b. membantu menyelesaikan perselisihan warga masyarakat yang dapat mengganggu ketertiban umum;
c. mencegah dan menanggulangi tumbuhnya penyakit masyarakat;
d. mengawasi aliran yang dapat menimbulkan perpecahan atau mengancam persatuan dan kesatuan bangsa;
e. mengeluarkan peraturan kepolisian dalam lingkup kewenangan administratif kepolisian;
f. melaksanakan pemeriksaan khusus sebagai bagian dari tindakan kepolisian dalam rangka pencegahan;
g. melakukan tindakan pertama di tempat kejadian;

h. mengambil sidik jari dan identitas lainnya serta memotret seseorang;
i. mencari keterangan dan barang bukti;
j. menyelenggarakan Pusat Informasi Kriminal Nasional;
k. mengeluarkan surat izin dan/atau surat keterangan yang diperlukan dalam rangka pelayanan masyarakat;
l. memberikan bantuan pengamanan dalam sidang dan pelaksanaan putusan pengadilan, kegiatan instansi lain, serta kegiatan masyarakat;
m. menerima dan menyimpan barang temuan untuk sementara waktu;

(2) Kepolisian Negara Republik Indonesia sesuai dengan peraturan perundang-undangan lainnya berwenang"
a. memberikan izin dan mengawasi kegiatan keramaian umum dan kegiatan masyarakat lainnya;
b. menyelenggarakan registrasi dan identifikasi kendaraan bermotor;
c. memberikan surat izin mengemudi kendaraan bermotor;
d. menerima pemberitahuan tentang kegiatan politik;
e. memberikan izin dan melakukan pengawasan senjata api, bahan peledak, dan senjata tajam;
f. memberikan izin operasional dan melakukan pengawasan terhadap badan usaha di bidang jasa pengamanan;
g. memberikan petunjuk, mendidik, dan melatih aparat kepolisian khusus dan petugas pengamanan swakarsa dalam bidang teknis kepolisian;
h. melakukan kerjasama dengan kepolisian negara lain dalam menyidik dan memberantas kejahatan internasional;
i. melakukan pengawasan fungsional kepolisian terhadap orang asing yang berada di wilayah Indonesia dengan koordinasi instansi terkait;
j. mewakili pemerintah Republik Indonesia dalam organisasi kepolisian internasional;
k. melaksanakan kewenangan lain yang termasuk dalam lingkup tugas kepolisian.

(3) Tata cara pelaksanaan ketentuan sebagaimana dimaksud dalam ayat (2) huruf a dan d diatur lebih lanjut dengan Peraturan Pemerintah.

4. Pasal 16 Undang-Undang Nomor 2 Tahun 2002 Tentang Kepolisian Negara Republik Indonesia

(1) Dalam rangka menyelenggarakan tugas sebagaimana dimaksud dalam Pasal 13 dan 14 di bidang proses pidana, Kepolisian negara Republik Indonesia berwenang untuk:
a. melakukan penangkapan, penahanan, penggeledahan dan penyitaan;
b. melarang setiap orang meninggalkan atau memasuki tempat kejadian perkara untuk kepentingan penyidikan;
c. membawa dan menghadapkan orang kepada penyidik dalam rangka penyidikan;
d. menyuruh berhenti orang yang dicurigai dan menanyakan serta memeriksa tanda pengenal diri;
e. melakukan pemeriksaan dan penyitaan surat;

f. memanggil orang untuk didengar dan diperiksa sebagai tersangka atau saksi;
g. mendatangkan orang ahli yang diperlukan dalam hubungannya dengan pemeriksaan perkara;
h. mengadakan penghentian penyidikan;
i. menyerahkan berkas perkara kepada penuntut umum;
j. mengajukan permintaan secara langsung kepada pejabat imigrasi yang berwenang di tempat pemeriksaan imigrasi dalam keadaan mendesak atau mendadak untuk mencegah atau menangkal orang yang disangka melakukan tindak pidana;
k. memberi petunjuk dan bantuan penyidikan kepada penyidik pegawai negeri sipil serta menerima hasil penyidikan penyidik pegawai negeri sipil untuk diserahkan kepada penuntut umum; dan
l. mengadakan tindakan lain menurut hukum yang bertanggung jawab.

(2) Tindakan lain sebagaimana dimaksud dalam Ayat (1) huruf 1 adalah tindakan penyelidikan dan penyidikan yang dilaksanakan jika memenuhi syarat sebagai berikut:
a. tidak bertentangan dengan suatu aturan hukum;
b. selaras dengan kewajiban hukum yang mengharuskan tindakan tersebut dilakukan;
c. harus patut, masuk akal, dan termasuk dalam lingkungan jabatannya;
d. pertimbangan yang layak berdasarkan keadaan yang memaksa; dan
e. menghormati hak asasi manusia.

5. Pasal 17 Undang-Undang Nomor 2 Tahun 2002 Tentang Kepolisian Negara Republik Indonesia

"Pejabat Kepolisian Negara Republik Indonesia menjalankan tugas dan wewenangnya di seluruh wilayah Negara Republik Indonesia, khususnya di daerah hukum pejabat yang bersangkutan ditugaskan sesuai dengan peraturan perundang-undangan."

6. Pasal 18 Undang-Undang Nomor 2 Tahun 2002 Tentang Kepolisian Negara Rpeublik Indonesia

(1) Untuk kepentingan umum pejabat Kepolisian Negara Republik Indonesia dalam melaksanakan tuigas dan wewenangnya dapat bertindak menurut penilaiannya sendiri.
(2) Pelaksanaan ketentuan sebagaimana dimaksud dalam ayat (1) hanya dapat dilakukan dalam keadaan yang sangat perlu dengan memperhatikan peraturan perundang-undangan, serta Kode Etik Profesi Kepolisian Negara Republik Indonesia.

7. Pasal 19 Undang-Undang Nomor 2 Tahun 2002 Tentang Kepolisian Negara Republik Indonesia

(1) Dalam melaksanakan tugas dan wewenangnya, pejabat Kepolisian Negara Republik Indonesia senantiasa bertindak berdasarkan norma hukum dan mengindahkan norma agama, kesopanan, kesusilaan, serta menjunjung tinggi hak asasi manusia.
(2) Dalam melaksanakan tugas dan wewenang sebagaimana dimaksud dalam ayat (1), Kepolisian Negara Republik Indonesia mengutamakan tindakan pencegahan.

B. Penyelidikan dan Penyidikan Tindak Pidana *Cybercrime*

1. Penyelidikan

Penyelidikan berdasarkan ketentuan Pasal 1 Angka 5 Kitab Undang-Undang Hukum Acara Pidana adalah serangkaian tindakan penyelidik untuk mencari dan menemukan suatu peristiwa yang diduga sebagai tindak pidana guna menentukan dapat atau tidaknya dilakukan penyidikan menurut cara yang diatur dalam undang-undang ini. Sedangkan penyelidik berdasarkan ketentuan Pasal 1 Angka 4 Kitab Undang-Undang Hukum Acara Pidana adalah pejabat polisi negara Republik Indonesia yang diberi wewenang oleh undang-undang ini untuk melakukan penyelidikan.

2. Penyidikan

Penyidikan berdasarkan ketentuan yang diatur dalam Pasal 1 Angka 2 Kitab Undang-Undang Hukum Acara Pidana adalah serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam undang-undang ini untuk mencari serta mengumpulkan bukti yang terjadi guna menemukan tersangkanya. Sedangkan penyidik diatur dalam Pasal 1 Angka 1 Kitab Undang-Undang Hukum

Acara Pidana yang mengatur bahwa penyidik adalah pejabat polisi negara Republik Indonesia atau pejabat pegawai negeri sipil tertentu yang diberi wewenang khusus oleh undang-undang untuk melakukan penyidikan.

Menurut de Pinto, menyidik (*opsporing*) berarti pemeriksaan permulaan oleh pejabat-pejabat yang untuk itu ditunjuk oleh undang-undang segera setelah mereka dengan jalan apapun mendengar kabar yang sekadar [Sic!] beralasan, bahwa ada terjadi suatu pelanggaran hukum[1]. Kemudian terhadap penyidikan tindak pidana *cybercrime* selain berlaku ketentuan dalam Kitab Undang-Undang Hukum Acara Pidana juga berlaku ketentuan-ketentuan yang diatur dalam Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik sebagaimana yang diatur dalam Pasal 42 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Pembuktian sebenarnya telah dimulai pada tahap penyidikan; pembuktian bukan dimulai pada tahap penuntutan maupun persidangan. Dalam penyidikan, penyidik akan mencari pemenuhan unsur pidana berdasarkan alat-alat bukti yang diatur dalam perundang-undangan. Pada tahap penuntutan dan persidangan kesesuaian dan hubungan antara alat-alat bukti dan pemenuhan unsur pidana akan diuji.[2]

Penyidikan terhadap tindak pidana *cybercrime* selain dilaksanakan berdasarkan ketentuan yang diatur mengenai penyidikan yang terdapat dalam Kitab Undang-Undang Hukum Acara Pidana juga dilaksanakan berdasarkan ketentuan khusus mengenai penyidikan yang diatur dalam Undang-Undang Nomor 11 Tahun 2008

---

[1] Lilik Mulyadi, *Hukum Acara Pidana (Suatu Tinjauan Khusu Terhadap Surat Dakwaan, Eksepsi, dan Putusan Peradilan)*, Bandung: PT. Citra Aditya Bakti, 2002, hlm, 19.

[2] Josua Sitompul, *Cyberspace, Cybercrime, Cyberlaw: Tinjauan Aspek Hukum Pidana*, Jakarta: PT. Tatanusa, 2012, hlm. 309.

Tentang Informasi dan Transaksi Elektronik, hal ini dilakukan agar penyidikan dan hasilnya dapat diterima secara hukum. Berikut adalah beberapa hal mengenai penyidikan yang diatur dalam Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik:

1. Pasal 43 Ayat (1) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang mengatur bahwa yang diizinkan untuk melakukan penyidikan di dalam undang-undang ini adalah Penyidik Kepolisian Negara Republik Indonesia dan Pejabat Pegawai Negeri Sipil tertentu yang lingkup tugas dan tanggung jawabnya di bidang teknologi informasi dan transaksi elektronik.
2. Pasal 43 Ayat (2) Undang-Undang Nomor 8 Tahun 2011 Tentang Informasi dan Transaksi Elektronik yang mengatur bahwa penyidikan terhadap tindak pidana *cybercrime* harus memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran layanan publik, integritas data, atau keutuhan data sesuai dengan ketentuan Peraturan Perundang-undangan.
3. Pasal 43 Ayat (3) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang mengatur bahwa penggeledahan dan/atau penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan atas izin ketua pengadilan negeri setempat.
4. Pasal 43 Ayat (6) Undang-Undang Nomor 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik yang mengatur bahwa Dalam hal melakukan penangkapan dan penahanan, penyidik melalui penuntut umum

wajib meminta penetapan ketua pengadilan negeri setempat dalam waktu satu kali dua puluh empat jam.

C. Alat Bukti dan Barang Bukti dalam Tindak Pidana *Cybercrime*

Pembuktian terhadap tindak pidana *cybercrime* dilakukan dengan melihat tata cara pembuktian baik itu yang diatur dalam Kitab Undang-Undang Hukum Acara Pidanan dan juga yang diatur di dalam Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Sistem pembuktian yang dianut oleh hukum acara pidana Indonesia diatur dalam Pasal 183 Kitab Undang-Undang Hukum Acara Pidana yang mengatur bahwa: "hakim tidak boleh menjatuhkan pidana kepada seseorang kecuali apabila dengan sekurang-kurangnya dua alat bukti yang sah ia memperoleh keyakinan bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukannya". Dari pasal tersebut mengatakan bahwa putusan hakim haruslah didasarkan pada dua syarat, yaitu:

a. minimum dua alat bukti, dan
b. dari alat bukti tersebut, hakim memperoleh keyakinan bahwa terdakwa bersalah melakukan tindak pidana.

Berdasarkan hal tersebut, proses penyidikan tindak pidana *cybercrime* harus memperoleh alat bukti yang cukup agar tindak pidana yang terjadi tersebut dapat dibuktikan di persidangan dan pelakunya dihukum berdasarkan dengan hukuman yang diatur dalam peraturan perundang-undangan yang berlaku.

1. Alat Bukti dalam Tindak Pidana *Cybercrime*

Seperti yang telah disebutkan sebelumnya bahwa pembuktian tindak pidana *cybercrime* dapat dilakukan berdasarkan ketentuan dalam Kitab Undang-Undang

Hukum Acara Pidana dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Macam-macam alat bukti yang sah diatur dalam Pasal 184 Ayat (1) Kitab Undang-Undang Hukum Acara Pidana yang mengatur sebagai berikut:

"alat bukti yang sah ialah:
1) keterangan saksi;
2) keterangan ahli;
3) surat;
4) petunjuk;
5) keterangan terdakwa."

Ad. 1 Keterangan saksi

Saksi berdasarkan ketentuan Pasal 1 Angka 26 Kitab Undang-Undang Hukum Acara Pidana adalah orang yang dapat memberikan keterangan guna kepentingan penyidikan, penuntutan dan peradilan tentang suatu perkara pidana yang ia dengar sendiri, yang ia lihat sendiri dan ia alami sendiri. Sedangkan yang dimaksud dengan Keterangan saksi dalam Pasal 1 Angka 27 Kitab Undang-Undang Hukum Acara Pidana adalah salah satu alat bukti dalam perkara pidana yang berupa keterangan dari saksi mengenai suatu peristiwa pidana yang ia dengar sendiri, ia lihat sendiri dan ia alami sendiri dengan menyebut alasan dari pengetahuannya itu.

Mengingat pelaku dalam tindak pidana *cybercrime* ini bersifat *virtual*, otomatis keterangan yang diberikan oleh para saksi atas suatu tindakan diperoleh secara tidak langsung. Dalam hukum acara kita dikenal dengan *testimonium de auditu* atau *hearsay evidence*, dimana keterangan saksi tersebut diperoleh dari orang lain. Sesuai dengan penjelasan Kitab Undang-Undang Hukum Acara Pidana, kesaksian yang demikian tidak diperkenankan sebagai alat bukti, yakni selaras dengan tujuan hukum acara pidana yaitu mencari kebenaran materil, selain itu untuk

perlindungan terhadap hak-hak asasi manusia, diamana keterangan seorang saksi tersebut merupakan hasil pembicaraan atau hanya mendengar dari orang lain. Namun, kesaksian yang demikian tidak begitu saja dibuang dan dikatakan tidak berguna. Meskipun tidak memiliki kekuatan pembuktian sebagai alat bukti yang sah, dapat dijadikan bahan pertimbangan bagi hakim untuk memperkuat keyakinannya sebelum menjatuhkan putusan. Kedudukan kesaksian *de auditu* dalam *cybercrime* kiranya perlu mendapat perhatian khusus dengan suatu pertimbangan bahwa kejahatan dengan menggunakan komputer ini memiliki suatu karakteristik tersendiri, dimana subjek, objek, tempat dilakukannya tindak pidana tersebut tidak berwujud sehingga dengan begitu aturan-aturan pidana dapat diberlakukan atas tindakan tersebut. Selain itu, dengan diterimanya kesaksian *de auditu* akan meminimalkan hilangnya alat bukti/barang bukti sehingga akan lebih memberikan keyakinan pada hakim dalam memutus suatu perkara.[3]

Kesaksian *de auditu* setelah adanya Putusan MK Nomor 65/PUU-VII/2010 telah diakui secara sah, dimana dalam putusan itu menyatakan bahwa Pasal 1 Angka 26 dan angka 27, Pasal 65 dan Pasal 116 Ayat (3) dan Ayat (4) telah dinyatakan bertentangan dengan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 dan tidak mempunyai kekuatan hukum tetap sepanjang pengertian saksi dalam pasal-pasal tersebut tidak dimaknai termasuk pada "orang yang dapat memberi keterangan dalam rangka penyidikan, penuntutan, dan peradilan suatu tindak pidana yang tidak ia selalu dengar sendiri, ia lihat sendiri, dan ia alami sendiri". Sehingga diharapkan dengan adanya putusan ini akan dapat

[3] Edmon Makarim, *Pengantar Hukum Telematika (Suatu Kompilasi Kajian)*, Jakarta: Raja Grafindo Persada, 2005, hlm. 464.

mempermudah dalam hal mengumpulkan alat bukti untuk mengungkap suatu tindak pidana *cybercrime* yang ada.

Ad. 2 Keterangan ahli

Keterangan ahli dalam ketentuan Pasal 1 Angka 28 Kitab Undang-Undang Hukum Acara Pidana adalah keterangan yang diberikan oleh seseorang yang memiliki keahlian khusus tentang hal yang diperlukan untuk membuat terang suatu perkara pidana guna kepentingan pemeriksaan. Sedangkan yang dimaksud dengan keterangan ahli dalam Pasal 186 Kitab Undang-Undang Hukum Acara Pidana ialah apa yang seorang ahli nyatakan dalam persidangan.

Peranan seorang ahli dalam pengungkapan tindak pidana *cybercrime* merupakan suatu hal yang tidak bisa ditawar-tawar lagi, mengingat metode dan cara-cara yang dilakukan memiliki karakter yang berbeda dengan tindak pidana biasa. Kedudukan seorang ahli dalam menerangkan atau menjelaskan alat bukti, dalam hal ini berupa bukti elektronik akan sangat penting dalam memberikan keyakinan pada hakim dalam memutus suatu perkara[4].

Ad. 3 Alat bukti surat

Surat sebagaimana tersebut pada Pasal 184 Ayat (1) huruf c, dibuat atas sumpah jabatan atau dikuatkan dengan sumpah, adalah:

a. Berita acara dan surat lain dalam bentuk resmi yang dibuat oleh pejabat umum yang berwenang atau yang dibuat di hadapannya, yang memuat keterangan tentang kejadian atau keadaan yang didengar, dilihat atau yang

[4]*Ibid.*, hlm. 466.

dialaminya sendiri, disertai dengan alasan yang jelas dan tegas tentang keterangannya itu;

b. Surat yang dibuat menurut ketentuan peraturan perundang-undangan atau surat yang dibuat oleh pejabat mengenai hal yang termasuk dalam tata laksana yang menjadi tanggung jawabnya dan yang diperuntukan bagi pembuktian suatu keadaan;
c. Surat keterangan dari seorang ahli yang memuat pendapat berdasarkan keahliannya mengenai sesuatu hal atau sesuatu keadaan yang diminta secara resmi daripadanya;
d. Surat lain yang hanya dapat berlaku jika ada hubungannya dengan isi dari alat pembuktian yang lain.

Alat bukti surat dalam sebuah sistem komputer yang telah disertifikasi akan ada dua kategori. Pertama, bila sebuah sistem telah disertifikasi oleh badan yang berwenang, hasil *print out* komputer dapat dipercaya keautentikannya. Sebagai contoh adalah *recipt* yang dikeluarkan oleh Bank BCA dalam transaksi ATM. Sistem komputer ATM tersebut telah disertifikasi oleh badan yang berwenang dalam hal ini adalah Bank Indonesia (lingkup perbankan), sehingga jika terjadi suatu kasus, bukti elektronik (hasil *print out*) tersebut mempunyai kekuatan pembuktian meski nantinya dibutuhkan keterangan lebih lanjut dari seorang ahli. Kedua, bukti sertifikasi dari badan yang berwenang tersebut dapat dikategorikan sebagai alat bukti surat karena dibuat oleh dan atau pejabat yang berwenang. Kendala dari penggunaan dua bukti surat tersebut adalah mengenai pengertian

dari pejabat yang berwenang, dimana di dalam perundang-undangan kita pejabat yang berwenang adalah notaris.[5]

Ad. 4 Alat bukti petunjuk

Petunjuk berdasarkan ketentuan yang diatur dalam Pasal 188 Ayat (1) Kitab Undang-Undang Hukum Acara Pidana adalah perbuatan, kejadian atau keadaan, yang karena persesuaiannya, baik antara yang satu dengan yang lain, maupun dengan tindak pidana itu sendiri, menandakan bahwa telah terjadi suatu tindak pidana dan siapa pelakunya.

Jika hakim ingin mendapatkan petunjuk dari sebuah tindak pidana *cybercrime* dapat mengumpulkan bukti-bukti lainnya (dalam hal ini alat bukti elektronik) ke depan persidangan kemudian yang bersangkutan (hakim) akan minta pendapat seorang ahli yang kemudian memasukkan pendapat seorang ahli tadi sebagai keterangan ahli (Pasal 1 butir 28 Kitab Undang-Undang Hukum Acara Pidana). Singkatnya perolehan petunjuk dari hakim, meskipun dalam ketentuan undang-undang (Pasal 188 Ayat (1) Kitab Undang-Undang Hukum Acara Pidana) tidak menyebutkan secara eksplisit adanya usaha lain guna mencari petunjuk yang menerangkan suatu tindak pidana sudah menjadi kewajiban seorang hakim untuk melakukan pencarian hukum (*rechtvinding*) jika suatu perbuatan atau tindakan tidak ada dasar hukumnya sehingga kembali pada *asas legalitas* itu sendiri bukanlah pagar yang membatasai seorang hakim menjatuhkan pidana yang tentunya dilakukan dengan penuh tanggung jawab dan pertimbangan hukum yang logis dan keadaan di dalam masyarakat. [6]

[5]*Ibid*., hlm. 471.
[6]*Ibid.*, hlm. 475.

Ad. 5 Alat bukti keterangan terdakwa

Keterangan terdakwa berdasarkan ketentuan Pasal 189 Ayat (1) Kitab Undang-Undang Hukum Acara Pidana ialah apa yang terdakwa nyatakan di sidang tentang perbuatan yang ia lakukan atau yang ia ketahui sendiri atau alami sendiri. Dalam tindak pidana *cybercrime*, pelaku tindak pidana sulit untuk diidentifikasi secara pasti. Berbeda dengan kejahatan biasa, sejak ditemukannya bukti-bukti awal maka terhadap tersangka dapat dilakukan suatu penangkapan dan jika diperlukan dilakukannya penahanan. Namun, bukan tidak mungkin pelaku tindak pidana ini dapat ditangkap. Kesulitannya adalah jika kita hanya menggantungkan keterangan terdakwa, akan sangat sedikit atau bahkan tidak ada keterangan yang menyudutkan terdakwa dalam kasus tersebut.[7]

Setelah diberlakukannya Undang-Undang Nomor 8 Tahun 2011 tentang Informasi dan Transaksi Elektronik terdapat penambahan macam alat bukti, dan diakuinya dokumen elektronik sebagai alat bukti yang sah, sebagaimana diatur dalam Pasal 5 Ayat (1) dan (2) jo. Pasal 6 Undang-Undang Nomor 8 Tahun 2011 tentang Informasi dan Transaksi Elektronik yang menentukan bahwa dokumen elektronik atau hasil cetaknya merupakan alat bukti yang sah dan dapat digunakan di muka persidangan, sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan, sehingga menerangkan suatu keadaan. Selain itu dokumen elektronik kedudukannya disetarakan dengan dokumen yang dibuat di atas kertas, sebagaimana ditentukan

[7] *Ibid.*, hlm. 477.

dalam penjelasan umum Undang-Undang Nomor 8 Tahun 2011 tentang Informasi dan Transaksi Elektronik.[8]

Informasi elektronik berdasarkan ketentuan Pasal 1 Ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik adalah suatu atau sekumpulan data elektonik, termasuk tapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

Pengertian di atas, menunjukan syarat utama agar sesuatu digolongkan sebagai informasi elektronik adalah harus merupakan satu atau sekumpulan data elektronik yang telah diolah dan memiliki arti. Data elektronik adalah data digital yang bersumber dari perangkat elektronik yang berbasis komputasi. Data elektronik ini bersifat sangat luas, bisa berarti data-data dalam bahasa *binary* (berjumlah 8 *bit* yang terdiri atas 0 dan 1), heksadesimal (berjumlah 16 *bit* yang terdiri atas 0,1,2,3, …s.d 9, a,b,, …s.d. f); teks (misalnya dengan bahasa *Unicode*, yaitu suatu bahasa pengodean yang bersifat universal yang memetakan karakter-karakter yang umum dan khusus dalam bidang heksadesimal); dan/atau data aplikasi (misalnya *office file, audio file, image file,* dan lain-lain).[9]

Dokumen elektronik dalam ketentuan Pasal 1 Ayat (4) Undang-Undang Nomor 8 Tahun 2011 tentang Informasi dan Transaksi Elektronik adalah setiap informasi

[8] Johan Wahyudi, "Dokumen Elektronik Sebagai Alat Bukti Pada Pembuktian di Pengadilan", *Perspektif,* volume XVII No. 2 Tahun 2012 Edisi Mei, hlm. 126.
[9] Muhammad Nuh Al-Azhar, *Digital Forensik: Panduan Praktis Investigasi Komputer,* Jakarta Selatan: Salemba Infotek, 2012, hlm. 44.

elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, atau sejenisnya yang dapat dilihat ditampilkan dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, atau sejenisnya, huruf, tanda, angka, kode akses,simbol, atau perforasi yang memiliki makna/arti atau dapat dipahami oleh orang yang mampu memahaminya.

Pengertian tersebut menunjukan bahwa sesuatu digolongkan menjadi dokumen elektronik jika: [10]

1) Merupakan informasi elektronik;
2) Yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya.
3) Yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau sistem elektronik;
4) Termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi;
5) Yang memiliki makna/arti.

Pasal 6 Undang-Undang Nomor 8 Tahun 2011 tentang Informasi dan Transaksi Elektronik informasi dan dokumen elektonik juga harus memenuhi syarat-syarat, berikut pengaturan yang terdapat dalam pasal tersebut:

"Dalam hal terdapat ketentuan lain selain yang diatur dalam Pasal 5 Ayat (4) yang mensyaratkan bahwa suatu informasi harus berbentuk tertulis atau asli, Informasi Elektronik dan/atau Dokumen Elektronik dianggap sah sepanjang informasi yang

[10] Muhammad Nuh Al-Azhar, *Op.Cit.*, hlm. 46.

tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan."

2. Barang Bukti

Barang bukti atau *corpus delicti* adalah barang mengenai mana delik dilakukan (objek delik) dan barang dengan mana delik dilakukan, yaitu alat yang dipakai untuk melakukan delik…, termasuk juga barang bukti ialah hasil dari delik…, barang yang memiliki hubungan langsung dengan tindak pidana.[11]

Barang bukti dengan alat bukti mempunyai hubungan yang erat dan merupakan rangkaian yang tidak terpisahkan. Dalam persidangan setelah semua alat bukti diperiksa, selanjutnya dilanjutkan dengan pemeriksaan barang bukti. Selain itu juga akan sangat berperan dalam memberikan keyakinan pada hakim dalam memutus suatu perkara.[12]

Barang bukti dalam tindak pidanba *cybercrime* dapat berupa barang bukti elektronik dan barang bukti digital. Barang bukti elektronik adalah barang bukti yang berbentuk fisik, sementara barang bukti digital memiliki isi yang bersifat digital, yang dalam Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dikenal dengan informasi elektronik dan dokumen elektronik. Barang bukti elektronik dapat berupa: komputer PC, *laptop/notebook*, *netbook*, *tablet*, *handphone*, *smartphone*, *flashdisk/thumb drive*, *floppydisk*, *harddisk*, CD/DVD, *router*, *switch*, *hub*, kamera video, CCTV, kamera digital, digital *recorder*, *music/video player*, dan lain-lain. Kemudian barang bukti digital misalnya: *logical file*, *deleted file*, *lost file, file slack, log file*, *encrypted file, steganography file, office file, audio file, video file*, *image file, email, user ID dan*

[11] Andi Hamzah, *Kamus Hukum*, Jakarta: Ghalia, 1986, hlm. 100.
[12] Edmon Makarim, *Op.Cit.*, hlm. 479.

password, short message service (SMS), *multimedia message service* (MMS), *call logs*.[13]

D. Tindak Pidana *Cybecrime*

Istilah *cybercrime* saat ini merujuk pada suatu tindakan kejahatan yang berhubungan dengan dunia maya (*cyberspace*) dan tindakan kejahatan yang menggunakan komputer. Ada ahli yang menyamakan antara tindak kejahatan *cyber* (*cybercrime*) dengan tindak kejahatan komputer, dan ada ahli yang membedakan diantara keduanya.[14]

Barda Nawawi Arief menunjuk pada kerangka (sistematik) *Draft Convention on Cyber Crime* dari Dewan Eropa (Draft No. 25, Desember 2000). Beliau menyamakan peristilahan antara keduanya dengan memberikan definisi *cybercrime* sebagai "*crime related to technology, computers, and the internet"* atau secara sederhana berarti kejahatan yang berhubungan dengan teknologi, komputer dan internet.[15]

Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi dalam beberapa literatur dan praktiknya dikelompokan dalam beberapa bentuk, antara lain:[16]

1. *Unauthorized access to computer system and service*, yaitu kejahatan yang dilakukan kedalam suatu sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa pengetahuan dari pemilik sistem jaringan komputer yang

[13] Muhammad Nuh Al-Azhar, *Digital Forensic: Panduan Praktis Investigasi Komputer*,Hal. 29.
[14] Dikdik M. Arief Mansur dan Elisatris Gultom, *Cyber Law: Aspek Hukum Teknologi Informasi*, Bandung: Refika Aditama, 2009, hlm.7.
[15] *Ibid.*, hlm. 8.
[16] Maskun, *Kejahatan Siber (Cyber Crime): Suatu Pengantar*, Jakarta: Kencana Prenada Media Group, 2013, hlm. 51.

dimasukinya. Biasanya pelaku kejahatan (*hacker*) melakukannya dengan maksud sabotase atau pun mencuri informasi penting dan rahasia. Namun begitu, ada juga yang melakukannya hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Kejahatan ini semakin marak dengan berkembangnya teknologi internet.

2. *Illegal contens,* yaitu kejahatan dengan memasukan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dianggap melanggar hukum atau mengganggu ketertiban umum. Sebagai contohnya adalah:
    a. Pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau harga diri pihak lain.
    b. Pemuatan yang berhubungan dengan pornografi.
    c. Pemuatan suatu informasi yang merupakan rahasia negara, agitasi, dan propaganda untuk melawan pemerintah yang sah dan sebagainya.
3. *Data forgery,* yaitu kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen *e-commerce* dengan membuat seolah-olah terjadi "salah ketik" yang pada akhirnya akan menguntungkan pelaku.
4. *Cyber espionage,* yaitu kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran. Kejahatan ini

biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu sistem komputerisasi.

5. *Cyber sabotage and extortion,* yaitu kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang tersambung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu *logic bomb*[17], virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku. Dalam beberapa kasus setelah hal tersebut terjadi, maka pelaku kejahatan tersebut menawarkan diri kepada korban untuk memperbaiki data, program komputer atau sitem jaringan komputer yang telah disabotase, tentunya dengan bayaran tertentu.
6. *Offence against intellectual property,* yaitu kejahatan yang ditujukan terhadap hak kekayaan intelektual yang dimiliki seseorang di internet. Sebagai contoh adalah peniruan tampilan *web page* suatu situs milik orang lain secara illegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.
7. *Infringements of privacy,* yaitu kejahtan yang ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara komputerisasi, yang apabila diketahui oleh orang lain, maka dapat merugikan orang secara material

[17]*Logic bomb* adalah suatu program yang dibuat dan dapat digunakan oleh pelakunya sewaktu-waktu atau tergantung dari keinginan dari si pelaku, dari situ terlihat bahwa informasi yang ada di dalam komputer tersebut dapat terganggu, rusak, atau bahkan hilang.

maupun immaterial, seperti nomor kartu kredit, nomor PIN ATM, keterangan tentang cacat atau penyakit tersembunyi, dan sebagainya.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik telah mengatur beberapa tindak pidana *cybercrime* diantaranya:[18]

1. Akses Tidak Sah (*Illegal Access)*

   Perbuatan yang memenuhi unsur tindak pidana akses secara tidak sah terhadap komputer dan/atau sistem elektronik milik orang lain diatur dalam Pasal 30 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagai berikut:

   1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun.
   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.
   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.

2. Penyadapan atau Intersepsi Tidak Sah (*Intercepting*)

   Tindak pidana intersepsi (pe-*nguping*-an) diatur dalam Pasal 31 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagai berikut:

   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.
   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

[18] Widodo, *Aspek Hukum Pidana Kejahatan Mayantara.*, Yogyakarta: Aswaja Pressindo, 2013, hlm. 107.

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.

3) Kecuali intersepsi sebagaimana dimaksud pada Ayat (1) dan Ayat (2), intersepsi yang dilakukan dalam penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang.
4) Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada Ayat (3) diatur dengan Peraturan Pemerintah.

Mahkamah Konstitusi (MK) melalui Putusan Nomor 5/PUU-VIII/2010 telah membatalkan ketentuan Pasal 31 Ayat (4) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang berisi tata cara penyadapan yang hanya diatur oleh peraturan pemerintah. Karena itu, ketentuan pasal tersebut tidak berlaku. Pengaturan penyadapan di Indonesia hanya dapat dilakukan dengan undang-undang, karena menyangkut pembatasan Hak Asasi Manusia (HAM) yang mendasar, sebagaimana diatur dalam Pasal 28 J Ayat (2) Undang-Undang Dasar Negara Republik Indonesia Tahun 1995.

3. Gangguan Terhadap Data Komputer (*Data Interference*)

Tindak pidana perubahan dan gangguan terhadap data komputer diatur dalam Pasal 32 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagai berikut:

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.
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.
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.

4. Gangguan terhadap Sistem Komputer (*Sistem Interference*)

Tindak pidana berupa gangguan terhadap sistem komputer diatur dalam Pasal 33 Undang-Undang Nomor 11 Tahun 2011 tentang Informasi dan Transaksi Elektronik sebagai berikut:

"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."

5. Penyalahgunaan Perangkat Komputer (*Misuse Of Device*)

Tindak pidana berupa penyalahgunaan perangkat komputer diatur dalam Pasal 34 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagai berikut:

1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, medistribusikan, 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.
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.

Dalam penjelasan Pasal 34 Ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik diuraikan bahwa yang dimaksud

dengan “kegiatan penelitian” adalah penelitian yang dilaksanakan oleh lembaga penelitian yang memiliki izin.

6. Pemalsuan Melalui Komputer (*Computer-Related Forgery*)

   Pemalsuan melalui komputer diatur dalam Pasal 35 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagai berikut:

   “Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengerusakan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik.”

7. Pornografi Melalui Komputer (*Pornography*)

   Tindak Pidana Pornografi diatur dalam Pasal 27 Ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagai berikut:

   “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 kesusialaan.”

8. Kejahatan “Tradisional” Yang Menggunakan Komputer

   Perbuatan pidana tradisional juga diatur dalam Pasal 27 Ayat (2), Ayat (3), dan Ayat (4) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagai berikut:

   1. Pasal 27 Ayat (2) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik:

"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."

2. Pasal 27 Ayat (3) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik:

   " Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuatdapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik."

3. Pasal 27 Ayat (4) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik:

   "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."

9. Tindak pidana penyebaran berita bohong

   Penyebaran berita bohong melalui internet diatur dalam Pasal 28 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik sebagai berikut:

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

10. Tindak pidana pengancaman

Tindak pidana pengancaman melalui internet diatur dalam Pasal 29 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagai berikut:

> "Setiap Orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi."