BAB IV

ANALISIS HUKUM TENTANG PERUSAKAN SITUS INSTANSI PEMERINTAH YANG DILAKUKAN MELALUI MEDIA INTERNET DIHUBUNGKAN DENGAN UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

A. Perlindungan Hukum Mengenai Perusakan Situs Instansi Pemerintah Yang Dilakukan Melalui Media Internet

Salah satu produk inovasi teknologi telekomunikasi adalah internet *(interconection networking*), yaitu suatu koneksi antar jaringan komputer. Aplikasi internet saat ini telah memasuki berbagai segmen aktivitas manusia, baik dalam sektor politik, sosial, budaya, ekonomi dan bisnis, maupun dalam sektor pemerintahan.

Pada instansi pemerintahan, media internet mulai banyak dimanfaatkan dengan membuat suatu situs internet instansi pemerintahan tersebut, yang dimaksudkan agar masyarakat dapat dengan mudah mencari informasi yang berhubungan dengan instansi termaksud hanya dengan mengakses situs instansi pemerintahan tersebut melalui media internet.

Perangkat hukum internasional mengenai *cybercrime* sendiri sudah dibentuk dengan adanya beberarapa kongres-kongres PBB, dan hal tersebut wajib untuk diratifikasi oleh negara anggota. Langkah yang

ditempuh adalah memasukkan *cybercrime* dalam sistem hukumnya masing-masing negara anggotanya.

Dalam rangka menanggulangi *cybercrime*, Resolusi Kongres PBB VIII/1990 mengenai *Computer Related Crimes* dan *International Industry Congres* (IIIC) 2000 *Millenium Congres* di Quebec pada tanggal 19 September 2000 dan Kongres PBB mengenai *The Prevention of Crime and The Treatment of Offenders*, mengajukan beberapa kebijakan antara lain :[1]

1. Menghimbau negara-negara anggota untuk mengintensifkan upaya-upaya penanggulangan penyalahgunaan komputer yang lebih efektif dengan mempertimbangkan langkah-langkah sebagai berikut:
   a. Melakukan modernisasi hukum pidana meteriil dan hukum acara pidana;
   b. Mengembangkan tindakan-tindakan pencegahan dan pengamanan komputer;
   c. Melakukan langkah-langkah untuk membuat warga masyarakat, aparat pengadilan dan penegak hukum sensitif terhadap pentingnya pencegahan kejahatan yang berhubungan dengan komputer (*cybercrime*);
   d. Memperluas *rules of ethics* dalam penggunaan komputer dan mengajarkannya dalam kurikulum informatika;
   e. Mengadopsi kebijakan perlindungan korban *cybercrime* sesuai dengan deklarasi PBB mengenai korban, dan mengambil langkah-langkah untuk mendorong korban melaporkan adanya *cybercrime*.

[1] Barda Nawawi Arif, *Dalam United Nations (Eighth UN Congress On The Prevention Of Crime And The Treatment Of Offenders Report)*, 1991, hal. 141

2. Menghimbau negara-negara anggota meningkatkan kegiatan internasional dalam upaya penanggulangan *cybercrime*.
3. Merekomendasikan kepada Komite Pengendalian dan Pencegahan Kejahatan (*committee on Crime Preventon And Control*) PBB untuk :
    a. Menyebarluaskan pedoman dan standar untuk membantu negara anggota menghadapi *cybercrime* di tingkat nasional, regional dan internasional;
    b. Mengembangkan penelitian dan analisa lebih lanjut guna menemukan cara-cara baru menghadapi masalah *cybercrime* di masa depan;
    c. Mempertimbangkan *cybercrime* pada saat meninjau pengimplementasian perjanjian ekstradisi dan bantuan kerjasama di bidang penanggulangan kejahatan.

Secara internasional, PBB telah menghimbau negara-negara anggota untuk menanggulangi *cybercrime*, namun dalam kenyataannya tidaklah mudah. Dokumen Kongres PBB X/2000 sendiri mengakui bahwa ada beberapa kesulitan dalam menanggulangi *cybercrime* dengan sarana pidana, antara lain:[2]

1. Perbuatan jahat yang dilakukan berada di lingkungan elektronik. Oleh karena itu penanggulangan *cybercrime* memerlukan keahlian khusus, prosedur investigasi dan kekuatan/ dasar hukum yang mungkin tidak tersedia di negara yang bersangkutan;

[2] *Ibid*, hlm. 9

2. *Cybercrime* melampaui batas-batas negara, sedangkan penyidikan dan penegakan hukum selama ini dibatasi dalam wilayah territorial negaranya sendiri;
3. Struktur terbuka dari jaringan komputer internasional memberi peluang kepada pengguna untuk memilih lingkungan hukum (negara) yang belum mengkriminalisasikan *cybercrime*. Terjadi "*data havens*" (negara tempat berlindung/ singgahnya data, yaitu negara yang tidak memprioritaskan pencegahan penyalahgunaan jaringan komputer) dapat menghalangi usaha negara lain untuk memberantas kejahatan itu.

Persoalan di atas sebenarnya berkaitan dengan kebijakan hukum pidana. Kebijakan hukum pidana terkait erat dengan proses kriminalisasi terhadap suatu perbuatan. Dalam Kongres PBB/X/2000 disebutkan bahwa dalam jaringan komputer global, kebijakan kriminal negara mempunyai pengaruh langsung pada masyarakat internasional. Para penjahat *cyber* dapat mengarahkan aktifitas elektroniknya melalui suatu negara yang belum melakukan kriminalisasi terhadap kejahatan yang dilakukan itu dan oleh karenaya ia merasa aman dan terlindungi oleh hukum yang berlaku di negara tersebut. Meskipun suatu negara tidak mempunyai kepentingan nasional khusus dalam melakukan kriminalisasi terhadap perbuatan tertentu, sudah semestinya dipertimbangkan untuk melakukan langkah sebagai upaya menghindari negara tersebut menjadi *data haven* (tempat berlindungnya data) dan menjadi terisolasi secara internasional. Harmonisasi hukum pidana substantif mengenai *cybercrime* merupakan hal

yang esensial apabila kerjasama internasional harus dicapai oleh beberapa negara yang berbeda.

Kekhawatiran terhadap kejahatan mayantara di dunia sebetulnya telah dibahas secara khusus dalam suatu lokakarya (yaitu, "*workshop on crimes to computer networks*") yang diorganisir oleh UNAFEI selama kongres PBB X/2000 berlangsung.

Adapun kesimpulan dari lokakarya tersebut adalah sebagai berikut:[3]

1. CRC (*computer related crime*) harus dikriminalisasikan;
2. Diperlukan hukum acara yang tepat untuk melakukan penyidikan dan penuntutan terhadap penjahat cyber (*cybercrimes*);
3. Harus ada kerjasama antara pemerintah dan industri terhadap tujuan umum pencegahan dan penanggulangan kejahatan komputer agar internet menjadi tempat yang aman;
4. Diperlukan kerjasama internasional untuk menelusuri/ mencari para penjahat di internet;
5. PBB harus mengambil langkah/ tindak lanjut yang berhubungan dengan bantuan dan kerjasama tekhnis dalam penanggulangan CRC.

Berdasarkan uraian di atas diketahui bahwa sebenarnya *cybercrime* khususnya kejahatan *hacking* adalah sebuah isu hukum internasional. Perbedaannya adalah di beberapa negara anggota PBB sudah meratifikasi hasil kongres internasional mengenai kejahatan ini dalam sebuah regulasi peraturan perundang-undangan secara khusus, sedangkan di Indonesia

[3] Teguh Arifandi, *Cyber Crime dan Upaya Antisipasinya Secara Yuridis (II),* http://www.depkominfo.go.id/portal/?act=detail&mod=artikel_itjen&view=1&id=BRT06100 2182401, 15 April 2010, Pkl. 00:30:21

pengaturan khusus mengenai kejahatan tersebut baru dibuat sekitar dua tahun yang lalu.

Ketentuan-ketentuan mengenai *cybercrime* dalam KUHP masih bersifat global, namun berdasarkan tingkat kemungkinan terjadinya kasus dalam dunia maya (*cyberspace*) dan kategorisasi kejahatan *cyber* menurut *draft convention on cyber crime* maupun pendapat para ahli, Teguh Arifandi (Inspektorat Jendral Depkominfo) mengkategorikan beberapa hal yang secara khusus diatur dalam KUHP dan disusun berdasarkan tingkat intensitas terjadinya kasus tersebut.

Penggunaan sarana jaringan melalui media internet di negara-negara dunia dewasa ini semakin berkembang pesat. Kehadiran internet tidak dapat dielakkan lagi dapat menunjang kerja dari komputer sehingga dapat mengolah data yang bersifat umum melalui suatu *terminal system*. Apabila ada orang asing yang masuk ke dalam jaringan komputer tersebut tanpa ijin dari pemilik *terminal* ataupun penanggung jawab sistem jaringan komputer, maka perbuatan ini dikategorikan sebagai *hacking*. Kejahatan komputer jenis *hacking* sangat berbahaya karena apabila seseorang berhasil masuk ke dalam sistem jaringan orang lain, maka implikasi hukumnya ia mungkin saja membaca dan menyalin informasi yang mungkin sangat rahasia, atau mungkin pula menhapus atau mengubah informasi atau program-program yang tersimpan pada sistem komputer. Ada kemungkinan seseorang mencuri dengan memerintahkan komputer melalui *software* khusus untuk mengirimkan barang kepadanya.

Perbuatan *hacking* tersebut saat ini telah diatur dalam pasal 32 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang berbunyi:

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

Pasal diatas merupakan landasan hukum atau perlindungan hukum bagi setiap pemilik situs internet termasuk juga dalam hal ini situs internet instansi pemerintah dari kejahatan para *hacker*. Pasal tersebut menyatakan bahwa seseorang yang dengan sengaja mengubah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dapat dipidana sebagaimana diatur dalam Pasal 48 ayat (1) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, yang berbunyi:

> "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)."

Uraian tersebut di atas menjelaskan bahwa bilamana seseorang dengan sengaja dan tanpa hak atau melawan hukum/ menambah/ merusak suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik, akan dikenakan sanksi pidana sebagaimana diatur dalam Pasal 48 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Penanggulangan terhadap *cybercrime* dalam bentuk *hacking* perlu diimbangi dengan pembenahan dan pembangunan sistem hukum pidana secara menyeluruh, yakni meliputi pembangunan kultur, struktur dan subtansi hukum pidana. Dalam hal ini kebijakan hukum pidana menduduki posisi yang strategis dalam pengembangan hukum pidana modern.

B. Kendala-Kendala Dihadapi Dalam Proses Penegakan Hukum Atas Perusakan Situs Resmi Instansi Pemerintah Yang Dilakukan Melalui Media Internet

Kejahatan internet yang marak di Indonesia meliputi penipuan kartu kredit, penipuan perbankan, *defacing*, *cracking*, transaksi seks, judi *online* dan terorisme dengan korban berasal selain dari negara-negara luar seperti AS, Inggris, Australia, Jerman, Korea serta Singapura, juga beberapa di tanah air.

Di tahun 2008, Indonesia sudah mempunyai Undang-Undang yang mengatur tentang kegiatan yang berkaitan dengan dunia siber (*cyberspace*), yaitu Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Meskipun terkesan terlambat namun kehadiran Undang-Undang Informasi dan Transaksi Elektronik dirasa membawa angin segar bagi para penegak hukum khususnya Polri dalam menghadang laju kejahatan yang dilakukan para *Hacker* yang semakin banyak muncul di dunia siber (*cyberspace*). Lahirnya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Ekonomi ini belum didukung dengan peraturan yang mengatur tentang hukum formilnya. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi

Elektronik ini mempunyai 13 (tiga belas) Bab dan 54 (lima puluh empat) Pasal di dalamnya yang mengatur berbagai kegiatan dunia siber serta menerapkan azas-azas Ekstra Teritorial, Azas Kepasatian Hukum, Azas Manfaat, Azas Kehati-hatian, Azas Itikad Baik dan Azas Netral Teknologi. Penegakkan hukum dalam Undang-Undang ini sebagai penyidiknya adalah institusi Polri dan Penyidik Pegawai Negeri Sipil (PPNS) dengan menggunakan hukum formil yang berlaku di Indonesia yaitu KUHAP. Prinsip pengaturan dalam Undang-Undang Informasi dan Transaksi Elektronik ini menggunakan sintesis hukum materiil dan *lex informatica*. Strategi pembentukan pengaturan Undang-Undang Informasi dan Transaksi Elektronik adalah dengan menetapkan prinsip-prinsip pembentukan dan pengembangan teknologi informasi, yang isinya antara lain sebagai berikut:

1. Mengikuti keunikan *cyberspace*;
2. Melibatkan unsur-unsur masyarakat, pemerintah, swasta dan profesional serta perguruan tinggi;
3. Mendorong peran sektor swasta;
4. Mendorong peran masyarakat, swasta, pemerintah, kelompok profesi dan perguruan tinggi;
5. Peran dan tanggung jawab pemerintah terhadap kepentingan publik;
6. Aturan hukum yang bersifat preventif, direktif dan futuristik yang tidak bersifat restriktif;
7. Mendorong harmonisasi dan uniformitas hukum regional dan internasional; dan

8. Melakukan pengkajian terhadap peraturan yang berkaitan langsung atau tidak langsung dengan munculnya persoalan-persoalan hukum akibat perkembangan teknologi informasi.

Banyak kegiatan beracara untuk mengajukan pelaku kejahatan *Cybercrime* masih banyak menemui kendala dan memaksakan Undang-Undang yang lama untuk beracara. Jalan yang harus ditempuh oleh aparat *Criminal Justice System* adalah mengakomodir Undang-Undang yang ada dengan melakukan perluasan makna yang tercantum dalam Pasal-Pasal perundangan yang ada yaitu Undang-Undang Nomor 8 Tahun 1981 tentang Kitab Undang-Undang Hukum formil Pidana. Pasal 183 KUHAP menyatakan bahwa hakim tidak boleh menjatuhkan pidana kepada seseorang kecuali dengan sekurang-kurangnya dua alat bukti yang sah ia memperoleh keyakinan bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukannya. Berdasarkan Pasal 183 KUHAP tersebut dapat diketahui bahwa peradilan di Indonesia menganut sistem pembuktian menurut undang-undang yang negatif (*Negatief-wettelijk*, sedangkan alat bukti yang dimaksud adalah alat bukti sebagaimana di atur dalam Pasal 184 KUHAP yaitu :

1. Keterangan saksi;
2. Keterangan ahli;
3. Surat;
4. Petunjuk;
5. Keterangan terdakwa.

Di antara kelima jenis alat bukti tersebut yang sering dipermasalahkan adalah keterangan ahli dan surat. Keterangan ahli yang

dimaksud adalah ahli komputer, masalahnya adalah hingga sampai saat ini Indonesia masih belum ada organisasi yang mewadahi profesi di bidang komputer, sehingga persoalannya adalah apakah setiap orang yang mahir mengoperasikan komputer dapat dikategorikan sebagai ahli komputer. Dalam KUHAP sendiri tidak terdapat penjelasan mengenai apakah yang dimaksud dengan keterangan ahli dan siapakah yang dimaksud dengan ahli. Padahal keterangan saksi ahli (*expert testimony*) merupakan salah satu ciri peradilan modern.

Surat menurut pengertian para ahli adalah setiap benda yang memuat tanda-tanda baca yang dapat dimengerti yang bertujuan untuk mengungkapkan isi pikiran. Permasalahan atau kendala yang timbul adalah apakah tanda-tanda dalam data/ program komputer dapat dianggap sebagai tulisan, dengan demikian apakah data/program komputer yang tersimpan dalam *disket, floppy disk* atau media penyimpanan lainnya (yang tidak dicetak) dapat dikategorikan sebagai surat sehingga dapat diajukan di sidang pengadilan sebagai alat bukti surat. Pentingnya Indonesia memiliki aturan hukum yang mengatur tentang semua kegiatan dunia siber (*cyberspace*) dapat dilihat dari maraknya kejahatan yang dilakukan melalui media ini saat ini, termasuk salah satunya perusakan situs instansi pemerintah.

Kendala-kendala dalam mengatasi permasalahan *cybercrime* ini dikategorikan menjadi dua, antara lain sebagai berikut:

1. Kendala dari sisi kemampuan penyidik;

   Secara umum penguasaan operasional komputer dan pemahaman terhadap hacking komputer serta kemampuan melakukan penyidikan

terhadap kasus-kasus tersebut dari para penyidik Polri masih sangat minim. Banyak factor yang mempengaruhi hal tersebut namun dari beberapa faktor tersebut ada yang sangat berpengaruh (determinan). Adapun faktor-faktor yang mempengaruhi adalah sebagai berikut:

a. Kurangnya pengetahuan tentang komputer dan sebagian besar dari para penyidik belum menggunakan internet atau menjadi pelanggan pada salah satu ISP (Internet Service Provider);
b. Pengetahuan dan pengalaman para penyidik dalam menangani kasus-kasus *cybercrime* masih terbatas. Mereka belum mampu memahami teknik *hacking*, modus-modus operandi para *hacker* dan profil-profilnya;
c. Faktor sistem pembuktian yang menyulitkan para penyidik karena Jaksa (PU) masih meminta keterangan saksi dalam bentuk Berita Acara Pemeriksaan (BAP) formal sehingga diperlukan pemanggilan saksi/ korban yang berada di luar negeri untuk dibuatkan berita acaranya di Indonesia, belum bisa menerima pernyataan korban atau saksi dalam bentuk *faksimili* atau *e-mail* sebagai alat bukti.

2. Kendala dari sisi fasilitas komputer forensik

Untuk membuktikan jejak-jejak para *hacker* dan *cracker* dalam melakukan aksinya terutama yang berhubungan dengan program-program dan data-data komputer, sarana Polri belum memadai karena belum ada komputer forensik. Fasilitas ini diperlukan untuk mengungkap data-data digital serta merekam dan menyimpan bukti-

bukti berupa *softcopy* (*image*, *program*, dsb). Dalam hal ini Polri masih belum mempunyai fasilitas *forensic computing* yang memadai.

Cybercrime merupakan fenomena sosial yang membuka cakrawala keilmuan dalam dunia hukum, betapa suatu kejahatan yang sangat dasyat dapat dilakukan dengan hanya duduk manis di depan computer. *Cybercrime* merupakan sisi gelap dari kemajuan tehnologi komunikasi dan informasi yang membawa implikasi sangat luas dalam seluruh bidang kehidupan karena terkait erat dengan *economic crime* dan *organized crimes*.

Berdasarkan beberapa jenis *cybercrime*, Kongres PBB X di Wina menetapkan *hacking* sebagai *first crime*. Persoalannya apakah hukum pidana positif dapat menjangkau kejahatan *hacking*, setidaknya ada dua wacana yang berkembang di antara para pakar hukum pidana. Pertama, kejahatan komputer (*hacking*) sebenarnya bukanlah kejahatan baru dan masih terjangkau oleh KUHP untuk menanganinya. Menurut pendapat ini pengaturan untuk menangani kejahatan komputer *hacking* sebaiknya dintegrasikan ke dalam KUHP dan bukan ke dalam undang-undang tersendiri. Kedua, pendapat ini menyatakan perlu pembaharuan hukum pidana dengan membentuk undang-undang baru yang mengatur masalah kejahatan komputer (*hacking*). Hal ini dilandasi kenyataan bahwa kejahatan ini memiliki karakteristik yang berbeda dengan tindak pidana konvensional, sementara instrument hukum pidana yang ada masih kesulitan untuk menanggulangi perkembangan kejahatan ini.

Adapun tindakan hukum yang dapat dilakukan terhadap pelaku kejahatan *hacking* (*hacker*), dimana proses hukum yang dapat ditempuh

oleh pemilik situs internet dalam hal ini instansi pemerintah antara lain melalui lembaga peradilan umum yaitu baik secara perdata maupun secara pidana.

Secara perdata, tindakan hukum yang dilakukan adalah berdasarkan pada Pasal 1365 Buku III BW dimana pelanggaran hukum *hacking* tersebut merupakan perbuatan yang dapat dikategorikan sebagai Perbuatan Melawan Hukum (*Onrechtmatigedaad*) sebagaimana ditentukan dalam Pasal 1365 BW yang menyatakan bahwa:

> "Tiap perbuatan melanggar hukum, yang membawa kerugian kepada seorang lain, mewajibkan orang yang karena salahnya menerbitkan kerugian itu, mengganti kerugian tersebut."

Berdasarkan isi pasal diatas, suatu perbuatan dapat dianggap perbuatan melawan hukum bilamana memenuhi unsur-unsurnya, dimana unsur-unsur tersebut yaitu :[4]

1. perbuatan melanggar hukum;
2. unsur kesalahan (ada sebuah niat);
3. adanya kerugian (kerugian materil);
4. hubungan sebab akibat/ kausal antara point 1, 2 dan 3.

Berdasarkan Pasal 1365 BW tersebut, dalam kegiatan yang terjadi di dunia internet, perbuatan melawan hukum mungkin dapat terjadi selama memenuhi unsur-unsur yang terdapat dalam pasal diatas. Jadi, selama unsur-unsur tersebut tidak terpenuhi, maka suatu perbuatan tidak dapat dikategorikan sebagai perbuatan melawan hukum. Dimana dalam hal ini pelaku/ pembobol situs KPU telah memenuhi unsur-unsur tersebut.

---

[4] Hetty Hassanah, *Diktat Mata Kuliah hukum Perdata,* Unikom, 2006

Penerapan ketentuan pasal 1365 termaksud dilakukan dengan cara melakukan penafsiran hukum ekstensif yaitu memperluas arti kata perbuatan melawan hukum itu sendiri, tidak hanya yang terjadi dalam dunia nyata, tetapi juga dimungkinkan perbuatan melawan hukum yang terjadi di dunia maya, dalam hal ini perbuatan perusakan situs instansi pemerintah tersebut. Selain itu, dapat pula diterapkan Pasal 1365 BW dengan melakukan konstruksi hukum analogi yakni dengan cara membandingkan antara perbuatan melawan hukum yang dilakukan di dunia nyata dengan dunia maya, sehingga pada akhirnya unsur-unsur perbuatan melawan hukum sebagaimana disyaratkan tetap dapat terpenuhi. Walaupun pada prakteknya muncul kesulitan-kesulitan dalam penerapannya, namun tetap diharapkan perbuatan melawan hukum yang terjadi harus tetap mendapat sanksi secara hukum sehingga tidak ada kekosongan hukum.

Suatu perbuatan dapat dikatakan perbuatan melawan hukum apabila perbuatan tersebut memang melanggar peraturan perundang-undangan, bertentangan dengan kesusilaan dan ketertiban umum. Meskipun demikian, suatu perbuatan yang telah dikategorikan sebagai perbuatan melawan hukum ini harus dapat dipertanggungjawabkan apakah mengandung unsur kesalahan atau tidak.[5]

Pasal 1365 BW tidak membedakan kesalahan dalam bentuk kesengajaan (*opzet-dolus*) dan kesalahan dalam bentuk kurang hati-hati *(culpa*), dengan demikian hakim harus dapat menilai dan mempertimbangkan berat ringannya kesalahan yang dilakukan sesorang

[5] *Ibid.*

dalam hubungannnya dengan perbuatan melawan hukum ini, sehingga dapat ditentukan ganti kerugian yang seadil-adilnya.[6]

Adapun perbuatan yang dianggap sebagai perbuatan melawan hukum, namun tidak dapat dituntut sebagai perbuatan melawan hukum, yaitu apabila perbuatan tersebut dilakukan dalam keadaan darurat, keadaan memaksa *(overmacht)*, karena perintah kepegawaian atau salah sangka yang dapat dimaafkan. Namun dalam hal ini, pengecualian tersebut tidak berlaku bagi pelaku karena pelaku melakukannya dengan sengaja untuk mencari keuntungan. Apabila unsur kesalahan dalam suatu perbuatan melawan hukum dapat dibuktikan, maka ia bertanggung jawab atas kerugian yang disebabkan perbuatannya tersebut.

Perbuatan melawan hukum sebagaimana diatur dalam Pasal 1365 BW ini dapat digunakan sebagai dasar untuk mengajukan ganti kerugian atas perbuatan yang dianggap melawan hukum karena telah menyebabkan kerugian kepada instansi pemerintah tersebut, baik materiil maupun immateril.

Tindakan hukum yang dapat dilakukan oleh instansi pemerintah secara pidana adalah berdasarkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dimana pelaku dapat dituntut karena telah melanggar pasal 32 ayat (1) UU ITE yang berbunyi :

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

[6] Subekti*, Pokok-Pokok Hukum Perdata*, Intermasa, Jakarta, hlm.56.

Pasal di atas menjelaskan bahwa bilamana seseorang dengan sengaja mengubah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik atau yang lebih dikenal sebagai "*situs*", merupakan salah satu perbuatan yang dilarang karena telah melanggar isi pasal tersebut. Adapun unsur-unsur yang terdapat dalam Pasal 32 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tersebut adalah :

1. Unsur Objektif

   Setiap orang, dimana manusia oleh hukum diakui sebagai penyandang hak dan kewajiban, sebagai subyek hukum atau sebagai orang.

2. Unsur Subjektif

   Melawan hukum/ menambah/ merusak, dimana dalam undang-undang diatur bahwa pada perbuatan tersebut seseorang terikat kepada akibat hukum yang muncul karena kehendaknya sendiri.

Berdasarkan unsur-unsur di atas, maka setiap orang atau badan atau dalam hal ini instansi pemerintah yang mengalami kerusakan suatu Informasi Elektronik yang dilakukan oleh seseorang dengan cara melawan hukum atau tanpa hak, dapat menggunakan pasal ini untuk menjerat setiap pelanggaran yang dilakukan oleh seseorang dengan cara melawan hukum tersebut.

Pada pasal tersebut dinyatakan bahwa seseorang yang dengan sengaja mengubah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dapat dipidana sebagaimana diatur dalam Pasal 48 ayat (1)

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, yang berbunyi:

> “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).”

Pasal diatas menyatakan bahwa bilamana seseorang dengan sengaja dan tanpa hak atau melawan hukum/ menambah/ merusak suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik, akan dikenakan sanksi pidana sebagaimana diatur dalam Pasal 48 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.