KEJAHATAN *DEFACING*
(PERBANDINGAN UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK DAN HUKUM PIDANA ISLAM)

SKRIPSI

DIAJUKAN KEPADA FAKULTAS SYARI'AH DAN HUKUM UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA YOGYAKARTA UNTUK MEMENUHI SEBAGIAN SYARAT MEMPEROLEH GELAR SARJANA STRATA SATU DALAM HUKUM ISLAM

Oleh:

AHMAD MUYASIR
11360052

Pembimbing:

Dr. SRI WAHYUNI, M.Ag., M.Hum

PERBANDINGAN MAZHAB

FAKULTAS SYARI'AH DAN HUKUM

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2015

ABSTRAK

Cybercrime atau kejahaan dunia maya tercipta akibat penyalahgunaan teknologi. Perkembangan teknologi yang semakin berkembang tentu bertujuan memberikan kemudahan dalam membantu manusia dalam aktifitas sehari-hari. Meskipun demikian, sebagian orang memanfaatkan untuk tujuan yang negatif. Banyak sekali macam *cybercrime*, dan salah satunya adalah *defacing*. *Defacing* merupakan kejahatan mayantara yaitu mengubah tampilan *website* orang lain tanpa izin baik sebagian ataupun menyeluruh dengan menerobos sistem orang lain terlebih dahulu.

Maraknya kejahatan jenis ini merupakan sebuah fenomena baru yang menarik untuk dikaji. Hal tersebut memberikan kesempatan penyusun untuk mengetahui bagaimana pandangan hukum pidana Indonesia dan Fiqih Jinayah terhadap *defacing*, dan perbandingan antara kedua jenis hukum tersebut.

Penelitian ini merupakan penelitian kepustakaan. Data diperoleh dari sumber-sumber kepustakaan. Setelah data terkumpul, kemudian dianalisis secara deskriptik analitik komparatif. Selain itu pendekatan yang digunakan dalam skripsi ini adalah pendekatan yuridis dan normatif yaitu dengan mendekati masalah *defacing* dari segi hukum yang terdapat dalam Undang-undang dan hukum Islam.

Berdasarkan metode yang digunakan, maka diketahui menurut Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) *defacing* merupakan perbuatan dilarang yaitu pada Pasal 30 dalam aktifitas menerobos sistem orang lain tanpa izin dan Pasal 32 ayat (1) pada aktifitas memodifikasi *website* tanpa hak. Sedangkan dalam hukum Islam *defacing* juga merupakan perbuatan dilarang karena merugikan seseorang atau memberi *maḍarat* bagi orang lain. Tidak ada dalil secara langsung tentang *defacing*, karena *defacing* merupakan kejahatan modern seperti sekarang ini, maka dalam hukum Islam *defacing* masuk kategori *jari□mah ta'zi□r*. Sanksi kejahatan *defacing* menurut Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik terdapat dalam Pasal 46 dan Pasal 48 ayat (1). Dalam hukum Islam *defacing* masuk kategori *jari□mah ta'zi□r* maka jenis hukumanya adalah *ta'zi□r* yaitu, jenis dan besar kecilnya hukuman diserahkan kepada *ulil amri* atau hakim, jadi belum ditetapkan seberapa besar hukuman itu, yang jelas sesuai dengan kemaslahatan.

Universitas Islam Negeri Sunan Kalijaga PM-UINSK-BM-05-07/RO

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

KepadaYth.
Dekan Fakultas Syariah dan Hukum
UIN Sunan Kalijaga Yogyakarta
Di Yogyakarta

Assalāmu'alaikum Wr.Wb

Setelah melakukan beberapa kali bimbingan dan mengadakan perbaikan seperlunya, baik dari segi isi, bahasa maupun teknik penulisan, dan setelah membaca skripsi Mahasiswa tersebut di bawah ini:

Nama : Ahmad Muyasir

NIM : 11360052

Jurusan : Perbandingan Mazhab

Judul :**"Kejahatan *Defacing* (Perbandingan Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Hukum Pidana Islam)"**

Maka selaku pembimbing, kami berpendapat bahwa skripsi tersebut sudah layak diajukan untuk dimunaqasyahkan. Demikian, mohon dimaklumi adanya.

Wassalāmu'alaikum Wr.Wb

Yogyakarta, 02 Sya'ban 1436 H
20 Mei 2015 M

Pembimbing,

Dr. Sri Wahyuni, M.Ag., M.Hum
NIP. 19770107 200604 2 002

Universitas Islam Negeri Sunan Kalijaga PM-UINSK-BM-05-07/RO

PENGESAHAN SKRIPSI
Nomor: UIN.02/K.PM-SKR/PP.00.9/09/2015

Skripsi dengan Judul: Kejahatan *Defacing* (Perbandingan Undang-undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik dan Hukum Pidana Islam)

Yang dipersiapkan dan disusun oleh:

Nama	: Ahmad Muyasir
NIM	: 11360052
Telah dimunaqosyahkan pada	: 27 Mei 2015
Nilai Munaqosyah	: A

dan dinyatakan telah diterima oleh Fakultas Syariah dan Hukum UIN Sunan Kalijaga

TIM MUNAQOSYAH:

Penguji I

Dr. Sri Wahyuni, M. Ag., M. Hum
NIP: 19770107 200604 2 002

Penguji II

Dr. Fathurrahman, S. Ag., M. S. I
NIP. 19760820 200501 1 005

Penguji III

Ahmad Arifasul Marom, S. H. I., M. A
NIP. 19811107 200912 1 002

Yogyakarta, 27 Mei 2015 M
Fakultas Syariah dan Hukum
UIN Sunan Kalijaga

Dekan,

Dr. H. Syafiq Mahmadah Hanafi, M. Ag
NIP. 19670518 199703 1 003

SURAT PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan di bawah ini :

Nama	: Ahmad Muyasir
NIM	: 11360052
Jurusan	: Perbandingan Mazhab
Fakultas	: Syariah dan Hukum

Menyatakan dengan sesungguhnya bahwa skripsi saya ini asli hasil karya atau penelitian saya sendiri dan bukan plagiatdari hasil karya orang lain. Kecuali secara tertulis diacu dalam penelitian ini dan disebutkan dalam acuan *footnote* dan atau daftar pustaka.

Yogyakarta, 05 Rajab 1436 H
25 April 2015 M

Yang menyatakan,

Ahmad Muyasir
NIM. 11360052

MOTTO

6 IMMPOSIBLE IS NOTHING 9

”لا اله الا انت سبحا نك اني كنت من الظا لمين“

“ Jika kamu menungguku untuk menyerah, maka kamu akan menungguku selama-lamanya”

-Uzumaki Naruto-

HALAMAN PERSEMBAHAN

" Skripsi ini saya persembahkan kepada Orang Tuaku tercinta dan Almamater Universitas Islam Negeri Sunan Kalijaga Yogyakarta"

PEDOMAN TRANSLITERASI

Transliterasi yang digunakan dalam penulisan skripsi ini, bersumber dari pedoman Arab-Latin yang diangkat dari Keputusan Bersama Menteri Agama dan Menteri Pendidikan dan Kebudayaan Republik Indonesia, Nomor 158 Tahun 1987 dan Nomor 0543 b/U/1987, selengkapnya adalah sebagai berikut:

1. Konsonan

Fonem konsonan bahasa Arab, yang dalam sistem tulisan Arab dilambangkan dengan huruf, dalam tulisan transliterasi ini sebagian dilambangkan dengan huruf, sebagian dengan tanda, dan sebagian dengan huruf dan tanda sekaligus, sebagai berikut :

Huruf Arab	Nama	Huruf Latin	Nama
ا	alif	Tidak dilambangkan	Tidak dilambangkan
ب	ba’	B	Be
ت	Ta’	T	Te
ث	a		es (dengan titik di atas)
ج	jim	J	Je
ح	a		ha (dengan titik di bawah)
خ	Kha	Kh	ka dan ha

د	dal	D	De
ذ	żal	Ż	zet (dengan titik di atas)
ر	ra	R	Er
ز	za’	Z	Zet
س	sin	S	Es
ش	syin	Sy	es dan ye
ص	ṣad	ṣ	es (dengan titik di bawah)
ض	ḍad	ḍ	de (dengan titik di bawah)
ط	ṭa	ṭ	te (dengan titik di bawah)
ظ	ẓa	ẓ	zet (dengan titik di bawah)
ع	‘ain	‘	koma terbalik (di atas)
غ	gain	G	Ge
ف	fa	F	Ef
ق	qaf	Q	Qi
ك	kaf	K	Ka
ل	lam	L	El

م	mim	M	Em
ن	nun	N	En
و	wau	W	We
ه	ha	H	Ha
ء	hamzah	‘	Apostrof
ي	Ya’	Y	Ya

2. Vokal

a. Vokal Tunggal :

Tanda/Vokal	Nama	Huruf Latin	Nama
ـَ	Fathah	a	A
ـِ	Kasrah	i	I
ـُ	Dammah	u	U

b. Vokal rangkap :

Tanda	Nama	Huruf Latin	Nama
ي.....َ	Fatḥah dan ya	Ai	a-i
.....وَ	Fatḥah dan Wau	Au	a-u

Contoh :

كيف ---- *kaifa* حول ---- *ḥaula*

c. Vokal Panjang (*maddah*)

Tanda	Nama	Huruf Latin	Nama
اَ	Fathah dan alif	ā	A dengan garis di atas
...يَ	Fathah dan ya	ā	A dengan garis di atas
...ي	Kasrah dan ya	i□	I dengan garis di atas
...وُ	Dammah dan wau	ū	U dengan garis di atas

Contoh :

قال ---- *qālā* قيل ---- *qi□la*

ر مي ---- *ramā* يقول ---- *yaqūlu*

3. Ta marbūtah

a. Transliterasi *Ta' Marbūtah* hidup adalah "t".

b. Transliterasi "mati adalah "h".

c. Jika *Ta' Marbūtah* diikuti kata yang menggunakan kata sandang "ال" ("al-"), dan bacaannya terpisa, maka *Ta' Marbūtah* tersebut ditransliterasikan dengan "h".

Contoh :

روضة الاطفال ------- *rauḍah al-aṭfāl*

المدينةالمنورة ------- *al-Madinah al-Munawwarah*

طلحة ---------- *Ṭalḥatu atau Ṭalḥah*

4. Huruf Ganda (Syaddah atau Tasydi□d)

Transliterasi *syaddah* dan *tasydi□d* dilambangkan dengan huruf yang sama, baik ketika berada di awal atau akhir kata.

Contoh :

نزل -------- *nazzala* البر -------- *al-birru*

5. Kata Sandang "ال"

Kata sandang "ال" ditransliterasikan dengan "al" diikuti dengan tanda penghubung "-", baik ketika bertemu dengan huruf *qamariyyah* maupun huruf *syamsiyyah*.

6. Huruf Kapital

Meskipun tulisan Arab tidak mengenal huruf kapital, tetapi dalam transliterasi huruf kapital digunakan untuk awal kalimat, nama diri, dan sebagainya seperti ketentuan dalam EYD. Awal kata sandang pada nama diri tidak tertulis dengan huruf kapital, kecuali jika terletak pada permulaan kalimat.

Contoh:

ومامحمدالارسول -------- *Wa ma□ Muhammadun illa□ rasu□l*

KATA PENGANTAR

بسم الله الرحمن الرحيم

الحمد لله رب العلمين والعاقبة للمتقين ولا عدوان إلا على الظا لمين، أشهد ان لا إله إلا الله الملك الحق المبين، وأشهد أن محمدا عبد وه ورسوله صادق الوعداللأمين، اللهم صلى على سيدنا محمد قا ءىد الغر المحجلين وعلى أله و صحبه أجمعين. أما بعد .

Segala puji hanya milik Allah SWT, yang telah melimpahkan rahmat dan hidayahnya kepada yang dikehendaki dan semoga kita selalu dalam petunjuk dan pertolongan-Nya. Amiin.

Sholawat dan salam senantiasa tercurahkan kepada Rasulallah Muhammad SAW, keluarga, sahabat dan umatnya yang berpegang teguh pada risalah yang dibawa sampai akhir zaman.

Skripsi merupakan tugas akhir bagi Mahasiswa sebagai persyaratan mendapatkan gelar strata satu di Perguruan Tinggi. Skripsi ini tidak akan selesai disusun tanpa dukungan, bantuan, dan bimbingan dari berbagai pihak yang bersifat moril, spiritual, maupun materiil. Oleh karena itu penyusun mengucapkan terimakasih kepada :

1. Rektor UIN Sunan Kalijaga Yogyakarta, Bapak Prof. Drs. H. Akhmad Minhaji, M.A.,Ph.D.
2. Dekan Fakultas Syariah dan Hukum UIN Sunan Kalijaga Yogyakarta, Bapak Dr. H.Syafiq Mahmadah Hanafi, M.Ag.

3. Ketua Jurusan Perbandingan Mazhab Fakultas Syariah dan Hukum, Bapak Dr. Fathurrahman, S.Ag., M.S.I.
4. Sekretaris Jurusan Perbandingan Mazhab Fakultas Syariah dan Hukum, Bapak Gusnam Haris, S.Ag., M.Ag.
5. Ibu Dr. Sri Wahyuni, M.Ag., M.Hum. Selaku dosen pembimbing akademik dan pembimbing skripsi, yang telah meluangkan tenaganya untuk memberikan arahan, bimbingan, koreksi, demi selesainya tugas ini dengan baik.
6. Kedua orang tua tercinta, (alm) Bapak Zamroni dan Ibu Juwariyah yang tidak akan mampu untuk membalas kebaikanya.
7. Saudara, Sahabat, teman, semuanya, yang tidak dapat ditulis satu persatu oleh penyusun.

Penyusun menyadari Skripsi ini jauh dari sempurna. Semua itu tiada lain karena keterbatasan dan kekurangan penyusun. Oleh karena itu, kritik dan masukan dari berbagai pihak sangat penulis harapkan, untuk kesempurnaanya. Akhirnya semoga bermanfaat, bagi penyusun khususnya, dan para pembaca pada umumnya.

Yogyakarta, 01 rajab 1436 H
20 April 2015 M

Penyusun,

Ahmad Muyasir
NIM. 11360052

DAFTAR ISI

HALAMAN COVER ..... **i**

ABSTRAK ..... **ii**

SURAT PERSETUJUAN SKRIPSI ..... **iii**

HALAMAN PENGESAHAN ..... **iv**

SURAT PERNYATAAN KEASLIAN SKRIPSI ..... **v**

HALAMAN MOTTO ..... **vi**

HALAMAN PERSEMBAHAN ..... **vii**

PEDOMAN TRANSLITERASI ..... **viii**

KATA PENGANTAR ..... **xiii**

DAFTAR ISI ..... **xv**

BAB I PENDAHULUAN

A. Latar Belakang Masalah 1

B. Rumusan Masalah 9

C. Tujuan dan Kegunaan Penelitian 10

D. Telaah Pustaka 10

E. Kerangka Teoretik 15

F. Metode Penelitian 20

G. Sistematika Pembahasan 23

BAB II TINJAUAN UMUM

A. Tinjauan Umum tentang *Defacing* 25

1. Definisi *Defacing*.....25
2. Jenis-jenis *Defacing*.....34

B. Tinjauan Umum tentang Kejahatan.....48

1. Menurut Hukum Positif.....48
2. Menurut Hukum Islam.....53

BAB III *DEFACING* MENURUT UU ITE DAN HUKUM PIDANA ISLAM

A. *Defacing* menurut UU ITE.....50

1. Unsur-unsur *Defacing* Menurut UU ITE 50
2. Sanksi *Defacing* Menurut UU ITE.....58

B. *Defacing* menurut Hukum Pidana Islam 62

1. Unsur-unsur *Defacing* dalam Hukum Pidana Islam.....62
2. Sanksi *Defacing* dalam Hukum Pidana Islam.....63

BAB IV ANALISIS HUKUM *DEFACING* MENURUT UU ITE DAN HUKUM PIDANA ISLAM

A. Persamaan *Defacing* Menurut UU ITE dan Hukum Pidana Islam.....72

1. Dari Segi Unsur.....73
2. Dari Segi Sanksi.....74

A. Perbedaan *defacing* UU ITE dan Hukum Pidana Islam.....74

1. Dari Segi Unsur.....74
2. Dari Segi Sanksi.....75

BAB V PENUTUP

A. Kesimpulan 77

B. Saran/Rekomendasi.....79

LAMPIRAN :

1. Daftar Terjemahan Al-Qura□n
2. Tabel Gambar
3. Tabel Sebab-sebab *website* dapat di*deface*
4. Tabel Cara Kerja dan Jenis Serangan *Defacing*
5. Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
6. Curiculum Vitae

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Kemajuan teknologi merupakan sesuatu yang tidak bisa kita hindari dalam kehidupan ini, karena kemajuan teknologi akan berjalan sesuai dengan kemajuan peradaban, teknologi dan ilmu pengetahuan.[1] Teknologi membantu manusia mampu berinteraksi dengan manusia lain tanpa adanya batasan ruang dan waktu. Setiap inovasi diciptakan untuk memberikan manfaat positif bagi kehidupan manusia. Memberikan banyak kemudahan, serta sebagai cara baru dalam melakukan aktifitas manusia. Khusus dalam bidang teknologi masyarakat sudah menikmati banyak manfaat yang dibawa oleh inovasi-inovasi yang telah dihasilkan dalam dekade terakhir ini. Berbagai teknologi seperti radio, majalah, koran, televisi merupakan teknologi yang diciptakan manusia untuk dapat mengirimkan informasi dari suatu tempat ke tempat lain, namun kurangnya dari teknologi tersebut, konsep komunikasinya masih bersifat satu arah, tidak adanya kemampuan untuk memberikan dan mendapatkan *feedback* antara *source* dan *receiver messages*.[2]

[1] Budi Agus Riswandi, *Hukum Internet di Indonesia*, (Yogyakarta: UII Press, 2003), hlm. 1.

[2] Rulli Nasrullah, *Teori dan Riset Media Siber*, (Jakarta: Kencana, 2014), hlm. 2.

Struktur masyarakat dirubah oleh kemajuan teknologi dari yang bersifat lokal menuju ke arah masyarakat yang berstruktur global.[3] Perubahan ini disebabkan oleh kehadiran teknologi informasi yang terus berkembang. Perkembangan teknologi informasi itu berpadu dengan media dan komputer, yang kemudian melahirkan piranti baru yang disebut internet dalam mengirimkan informasi. sehingga, internet sangat membantu manusia dalam menyelesaikan masalahnya. [4]

Website sebagai salah satu aplikasi dari internet merupakan media yang sangat membantu dalam perkembangan teknologi komunikasi dalam masa kini. *Website* juga merupakan media untuk mendapatkan informasi dan promosi di dunia internet seperti personal, profil sekolah, profil perusahaan, berita pendidikan, bisnis, berita terkini dan semua hal yang dibutuhkan manusia dapat diakses melalui internet. Dengan *website* kita mudah menyebarkan dan mendapatkan informasi yang kita butuhkan. *Website* berfungsi sebagai media promosi, media pemasaran, media informasi, media pendidikan, dan media komunikasi.[5] Meskipun demikian, dengan melihat banyak sekali manfaat seperti manfaat *website* tersebut, kehadiran internet telah memunculkan paradigma baru dalam kehidupan manusia. Kehidupan berubah dari yang hanya bersifat nyata (*real*) ke realitas baru yang bersifat

[3] Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cybercrime),* (Jakarta: Refika Aditama, 2005), hlm. 103.

[4] *Ibid.*

[5] Deni Darmawan dan Deden Hendra Permana, *Desain dan Pemrograman Website*, (Bandung: Remaja Rosdakarya, 2013), hlm. 5.

maya (*virtual*). Realitas yang kedua ini biasa dikaitkan dengan internet dan ruang di dunia maya *(cyberspace)*.[6] Internet dengan kelebihan-kelebihanya mempunyai sisi kelemahan dan memiliki dampak buruk jika dipergunakan orang yang tidak bertanggungjawab. Adanya *cyberspace* memberi peluang terjadinya kejahatan atau lebih dikenal dengan *cybercrime* (kejahatan dunia maya), banyak sekali jenis *cybercrime* salah satunya adalah *defacing*.[7]

Defacing yang merupakan salah satu kejahatan dunia maya yaitu kegiatan merubah tampilan suatu *website* orang lain tanpa izin baik halaman utama atau *index file*nya ataupun halaman lain yang masih terkait dalam satu *URL*[8] dengan *website*[9] tersebut (bisa di folder atau di *file*). *Defacing* terdiri dari dua tahap, yaitu mula-mula menerobos sistem orang lain atau kedalam *web server* dan tahab kedua adalah mengganti halaman *website (web page)*.[10] Antara *hacking* dan *defacing* tidak dapat terpisahkan satu sama lain, karena *defacing* merupakan salah satu kegiatan *hacking* yaitu, kegiatan menerobos program komputer milik orang atau pihak lain tanpa izin. Pada awalnya *hacking* tidak

---

[6] Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cybercrime)*…., hlm. 103.

[7] Dikdik M. Arief Mansur dan Elisatris Gultom, *Cyberlaw Aspek Hukum Teknologi Informasi*, cet. II (Bandung: Refika Aditama, 2009), hlm. 4.

[8] URL singkatan dari *Uniform Resource Locator*, adalah rangkaian karakter menurut suatu format standar tertentu, yang digunakan untuk menunjukkan alamat suatu sumber seperti dokumen dan gambar di Internet. http://id.wikipedia.org/wiki/URL diakses tanggal 4 Maret 2015 pukul 15.00 WIB.

[9] *Website* merupakan kumpulan dari halaman-halaman situs, yang biasanya terangkum dalam sebuah *domain* atau *subdomain*, yang tempatnya berada di dalam *world wide web* (WWW) di internet. Lihat Ujang Rusdianto, *Web CS*, (Yogyakarta; Graha ilmu, 2014), hlm. 74.

[10] Sutan Remi Syahdeini, *Kejahatan dan Tindak Pidana Komputer*, (Jakarta: Pustaka Utama Grafiti, 2009), hlm. 124.

selalu berkonotasi negatif, karena sebenarnya tujuan *hacking* adalah untuk mengetahui sistem keamanan milik orang tertentu dan memberi tahu celahnya. Tetapi dalam perkembanganya di masyarakat *hacking* di nilai dan di anggap kata yang mewakilili sebuah kejahatan dunia maya, dan pada kenyataanya memang *hacking* dilakukan tanpa izin.

Telah banyak kasus *defacing* yang telah terjadi di luar negeri dan dalam negeri, contoh kasus di luar negeri dapat dilihat *defacing* yang dilancarkan oleh Nuker anggota dari *Pakistani hackerz club*. Nuker sering menyerang situs *website* Amerika Serikat, India dan Israel dengan cara mengganti isi situs *website* dengan pesan mengenai pelanggaran-pelanggaran HAM di Kashmir dan Palestina. Misalnya Nuker menulis sebagai berikut:

> *I can't go and and fight for all nations suffering, but I can do something to make the world know about the injustice going around. Defacing a websites will cost nothing to the target….united nations is responsible to solve disputes among different countries.the united states being the "super power" loves to intercept any country in any of their internal affairs, they do use their powers when they see income, but loves to neglect in the same way when it comes to the "real' problems*.[11]

Indonesia juga tak luput dari kegiatan *defacing*, seperti pada tanggal 26 maret 2008 situs Depkominfo telah dibobol. Pembobolan tersebut di duga berkaitan dengan pengesahan RUU tentang Informasi dan Transaksi Elektronik (ITE) sebagai Undang-undang oleh DPR. Sehari sebelumnya yaitu 25 maret 2008. *Defacer* meninggalkan pesan yang berbunyi sebagai berikut:

[11] *Ibid.*, hlm. 126.

> Selamat yeee pemerintah "suit..suit". kami mengucapkan selamat atas disahkanya UU ITE dan rencana pemblokiran situs porno se-Indonesia. Buktikan ini bukan untuk menutupi kebodohan pemerintah cihuyyyyyyyyy.[12]

Contoh lain yang cukup menghebohkan adalah *defacing* yang dilakukan oleh Dani Hermansyah pada tanggal 17 April 2004, pada waktu ini UU ITE belum dibuat dan disahkan. Nama-nama partai diubah dengan nama-nama buah dalam *website* www.kpu.go.id yang mengakibatkan berkurangnya kepercayaan masyarakat terhadap pemilu yang sedang berlangsung pada saat itu.[13] Selain itu, *website* UIN Sunan Kalijaga yang beralamatkan uin-suka.ac.id dibobol *defacer*, Muncul kiriman poster yang menampilkan sebuah gambar hitam putih dan beberapa kalimat pernyataan sampai peringatan yang terpampang di laman *website*. Di sebelah pojok kiri bawah poster terdapat foto kepala manusia misterius.[14] Untuk mengingatkan bahwa sistem keamanan Pusat Teknologi dan Pangkalan Data (PTIPD) milik UIN Sunan Kalijaga tidak terlalu kuat. Terbukti dengan isi kalimatnya *"Knowledge Is Free. We are anonymous. We are legion. We do not forgive. We do not forget. Expect Us"*. [15] Selain

---

[12] *Ibid.*, hlm. 128.

[13] Budi Surhariyanto, *Tindak Pidana Teknologi Informasi (Cybercrime)*, (Jakarta: Raja Grafindo Persada, 2013), hlm. 89.

[14] Kiriman tersebut beralamat di http://uinsuka.ac.id/index.php/page/berita/detail/818/we-are-anonymous

[15] http://lpmarena.com/2014/01/10/website-uin-suka-sempat-kebobolan/ diakses tanggal 1 Mei 2014 pukul 07.01 WIB. Lihat tabel gambar no 1.

itu terdapat pula *defacing* situs resmi mantan presiden SBY,[16] *defacing* pada *website* TV One,[17] *defacing* situs resmi kepolisian yang beralamat http://www.polri.go.id[18] dan lain sebagainya.

Sebagaimana gambaran dan contoh kasus *defacing* di atas maka agar hal tersebut tidak terjadi, diperlukan perangkat hukum yang mengatur hal itu. Oleh karena itu, dengan dibentuknya Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik oleh pemerintah yang disahkan pada tanggal 28 April 2008, diharapkan agar semua kejahatan mayantara dapat terakomodir oleh Undang-undang tersebut, termasuk *defacing* yang telah diatur di dalamnya. Dalam Undang-undang tersebut *defacing* telah diatur pada Pasal 30:

(1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau Sistem Elektronik milik orang lain dengan cara apapun.

(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.

---

[16] Pengertian *deface* dan contoh kasus, www.apriyandis.wordpress.com, diakses tanggal 1 April 2015 pukul 09.30 WIB. Lihat tabel gambar no 2.

[17] *Ibid*., Lihat tabel gambar no 3.

[18] Kronologis *web deface* di Idonesia, www.just1nfo.wordpress.com, diakses tanggal 25 april 2015 pukl 11.00 WIB. Lihat juga tabel gambar no 4.

Pasal di atas dari ayat (1) sampai ayat (3) menerangkan tentang *illegal acces* karena langkah awal *deface* yaitu memasuki sistem orang lain atau melakukan *hacking*. Dan berikutnya *defacing* diatur pada Pasal 32 ayat (1) yang berbunyi:

> (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.

Adapun pasal tersebut di atas menerangkan larangan melakukan modifikasi terhadap suatu *website* atau masuk dalam kategori *data interference* pada bab tentang perbuatan dilarang, seperti yang dijelaskan sebelumnya bahwa *defacing* dilakukan dengan dua tahap, pertama melakukan *hacking* dan selanjutnya memodifikasi *website*.

Terlihat dengan jelas bahwa *defacing* merupakan suatu tindak pidana yang tentunya ada sanksi hukumnya. Adanya Undang-undang dibuat untuk dipatuhi dan dilaksanakan guna memenuhi kebutuhan masyarakat dan mencegah anggota masyarakat untuk berbuat serta bertindak sesuatu yang merugikan orang lain. Salah satu yang merugikan masyarakat adalah kejahatan mayantara dalam hal ini *defacing* tentu menjadi salah satu perbuatan pidana yang terdapat sanksi atau hukuman yang setara dengan perbuatan yang dilakukan sehingga terwujudnya sebuah keadilan.

Islam sebagai sebuah agama hukum tentunya memiliki andil untuk mengapresiasi fenomena yang sedang terjadi di masyarakat. perubahan dan

situasi masyarakat, termasuk akibat buruk yang ditimbulkan dari perkembangan informasi, mengharuskan hukum Islam menjawab dari sekian pokok permasalahan dari perkembangan teknologi informasi, mengingat hukum Islam terus berkembang seiring tempat dan waktu. Islam juga menghormati hak pribadi atau *privacy* seseorang seperti dalam ayat Al-Qura□n berikut ini:

يا ايها الذين أمنوا لا تدخلوا بيو تا غير بيوتكم حتي تستأ نسوا وتسلموا على أهلها ذالكم خيرلكم لعلكم تذكرون [١٩]{} فإن لم تجدوا فيها أحدا فلا تدخلوها حتي يؤذ ن لكم وإن قيل لكم ارجعوا فارجعوا هو أزكى لكم والله بما تعملون عليم[٢٠]

Ayat di atas menjelaskan larangan memasuki rumah tanpa izin, dari hal ini dapat dilihat bahwa pelanggaran terhadap privasi adalah dilarang. Apabila seseorang melanggar perbuatan tersebut maka termasuk perbuatan *jari□mah. Jari□mah* diartikan yaitu larangan-larangan *syara'* yang diancam oleh Allah dengan hukuman *ḥad* (hukuman yang sudah ada *naṣ*nya) atau *ta'zi□r* (hukuman yang tidak ada *naṣ*nya).[21] Mengingat *defacing* merupakan sebuah tindak kejahatan yang baru atau modern, sehingga *defacing* dikategorikan *jari□mah ta'zi□r*. *Defacing* tidak dapat di*qiya□s*kan dengan *jari□mah ḥudu□d* lain, tidak seperti *carding* yang bisa di*qiya□s*kan dengan pencurian, karena *carding* adalah pembobolan kartu kredit. Hukum Islam tersebut mengatur dan menetapkan hukuman bagi seorang yang melanggar. Tujuan

[19] Q.S An-Nu□r (24): 27.

[20] Q.S An-Nu□r (24): 28.

[21] Ahmad Hanafi, A*saz-asas Hukum Pidana Islam*, (Jakarta: Bulan Bintang, 2002), hlm. 121.

dari hukuman itu adalah memberi rasa jera guna menghentikan kejahatan sehingga bisa diciptakan rasa perdamaian dan ketenangan di masyarakat.

Berdasarkan latar belakang yang disampaikan penyusun di atas, menarik minat penyusun untuk mengetahui mengenai kejahatan *cybercrime* yang marak terjadi sekarang yang akibatnya meresahkan dan merugikan banyak pihak. Khususnya mengenai *defacing* yang telah diatur dalam Undang-undang Nomor 11 Tahun 2008 tentang ITE dan dalam Hukum Pidana Islam, kemudian penyusun mencoba menganalisis dalam bentuk karya ilmiah yang di susun dalam skripsi yang berjudul: *Kejahatan Defacing (Perbandingan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (ITE) dan Hukum Pidana Islam.*

B. Rumusan Masalah

Berdasarkan latar belakang permasalahan yang telah diuraikan di atas, maka penyusun perlu untuk membahasnya melalui beberapa hal yang menjadi objek kajian permasalahan dalam penelitian ini, dan mengangkat rumusan permasalahan sebagai berikut :

1. Bagaimana tinjauan Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) mengenai *defacing*?
2. Bagaimana tinjauan hukum pidana Islam mengenai *defacing*?
3. Apa persamaan dan perbedaan Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) dan hukum pidana Islam tentang *defacing* ?

C. Tujuan dan Kegunaan Penelitian

Dari rumusan masalah di atas, maka tulisan ini bertujuan :

1. Untuk menjelaskan tinjauan Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) mengenai *defacing*
2. Untuk menjelaskan tinjauan hukum pidana Islam mengenai *defacing*
3. Untuk menjelaskan persamaan dan perbedaan tinjauan Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) dan hukum pidana Islam mengenai *defacing*

Sedangkan Kegunaanya adalah sebagai berikut :

1. Diharapkan tulisan ini dapat menambah pengetahuan, terutama menyangkut hubungan teknologi informasi dan hukum Islam.

2. Memperluas cakrawala keilmuan bagi perkembangan hukum positif dan hukum Islam.

D. Telaah Pustaka

Pembahasan tentang *defacing* sebenarnya bukanlah hal baru mengingat *defacing* merupakan bagian dari *cybercrime.* Tetapi dalam pembahasan ini lebih fokus membahas tentang pelaku *defacing* dan hukum-hukum yang mengaturnya. Beberapa contoh kajian yang membahas tentang *cybercrime* diantaranya: Sutan Remy Syahdeini dalam bukunya *"Kejahatan dan Tindak Pidana Komputer"* membahas gambaran umum tentang aktifitas *defacing* serta kasus yang pernah terjadi di Negara-negara di dunia. Ia memaparkan internet pada masa kini dan juga sejarah lahirnya internet, selain itu

dipaparkan pula *cybercrime* hubunganya dengan hukum dan kriteria-kriteria kejahatan dunia maya serta membahas Undang-undang pidana komputer di dalam negeri dan di luar negeri termasuk Amerika Serikat, Kanada, Inggris, Australia, Jerman dan lain sebagainya.

Budi Surharianto dalam bukunya *"Tindak Pidana Teknologi Informasi* (*Cybercrime*)*"* membahas *cybercrime* dari aspek hukum positif. Dalam buku ini diuraikan tentang pentingnya pengaturan terhadap kejahatan mayantara dan membahas celah hukum pada Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Buku "*Hukum Pidana di Bidang Teknologi Informasi*" karangan Widodo juga membahas kasus *defacing* dianalisis dengan Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi. Di dalamnya membahas jenis-jenis *cybercrime* yang dijelaskan secara umum, tidak spesifik pada suatu permasalahan atau jenis kejahatan tertentu. Baik buku karangan Sutan Remy Syahdeini, Budi Surharianto dan Widodo hanya dianalisis dengan hukum positif, bahwa hukum Islam belum masuk pembahasan dan tentu akan berbeda dengan yang ditulis penyusun. Selain itu terdapat skripsi yang membahas tentang *cybercrime,* seperti sebagai berikut:

Mochammad Haris Cholil Barro dalam skripsinya *"Cybercrime: Studi Komparasi antara Hukum Pidana Indonesia dan hukum Islam"*.[22] Membahas

[22] Mochammad Haris Collil Barro, *Studi Komparasi antara Hukum Pidana Indonesia dan Hukum Islam*, Skripsi Fakultas Syariah 2007 UIN Sunan Kalijaga, tidak diterbitkan.

kejahatan dunia maya secara umum dengan menggunakan KUHP sebagai acuanya. Di situ diuraikan kriteria *cybercrime* dan hukum yang mengatur dalam hukum positif dijelaskan dan dianalisis dengan KUHP dan diuraikan pula perbandinganya dengan hukum Islam.

Ilham Marwati dalam skripsinya "*Sanksi Pidana bagi Pelaku Pencurian File di Internet Menurut Hukum Positif dan Hukum Islam*".[23] Skripsi ini membahas pengambilan *file* di internet dan dianalisis dengan Undang-undang hak cipta. Di dalamnya dipaparkan pencurian *file* termasuk kejahatan dalam hukum positif dan dalam hukum Islam di*qiya□s*kan dengan *sari□qah* atau pencurian.

Sedangkan Khairil Anam dalam skripsinya yang berjudul, *Hacking (Perspektif Hukum Islam dan Hukum Positif).*[24] Skripsi ini membahas *hacking* secara umum, didalamnya dijelaskan bahwa *hacking* tidak dapat dikategorikan suatu perbuatan pidana, disitu dijelaskan bahwa tujuan *hacking* sebenarnya adalah untuk perbuatan baik yaitu menguji keamanan suatu sistem dan memberi tahu kepada pemilik *website* ataupun yang membuat sistem tersebut.

Skripsi Hidayat Lubis yang berjudul "*Tinjauan Hukum Pidana Islam terhadap Cyberporn pada UU RI No. 11 Tahun 2008 Tentang Informasi dan*

[23] Ilham Marwati, *Sanksi Pidana Bagi Pelaku Pencurian File di Internet Menurut Hukum Positif dan Hukum Islam,* Skripsi Fakultas Syariah 2008 UIN Sunan Kalijaga, tidak diterbitkan.

[24]Khairul Anam, *Hacking (Perspektif Hukum Islam dan Hukum Positif*), Skripsi Fakultas Syariah UIN Sunan Kalijaga, tidak diterbitkan.

Transaksi Elektronik".[25] Di dalamnya diuraikan pandangan hukum Islam tentang kriteria *cyberporn* pada UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Dalam skripsi tersebut tidak menyinggung tentang *defacing*, akan tetapi menjelaskan *cyberporn* merupakan jenis kejahatan kesusilaan pada UU No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Comex Chrisna Wijaya dalam skripsinya yang berjudul *"Kejahatan Carding dalam Perspektif Undang-undang ITE dan Hukum Islam"*. [26] Pada skripsi ini diuraikan *carding* merupakan kejahatan yang termasuk kategori pencurian, yang dianalisis dan diperbandingkan sanksi dalam UU ITE dan hukum Islam. *Defacing* tidak dibahas dalam skripsi ini walaupun ada kesamaan yaitu sama-sama kejahatan dunia maya (*cybercrime*) dan persamaanya yang lain yaitu sama-sama menggunakan Undang-undang ITE dan Hukum pidana Islam sebagai acuanya.

Ada juga skripsi yang ditulis oleh Lailin Nafsiah yang berjudul, "*Cybercrime dalam Perspektif Hukum Pidana Islam"*[27]. Skripsi ini menjelaskan *cybercrime* secara umum dalam kacamata hukum pidana Islam akan tetapi belum spesifik pada macam-macam *cybercrime*. Disini tidak

[25] Lubis Hidayat, *Tinjauan Hukum Pidana Islam terhadap Cyberporn pada UU RI No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik*, Skripsi Fakultas Syariah 2010 UIN Sunan Kalijaga, tidak diterbitkan.

[26] Comex Khrisna Wijaya, *Kejahatan Carding dalam Perspektif Undang-undang ITE dan Hukum Islam*, Skripsi Fakultas Syariah dan Hukum 2010 UIN Sunan Kalijaga, tidak diterbitkan.

[27] Lailin Nafsiah, *Cybercrime dalam Perspektif Hukum Pidana Islam*, Skripsi Fakultas Syariah dan Hukum 2005 UIN Sunan Kalijaga. tidak diterbitkan

membahas secara rinci masing-masing tiap jenis *cybercrime*. Jadi pemahasanya masih umum belum spesifikasi pada suatu tindak kejahatan tertentu.

Dari kajian beberapa skripsi di atas, dapat diketahui bahwa penelitian di atas menjelaskan bahwa *cybercrime* merupakan kejahatan yang melanggar batas wilayah. Semuanya membahas secara keseluruhan atau global tentang tindak pidana *cybercrime*. Dalam skripsi Muhammad Cholil Barro menjabarkan *cybercrime* secara umum. membahas tentang penanggulangan *cybercrime* di Indonesia dengan mengoptimalisasi KUHP. Berbeda yang akan ditulis penyusun yakni *defacing* secara khusus dianalisis dengan UU ITE. Sedang skripsi ilham marwati tidak membahas *defacing* sama sekali, meskipun sama-sama membandingkan hukum positif dan hukum Islam. Khairil Anam menjelaskan pada skripsinya tidak membahas *defacing* secara khusus hanya terbatas pada *hacking* pada pengertian secara umum. Comex membatasi permasalahan mengenai kasus *carding* yaitu mengenai kasus pencurian kartu kredit secara *online*, dari penjelasan di atas maka pembahasan dalam skripsi ini sangat berbeda dengan skripsi-skripsi sebelumnya karena dalam penelitian ini akan membahas secara lebih khusus dan mendetail mengenai tindak pidana *defacing*, yaitu pengubahan dokumen elektronik yang berkaitan dengan Undang-undang tentang Informasi dan Transaksi elektronik yang akan ditinjau dalam perspektif Fiqih Jinayah.

E. Kerangka Teoretik

Pemahaman terhadap kejahatan dunia mayantara tidak selalu mudah, namun masih bisa dilakukan semua orang sepanjang didukung oleh kemampuan yang memadahi dalam melakukan abstraksi dan analisis. Mengingat *cybercrime* merupakan kejahatan berteknologi tinggi dan terjadi dalam dimensi *virtual* yang menyerang pada objek-objek yang tidak dapat disentuh secara fisik. Karena *cybercrime* merupakan tindakan kejahatan, maka para pelakunya akan dikenakan sanksi berupa hukuman sebagai reaksi bagi yang melanggar hukum, dan peraturan hukum itu tidak bertentangan dengan asas-asas keadilan di masyarakat.[28]

Suatu hukum yang menghendaki adanya kebenaran di dalam masyarakat, orang yang bersalah harus dihukum sesuai dengan peraturan yang berlaku. Keberhasilan suatu aturan hukum dalam masyarakat akan dicapai apabila diimplementasikan menurut prinsip dan tujuan hukum itu sendiri, yaitu terciptanya keadilan. Selain itu upaya untuk melaksanakan hukum pidana yang sesuai dengan peraturan yang telah ada merupakan hal yang penting untuk mengurangi kejahatan dan untuk menjalin terciptanya keamanan untuk merealisasikan keseimbangan hak dan kewajiban manusia serta kemaslahatan semua manusia.

[28] C.S.T Kansil, *Pengantar Ilmu Hukum dan Hukum Indonesia*, (Jakarta: Balai Pustaka, 1984), hlm. 80.

Untuk menunjukkan alasan apakah yang dapat dipakai sebagai tolak ukur untuk membenarkan penghukuman terdapat beberapa jenis teori hukuman *(Starf theorien),* yang ada garis besarnya dapat dibagi menjadi tiga teori:[29]

1. Teori Relatif atau tujuan (*doeltheorien*)

   Teori relatif atau teori tujuan, berpokok pangkal pada dasar bahwa pidana adalah alat untuk menegakkan tata tertib (hukum) dalam masyarakat. Teori ini berbeda dengan teori absolut, dasar pemikiran agar kejahatan dapat dijatuhi hukuman artinya penjatuhan pidana mempunyai tujuan tertentu, misalnya memperbaiki sikap mental atau membuat pelaku tidak berbahaya lagi, dibutuhkan pembinaan sikap mental. Teori relatif ini berasas pada tiga tujuan utama pemidanaan yaitu *preventive, deterrence,* dan *reformative.*

2. Teori Absolut atau teori pembalasan (*vergeldingstheorien*)

   Menurut teori ini pidana dijatuhkan semata-mata karena orang telah melakukan kejahatan atau tindak pidana. Teori absolut didasarkan pada pemikiran bahwa pidana tidak bertujuan praktis, seperti memperbaiki penjahat tetapi pidana merupakan tuntutan mutlak, bukan hanya sesuatu perlu dijatuhkan keharusan, dengan kata lain hakikat pidana adalah pembalasan (*revegen*).

3. Teori Gabungan (*verenigingsthrorien*)

   Teori gabungan atau teori modern memandang bahwa tujuan pemidanaan bersifat plural, karena mengggabungkan antara prinsip-prinsip

[29] Wiryono Prodjodikoro, *Azaz-azaz Hukum Pidana*, (Bandung: Eresko), hlm. 21-24.

relatif dan absolut sebagai suatu kesatuan. Teori ini bercorak ganda, di mana pemidanaan mengandung karakter pembalasan sejauh pemidanaan dilihatsebagai kritik moral dalam menjawab tindakan yang salah. Sedangkan karakter tujuanya terletak pada ide bahwa tujuan kritik moral tersebut ialah reformasi atau perubahan perilaku terpidana di kemudian hari.

Di dalam Hukum Pidana Islam mengatur klasifikasi tindak pidana *(Jari□mah)* dilihat dari berat dan ringanya hukumanya. berikut adalah macam-macam *jari□mah*:[30]

1. *Jari□mah Ḥudu□d* merupakan tindakan yang sanksinya berasal dari Allah secara langsung, karena dirasa telah dijelaskan hukumannya secara definitif dalam Al-Qura□n, serta permasalah disini dirasa sangat vital bagi kehidupan pribadi maupun kolektif. Jumhur ulama' merumuskan *jari□mah ḥudu□d* ada 7 :
   a. Zina
   b. *Qozaf* (tuduhan palsu zina)
   c. *Sari□qoh* (pencurian)
   d. *Ḥira□bah* (perampokan)
   e. *Riddah* (murtad)
   f. *Al-baghy* (pemberontakan)
   g. *Syurb al-khamr* (meminum khamr)s

[30] Makhrus Munajat, *Hukum Pidana Islam (Fiqih Jinayat)*, (Yogyakarta: Pesantren Nawasea Press, 2010), hlm. 105.

2. *Jari□mah Qiṣa□ṣ Diya□t* Yaitu kejahatan terhadap jiwa (membunuh) dan anggota badan (pelukaan) yang diancam dengan hukuman *Qiṣa□ṣ Diya□t* (serupa) atau *diya□t* (ganti rugi pelaku kepada pihak korban). Dalam hukum pidana Islam yang termasuk *qiṣa□ṣ diya□t* adalah 1) pembunuhan dengan sengaja 2) pembunuhan semi sengaja 3) menyebabkan kematian orang karena kealpaan atau kesalahan 4) penganiayaan dengan sengaja dan 5) menyebabkan orang luka karena kealpaan atau kesalahan.[31]
3. *Jari□mah Ta'zi□r,* Secara bahasa *ta'zi□r* berarti mencegah dan menolak. *Ta'zi□r* dimaksudkan untuk member efek jera pada pelaku supaya tidak mengulangi perbuatannya. Wahbah Zuhaili menjelaskan, yang dimaksud *ta'zi□r* adalah hukuman yang ditetapkan atas perbuatan maksiat atau jinayah yang tidak dikarenakan *ḥad* dan *kafarat*. [32] Abdul Qadir Awdah sebagaimana juga dikutip oleh Makhrus Munajat, menyatakan bahwa *jari□mah ta'zi□r* menjadi tiga (3) bagian yaitu:
   a. *Jari□mah ḥudu□d* dan *qiṣa□ṣ diyat* yang mengandung unsur subhat atau tidak memenuhi syarat, namun hal itu sudah dianggap sebagai perbuatan maksiat, seperti *wạti'*, subhat, pencurian harta *syirkah*, pembunuhan ayah terhadap anaknya, pencurian yang bukan harta benda.

[31] *Ibid.*, hlm. 135.

[32] *Ibid.*, hlm. 145.

b. *Jari□mah ta'zi□r* yang jenis *jarima□hnya* ditentukan oleh *naṣ*, tetapi sanksinya oleh syar'i diserahkan kepada penguasa, seperti sumpah palsu, saksi palsu, mengurangi timbangan, menipu, mengingkari janji, menghianati amanat, dan menghina agama.

c. *Jari□mah ta'zi□r* yang *jarima□h* dan jenis sanksinya secara penuh menjadi wewenang penguasa demi terealisasinya kemaslahatan umat. Dalam hal ini unsur akhlak menjadi pertimbangan yang paling utama. Misalnya pelanggaran terhadap peraturan lingkungan hidup, lalu lintas, dan pelanggaran terhadap pemerintah lainnya.[33]

Suatu perbuatan dikatakan *jari□mah* dan diberikan sanksi apabila telah memenuhi unsur-unsur. Unsur-unsur ini ada yang umum dan ada yang khusus. Unsur umum berlaku untuk semua *jari□mah*, sedangkan unsur khusus hanya berlaku untuk masing-masing *jari□mah* dan berbeda antara *jari□mah* satu dengan yang lain. Menurut Abdul Qadir Audah yang dikutip Makhrus Munajat mengemukakan bahwa unsur-unsur umum untuk *jari□mah* itu ada tiga macam yaitu:

a. Unsur formal, yaitu adanya *naṣ* atau ketentuan yang menunjukkan sebagai *jari□mah.*

b. Unsur materiil, yaitu adanya perbuatan melawan hukum yang benar-benar dilakukan.

[33] Makhrus Munajat, *Reaktualisasi Pemikiran Hukum Pidana Islam*, (Yogyakarta: Cakrawala, 2006), hlm. 13.

c. Unsur moril, yaitu niat pelaku untuk berbuat jarimah. Unsur ini menyangkut tanggung jawab pidana yang anya dikenakan atas orang yang telah *balig*, sehat akal, dan *ikhtiyar* (kebebasan berbuat).[34]

Sedangkan unsur-unsur khusus yaitu :

a. Unsur niat
b. Permulaan pelakasanaan
c. Tidak selesainya perbuatan karena kehendaknya sendiri

Unsur-unsur tersebut di atas harus terdapat pada sesuatu perbuatan untuk digolongkan dalam *jari□mah* dan dapat dijatuhi hukuman. fuqoha' biasanya tidak terpengaruh dan tidak memilah kedua unsur tersebut, dalam pembahasan para fuqoha' mempersamakan kedua unsur di atas.

F. Metode Penelitian

1. Jenis Penelitian

Jenis penelitian yang digunakan dalam penyusunan skripsi ini adalah penelitian kepustakaan (*Library Research*). *Library Research* digunakan untuk mendapatkan dokumen-dokumen atau karya tulis yang relevan dengan pokok pembahasan atau objek penelitian.[35]

[34] *Ibid.*

[35] Winarno Surakhmad, *Pengantar Penelitian Ilmiah: Dasar, Metode dan Tekni*k, (Bandung: Tarsito, 1990), hlm. 191.

2. Sifat Penelitian

Sifat penelitian ini adalah *deskriptif* [36]*-analitik-comparatif,* yaitu memaparkan beberapa pokok pikiran dari undang-undang ITE dan fiqih jinayat tentang *defacing* secara fokus, kemudian membandingakan keduanya.

3. Pendekatan Penelitian

Metode pendekatan yang digunakan dalam penelitian ini adalah yuridis dan normatif yaitu mendekati masalah *defacing* dari segi hukum yang terdapat dalam Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Hukum Pidana Islam.

4. Metode Pengumpulan Data

Untuk Mencari kebenaran dari sebuah laporan ilmiah, maka studi yang akan dilakukan penulis dalam pengumpulan data adalah dengan metode dokumenter yakni mencari data mengenai hal-hal berupa catatan, transkrip, buku, surat kabar, majalah, notulen, agenda dan sebagainya. Sehingga sering disamakan dengan studi literatur atau studi kepustakaan (*library research*).[37] Contoh buku *Cyberspace, Cybercrime, Cyberlaw Tinjauan Aspek Hukum Pidana* karangan Josua Sitompul, buku *Tindak Pidana Teknologi Informasi Urgensi Pengaturan dan Celah Hukumnya*

[36] Lexy J. Moleong, *Metode Penelitian Kualitatif,* (Bandung: Remaja Rosda Karya, 2000), hlm. 6

[37] *Ibid.*, hlm. 170.

karangan Budi Surharianto, Buku *Kejahatan dan Tindak Pidana Komputer* karangan Sutan Reimy Syahdeini, Buku *Hukum Pidana Islam di Indonesia* karangan Makhrus Munajat dan lan-lain.

Untuk mengumpulkan data yang diperlukan, akan dilakukan penelusuran kepustakaan baik dari sumber primer maupun sumber sekunder. Adapun sumber primer yakni sumber asli yang memuat informasi atau data tersebut. sedangkan sumber sekunder adalah data yang diperoleh dari sumber bukan asli yang memuat informasi atau data tersebut.[38] Penelusuran terhadap data primer akan dilakukan terhadap literatur yang berkaitan dengan aktifitas *defacing* dan hukum yang mengakomodirnya. sumber primer diantaranya, Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, buku-buku yang berkaitan dengan *cybercrime* dan Fiqih Jinayah. sedangkan sumber sekunder adalah literatur yang menunjang hukum primer tersebut yang diperoleh dari buku, majalah, internet dan lain sebagainya.

5. Metode Analisis data

Data yang dikumpulkan dari penelitian ini akan dianalisis secara komparatif yaitu mendekati masalah ini dengan membandingkan perspektif hukum positif Indonesia dan hukum Islam menggunakan analisis kualitatif, yaitu dengan menganalisis data tanpa menggunakan angka-angka melainkan dengan sumber informasi yang relevan untuk memperlengkap data penyusun. sedang berfikir yang digunakan untuk

[38] *Ibid.*, hlm. 133.

menganalisis data tersebut dengan induktif, yaitu berangkat dari fakta-fakta khusus yaitu kasus yang pernah terjadi kemudian hal tersebut ditarik generalisasinya yaitu ditarik ke ranah hukum yang sifatnya umum dan diperbandingkan.

G. Sistematika Pembahasan

Untuk memudahkan pembahasan dan pemahaman dalam penyusunan skripsi ini, maka disusun dalam sistematika yang terdiri dari lima bab, pada bab pertama memuat pendahuluan berisi latar belakang masalah dari bahasan skripsi, dari latar belakang masalah tersebut dapat ditarik rumusan masalah. Dijelaskan juga tujuan dan kegunaan yang mencangkup tentang kepastian manfaat dari hasil penelitian ini. Kemudian telaah pustaka yakni menelaah karya-karya ilmiah yang berkaitan dengan penelitian ini. sedangkan kerangka teoretik yakni sebagai dasar acuan yang ditempuh dalam skripsi ini. Dan metode penelitian ini masuk jenis penelitian kepustakaan *(library research).*

Bab kedua, menguraikan tinjauan umum tentang *defacing*, meliputi definisi *defacing* yang merupakan salah satu kejahatan mayantara *(cybercrime)* lebih spesifiknya *defacing* merupakan bagian dari *hactivism* dan termasuk kategori *illegal acces*. Dan juga membahas jenis-jenis *defacing* dan tinjauan umum kejahatan dalam hukum positif dan hukumIslam.

Bab ketiga, membahas kejahatan *defacing* dalam Undang-undang Nomor 11 tahun 2008 tentang informasi dan transaksi elektronik yaitu menyangkut

pasal-pasal yang berkaitan dengan larangan *defacing*. Dan di dalam Fiqih Jinayah dipaparkan kategori *defacing*.

Bab keempat, analisis hukum membahas tentang persamaan dan perbedaan kejahatan *defacing* perspektif Undang-undang Nomor 11 Tahun 2008 tentang informasi dan transaksi elektronik dan Fiqih Jinayah. Unsur-unsur tindak pidana dan sanksi merupakan yang akan dianalisis dan kemudian diperbandingkan.

Bab kelima, sebagai bab terakhir dalam skripsi ini merupakan penutup. berisi kesimpulan secara singkat tentang pembahasan skripsi ini, sekaligus menjawab rumusan masalah dan saran-saran yang berkaitan dengan pembahasan ini. Kemudian disertakan daftar pustaka dan lampiran dari penelitian ini.

BAB V

PENUTUP

A. KESIMPULAN

Dalam bab penutup ini akan ditarik sebuah kesimpulan yang merupakan jawaban dari pokok permasalahan yang menjadi fokus studi penelitian dalam rangka skripsi ini. Kesimpulan disesuaikan dengan urutan rumusan masalah yang diajukan pada pendahuluan yaitu tentang tinjaan UU ITE dan hukum pidana Islam mengenai *defacing* dan persamaan dan perbedaan *defacing* menurut UU ITE dan Hukum Pidana Islam.

1. *Defacing* menurut UU ITE merupakan perbuatan dilarang yang telah diatur pada Pasal 30 dalam hal *illegal acces* dan pada Pasal 32 ayat (1) dalam hal *data interference* mengingat langkah awal dalam *defacing* adalah melakukan *hacking* kemudian memodifikasi dari *website* tersebut.
2. *Defacing* yang merupakan salah satu bentuk *cybercrime* di dalam hukum Islam masuk ranah *jari□mah ta'zi□r*, bukan termasuk *jari□mah qiṣa□ṣ* dan *ḥudu□d*. Sebab bisa dipastikan di zaman Rasulallah SAW belum diketemukan teknologi komputer dan internet seperti saat ini. Maka tidak ada ayat dan hadis yang menyebutkan secara eksplisit eksistensi kejahatan dunia maya.
3. Persamaan *Defacing* antara UU ITE dan Hukum Pidana Islam yaitu, Undang-undang Nomor 11 Tahun 2008 dan hukum pidana Islam masing-

masing mengenal pemidanaan kawalan/kurungan sebagai sanksi dari tindak pidana yang dilakukan, yang secara garis besar memiliki tujuan yang sama yaitu sebagai upaya preventif, represif, reformatif dan memberikan efek jera terhadap pelaku tindak pidana, serta memberikan rasa aman nyaman dan tenteram di dalam masyarat. Sedangkan perbedaanya adalah pada kriteria umur yang dapat dimintai pertanggungjawaban pidana pada subjek hukum atau pelaku *defacing* adalah enam belas tahun pada hukum pidana Indonesia dan *balig* pada hukum Islam. Dasar hukum dalam hukum pidana Indonesia untuk *defacing* sudah diatur dalam Undang-undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik pada Pasal 30 dan Pasal 32 ayat (1), sedangkan dalam hukum pidana Islam tidak ada *naṣ* yang mengatur secara khusus mengenai *defacing* karena merupakan bentuk kejahatan dan tindak pidana yang modern seperti sekarang ini. Sanksi hukum *defacing* di Indonesia sudah jelas diatur pada Pasal 46 dan Pasal 48 ayat (1) UU ITE, sedangkan dalam hukum Islam sanksi *defacing* belum ditentukan kadarnya, artinya diserahkan sepenuhnya kepadal *ulil amri* atau hakim. hakim diberi keleluasaan untuk menetapkan atau memutuskan seberapa lama sanksi pidana penjara itu diberikan kepada si pelaku, akan tetapi berpedoman pada kemashlahatan umat. Sedangkan dalam pidana Indonesia seorang hakim memberi sanksi pidana penjara harus sesuai dengan ketentuan Undang-undang yang berlaku.

B. SARAN/REKOMENDASI

Berdasarkan pelitian di atas, secara umum Undang-undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik sudah cukup mengakomodir ketentuan yang belum ada pada Undang-undang sebelumnya seperti KUHP, KUHAP, Undang-undang tentang telekomunikasi dan sebagainya. Namun, ada beberapa hal sebagai bahan evaluasi dan saran, antara lain:

1. Bagi Pengguna internet

   Hendaknya pengguna internet mematuhi norma dan etika di dunia maya dan tidak melanggar Undang-undang yang berlaku karena jika melanggar Undang-undang maka dapat dikategorikan sebagai tindak kejahatan yang terdapat sanksi hukum bagi yang melanggar.

2. Bagi Pemerintah

   a. Hendaknya pemerintah menyempurnakan lagi UU ITE karena masih ada yang terlewatkan dalam UU ITE tersebut seperti *spamming*. Dan perlu di evaluasi lagi pasal 27 UU ITE tentang pencemaran nama baik karena banyak yang menjadi korban atas pasal ini, atau banyak disalahgunakan oleh atasan kepada bawahan dan oleh pemerintah kepada rakyat.

   b. Hendaknya pemerintah meningkatkan sistem pengamanan jaringan komputer nasional dan meningkatkan pemahaman serta keahlian aparatur negara mengenai upaya pencegahan, investigasi dan

penuntutan perkara-perkara yang berhubungan dengan kejahatan mayantara.

c. Hendaknya pemerintah meningkatkan kesadaran warga negara mengenai kejahatan dunia maya serta pentingnya mencegah kejahatan tersebut dan meningkatkan kerjasama antarnegara dalam upaya penanganan kejahatan mayantara.

DAFTAR PUSTAKA

Al-Qura□n

Departemen Agama RI, *Al-Qura□n dan terjemahanya*

Fiqh dan Ushul Fiqh

Az-Zuhaili, Wahbah, (Terj) *Fiqih Islam Wa Adillatuhu*, Cet. X, Jakarta: Gema Insani, 2007

Asjmuni, A. Rahman, *Qaidah-qaidah Fiqhiyah*, Jakarta: Bulan Bintang, 1967

Irfan, M. Nurul dan Masyrofah, *Fiqih Jinayat*, cet. I, Jakarta: Amzah, 2013

Jazuli, Ahmad, *Hukum Pidana Islam*, cet. II, Jakarta: Raja Grafindo Persada, 1997

Munajat, Makhrus, *Hukum Pidana Islam (Fiqih Jinayat)*, Yogyakarta: Pesantren Nawasea Press, 2010

----------, *Hukum Pidana Islam di Indonesia*, cet. I, Yogyakarta: Suka Press, 2008

----------, *Reaktualisasi Pemikiran Hukum Pidana Islam*, Yogyakarta: Cakrawala, 2006

Muslich, Ahmad Wardi, *Hukum Pidana Islam*, cet. II, Jakarta: Sinar Grafika, 2005

----------, *Pengantar dan Asas Hukum Pidana Islam*, Cet. II, Jakarta: Sinar Grafika, 2006

Hasan, Mustofa dan Saebani, Beni Ahmad, *Hukum Pidana Islam Fiqh Jinayah*, Bandung: Pustaka Setia, 2013

Sabiq, Sayyid, (terj) *Fiqih Sunnah X*, Bandung: Al-Ma'arif, 1997

Buku Umum

Amirin, M.Tatang , *Menyusun Rencana Penelitian Ilmiah*, cet. III, Jakarta: Raja Grafindo Persada, 1995

Chazawi, Adami, *Pelajaran Hukum Pidana Bagian I*, Jakarta: Raja Grafindo Persada, 2001

Darmawan, Deni dan Permana, Deden Hendra, *Desain dan Pemrograman Website*, Bandung: Remaja Rosdakarya, 2013

Hanafi, Ahmad, A*sas-asas Hukum Pidana Islam*, Jakarta: Bulan Bintang, 2002

Hidayat, Bunadi, *Pemidanaan Anak di Bawah Umur*, Cet. II, Bandung: Alumni, 2014

Indrajit, Richardus Eko, *Konsep dan Strategi Kemanan Informasi di Dunia Cyber*, Yogyakarta: Graha ilmu, 2014

Kansil, C.S.T, *Pengantar Ilmu Hukum dan Hukum Indonesia*, Jakarta: Balai Pustaka, 1984

Mansur, Dikdik M. Arief dan Gultom, Elesatris, *Cyberlaw Aspek Hukum Teknologi Informasi*, Bandung: Refika Aditama, 2009

Moeljatno, *Asas-asas Hukum Pidana*, Cet-VI, Yogyakarta: Rineka Cipta, 2000

Moleong, Lexy J, *Metode Penelitian Kualitatif*, Bandung: Remaja Rosda Karya, 2000

Nasrullah, Rulli, *Teori dan Riset Media Siber*, Jakarta: Kencana, 2014

Prodjodikoro, Wiryono, *Azaz-azaz Hukum Pidana*, Bandung : Eresko,t.t

Riswandi, Budi Agus ,*Hukum Internet di Indonesia*, Yogyakarta: UII Press, 2003

Rusdianto, Ujang, *Web CS*, Yogyakarta: Graha ilmu, 2014

Sholehuudin, *Sistem Sanksi dalam Hukum Pidana*, Cet. II, Jakarta: Raja Grafindo Persada, 2004

Simanjutak, Usman, *Teknik Penuntutan dan Upaya Hukum*, Jakarta: Bina Cipta, 1994

Sitompul, Josua, *Cyberspace, Cybercrime, Cyberlaw Tinjauan Aspek Hukum Pidana*, Jakarta: Tata Nusa, 2012

Suharto, *Hukum Pidana Materiil Unsur-unsur Obyektif sebagai Dakwaan*, Jakarta: Sinar Grafika, 2002

Sulistyo, Faizin, *Hukum Pidana dalam Perspektif*, Denpasar: Pustaka Larasan, 2012

Sunarso, Siswanto, *Hukum Informasi dan Transaksi Elektronik Studi Kasus Prita Mulyasari*, Jakarta: Rineka Cipta, 2009

Surakhmad, Winarno, *Pengantar Penelitian Ilmiah: Dasar, Metode dan Tekni*k, Bandung: Tarsito, 1990

Surhariyanto, Budi, *Tindak Pidana Teknologi Informasi Urgensi Pengaturan dan Celah Hukumnya*, Jakarta: Raja Grafindo Persada, 2013

Syahdeini, Sutan Remi, *Kejahatan dan Tindak Pidana Komputer*, Jakarta: Pustaka Utama Grafiti, 2009

Tahir, Achmad, *Cybercrime (Akar Masalah, Solusi, dan Penanggulanganya)*, Yogyakarta: Suka Press, 2011

Tresna, R, *Azas-azas Hukum Pidana*, cet-III, Jakarta: Tiara, 1990

Wahid, Abdul dan Labib, Mohammad, *Kejahatan Mayantara (Cybercrime)*, Jakarta: Refika Aditama, 2005

Widodo, Aspek *Hukum Pidana Kejahatan Mayantara*, Yogyakarta: Aswaja pressindo, 2013

----------, *Hukum Pidana di Bidang Teknologi Informasi*, Yogyakarta: Aswaja pressindo, 2013

----------, *Memerangi Cybercrime Karakteristik Motivasi dan Strategi Penangananya dalam Perspektif Kriminologi*, Yogyakarta: Aswaja Pressindo, 2013

Undang-undang

KUHP

Undang-undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik

Undang-undang Nomor 6 tahun 19999 tentang Telekomunikasi

Lain-lain

http://germy-x-forty.blogspot.com

http://id.wikipedia.org

http://lpmarena.com

http://profesiti.blogspot.com

https://apriyandis.wordpress.com

https://just1nfo.wordpress.com

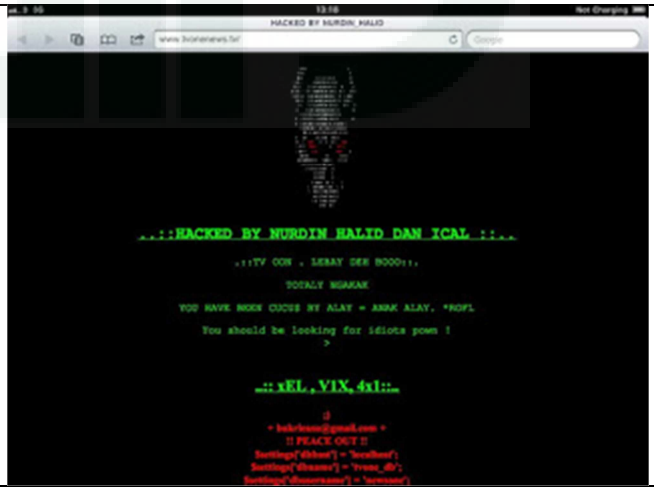
Lampiran I

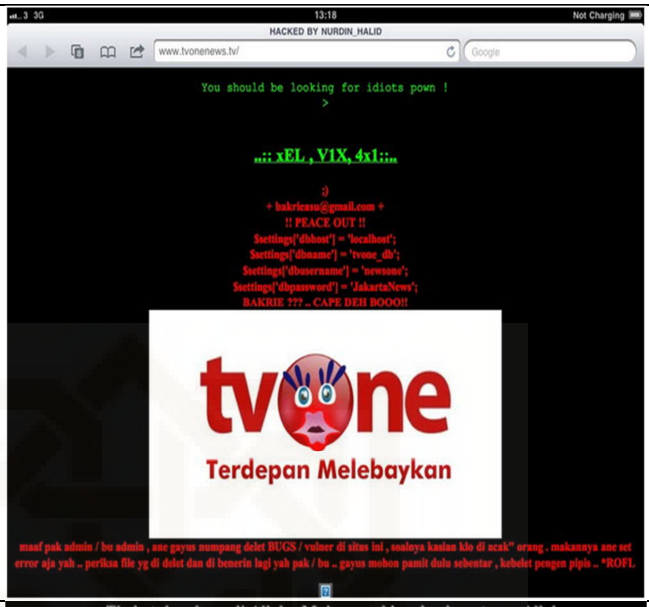
DAFTAR TERJEMAHAN AL-QURA□N

No	Hlm	Fn	Terjemahan
			BAB I
1	**7**	**15**	Hai orang-orang yang beriman, janganlah kamu memasuki rumah yang bukan rumahmu sebelum meminta izin dan memberi salam kepada penghuninya. yang demikian itu lebih baik bagimu, agar kamu (selalu) ingat
2	**7**	**16**	Jika kamu tidak menemui seorangpun didalamnya, Maka janganlah kamu masuk sebelum kamu mendapat izin. dan jika dikatakan kepadamu: Kembali (saja)lah, Maka hendaklah kamu kembali. itu bersih bagimu dan Allah Maha mengetahui apa yang kamu kerjakan

Lampiran II

TABEL GAMBAR

No	Hlm	Fn	GAMBAR
			BAB I
1	5	15	
2	6	16	
3	6	17	

			 HACKED BY NURDIN_HALID www.tvonenews.tv/ You should be looking for idiots pown ! >..:: xEL , V1X, 4x1::.. :) + bakrieasu@gmail.com + !! PEACE OUT !! $settings['dbhost'] = 'localhost'; $settings['dbname'] = 'tvone_db'; $settings['dbusername'] = 'newsone'; $settings['dbpassword'] = 'JakartaNews'; BAKRIE ??? .. CAPE DEH BOOO!! tvone Terdepan Melebaykan maaf pak admin / bu admin , ane gayus numpang delet BUGS / vulner di situs ini , soalnya kasian klo di acak" orang . makannya ane set error aja yah .. periksa file yg di delet dan di benerin lagi yah pak / bu .. gayus mohon pamit dulu sebentar , kebelet pengen pipis .. *ROFL
4	**6**	**18**	 Tiada tuhan kecuali Allah - Muhammad hamba dan utusan Allah Bangkitlah singa-singa Islam! memperingati hari nakba mengingat apa yang telah mereka perbuat kepada kaum Muslimin di negeri kaum Muslimin mengingatkan untuk tidak lupa mendo'akan Mujahidin di manapun berada (Allahu A'lam) harus tetap sadar akan upaya pembusukan Islam & Jihad yang dilakukan intelejen dan pejuang-pejuang anti Syari'ah Islam kami tidak memiliki keterkaitan dengan kelompok manapun, menggunakan media ini untuk mendukung Mujahidin dan menyampaikan pesa Bangkitlah singa-singa Islam!

Lampiran III

SEBAB-SEBAB WEB DAPAT DI*DEFACE*
Sumber: profesiti.blogspot.com

1	Internal	Kesalahan konfigurasi	
		Kelalaian admin	1) *Install file* dan *folder, Webmaster* atau *admi*n biasanya lalai dalam menghapus *file* yang digunakan untuk mengintallasi web model CMS. Contoh: *folder /install* dan *file install.php* pada *phpnuke, postnuke, phpbb.* 2) *File konfigurasi* dan *permission, Webmaster* atau *admin* lupa mengatur permisi pada *file-file* konfigurasi yang penting, yang menyangkut administrasi dan konfigurasi *file*, khususnya *file-file* yang mencatat *password*, baik *password database* dan sebagainya. Contoh: *file config.txt, config.php, config.inc.* 3) *Run of date,* Terlalu lama peng*updet*an suatu web atau tidak secara terus-terusan meng*update* webnya khususnya portal yang dibundel dalam CMS, serta juga *packet-packet* yang terinstalasi di mesin baik itu web server sendiri, *database server* dan sebagainya yang bisa menjadi pintu masuk bagi *defacer*. 4) *Run of service,* Kesalahan konfigurasi terhadap *services*/layanan yang diberikan khususnya terlalu banyak menjalankan layanan yang tidak diperlukan pada setiap *server*. 5) *Cannot keep secret,* Berkaitan dengan *social engineering*, maka kepercayaan adalah hal terpenting, *trust no body* mungkin pilihan yang sangat masuk akal dalam menanggulangi hal ini. Pribadi dan mental seorang webmaster atau *admin* sangat menentukan. 6) Kurang hati-hati saat login ke mesin, *Sniffing* yang dilakukan dari jaringan lokal sangat berkemungkinan untuk

			mendapatkan password yang di pakai oleh *root*, *admin*, *webmaster* dan sebagainya.
2	Eksternal	*Sofware vulnerabilities*	
		Sistem *vulnerabilities*	
		Run of control	1) *Brute forcing* yaitu, jenis serangan yang dilakukan dengan melakukan berbagai bentuk kombinasi karakter yang akan di cobakan sebagai *password* detil soal BFA (*Brute Force Attack*). Metode ini mungkin yang paling lama, tetapi tetap dipakai dikarenakan kelebihannya yaitu tidak perlu mengetahui sistem enkripsi, atau metoda pengamanan khususnya untuk *login*. tetapi memiliki berbagai keterbatasan tersendiri, baik dalam hal kecepatan khususnya. Contoh: penggunaan *brutus* sebagai program yang cukup cepat untuk mem*brute password* baik, *ftp, http, smtp* dan sebagainya. 2) *Dictionarry attack,* Metode ini menggunakan kamus kata yang sering di gunakan, walau tetap memiliki prinsip yang sama dengan *Brute forcing*. target serangan ini adalah *password*, atau bisa dikatakan *attack* terhadap *authentication.* 3) *DOS attack* atau *Denial of Service* adalah aktifitas menghambat kerja sebuah layanan (*servis*) atau mematikannya, sehingga *user* yang berkepentingan tidak dapat menggunakan layanan tersebut. 4) *Sniffing,* merupakan kegiatan

			menyadap atau menginfeksi paket data menggunakan *sniffer software* atau *hardware* di internet. Biasanya di gunakan *ettercap*, *ethereal*, dan sebagainya.

Lampiran IV

CARA KERJA DAN JENIS-JENIS *DEFACING*

Sumber: http://germy-x-forty.blogspot.com

1	***IP Spoofing***, juga dikenal sebagai *Source Address Spoofing*, yaitu pemalsuan alamat IP *attacker* sehingga sasaran menganggap alamat IP *attacker* adalah alamat IP dari *host* di dalam *network* bukan dari luar *network*. Misalkan *attacker* mempunyai *IP address type* A 66.25.xx.xx ketika *attacker* melakukan serangan jenis ini maka *network* yang diserang akan menganggap *IP attacker* adalah bagian dari jaringanya misal 192.xx.xx.xx yaitu *IP type C*. *IP Spoofing* terjadi ketika seorang *attacker* mengakali *packet routing* untuk mengubah arah dari data atau transmisi ke tujuan yang berbeda. *Packet* untuk *routing* biasanya di transmisikan secara transparan dan jelas sehingga membuat *attacker* dengan mudah untuk memodifikasi asal data ataupun tujuan dari data. Teknik ini bukan hanya dipakai oleh *attacker* tetapi juga dipakai oleh para *security* profesional untuk men*tracing* identitas dari para *attacker*.
	FTP Attack, Salah satu serangan yang dilakukan terhadap *File Transfer Protocol* (FTP) adalah serangan *buffer overflow* yang diakibatkan oleh *malformed command*. Tujuan menyerang FTP *server* ini rata-rata adalah untuk mendapatkan *command shell* ataupun untuk melakukan *Denial Of Service*. Serangan *Denial Of Service* akhirnya dapat menyebabkan seorang *user* atau *attacker* untuk mengambil *resource* di dalam *network* tanpa adanya autorisasi, sedangkan *command shell* dapat membuat seorang *attacker* mendapatkan akses ke sistem *server* dan *file-file* data yang akhirnya seorang *attacker* bisa membuat anonymous *root-acces* yang mempunyai hak penuh terhadap sistem bahkan *network* yang diserang.
3	***Unix Finger Exploits***.Pada masa awal internet, *Unix OS finger utility* digunakan secara efisien untuk mengirim informasi diantara pengguna. Karena permintaan informasi terhadap informasi *finger* ini tidak menyalahkan peraturan, kebanyakan *system Administrator* meninggalkan *utility* ini (*finger*) dengan keamanan yang sangat minim, bahkan tanpa kemanan sama sekali. Bagi seorang *attacker utility* ini sangat berharga untuk melakukan informasi tentang *footprinting*, termasuk nama *login* dan *informasi contact*. *Utility* ini juga menyediakan keterangan yang sangat baik tentang aktivitas *user* di dalam sistem, berapa lama *user* berada dalam sistem dan seberapa jauh *user* merawat sistem. Informasi yang dihasilkan dari *finger* ini dapat meminimalisasi usaha *cracker* dalam menembus sebuah sistem. Keterangan pribadi tentang *use*r yang dimunculkan oleh *finger daemo*n ini sudah cukup bagi seorang *attacker* untuk melakukan *social engineering* dengan menggunakan sosial skillnya untuk memanfaatkan *user* agar memberitahu *password* dan kode akses terhadap sistem.

4	***Flooding & Broadcastin,***Seorang *attacker* bisa mengurangi kecepatan *network* dan *host-host* yang berada di dalamnya secara *significant* dengan cara terus melakukan *request*/permintaan terhadap suatu informasi dari *server* yang bisa menangani serangan klasik *Denial Of Service* (DoS), mengirim *request* ke satu *port* secara berlebihan dinamakan *flooding*, kadang hal ini juga disebut *spraying*. Tujuan dari kedua serangan ini adalah sama yaitu membuat *network resource* yang Menyediakan informasi menjadi lemah dan akhirnya menyerah. Serangan dengan cara *Flooding* bergantung kepada dua faktor yaitu: ukuran dan/atau volume (*size and/or volume*). Seorang *attacker* dapat menyebabkan *Denial Of Service* dengan cara melempar *file* berkapasitas besar atau volume yang besar dari paket yang kecil kepada sebuah sistem. Dalam keadaan seperti itu *network server* akan menghadapi kemacetan: terlalu banyak informasi yang diminta dan tidak cukup *power* untuk mendorong data agar berjalan. Pada dasarnya paket yang besar membutuhkan kapasitas proses yang besar pula, tetapi secara tidak normal paket yang kecil dan sama dalam *volume* yang besar akan menghabiskan *resource* secara percuma, dan mengakibatkan kemacetan.
5	***Fragmented Packet Attacks.***Data-data internet yang di transmisikan melalui TCP/IP bisa dibagi lagi ke dalam paket-paket yang hanya mengandung paket pertama yang isinya berupa informasi bagian utama (*header*/ kepala) dari TCP. Beberapa *firewall* akan mengizinkan untuk memproses bagian dari paket-paket yang tidak mengandung informasi alamat asal pada paket pertamanya, hal ini akan mengakibatkan beberapa tipe sistem menjadi *crash*. Contohnya, *server NT* akan menjadi *crash* jika paket-paket yang dipecah (*fragmented packet*) cukup untuk menulis ulang informasi paket pertama dari suatu *protocol*.
6	***E-mail Exploits,*** Pengekploitasian *e-mail* terjadi dalam lima bentuk yaitu: *mail floods*, manipulasi perintah (*command manipulation*), serangan tingkat transportasi (*transport level attack*), memasukkan berbagai macam kode (*malicious code inserting*) dan *social engineering* (memanfaatkan sosialisasi secara fisik). Penyerangan *email* bisa membuat sistem menjadi *crash*, membuka dan menulis ulang bahkan mengeksekusi *file-file* aplikasi atau juga membuat akses ke fungsi-fungsi perintah (*command function*).
7	***DNS and BIND Vulnerabilities***, Berita baru-baru ini tentang kerawanan (*vulnerabilities*) tentang aplikasi *Barkeley Internet Name Domain* (BIND) dalam berbagai versi mengilustrasikan kerapuhan dari *Domain Name System* (DNS), yaitu krisis yang diarahkan pada operasi dasar dari Internet (*basic internet operatio*n).
8	***Password Attacks,*** *Password* merupakan sesuatu yang umum jika kita bicara tentang keamanan. Kadang seorang *user* tidak perduli dengan nomor pin yang mereka miliki, seperti bertransaksi *online* di warnet,

	bahkan bertransaksi *online* dirumah pun sangat berbahaya jika tidak dilengkapi dengan *software security* seperti SSL dan PGP. *Password* adalah salah satu prosedur kemanan yang sangat sulit untuk diserang, seorang *attacker* mungkin saja mempunyai banyak *tools* (secara teknik maupun dalam kehidupan sosial) hanya untuk membuka sesuatu yang dilindungi oleh *password*. Ketika seorang *attacker* berhasil mendapatkan *password* yang dimiliki oleh seorang *user*, maka ia akan mempunyai kekuasaan yang sama dengan *user* tersebut. Melatih karyawan/*user* agar tetap waspada dalam menjaga *password*nya dari *social engineering* setidaknya dapat meminimalisir risiko, selain berjaga-jaga dari praktek *social enginering* organisasi pun harus mewaspadai hal ini dengan cara teknikal. Kebanyakan serangan yang dilakukan terhadap *password* adalah menebak *(guessing), brute force, cracking* dan *sniffing*.
9	***Proxy Server Attacks,*** Salah satu fungsi *Proxy server* adalah untuk mempercepat waktu response dengan cara menyatukan proses dari beberapa *host* dalam suatu *trusted network.*
10	***Remote Command Processing Attacks,*** *Trusted Relationship* antara dua atau lebih *host* menyediakan fasilitas pertukaran informasi dan *resource sharing*. Sama halnya dengan *proxy server, trusted relationship* memberikan kepada semua anggota *network* kekuasaan akses yang sama di satu dan lain sistem (dalam *network*). *Attacker* akan menyerang *server* yang merupakan anggota dari *trusted system*. Sama seperti kerawanan pada *proxy server*, ketika akses diterima, seorang *attacke*r akan mempunyai kemampuan mengeksekusi perintah dan mengkases data yang tersedia bagi *user* lainnya.
11	***Remote File System Attack.*** Protokol-protokol untuk tranportasi data (tulang punggung dari internet) adalah tingkat TCP (TCP Level) yang mempunyai kemampuan dengan mekanisme untuk baca/tulis (*read/write*) Antara *network* dan *host*. *Attacker* bisa dengan mudah mendapatkan jejak informasi dari mekanisme ini untuk mendapatkan akses ke direktori *file*.
12	***Selective Program Insertions,*** *Selective Program Insertions* adalah serangan yang dilakukan ketika *attacker* menaruh program-program penghancur, seperti virus, *worm* dan *trojan* pada sistem sasaran. Program-program penghancur ini sering juga disebut *malware*. Program-program ini mempunyai kemampuan untuk merusak sistem, pemusnahan *file*, pencurian *password* sampai dengan membuka *backdoor*.
13	***Port Scanning,*** Melalui *port scanning* seorang *attacker* bisa melihat fungsi dan cara bertahan sebuah sistem dari berbagai macam *por*t. Seorang *attacke*r bisa mendapatkan akses kedalam sistem melalui port yang tidak dilindungi. Sebagai contoh, *scaning* bisa digunakan untuk menentukan dimana *default SNMP string* di buka untuk publik, yang artinya informasi

	bisa di *extract* untuk digunakan dalam *remote command attack*.
14	***TCP/IP Sequence Stealing, Passive Port Listening and Packet,*** *Interception TCP/IP Sequence Stealing, Passive Port Listening dan Packet Interception* berjalan untuk mengumpulkan informasi yang sensitif untuk mengkases *network*. Tidak seperti serangan aktif maupun *brute-force*, serangan yang menggunakan metode ini mempunyai lebih banyak kualitas *stealth-like.*
15	***HTTPD Attacks***, Kerawanan yang terdapat dalam HTTPD ataupun *webserver* ada lima macam: *buffer overflows, httpd bypasses, cross scripting, web code vulnerabilities, dan URL floods.*

Lampiran V

UNDANG-UNDANG REPUBLIK INDONESIA

NOMOR 11 TAHUN 2008

TENTANG

INFORMASI DAN TRANSAKSI ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

PRESIDEN REPUBLIK INDONESIA,

Menimbang :

a. bahwa pembangunan nasional adalah suatu proses yang berkelanjutan yang harus senantiasa tanggap terhadap berbagai dinamika yang terjadi di masyarakat;

b. bahwa globalisasi informasi telah menempatkan Indonesia sebagai bagian dari masyarakat informasi dunia sehingga mengharuskan dibentuknya pengaturan mengenai pengelolaan Informasi dan Transaksi Elektronik di tingkat nasional sehingga pembangunan Teknologi Informasi dapat dilakukan secara optimal, merata, dan menyebar ke seluruh lapisan masyarakat guna mencerdaskan kehidupan bangsa;

c. bahwa perkembangan dan kemajuan Teknologi Informasi yang demikian pesat telah menyebabkan perubahan kegiatan kehidupan manusia dalam berbagai bidang yang secara langsung telah memengaruhi lahirnya bentuk-bentuk perbuatan hukum baru;

d. bahwa penggunaan dan pemanfaatan Teknologi Informasi harus terus dikembangkan untuk menjaga, memelihara, dan memperkukuh persatuan dan kesatuan nasional berdasarkan Peraturan Perundang-undangan demi kepentingan nasional;

e. bahwa pemanfaatan Teknologi Informasi berperan penting dalam perdagangan dan pertumbuhan perekonomian nasional untuk mewujudkan kesejahteraan masyarakat;

f. bahwa pemerintah perlu mendukung pengembangan Teknologi Informasi melalui infrastruktur hukum dan pengaturannya sehingga pemanfaatan Teknologi Informasi dilakukan secara aman untuk mencegah penyalahgunaannya dengan memperhatikan nilai-nilai agama dan sosial budaya masyarakat Indonesia;

g. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, huruf c, huruf d, huruf e, dan huruf f, perlu membentuk Undang-Undang tentang Informasi dan Transaksi Elektronik;

Mengingat :. . .

Mengingat : Pasal 5 ayat (1) dan Pasal 20 Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;

Dengan Persetujuan Bersama

DEWAN PERWAKILAN RAKYAT REPUBLIK INDONESIA

dan

PRESIDEN REPUBLIK INDONESIA

MEMUTUSKAN:

Menetapkan: UNDANG-UNDANG TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK.

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Undang-Undang ini yang dimaksud dengan:

1. Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi 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.
2. Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan Komputer, jaringan Komputer, dan/atau media elektronik lainnya.
3. Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi.
4. Dokumen Elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, 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 atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

5. Sistem . . .

5. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.
6. Penyelenggaraan Sistem Elektronik adalah pemanfaatan Sistem Elektronik oleh penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat.
7. Jaringan Sistem Elektronik adalah terhubungnya dua Sistem Elektronik atau lebih, yang bersifat tertutup ataupun terbuka.
8. Agen Elektronik adalah perangkat dari suatu Sistem Elektronik yang dibuat untuk melakukan suatu tindakan terhadap suatu Informasi Elektronik tertentu secara otomatis yang diselenggarakan oleh Orang.
9. Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat Tanda Tangan Elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam Transaksi Elektronik yang dikeluarkan oleh Penyelenggara Sertifikasi Elektronik.
10. Penyelenggara Sertifikasi Elektronik adalah badan hukum yang berfungsi sebagai pihak yang layak dipercaya, yang memberikan dan mengaudit Sertifikat Elektronik.
11. Lembaga Sertifikasi Keandalan adalah lembaga independen yang dibentuk oleh profesional yang diakui, disahkan, dan diawasi oleh Pemerintah dengan kewenangan mengaudit dan mengeluarkan sertifikat keandalan dalam Transaksi Elektronik.
12. Tanda Tangan Elektronik adalah tanda tangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.
13. Penanda Tangan adalah subjek hukum yang terasosiasikan atau terkait dengan Tanda Tangan Elektronik.
14. Komputer adalah alat untuk memproses data elektronik, magnetik, optik, atau sistem yang melaksanakan fungsi logika, aritmatika, dan penyimpanan.
15. Akses adalah kegiatan melakukan interaksi dengan Sistem Elektronik yang berdiri sendiri atau dalam jaringan.
16. Kode Akses adalah angka, huruf, simbol, karakter lainnya atau kombinasi di antaranya, yang merupakan kunci untuk dapat mengakses Komputer dan/atau Sistem Elektronik lainnya.

17. Kontrak . . .

17. Kontrak Elektronik adalah perjanjian para pihak yang dibuat melalui Sistem Elektronik.
18. Pengirim adalah subjek hukum yang mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik.
19. Penerima adalah subjek hukum yang menerima Informasi Elektronik dan/atau Dokumen Elektronik dari Pengirim.
20. Nama Domain adalah alamat internet penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat, yang dapat digunakan dalam berkomunikasi melalui internet, yang berupa kode atau susunan karakter yang bersifat unik untuk menunjukkan lokasi tertentu dalam internet.
21. Orang adalah orang perseorangan, baik warga negara Indonesia, warga negara asing, maupun badan hukum.
22. Badan Usaha adalah perusahaan perseorangan atau perusahaan persekutuan, baik yang berbadan hukum maupun yang tidak berbadan hukum.
23. Pemerintah adalah Menteri atau pejabat lainnya yang ditunjuk oleh Presiden.

Pasal 2

Undang-Undang ini berlaku untuk setiap Orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-Undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia.

BAB II

ASAS DAN TUJUAN

Pasal 3

Pemanfaatan Teknologi Informasi dan Transaksi Elektronik dilaksanakan berdasarkan asas kepastian hukum, manfaat, kehati-hatian, iktikad baik, dan kebebasan memilih teknologi atau netral teknologi.

Pasal 4

Pemanfaatan Teknologi Informasi dan Transaksi Elektronik dilaksanakan dengan tujuan untuk:

a. mencerdaskan kehidupan bangsa sebagai bagian dari masyarakat informasi dunia;
b. mengembangkan perdagangan dan perekonomian nasional dalam rangka meningkatkan kesejahteraan masyarakat;
c. meningkatkan efektivitas dan efisiensi pelayanan publik;
d. membuka kesempatan seluas-luasnya kepada setiap Orang untuk memajukan pemikiran dan kemampuan di bidang penggunaan dan pemanfaatan Teknologi Informasi seoptimal mungkin dan bertanggung jawab; dan
e. memberikan rasa aman, keadilan, dan kepastian hukum bagi pengguna dan penyelenggara Teknologi Informasi.

BAB III

INFORMASI, DOKUMEN, DAN TANDA TANGAN ELEKTRONIK

Pasal 5

(1) Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.
(2) Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia.
(3) Informasi Elektronik dan/atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik sesuai dengan ketentuan yang diatur dalam Undang-Undang ini.
(4) Ketentuan mengenai Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud pada ayat (1) tidak berlaku untuk:
    a. surat yang menurut Undang-Undang harus dibuat dalam bentuk tertulis; dan
    b. surat beserta dokumennya yang menurut Undang-Undang harus dibuat dalam bentuk akta notaril atau akta yang dibuat oleh pejabat pembuat akta.

Pasal 6

Pasal 6 . . .

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

Pasal 7

Setiap Orang yang menyatakan hak, memperkuat hak yang telah ada, atau menolak hak Orang lain berdasarkan adanya Informasi Elektronik dan/atau Dokumen Elektronik harus memastikan bahwa Informasi Elektronik dan/atau Dokumen Elektronik yang ada padanya berasal dari Sistem Elektronik yang memenuhi syarat berdasarkan Peraturan Perundang-undangan.

Pasal 8

(1) Kecuali diperjanjikan lain, waktu pengiriman suatu Informasi Elektronik dan/atau Dokumen Elektronik ditentukan pada saat Informasi Elektronik dan/atau Dokumen Elektronik telah dikirim dengan alamat yang benar oleh Pengirim ke suatu Sistem Elektronik yang ditunjuk atau dipergunakan Penerima dan telah memasuki Sistem Elektronik yang berada di luar kendali Pengirim.

(2) Kecuali diperjanjikan lain, waktu penerimaan suatu Informasi Elektronik dan/atau Dokumen Elektronik ditentukan pada saat Informasi Elektronik dan/atau Dokumen Elektronik memasuki Sistem Elektronik di bawah kendali Penerima yang berhak.

(3) Dalam hal Penerima telah menunjuk suatu Sistem Elektronik tertentu untuk menerima Informasi Elektronik, penerimaan terjadi pada saat Informasi Elektronik dan/atau Dokumen Elektronik memasuki Sistem Elektronik yang ditunjuk.

(4) Dalam hal terdapat dua atau lebih sistem informasi yang digunakan dalam pengiriman atau penerimaan Informasi Elektronik dan/atau Dokumen Elektronik, maka:

a. waktu pengiriman adalah ketika Informasi Elektronik dan/atau Dokumen Elektronik memasuki sistem informasi pertama yang berada di luar kendali Pengirim;

b. waktu . . .

b. waktu penerimaan adalah ketika Informasi Elektronik dan/atau Dokumen Elektronik memasuki sistem informasi terakhir yang berada di bawah kendali Penerima.

Pasal 9

Pelaku usaha yang menawarkan produk melalui Sistem Elektronik harus menyediakan informasi yang lengkap dan benar berkaitan dengan syarat kontrak, produsen, dan produk yang ditawarkan.

Pasal 10

(1) Setiap pelaku usaha yang menyelenggarakan Transaksi Elektronik dapat disertifikasi oleh Lembaga Sertifikasi Keandalan.

(2) Ketentuan mengenai pembentukan Lembaga Sertifikasi Keandalan sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah.

Pasal 11

(1) Tanda Tangan Elektronik memiliki kekuatan hukum dan akibat hukum yang sah selama memenuhi persyaratan sebagai berikut:

a. data pembuatan Tanda Tangan Elektronik terkait hanya kepada Penanda Tangan;
b. data pembuatan Tanda Tangan Elektronik pada saat proses penandatanganan elektronik hanya berada dalam kuasa Penanda Tangan;
c. segala perubahan terhadap Tanda Tangan Elektronik yang terjadi setelah waktu penandatanganan dapat diketahui;
d. segala perubahan terhadap Informasi Elektronik yang terkait dengan Tanda Tangan Elektronik tersebut setelah waktu penandatanganan dapat diketahui;
e. terdapat cara tertentu yang dipakai untuk mengidentifikasi siapa Penandatangannya; dan
f. terdapat cara tertentu untuk menunjukkan bahwa Penanda Tangan telah memberikan persetujuan terhadap Informasi Elektronik yang terkait.

(2) Ketentuan . . .

(2) Ketentuan lebih lanjut tentang Tanda Tangan Elektronik sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah.

Pasal 12

(1) Setiap Orang yang terlibat dalam Tanda Tangan Elektronik berkewajiban memberikan pengamanan atas Tanda Tangan Elektronik yang digunakannya.

(2) Pengamanan Tanda Tangan Elektronik sebagaimana dimaksud pada ayat (1) sekurang-kurangnya meliputi:

a. sistem tidak dapat diakses oleh Orang lain yang tidak berhak;

b. Penanda Tangan harus menerapkan prinsip kehati-hatian untuk menghindari penggunaan secara tidak sah terhadap data terkait pembuatan Tanda Tangan Elektronik;

c. Penanda Tangan harus tanpa menunda-nunda, menggunakan cara yang dianjurkan oleh penyelenggara Tanda Tangan Elektronik ataupun cara lain yang layak dan sepatutnya harus segera memberitahukan kepada seseorang yang oleh Penanda Tangan dianggap memercayai Tanda Tangan Elektronik atau kepada pihak pendukung layanan Tanda Tangan Elektronik jika:

1. Penanda Tangan mengetahui bahwa data pembuatan Tanda Tangan Elektronik telah dibobol; atau

2. keadaan yang diketahui oleh Penanda Tangan dapat menimbulkan risiko yang berarti, kemungkinan akibat bobolnya data pembuatan Tanda Tangan Elektronik; dan

d. dalam hal Sertifikat Elektronik digunakan untuk mendukung Tanda Tangan Elektronik, Penanda Tangan harus memastikan kebenaran dan keutuhan semua informasi yang terkait dengan Sertifikat Elektronik tersebut.

(3) Setiap Orang yang melakukan pelanggaran ketentuan sebagaimana dimaksud pada ayat (1), bertanggung jawab atas segala kerugian dan konsekuensi hukum yang timbul.

BAB IV

PENYELENGGARAAN SERTIFIKASI ELEKTRONIK DAN SISTEM ELEKTRONIK

Bagian Kesatu

Penyelenggaraan Sertifikasi Elektronik

Pasal 13

(1) Setiap Orang berhak menggunakan jasa Penyelenggara Sertifikasi Elektronik untuk pembuatan Tanda Tangan Elektronik.

(2) Penyelenggara Sertifikasi Elektronik harus memastikan keterkaitan suatu Tanda Tangan Elektronik dengan pemiliknya.

(3) Penyelenggara Sertifikasi Elektronik terdiri atas:

a. Penyelenggara Sertifikasi Elektronik Indonesia; dan

b. Penyelenggara Sertifikasi Elektronik asing.

(4) Penyelenggara Sertifikasi Elektronik Indonesia berbadan hukum Indonesia dan berdomisili di Indonesia.

(5) Penyelenggara Sertifikasi Elektronik asing yang beroperasi di Indonesia harus terdaftar di Indonesia.

(6) Ketentuan lebih lanjut mengenai Penyelenggara Sertifikasi Elektronik sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.

Pasal 14

Penyelenggara Sertifikasi Elektronik sebagaimana dimaksud dalam Pasal 13 ayat (1) sampai dengan ayat (5) harus menyediakan informasi yang akurat, jelas, dan pasti kepada setiap pengguna jasa, yang meliputi:

a. metode yang digunakan untuk mengidentifikasi Penanda Tangan;

b. hal yang dapat digunakan untuk mengetahui data diri pembuat Tanda Tangan Elektronik; dan

c. hal yang dapat digunakan untuk menunjukkan keberlakuan dan keamanan Tanda Tangan Elektronik.

Bagian Kedua . . .

Bagian Kedua

Penyelenggaraan Sistem Elektronik

Pasal 15

(1) Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya.

(2) Penyelenggara Sistem Elektronik bertanggung jawab terhadap Penyelenggaraan Sistem Elektroniknya.

(3) Ketentuan sebagaimana dimaksud pada ayat (2) tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik.

Pasal 16

(1) Sepanjang tidak ditentukan lain oleh undang-undang tersendiri, setiap Penyelenggara Sistem Elektronik wajib mengoperasikan Sistem Elektronik yang memenuhi persyaratan minimum sebagai berikut:

a. dapat menampilkan kembali Informasi Elektronik dan/ atau Dokumen Elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan Peraturan Perundang-undangan;

b. dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan Informasi Elektronik dalam Penyelenggaraan Sistem Elektronik tersebut;

c. dapat beroperasi sesuai dengan prosedur atau petunjuk dalam Penyelenggaraan Sistem Elektronik tersebut;

d. dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan Penyelenggaraan Sistem Elektronik tersebut; dan

e. memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk.

(2) Ketentuan lebih lanjut tentang Penyelenggaraan Sistem Elektronik sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah.

BAB V

TRANSAKSI ELEKTRONIK

Pasal 17

(1) Penyelenggaraan Transaksi Elektronik dapat dilakukan dalam lingkup publik ataupun privat.
(2) Para pihak yang melakukan Transaksi Elektronik sebagaimana dimaksud pada ayat (1) wajib beriktikad baik dalam melakukan interaksi dan/atau pertukaran Informasi Elektronik dan/atau Dokumen Elektronik selama transaksi berlangsung.
(3) Ketentuan lebih lanjut mengenai penyelenggaraan Transaksi Elektronik sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah.

Pasal 18

(1) Transaksi Elektronik yang dituangkan ke dalam Kontrak Elektronik mengikat para pihak.
(2) Para pihak memiliki kewenangan untuk memilih hukum yang berlaku bagi Transaksi Elektronik internasional yang dibuatnya.
(3) Jika para pihak tidak melakukan pilihan hukum dalam Transaksi Elektronik internasional, hukum yang berlaku didasarkan pada asas Hukum Perdata Internasional.
(4) Para pihak memiliki kewenangan untuk menetapkan forum pengadilan, arbitrase, atau lembaga penyelesaian sengketa alternatif lainnya yang berwenang menangani sengketa yang mungkin timbul dari Transaksi Elektronik internasional yang dibuatnya.
(5) Jika para pihak tidak melakukan pilihan forum sebagaimana dimaksud pada ayat (4), penetapan kewenangan pengadilan, arbitrase, atau lembaga penyelesaian sengketa alternatif lainnya yang berwenang menangani sengketa yang mungkin timbul dari transaksi tersebut, didasarkan pada asas Hukum Perdata Internasional.

Pasal 19

Para pihak yang melakukan Transaksi Elektronik harus menggunakan Sistem Elektronik yang disepakati.

Pasal 20 . . .

Pasal 20

(1) Kecuali ditentukan lain oleh para pihak, Transaksi Elektronik terjadi pada saat penawaran transaksi yang dikirim Pengirim telah diterima dan disetujui Penerima.

(2) Persetujuan atas penawaran Transaksi Elektronik sebagaimana dimaksud pada ayat (1) harus dilakukan dengan pernyataan penerimaan secara elektronik.

Pasal 21

(1) Pengirim atau Penerima dapat melakukan Transaksi Elektronik sendiri, melalui pihak yang dikuasakan olehnya, atau melalui Agen Elektronik.

(2) Pihak yang bertanggung jawab atas segala akibat hukum dalam pelaksanaan Transaksi Elektronik sebagaimana dimaksud pada ayat (1) diatur sebagai berikut:

a. jika dilakukan sendiri, segala akibat hukum dalam pelaksanaan Transaksi Elektronik menjadi tanggung jawab para pihak yang bertransaksi;

b. jika dilakukan melalui pemberian kuasa, segala akibat hukum dalam pelaksanaan Transaksi Elektronik menjadi tanggung jawab pemberi kuasa; atau

c. jika dilakukan melalui Agen Elektronik, segala akibat hukum dalam pelaksanaan Transaksi Elektronik menjadi tanggung jawab penyelenggara Agen Elektronik.

(3) Jika kerugian Transaksi Elektronik disebabkan gagal beroperasinya Agen Elektronik akibat tindakan pihak ketiga secara langsung terhadap Sistem Elektronik, segala akibat hukum menjadi tanggung jawab penyelenggara Agen Elektronik.

(4) Jika kerugian Transaksi Elektronik disebabkan gagal beroperasinya Agen Elektronik akibat kelalaian pihak pengguna jasa layanan, segala akibat hukum menjadi tanggung jawab pengguna jasa layanan.

(5) Ketentuan sebagaimana dimaksud pada ayat (2) tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik.

Pasal 22 . . .

Pasal 22

(1) Penyelenggara Agen Elektronik tertentu harus menyediakan fitur pada Agen Elektronik yang dioperasikannya yang memungkinkan penggunanya melakukan perubahan informasi yang masih dalam proses transaksi.

(2) Ketentuan lebih lanjut mengenai penyelenggara Agen Elektronik tertentu sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah.

BAB VI

NAMA DOMAIN, HAK KEKAYAAN INTELEKTUAL,

DAN PERLINDUNGAN HAK PRIBADI

Pasal 23

(1) Setiap penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat berhak memiliki Nama Domain berdasarkan prinsip pendaftar pertama.

(2) Pemilikan dan penggunaan Nama Domain sebagaimana dimaksud pada ayat (1) harus didasarkan pada iktikad baik, tidak melanggar prinsip persaingan usaha secara sehat, dan tidak melanggar hak Orang lain.

(3) Setiap penyelenggara negara, Orang, Badan Usaha, atau masyarakat yang dirugikan karena penggunaan Nama Domain secara tanpa hak oleh Orang lain, berhak mengajukan gugatan pembatalan Nama Domain dimaksud.

Pasal 24

(1) Pengelola Nama Domain adalah Pemerintah dan/atau masyarakat.

(2) Dalam hal terjadi perselisihan pengelolaan Nama Domain oleh masyarakat, Pemerintah berhak mengambil alih sementara pengelolaan Nama Domain yang diperselisihkan.

(3) Pengelola Nama Domain yang berada di luar wilayah Indonesia dan Nama Domain yang diregistrasinya diakui keberadaannya sepanjang tidak bertentangan dengan Peraturan Perundang-undangan.

(4) Ketentuan lebih lanjut mengenai pengelolaan Nama Domain sebagaimana dimaksud pada ayat (1), ayat (2), dan ayat (3) diatur dengan Peraturan Pemerintah.

Pasal 25 . . .

Pasal 25

Informasi Elektronik dan/atau Dokumen Elektronik yang disusun menjadi karya intelektual, situs internet, dan karya intelektual yang ada di dalamnya dilindungi sebagai Hak Kekayaan Intelektual berdasarkan ketentuan Peraturan Perundang-undangan.

Pasal 26

(1) Kecuali ditentukan lain oleh Peraturan Perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan.

(2) Setiap Orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini.

BAB VII

PERBUATAN YANG DILARANG

Pasal 27

(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.

(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.

(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.

(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.

Pasal 28 . . .

Pasal 28

(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).

Pasal 29

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.

Pasal 30

(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.

Pasal 31

(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 . . .

(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.

(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.

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

Pasal 32

(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.

Pasal 33

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.

Pasal 34 . . .

Pasal 34

(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.

(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.

Pasal 35

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.

Pasal 36

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.

Pasal 37

Setiap Orang dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada di wilayah yurisdiksi Indonesia.

BAB VIII

PENYELESAIAN SENGKETA

Pasal 38

(1) Setiap Orang dapat mengajukan gugatan terhadap pihak yang menyelenggarakan Sistem Elektronik dan/atau menggunakan Teknologi Informasi yang menimbulkan kerugian.

(2) Masyarakat dapat mengajukan gugatan secara perwakilan terhadap pihak yang menyelenggarakan Sistem Elektronik dan/atau menggunakan Teknologi Informasi yang berakibat merugikan masyarakat, sesuai dengan ketentuan Peraturan Perundang-undangan.

Pasal 39

(1) Gugatan perdata dilakukan sesuai dengan ketentuan Peraturan Perundang-undangan.

(2) Selain penyelesaian gugatan perdata sebagaimana dimaksud pada ayat (1), para pihak dapat menyelesaikan sengketa melalui arbitrase, atau lembaga penyelesaian sengketa alternatif lainnya sesuai dengan ketentuan Peraturan Perundang-undangan.

BAB IX

PERAN PEMERINTAH DAN PERAN MASYARAKAT

Pasal 40

(1) Pemerintah memfasilitasi pemanfaatan Teknologi Informasi dan Transaksi Elektronik sesuai dengan ketentuan Peraturan Perundang-undangan.

(2) Pemerintah melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik yang mengganggu ketertiban umum, sesuai dengan ketentuan Peraturan Perundang-undangan.

(3) Pemerintah menetapkan instansi atau institusi yang memiliki data elektronik strategis yang wajib dilindungi.

(4) Instansi atau institusi sebagaimana dimaksud pada ayat (3) harus membuat Dokumen Elektronik dan rekam cadang elektroniknya serta menghubungkannya ke pusat data tertentu untuk kepentingan pengamanan data.

(5) Instansi . . .

(5) Instansi atau institusi lain selain diatur pada ayat (3) membuat Dokumen Elektronik dan rekam cadang elektroniknya sesuai dengan keperluan perlindungan data yang dimilikinya.

(6) Ketentuan lebih lanjut mengenai peran Pemerintah sebagaimana dimaksud pada ayat (1), ayat (2), dan ayat (3) diatur dengan Peraturan Pemerintah.

Pasal 41

(1) Masyarakat dapat berperan meningkatkan pemanfaatan Teknologi Informasi melalui penggunaan dan Penyelenggaraan Sistem Elektronik dan Transaksi Elektronik sesuai dengan ketentuan Undang-Undang ini.

(2) Peran masyarakat sebagaimana dimaksud pada ayat (1) dapat diselenggarakan melalui lembaga yang dibentuk oleh masyarakat.

(3) Lembaga sebagaimana dimaksud pada ayat (2) dapat memiliki fungsi konsultasi dan mediasi.

BAB X

PENYIDIKAN

Pasal 42

Penyidikan terhadap tindak pidana sebagaimana dimaksud dalam Undang-Undang ini, dilakukan berdasarkan ketentuan dalam Hukum Acara Pidana dan ketentuan dalam Undang-Undang ini.

Pasal 43

(1) Selain Penyidik Pejabat Polisi Negara Republik Indonesia, Pejabat Pegawai Negeri Sipil tertentu di lingkungan Pemerintah yang lingkup tugas dan tanggung jawabnya di bidang Teknologi Informasi dan Transaksi Elektronik diberi wewenang khusus sebagai penyidik sebagaimana dimaksud dalam Undang-Undang tentang Hukum Acara Pidana untuk melakukan penyidikan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik.

(2) Penyidikan . . .

(2) Penyidikan di bidang Teknologi Informasi dan Transaksi Elektronik sebagaimana dimaksud pada ayat (1) dilakukan dengan memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran layanan publik, integritas data, atau keutuhan data sesuai dengan ketentuan Peraturan Perundang-undangan.

(3) Penggeledahan dan/atau penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan atas izin ketua pengadilan negeri setempat.

(4) Dalam melakukan penggeledahan dan/atau penyitaan sebagaimana dimaksud pada ayat (3), penyidik wajib menjaga terpeliharanya kepentingan pelayanan umum.

(5) Penyidik Pegawai Negeri Sipil sebagaimana dimaksud pada ayat (1) berwenang:

a. menerima laporan atau pengaduan dari seseorang tentang adanya tindak pidana berdasarkan ketentuan Undang-Undang ini;

b. memanggil setiap Orang atau pihak lainnya untuk didengar dan/atau diperiksa sebagai tersangka atau saksi sehubungan dengan adanya dugaan tindak pidana di bidang terkait dengan ketentuan Undang-Undang ini;

c. melakukan pemeriksaan atas kebenaran laporan atau keterangan berkenaan dengan tindak pidana berdasarkan ketentuan Undang-Undang ini;

d. melakukan pemeriksaan terhadap Orang dan/atau Badan Usaha yang patut diduga melakukan tindak pidana berdasarkan Undang-Undang ini;

e. melakukan pemeriksaan terhadap alat dan/atau sarana yang berkaitan dengan kegiatan Teknologi Informasi yang diduga digunakan untuk melakukan tindak pidana berdasarkan Undang-Undang ini;

f. melakukan penggeledahan terhadap tempat tertentu yang diduga digunakan sebagai tempat untuk melakukan tindak pidana berdasarkan ketentuan Undang-Undang ini;

g. melakukan penyegelan dan penyitaan terhadap alat dan atau sarana kegiatan Teknologi Informasi yang diduga digunakan secara menyimpang dari ketentuan Peraturan Perundang-undangan;

h. meminta . . .

h. meminta bantuan ahli yang diperlukan dalam penyidikan terhadap tindak pidana berdasarkan Undang-Undang ini; dan/atau

i. mengadakan penghentian penyidikan tindak pidana berdasarkan Undang-Undang ini sesuai dengan ketentuan hukum acara pidana yang berlaku.

(6) 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.

(7) Penyidik Pegawai Negeri Sipil sebagaimana dimaksud pada ayat (1) berkoordinasi dengan Penyidik Pejabat Polisi Negara Republik Indonesia memberitahukan dimulainya penyidikan dan menyampaikan hasilnya kepada penuntut umum.

(8) Dalam rangka mengungkap tindak pidana Informasi Elektronik dan Transaksi Elektronik, penyidik dapat berkerja sama dengan penyidik negara lain untuk berbagi informasi dan alat bukti.

Pasal 44

Alat bukti penyidikan, penuntutan dan pemeriksaan di sidang pengadilan menurut ketentuan Undang-Undang ini adalah sebagai berikut:

a. alat bukti sebagaimana dimaksud dalam ketentuan Perundang-undangan; dan

b. alat bukti lain berupa Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud dalam Pasal 1 angka 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3).

BAB XI

KETENTUAN PIDANA

Pasal 45

(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 Rp1.000.000.000,00 (satu miliar rupiah).

(2) Setiap . . .

(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 Rp1.000.000.000,00 (satu miliar rupiah).

(3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 29 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah).

Pasal 46

(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 banyak Rp600.000.000,00 (enam ratus juta rupiah).

(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 Rp700.000.000,00 (tujuh ratus juta rupiah).

(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 Rp800.000.000,00 (delapan ratus juta rupiah).

Pasal 47

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 Rp800.000.000,00 (delapan ratus juta rupiah).

Pasal 48

(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 Rp2.000.000.000,00 (dua miliar rupiah).

(2) Setiap . . .

(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 Rp3.000.000.000,00 (tiga miliar rupiah).

(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 Rp5.000.000.000,00 (lima miliar rupiah).

Pasal 49

Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 33, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).

Pasal 50

Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 34 ayat (1) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).

Pasal 51

(1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah).

(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 Rp12.000.000.000,00 (dua belas miliar rupiah).

Pasal 52

(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.

(2) Dalam . . .

(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.

(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 dua pertiga.

(4) Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga.

BAB XII

KETENTUAN PERALIHAN

Pasal 53

Pada saat berlakunya Undang-Undang ini, semua Peraturan Perundang-undangan dan kelembagaan yang berhubungan dengan pemanfaatan Teknologi Informasi yang tidak bertentangan dengan Undang-Undang ini dinyatakan tetap berlaku.

BAB XIII

KETENTUAN PENUTUP

Pasal 54

(1) Undang-Undang ini mulai berlaku pada tanggal diundangkan.

(2) Peraturan Pemerintah harus sudah ditetapkan paling lama 2 (dua) tahun setelah diundangkannya Undang-Undang ini.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Undang-Undang ini dengan penempatannya dalam Lembaran Negara Republik Indonesia.

Disahkan di Jakarta
pada tanggal 21 April 2008

PRESIDEN REPUBLIK INDONESIA,

ttd

DR. H. SUSILO BAMBANG YUDHOYONO

Diundangkan di Jakarta
pada tanggal 21 April 2008

MENTERI HUKUM DAN HAK ASASI MANUSIA
REPUBLIK INDONESIA,

ttd

ANDI MATTALATA

LEMBARAN NEGARA REPUBLIK INDONESIA TAHUN 2008 NOMOR 58

Salinan sesuai dengan aslinya
DEPUTI MENTERI SEKRETARIS NEGARA
BIDANG PERUNDANG-UNDANGAN,

MUHAMMAD SAPTA MURTI

PENJELASAN

ATAS

UNDANG-UNDANG REPUBLIK INDONESIA

NOMOR 11 TAHUN 2008

TENTANG

INFORMASI DAN TRANSAKSI ELEKTRONIK

I. UMUM

Pemanfaatan Teknologi Informasi, media, dan komunikasi telah mengubah baik perilaku masyarakat maupun peradaban manusia secara global. Perkembangan teknologi informasi dan komunikasi telah pula menyebabkan hubungan dunia menjadi tanpa batas *(borderless)* dan menyebabkan perubahan sosial, ekonomi, dan budaya secara signifikan berlangsung demikian cepat. Teknologi Informasi saat ini menjadi pedang bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum.

Saat ini telah lahir suatu rezim hukum baru yang dikenal dengan hukum siber atau hukum telematika. Hukum siber atau *cyber law*, secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan teknologi informasi dan komunikasi. Demikian pula, hukum telematika yang merupakan perwujudan dari konvergensi hukum telekomunikasi, hukum media, dan hukum informatika. Istilah lain yang juga digunakan adalah hukum teknologi informasi *(law of information technology*), hukum dunia maya (*virtual world law*), dan hukum mayantara. Istilah-istilah tersebut lahir mengingat kegiatan yang dilakukan melalui jaringan sistem komputer dan sistem komunikasi baik dalam lingkup lokal maupun global (Internet) dengan memanfaatkan teknologi informasi berbasis sistem komputer yang merupakan sistem elektronik yang dapat dilihat secara virtual. Permasalahan hukum yang seringkali dihadapi adalah ketika terkait dengan penyampaian informasi, komunikasi, dan/atau transaksi secara elektronik, khususnya dalam hal pembuktian dan hal yang terkait dengan perbuatan hukum yang dilaksanakan melalui sistem elektronik.

Yang dimaksud dengan sistem elektronik adalah sistem komputer dalam arti luas, yang tidak hanya mencakup perangkat keras dan perangkat lunak komputer, tetapi juga mencakup jaringan telekomunikasi dan/atau sistem komunikasi elektronik. Perangkat lunak atau program komputer adalah sekumpulan instruksi yang diwujudkan dalam bentuk bahasa, kode, skema, ataupun bentuk lain, yang apabila digabungkan dengan media yang dapat dibaca dengan komputer akan mampu membuat komputer

Sistem . . .

bekerja untuk melakukan fungsi khusus atau untuk mencapai hasil yang khusus, termasuk persiapan dalam merancang instruksi tersebut.

Sistem elektronik juga digunakan untuk menjelaskan keberadaan sistem informasi yang merupakan penerapan teknologi informasi yang berbasis jaringan telekomunikasi dan media elektronik, yang berfungsi merancang, memproses, menganalisis, menampilkan, dan mengirimkan atau menyebarkan informasi elektronik. Sistem informasi secara teknis dan manajemen sebenarnya adalah perwujudan penerapan produk teknologi informasi ke dalam suatu bentuk organisasi dan manajemen sesuai dengan karakteristik kebutuhan pada organisasi tersebut dan sesuai dengan tujuan peruntukannya. Pada sisi yang lain, sistem informasi secara teknis dan fungsional adalah keterpaduan sistem antara manusia dan mesin yang mencakup komponen perangkat keras, perangkat lunak, prosedur, sumber daya manusia, dan substansi informasi yang dalam pemanfaatannya mencakup fungsi *input*, *process*, *output*, *storage,* dan *communication.*

Sehubungan dengan itu, dunia hukum sebenarnya sudah sejak lama memperluas penafsiran asas dan normanya ketika menghadapi persoalan kebendaan yang tidak berwujud, misalnya dalam kasus pencurian listrik sebagai perbuatan pidana. Dalam kenyataan kegiatan siber tidak lagi sederhana karena kegiatannya tidak lagi dibatasi oleh teritori suatu negara, yang mudah diakses kapan pun dan dari mana pun. Kerugian dapat terjadi baik pada pelaku transaksi maupun pada orang lain yang tidak pernah melakukan transaksi, misalnya pencurian dana kartu kredit melalui pembelanjaan di Internet. Di samping itu, pembuktian merupakan faktor yang sangat penting, mengingat informasi elektronik bukan saja belum terakomodasi dalam sistem hukum acara Indonesia secara komprehensif, melainkan juga ternyata sangat rentan untuk diubah, disadap, dipalsukan, dan dikirim ke berbagai penjuru dunia dalam waktu hitungan detik. Dengan demikian, dampak yang diakibatkannya pun bisa demikian kompleks dan rumit.

Permasalahan yang lebih luas terjadi pada bidang keperdataan karena transaksi elektronik untuk kegiatan perdagangan melalui sistem elektronik (*electronic commerce)* telah menjadi bagian dari perniagaan nasional dan internasional. Kenyataan ini menunjukkan bahwa konvergensi di bidang teknologi informasi, media, dan informatika (telematika) berkembang terus tanpa dapat dibendung, seiring dengan ditemukannya perkembangan baru di bidang teknologi informasi, media, dan komunikasi.

Kegiatan melalui media sistem elektronik, yang disebut juga ruang siber (*cyber space*), meskipun bersifat virtual dapat dikategorikan sebagai tindakan atau perbuatan hukum yang nyata. Secara yuridis kegiatan pada ruang siber tidak dapat didekati dengan ukuran dan kualifikasi hukum konvensional saja sebab jika cara ini yang ditempuh akan terlalu banyak kesulitan dan hal yang lolos dari pemberlakuan hukum. Kegiatan dalam

Dengan . . .

ruang siber adalah kegiatan virtual yang berdampak sangat nyata meskipun alat buktinya bersifat elektronik.

Dengan demikian, subjek pelakunya harus dikualifikasikan pula sebagai Orang yang telah melakukan perbuatan hukum secara nyata. Dalam kegiatan *e-commerce* antara lain dikenal adanya dokumen elektronik yang kedudukannya disetarakan dengan dokumen yang dibuat di atas kertas.

Berkaitan dengan hal itu, perlu diperhatikan sisi keamanan dan kepastian hukum dalam pemanfaatan teknologi informasi, media, dan komunikasi agar dapat berkembang secara optimal. Oleh karena itu, terdapat tiga pendekatan untuk menjaga keamanan di *cyber space,* yaitu pendekatan aspek hukum, aspek teknologi, aspek sosial, budaya, dan etika. Untuk mengatasi gangguan keamanan dalam penyelenggaraan sistem secara elektronik, pendekatan hukum bersifat mutlak karena tanpa kepastian hukum, persoalan pemanfaatan teknologi informasi menjadi tidak optimal.

II. PASAL DEMI PASAL

Pasal 1

Cukup jelas.

Pasal 2

Undang-Undang ini memiliki jangkauan yurisdiksi tidak semata-mata untuk perbuatan hukum yang berlaku di Indonesia dan/atau dilakukan oleh warga negara Indonesia, tetapi juga berlaku untuk perbuatan hukum yang dilakukan di luar wilayah hukum (yurisdiksi) Indonesia baik oleh warga negara Indonesia maupun warga negara asing atau badan hukum Indonesia maupun badan hukum asing yang memiliki akibat hukum di Indonesia, mengingat pemanfaatan Teknologi Informasi untuk Informasi Elektronik dan Transaksi Elektronik dapat bersifat lintas teritorial atau universal.

Yang dimaksud dengan “merugikan kepentingan Indonesia” adalah meliputi tetapi tidak terbatas pada merugikan kepentingan ekonomi nasional, perlindungan data strategis, harkat dan martabat bangsa, pertahanan dan keamanan negara, kedaulatan negara, warga negara, serta badan hukum Indonesia.

Pasal 3

“Asas kepastian hukum” berarti landasan hukum bagi pemanfaatan Teknologi Informasi dan Transaksi Elektronik serta segala sesuatu yang mendukung penyelenggaraannya yang mendapatkan pengakuan hukum di dalam dan di luar pengadilan.

“Asas manfaat” berarti asas bagi pemanfaatan Teknologi Informasi dan Transaksi Elektronik diupayakan untuk mendukung proses

berinformasi sehingga dapat meningkatkan kesejahteraan masyarakat.

“Asas kehati-hatian” berarti landasan bagi pihak yang bersangkutan harus memperhatikan segenap aspek yang berpotensi mendatangkan kerugian, baik bagi dirinya maupun bagi pihak lain dalam pemanfaatan Teknologi Informasi dan Transaksi Elektronik.

“Asas iktikad baik” berarti asas yang digunakan para pihak dalam melakukan Transaksi Elektronik tidak bertujuan untuk secara sengaja dan tanpa hak atau melawan hukum mengakibatkan kerugian bagi pihak lain tanpa sepengetahuan pihak lain tersebut.

“Asas kebebasan memilih teknologi atau netral teknologi” berarti asas pemanfaatan Teknologi Informasi dan Transaksi Elektronik tidak terfokus pada penggunaan teknologi tertentu sehingga dapat mengikuti perkembangan pada masa yang akan datang.

Pasal 4

Cukup jelas.

Pasal 5

Ayat 1

Cukup jelas.

Ayat 2

Cukup jelas.

Ayat 3

Cukup jelas.

Ayat 4

Huruf a

Surat yang menurut undang-undang harus dibuat tertulis meliputi tetapi tidak terbatas pada surat berharga, surat yang berharga, dan surat yang digunakan dalam proses penegakan hukum acara perdata, pidana, dan administrasi negara.

Huruf b

Cukup jelas.

Pasal 6

Selama ini bentuk tertulis identik dengan informasi dan/atau dokumen yang tertuang di atas kertas semata, padahal pada hakikatnya informasi dan/atau dokumen dapat dituangkan ke dalam media apa saja, termasuk media elektronik. Dalam lingkup Sistem Elektronik, informasi yang asli dengan salinannya tidak relevan lagi untuk dibedakan sebab Sistem Elektronik pada dasarnya beroperasi dengan

cara penggandaan yang mengakibatkan informasi yang asli tidak dapat dibedakan lagi dari salinannya.

Pasal 7

Ketentuan ini dimaksudkan bahwa suatu Informasi Elektronik dan/atau Dokumen Elektronik dapat digunakan sebagai alasan timbulnya suatu hak.

Pasal 8

Cukup jelas.

Pasal 9

Yang dimaksud dengan “informasi yang lengkap dan benar” meliputi:

a. informasi yang memuat identitas serta status subjek hukum dan kompetensinya, baik sebagai produsen, pemasok, penyelenggara maupun perantara;
b. informasi lain yang menjelaskan hal tertentu yang menjadi syarat sahnya perjanjian serta menjelaskan barang dan/atau jasa yang ditawarkan, seperti nama, alamat, dan deskripsi barang/jasa.

Pasal 10

Ayat (1)

Sertifikasi Keandalan dimaksudkan sebagai bukti bahwa pelaku usaha yang melakukan perdagangan secara elektronik layak berusaha setelah melalui penilaian dan audit dari badan yang berwenang. Bukti telah dilakukan Sertifikasi Keandalan ditunjukkan dengan adanya logo sertifikasi berupa *trust mark* pada laman *(home page)* pelaku usaha tersebut.

Ayat (2)

Cukup jelas.

Pasal 11

Ayat (1)

Undang-Undang ini memberikan pengakuan secara tegas bahwa meskipun hanya merupakan suatu kode, Tanda Tangan Elektronik memiliki kedudukan yang sama dengan tanda tangan manual pada umumnya yang memiliki kekuatan hukum dan akibat hukum.

Persyaratan sebagaimana dimaksud dalam Pasal ini merupakan persyaratan minimum yang harus dipenuhi dalam setiap Tanda Tangan Elektronik. Ketentuan ini membuka kesempatan seluas-luasnya kepada siapa pun untuk mengembangkan metode, teknik, atau proses pembuatan Tanda Tangan Elektronik.

Ayat (2)

Peraturan Pemerintah dimaksud, antara lain, mengatur tentang teknik, metode, sarana, dan proses pembuatan Tanda Tangan Elektronik.

Pasal 12 . . .

Pasal 12

Cukup jelas.

Pasal 13

Cukup jelas.

Pasal 14

Informasi sebagaimana dimaksud dalam Pasal ini adalah informasi yang minimum harus dipenuhi oleh setiap penyelenggara Tanda Tangan Elektronik.

Pasal 15

Ayat (1)

"Andal" artinya Sistem Elektronik memiliki kemampuan yang sesuai dengan kebutuhan penggunaannya.

"Aman" artinya Sistem Elektronik terlindungi secara fisik dan nonfisik.

"Beroperasi sebagaimana mestinya" artinya Sistem Elektronik memiliki kemampuan sesuai dengan spesifikasinya.

Ayat (2)

"Bertanggung jawab" artinya ada subjek hukum yang bertanggung jawab secara hukum terhadap Penyelenggaraan Sistem Elektronik tersebut.

Ayat (3)

Cukup jelas.

Pasal 16

Cukup jelas.

Pasal 17

Ayat (1)

Undang-Undang ini memberikan peluang terhadap pemanfaatan Teknologi Informasi oleh penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat.

Pemanfaatan Teknologi Informasi harus dilakukan secara baik, bijaksana, bertanggung jawab, efektif, dan efisien agar dapat diperoleh manfaat yang sebesar-besarnya bagi masyarakat.

Ayat (2)

Cukup jelas.

Ayat (3)

Cukup jelas.

Pasal 18 ...

Pasal 18

Ayat (1)

Cukup jelas.

Ayat (2)

Pilihan hukum yang dilakukan oleh para pihak dalam kontrak internasional termasuk yang dilakukan secara elektronik dikenal dengan *choice of law*. Hukum ini mengikat sebagai hukum yang berlaku bagi kontrak tersebut.

Pilihan hukum dalam Transaksi Elektronik hanya dapat dilakukan jika dalam kontraknya terdapat unsur asing dan penerapannya harus sejalan dengan prinsip hukum perdata internasional (HPI).

Ayat (3)

Dalam hal tidak ada pilihan hukum, penetapan hukum yang berlaku berdasarkan prinsip atau asas hukum perdata internasional yang akan ditetapkan sebagai hukum yang berlaku pada kontrak tersebut.

Ayat (4)

Forum yang berwenang mengadili sengketa kontrak internasional, termasuk yang dilakukan secara elektronik, adalah forum yang dipilih oleh para pihak. Forum tersebut dapat berbentuk pengadilan, arbitrase, atau lembaga penyelesaian sengketa alternatif lainnya.

Ayat (5)

Dalam hal para pihak tidak melakukan pilihan forum, kewenangan forum berlaku berdasarkan prinsip atau asas hukum perdata internasional. Asas tersebut dikenal dengan asas tempat tinggal tergugat *(the basis of presence)* dan efektivitas yang menekankan pada tempat harta benda tergugat berada *(principle of effectiveness)*.

Pasal 19

Yang dimaksud dengan “disepakati” dalam pasal ini juga mencakup disepakatinya prosedur yang terdapat dalam Sistem Elektronik yang bersangkutan.

Pasal 20

Ayat (1)

Transaksi Elektronik terjadi pada saat kesepakatan antara para pihak yang dapat berupa, antara lain pengecekan data, identitas, nomor identifikasi pribadi *(personal identification number/PIN)* atau sandi lewat *(password)*.

Ayat (2)

Cukup jelas.

Pasal 21 ...

Pasal 21

Ayat (1)

Yang dimaksud dengan “dikuasakan” dalam ketentuan ini sebaiknya dinyatakan dalam surat kuasa.

Ayat (2)

Cukup jelas.

Ayat (3)

Cukup jelas.

Ayat (4)

Cukup jelas.

Ayat (5)

Cukup jelas.

Pasal 22

Ayat (1)

Yang dimaksud dengan “fitur” adalah fasilitas yang memberikan kesempatan kepada pengguna Agen Elektronik untuk melakukan perubahan atas informasi yang disampaikannya, misalnya fasilitas pembatalan *(cancel)*, edit, dan konfirmasi ulang.

Ayat (2)

Cukup jelas.

Pasal 23

Ayat (1)

Nama Domain berupa alamat atau jati diri penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat, yang perolehannya didasarkan pada prinsip pendaftar pertama *(first come first serve)*.

Prinsip pendaftar pertama berbeda antara ketentuan dalam Nama Domain dan dalam bidang hak kekayaan intelektual karena tidak diperlukan pemeriksaan substantif, seperti pemeriksaan dalam pendaftaran merek dan paten.

Ayat (2)

Yang dimaksud dengan “melanggar hak Orang lain”, misalnya melanggar merek terdaftar, nama badan hukum terdaftar, nama Orang terkenal, dan nama sejenisnya yang pada intinya merugikan Orang lain.

Ayat (3)

Yang dimaksud dengan “penggunaan Nama Domain secara tanpa hak” adalah pendaftaran dan penggunaan Nama Domain yang semata-mata ditujukan untuk menghalangi atau menghambat Orang lain untuk menggunakan nama yang intuitif dengan keberadaan nama dirinya atau nama produknya, atau untuk mendompleng reputasi Orang yang sudah terkenal atau ternama, atau untuk menyesatkan konsumen.

Pasal 24 . . .

Pasal 24

Cukup jelas.

Pasal 25

Informasi Elektronik dan/atau Dokumen Elektronik yang disusun dan didaftarkan sebagai karya intelektual, hak cipta, paten, merek, rahasia dagang, desain industri, dan sejenisnya wajib dilindungi oleh Undang-Undang ini dengan memperhatikan ketentuan Peraturan Perundang-undangan.

Pasal 26

Ayat (1)

Dalam pemanfaatan Teknologi Informasi, perlindungan data pribadi merupakan salah satu bagian dari hak pribadi *(privacy rights).* Hak pribadi mengandung pengertian sebagai berikut:

a. Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan.
b. Hak pribadi merupakan hak untuk dapat berkomunikasi dengan Orang lain tanpa tindakan memata-matai.
c. Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang.

Ayat (2)

Cukup jelas.

Pasal 27

Cukup jelas.

Pasal 28

Cukup jelas.

Pasal 29

Cukup jelas.

Pasal 30

Ayat (1)

Cukup jelas.

Ayat (2)

Secara teknis perbuatan yang dilarang sebagaimana dimaksud pada ayat ini dapat dilakukan, antara lain dengan:

a. melakukan komunikasi, mengirimkan, memancarkan atau sengaja berusaha mewujudkan hal-hal tersebut kepada siapa pun yang tidak berhak untuk menerimanya; atau

b. sengaja . . .

b. sengaja menghalangi agar informasi dimaksud tidak dapat atau gagal diterima oleh yang berwenang menerimanya di lingkungan pemerintah dan/atau pemerintah daerah.

Ayat (3)

Sistem pengamanan adalah sistem yang membatasi akses Komputer atau melarang akses ke dalam Komputer dengan berdasarkan kategorisasi atau klasifikasi pengguna beserta tingkatan kewenangan yang ditentukan.

Pasal 31

Ayat (1)

Yang dimaksud dengan “intersepsi atau penyadapan” adalah kegiatan untuk mendengarkan, merekam, membelokkan, mengubah, menghambat, dan/atau mencatat transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik, baik menggunakan jaringan kabel komunikasi maupun jaringan nirkabel, seperti pancaran elektromagnetis atau radio frekuensi.

Ayat (2)

Cukup jelas.

Ayat (3)

Cukup jelas.

Ayat (4)

Cukup jelas.

Pasal 32

Cukup jelas.

Pasal 33

Cukup jelas.

Pasal 34

Ayat (1)

Cukup jelas.

Ayat (2)

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

Pasal 35

Cukup jelas.

Pasal 36

Cukup jelas.

Pasal 37 ...

Pasal 37
Cukup jelas.

Pasal 38
Cukup jelas.

Pasal 39
Cukup jelas.

Pasal 40
Cukup jelas.

Pasal 41
Ayat (1)
Cukup jelas.

Ayat (2)
Yang dimaksud dengan “lembaga yang dibentuk oleh masyarakat” merupakan lembaga yang bergerak di bidang teknologi informasi dan transaksi elektronik.

Ayat (3)
Cukup jelas.

Pasal 42
Cukup jelas.

Pasal 43
Ayat (1)
Cukup jelas.

Ayat (2)
Cukup jelas.

Ayat (3)
Cukup jelas.

Ayat (4)
Cukup jelas.

Ayat (5)
Huruf a
Cukup jelas.

Huruf b
Cukup jelas.

Huruf c
Cukup jelas.

Huruf d ...

Huruf d
Cukup jelas.

Huruf e
Cukup jelas.

Huruf f
Cukup jelas.

Huruf g
Cukup jelas.

Huruf h
Yang dimaksud dengan “ahli” adalah seseorang yang memiliki keahlian khusus di bidang Teknologi Informasi yang dapat dipertanggungjawabkan secara akademis maupun praktis mengenai pengetahuannya tersebut.

Huruf i
Cukup jelas.

Ayat (6)
Cukup jelas.

Ayat (7)
Cukup jelas.

Ayat (8)
Cukup jelas.

Pasal 44
Cukup jelas.

Pasal 45
Cukup jelas.

Pasal 46
Cukup jelas.

Pasal 47
Cukup jelas.

Pasal 48
Cukup jelas.

Pasal 49
Cukup jelas.

Pasal 50
Cukup jelas.

Pasal 51 ...

Pasal 51

Cukup jelas.

Pasal 52

Ayat (1)

Cukup jelas.

Ayat (2)

Cukup jelas.

Ayat (3)

Cukup jelas.

Ayat (4)

Ketentuan ini dimaksudkan untuk menghukum setiap perbuatan melawan hukum yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 yang dilakukan oleh korporasi *(corporate crime)* dan/atau oleh pengurus dan/atau staf yang memiliki kapasitas untuk:

a. mewakili korporasi;
b. mengambil keputusan dalam korporasi;
c. melakukan pengawasan dan pengendalian dalam korporasi;
d. melakukan kegiatan demi keuntungan korporasi.

Pasal 53

Cukup jelas.

Pasal 54

Cukup jelas.

TAMBAHAN LEMBARAN NEGARA REPUBLIK INDONESIA NOMOR 4843

Lampiran VI

CURICULUM VITAE

Nama	: Ahmad Muyasir
Tempat, Tanggal Lahir	: Ngawi, 25 Mei 1991
Jenis Kelamin	: Laki-laki
Agama	: Islam
Alamat Asal	: Pohjenggel, Rt 03/Rw 01 Katikan, Kedunggalar, Ngawi, Jawa Timur
Alamat di Jogjakarta	: Glagah, Rt 09/Rw 02 No. 303, Warungboto, UH IV, Yogyakarta
No HP	: 0857 2578 2399
E-Mail	: ahmadmuyasir7@gmail.com
Riwayat Pendidikan	:

1. TK Dharma Wanita Katikan II tahun 1996-1997
2. MI Nurul Islam Katikan tahun 1997-2003
3. MTsN Jogorogo tahun 2003-2006
4. SMAN 1 Jogorogo tahun 2006-2009
5. Program S-1 Hukum Islam UIN Sunan Kalijaga Yogyakarta tahun 2011-2015