Rancangan Undang – Undang

Nomor Tahun

Tentang

Tindak Pidana Di Bidang Teknologi Informasi

DENGAN RAHMAT TUHAN YANG MAHA ESA

PRESIDEN REPUBLIK INDONESIA

Menimbang:

a. bahwa dalam mewujudkan tujuan nasional sebagaimana dimaksud dalam pembukaan Undang-Undang Dasar 1945 yakni melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia, memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa dan ikut serta dalam memelihara ketertiban dunia yang berdasarkan kemerdekaan dan perdamaian abadi dan keadilan sosial, maka diperlukan penegakan hukum dan ketertiban secara konsisten dan berkesinambungan dalam pemanfaatan teknologi khususnya teknologi informasi, secara aman, merata dan penyebaran di seluruh lapisan masyarakat Indonesia;
b. bahwa salah satu sarana untuk mewujudkan masyarakat sejahtera sebagaimana diamanatkan dalam Pancasila dan Undang – Undang Dasar 1945 adalah pemanfaatan teknologi khususnya teknologi informasi secara aman, optimal, merata dan menyebar ke seluruh lapisan warga negara Indonesia;
c. bahwa pemanfaatan teknologi informasi disamping memberi manfaat bagi kemaslahatan masyarakat, juga memiliki peluang untuk digunakan sebagai alat untuk melakukan kejahatan;
d. bahwa kejahatan yang dilakukan dengan menggunakan teknologi informasi dapat terjadi pada kejahatan kriminal pada umumnya maupun pada kejahatan yang secara khusus menargetkan sesama teknologi informasi sebagai korbannya;
e. bahwa dampak kejahatan yang timbul dari penggunaan teknologi informasi secara negatif dapat menyebabkan ambruknya tatanan sosial, lumpuhnya

perekonomian nasional, lemahnya sistem pertahanan dan keamanan, serta memiliki peluang untuk digunakan sebagai alat untuk melakukan teror;

f. bahwa peraturan perundangan – undangan yang berlaku sampai saat ini belum dapat secara komprehensif dan memadai mengantisipasi tidak pidana di bidang teknologi informasi;

g. bahwa berdasarkan pertimbangan huruf a, b, c, d dan e tersebut di atas, dipandang perlu ditetapkan Undang-Undang tentang Tindak Pidana Di Bidang Teknologi Informasi.

Mengingat:

1. Pasal 28 Undang-Undang Dasar 1945 dan perubahannya ;
2. Kitab Undang – Undang Hukum Pidana;
3. Undang – Undang No. 8 Tahun 1981 tentang Hukum Acara Pidana
4. Undang – Undang No. 36 Tahun 1999 tentang Telekomunikasi
5. Undang – Undang No. 19Tahun 2002 tentang Hak Cipta ;
6. Undang – Undang No. 32 Tahun 2002 tentang Penyiaran;
7. ~~7.~~Undang – Undang No. xx Tahun 200x~~zzzz~~ tentang ~~Pemanfaatan Teknologi Informasi~~
8. ~~8.~~7. ~~Undang – Udang No. yy Tahun xxxx tentang~~ Informasi dan Transaksi Elektronik; ~~dan Transaksi Elektronik.;~~
9. ~~9.~~8. Undang – Undang No. vv Tahun zzzz tentang Kebebasan Memperoleh Informasi Publik;
10. ~~10.~~9. Undang – Undang No. zz Tahun yyyy tentang Pencucian Uang;
11. ~~11.~~10. Undang – Undang No. xx Tahun zzzz tentang Perbankan

Formatted: Bullets and Numbering

Dengan persetujuan

DEWAN PERWAKILAN RAKYAT

REPUBLIK INDONESIA

Memutuskan:

Menetapkan:

UNDANG – UNDANG TENTANG
TINDAK PIDANA DI BIDANG TEKNOLOGI INFORMASI

Bab I
Ketentuan Umum

Pasal 1

Dalam undang-undang ini yang dimaksud dengan:

1. Data adalah fakta berupa angka, karakter, symbol, gambar, tanda-tanda, isyarat, tulisan, suara, bunyi yang merepresentasikan keadaan sebenarnya yang selanjutnya digunakan sebagai masukan suatu Sistem Informasi.
2. Data Elektronik adalah Data yang merupakan hasil luaran dari suatu Elektronik.
3. Elektronik adalah segala macam alat dan peralatan yang dibuat dan bekerja berdasarkan prinsip elektronika untuk memperoleh, mengolah, menyimpan dan atau menyampaikan informasi dalam format digital, dalam media elektromagnetik, optikal atau sejenisnya;
4. Informasi adalah Data hasil pengolahan Sistem Informasi yang bermanfaat bagi penggunanya.
5. Informasi Elektronik adalah Data Elektronik hasil pengolahan Sistem Informasi yang bermanfaat bagi penggunanya.
6. Sistem Informasi adalah tata cara pengelolaan Informasi menggunakan Teknologi Informasi
7. Teknologi Informasi adalah suatu teknik atau cara Elektronik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisa, dan menyebarkan informasi.

8. Komputer adalah Elektronik yang melaksanakan fungsi logika, aritmatika, dan penyimpanan.
9. Sistem Komputer adalah Komputer atau sekumpulan Komputer yang terhubung dengan Elektronik dan atau sekumpulan Komputer lainnya, menuruti perintah suatu program, melaksanakan pemrosesan Data dan menghasilkan Data Elektronik.
10. Jaringan Komputer adalah Komputer dan atau Sistem Komputer yang saling terhubung menggunakan media komunikasi, masing-masing memiliki otoritas untuk melaksanakan tugas berdasarkan program.
11. Internet adalah Jaringan Komputer global atau jaringan yang menghubungkan Jaringan Komputer di seluruh dunia dengan menggunakan protokol komunikasi Internet Protocol.
12. Intranet adalah Jaringan Komputer privat yang menggunakan protokol komunikasi Internet Protocol, dapat namun tidak selalu, terhubung ke Internet, dan hanya dapat digunakan dalam lingkungan terbatas.
13. Nama Domain adalah kode atau susunan karakter yang bersifat unik, menunjukkan lokasi tertentu dalam Internet, berhubungan dengan berkas elektronik (*file*) yang disimpan dalam alat penyimpan dalam Sistem Komputer, yang digunakan untuk menyimpan Informasi atau Data Elektronik lainnya yang berkaitan dengan pemilik atau pengelola Nama Domain.
14. Surat Elektronik adalah suatu jenis layanan yang memungkinkan pengguna Komputer untuk mengirim Data, Informasi, atau pesan melalui Internet atau Jaringan Komputer kepada pengguna Komputer lainnya.
15. Alamat Surat Elektronik adalah alamat Internet dari seseorang, perkumpulan, organisasi, atau badan usaha, untuk berkomunikasi melalui Internet atau komunikasi Elektronik lainnya.
16. Nomor Internet Protokol adalah tanda pengenal unik dalam bentuk sederetan angka menggunakan ketentuan baku untuk menandai setiap Elektronik yang terhubung ke Internet.
17. Situs Internet adalah suatu lokasi di dalam Internet yang digunakan untuk menempatkan Data Elektronik atau aplikasi Internet yang dapat diakses oleh pengguna Internet.

18. Sandi Akses (*password*) adalah angka, karakter, simbol lainnya atau kombinasi diantaranya yang merupakan kunci untuk dapat mengakses komputer, sistem komputer, jaringan komputer, Internet, atau media elektronik lainnya.
19. Privasi adalah hak individu untuk mengendalikan penggunaan informasi tentang identitas pribadi baik oleh dirinya sendiri atau oleh pihak lainnya.
20. Database adalah semua data yang terdapat dalam suatu organisasi terutama yang tersimpan dalam alat penyimpan sistem komputer yang dapat diakses menggunakan kentuan-ketentuan tertentu.
21. Komunikasi Data adalah pengiriman dan penerimaan data dalam jaringan komputer.
22. Penyedia Layanan Teknologi Informasi adalah organisasi atau badan hukum yang memberikan layanan jasa di bidang teknologi informasi, meliputi namun tidak terbatas pada penyedia akses Internet, penyedia jasa pembangunan perangkat lunak komputer dan aplikasi Internet, penyedia jasa pemandu sistem informasi, serta penyedia jaringan telekomunikasi dan jasa telekomunikasi.
23. Penerima adalah seseorang yang menerima atau dimaksudkan untuk menerima data elektronik dari pengirim.
24. Pengirim adalah seseorang yang mengirim, meneruskan, menyimpan, atau menyalurkan setiap pesan elektronik atau menjadikan setiap pesan elektronik dapat dikirim, disimpan, atau disalurkan kepada orang lain.
25. Pelanggan adalah orang, badan usaha, badan hukum, atau instansi pemerintah yang menggunakan layanan teknologi informasi berdasarkan kontrak
26. Pemakai adalah orang, badan usaha, badan hukum, atau instansi pemerintah yang menggunakan layanan teknologi informasi yang tidak berdasarkan kontrak.
27. Pengguna adalah pelanggan dan pemakai.
28. Teknologi Enkripsi adalah penggunaan algoritma matematika untuk membuat data elektronik terkodekan sedemikian rupa sehingga hanya dapat dibaca oleh mereka yang memiliki kunci pembukanya.
29. Tanda Tangan Digital atau tandatangan elektronik adalah tanda jati diri berupa informasi elektronik yang berfungsi sebagai pengesahan oleh pengguna melalui metode elektronik atau prosedur yang telah ditentukan.

30. Transaksi Elektronik adalah setiap transaksi yang dilakukan oleh dua pihak atau lebih melalui jaringan komputer atau media elektronik lainnya, dengan menggunakan system informasi elektronik yang menimbulkan hak dan kewajiban kepada masing-masing pihak yang bertransaksi.
31. Perdagangan secara elektronik adalah setiap perdagangan baik barang ataupun jasa yang dilakukan melalui jaringan komputer atau media elektronik lainnya, dengan system informasi elektronik
32. Alat Pembayaran adalah uang atau semua jenis mekanisme pembayaran lainnya yang berfungsi untuk menggantikan uang
33. Kartu kredit adalah bagian dari alat pembayaran berupa kartu beridentitas unik yang diberikan oleh perusahaan penjamin pembayaran kepada perorangan atau perusahaan berdasarkan kontrak, yang digunakan oleh pengguna untuk melakukan transaksi eletronik dan atas penggunaan kartu kredit tersebut , pengguna kartu dinyatakan berhutang kepada perusahaan penjamin pembayaran selaku penerbit kartu kredit.
34. Kartu Debit adalah bagian dari alat pembayaran berupa kartu beridentitas unik yang diterbitkan oleh lembaga perbankan kepada nasabah tabungan pada bank bersangkutan berdasarkan kontrak, yang digunakan oleh pengguna untuk alat pembayaran dalam transaksi elektronik dan. atas penggunaan kartu debit tersebut, maka tabungan yang dimiliki oleh pengguna, dipotong langsung oleh Bank.
35. Akses adalah perbuatan memasuki, memberikan instruksi atau melakukan komunikasi dengan fungsi logika, aritmatika, atau memori dari komputer, sistem komputer, atau jaringan komputer.
36. Intersepsi adalah tindakan seseorang, badan usaha atau badan hukum untuk melakukan pencegatan terhadap lalu lintas komunikasi data melalui media kawat, serat optik maupun gelombang elektromagnetik dalam suatu sistem komputer baik menggunakan sarana teknis atau non-teknis.
37. Alat bukti elektronik meliputi: perangkat keras sistem komputer atau jaringan komputer peralatan lain yang tersambung ke komputer, perangkat lunak yang dapat berupa sistem operasi, sistem data base, dan atau sistem aplikasi yang tersimpan atau terpasang dalam sistem komputer atau jaringan komputer.

BAB II

Asas Dan Tujuan

Pasal 2

Undang – Undang Tindak Pidana di Bidang Teknologi Informasi ini dibuat berdasarkan asas keamanan, kepastian hukum**,** etika, manfaat**,** adil, dan merata.

Pasal 3

Undang – Undang Tindak Pidana di Bidang Teknologi Informasi ini dibuat dengan tujuan untuk mendukung ketertiban pemanfaatan Teknologi Informasi yang digunakan oleh orang berkewarga-negaraan Indonesia, dan atau badan hukum yang berkedudukan di Indonesia, orang asing, atau badan hukum asing yang melakukan kegiatan atau transaksi dengan orang, atau badan hukum yang lahir dan berkedudukan di Indonesia, dengan tetap menjunjung tinggi hukum Indonesia dan hak asasi manusia, tidak diskriminatif baik berdasarkan suku, agama, ras maupun antar golongan.

Bab III

Lingkup Berlakunya Undang- Undang Tindak Pidana di Bidang Teknologi Informasi

Pasal 43

1. Undang - Undang Tindak Pidana di Bidang Teknologi Informasi ini berlaku terhadap setiap ~~orang~~ orang atau badan hukum yang melakukan tindak pidana di bidang Teknologi Informasi di wilayah negara Republik Indonesia dan atau negara lain -yang mempunyai yurisdiksi dan menyatakan maksudnya untuk melakukan penuntutan terhadap pelaku tersebut.
2. Negara lain mempunyai yuridiksi sebagaimana dimaksud dalam ayat (1), apabila :
   a. Kejahatan dilakukan oleh warga negara dari negara yang bersangkutan;
   b. Kejahatan dilakukan terhadap warga negara dari negara yang bersangkutan;
   c. Kejahatan tersebut juga dilakukan di negara yang bersangkutan;

d. Kejahatan dilakukan terhadap suatu negara atau atau fasilitas pemerintah dari negara yang bersangkutan di luar negeri termasuk fasilitas kantor perwakilan atau tempat fasilitas pejabat diplomatik atau konsuler dari negara yang bersangkutan;
e. Kejahatan dilakukan dalam pesawat udara yang dioperasikan oleh pemerintah negara yang bersangkutan; atau
f. Kejahatan dilakukan dalam kapal yang berbendera negara tersebut atau pesawat udara yang terdaftar berdasarkan Undang-Undang negara yang bersangkutan pada saat kejahatan itu dilakukan.~~;~~

Pasal 54

Undang-Undang Tindak Pidana di Bidang Teknologi Informasi ini berlaku juga terhadap tindak pidana pemanfaatan teknologi informasi yang dilakukan :

a. Terhadap warga negara Republik Indonesia yang berkedudukan di luar wilayah negara Republik Indonesia;
b. Terhadap fasilitas negara Republik Indonesia di luar negeri, termasuk fasilitas pejabat diplomatik dan konsuler Republik Indonesia;
c. Dalam kapal yang berbendera negara Republik Indonesia atau pesawat udara yang terdaftar berdasarkan undang-undang negara Republik Indonesia pada saat kejahatan itu dilakukan; atau
d. Oleh setiap orang yang tidak memiliki kewarganegaraan dan ~~dan~~ bertempat tinggal di wilayah negara Republik Indonesia;

BAB IV

Lingkup Tindak Pidana Pemanfaatan Tek~~h~~nologi Informasi

Pasal 65

Seluruh jenis kejahatan baik yang telah diatur maupun belum diatur dalam Kitab Undang – Undang Hukum Pidana (KUHP) dan yang terbukti dilakukan ~~dengan sengaja~~ oleh setiap orang dengan ~~–~~memanfaatkan ~~—~~Teknologi Informasi dimaksud dalam Undang-

Undang ini, dikenakan ancaman dan hukuman berdasarkan ketentuan-ketentuan yang diatur dalam Uundang – Uundang ini.

Pasal 76

Penentuan ancaman dan hukuman dimaksud pasal 65 berdasarkan bobot pemanfaatan Teknologi Informasi dalam kejahatan dimaksud dan besarnya ancaman hukuman. Semakin besar bobot pemanfaatan – Teknologi Informasi dalam kejahatan dimaksud semakin besar peluang penggunaan Undang – Undang ini

BAB V

Pelanggaran ~~Tindak Pidana~~ Pemanfaatan Teknologi Informasi

Pasal 87

Hal- hal yang merupakan pelanggaran dalam Undang-Undang ini :

a. Barangsiapa~~Setiap orang, badan usaha atau badan hukum~~ ~~dengan sengaja dan melawan hukum~~ memanfaatkan Teknologi Informasi dengan melawan hukum.
b. Barangsiapa ~~Setiap orang, badan usaha atau badan hukum dengan sengaja dan melawan hukum~~ melakukan intersepsi dengan melawan hukum.
c. Barangsiapa ~~Setiap orang , badan usaha atau badan hukum~~ dengan sengaja ~~-~~dan melawan hukum merusak atau mengganggu data yang tersimpan dalam alat penyimpan data elektronik yang tersusun sebagai bagian dari sistem komputer.
d. Barangsiapa ~~Setiap orang, badan usaha atau badan hukum~~ dengan sengaja menghilangkan bukti – bukti elektronik yang ~~-~~dapat dijadikan alat bukti ~~-~~sah di pengadilan yang terdapat pada suatu sistem informasi atau sistem komputer.
e. Barangsiapa ~~Setiap orang, badan uasaha atau badan hukum~~ dengan sengaja merusak atau mengganggu sistem informasi, sistem komputer, jaringan komputer, dan Internet.
f. Barangsiapa ~~Setiap orang, badan usaha atau badan hukum dengan sengaja~~ memanfaatkan T–teknologi Informasi untuk menipu, menghasut, memfitnah, menjatuhkan nama baik seseorang atau organisasi.

g. BarangsiapaSetiap orang, badan usaha atau badan hukum dengan sengaja memanfaatkan T-teknologi I-informasi untuk menyebarkan gambar, tulisan atau kombinasi dari keduanya yang mengandung sifat – sifat pornografi.

h. Barangsiapa Setiap orang, badan usaha ataau badan hukum dengan sengaja memanfaatkan T-teknologi I-informasi untuk membantu terjadinya percobaan, atau persekongkolan yang menjurus pada kejahatan.

i. Setiap badan hukum penyelenggara jasa akses Internet atau penyelenggara layanan T-teknologi I-informasi dengan sengaja , baik untuk keperluan komersial maupun keperluan internal perusahaan, dengan sengaja tidak menyimpan atau tidak dapat menyediakan -catatan transaksi elektronik -sedikitnya untuk jangka waktu dua tahun.-

BAB VI

Tindak Pidana Pemanfaatan Teknologi Informasi

Pasal 9

Kejahatan terhadap nyawa dan keselamatan negara8

BarangsiapaSetiap orang yang dengan sengaja dan melawan hukum memanfaatkan T-teknologi I-informasi dengan maksud untuk menghilangkan nyawa, harta benda orang lain, atau mengakibatkan kerusakan atau kehancuran obyek-obyek vital dan strategis atau lingkungan hidup atau fasilitas umum atau fasilitas internasional, usaha menggulingkan pemerintahan yang sah, atau membahayakan keamanan negara atau -untuk memisahkan sebagian dari wilayah negara atau sebagai bagian dari kegiatan teror kepada orang atau negara lain, dipidana dengan pidana mati atau penjara seumur hidup atau pidana penjara, paling singkat -10 (sepuluh) tahun dan paling lama 20 (dua puluh) tahun .

Pasal 109

Pencurian

Barangsiapa Setiap orang yang dengan sengaja dan melawan hukum memanfaatkan teknologi informasi untuk melakukan pencurian sebagaimana dimaksud pasal 362 Kitab Undang-Undang Hukum Pidana, sehingga memenuhi ketentuan sebagaimana dinyatakan

pada pasal 362 Kitab Undang – Undang Hukum Pidana, dipidana penjara paling singkat 5 (lima) tahun, dan paling lama 15 ~~8~~ (lima belas~~delapan~~) tahun atau denda sedikit – dikitnya Rp. 500.000.000,- (lima ratus juta rupiah) dan sebanyak-banyaknya Rp.2.000.000.000,-(dua milyar rupiah).

Pasal 1~~0~~10

Mengakses Tanpa Hak

Barangsiapa ~~Setiap orang yang~~ dengan sengaja dan melawan hukum ~~–~~memasuki lingkungan dan atau sarana fisik Sistem Informasi tanpa hak atau secara tidak sah menggunakan sandi akses palsu, melakukan pembongkaran tanpa seijin pemiliknya yang sah atau perusakan dengan atau tanpa maksud merugikan pemilik sah, ~~-~~dipidana penjara paling singkat ~~–~~2 (dua) tahun dan paling lama ~~-~~4 (empat) tahun atau denda sedikit – dikitnya Rp. 200.000.000,- (dua ratus juta rupiah) dan sebanyak-banyaknya Rp 800.000.000,- (delapan ratus juta rupiah).

Pasal 1~~1~~21

Mengakses Tanpa Hak Terhadap Sistem Informasi Strategis

~~1.~~1. Barangsiapa ~~Setiap orang yang dengan sengaja dan melawan hukum memasuki lingkungan dan atau sarana fisik Sistem Informasi milik instansi pemerintah, militer, perbankan, atau instansi strategis lainnya tanpa hak atau secara tidak sah dengan menggunakan sandi akses palsu, melakukan pembongkaran atau perusakan dengan atau tanpa maksud merugikan instansi yang dituju, dipidana penjara paling singkat 7 (tujuh) tahun dan paling lama 12 (dua belas) tahun atau denda sedikit – dikitnya Rp. 700.000.000, (tujuh ratus juta rupiah) dan sebanyak banyaknya Rp. 1.500.000.000,- (satu milyar lima ratur juta rupiah).~~

1. dengan sengaja dan melawan hukum memasuki lingkungan dan atau sarana fisik Sistem Informasi milik instansi pemerintah, militer, perbankan, atau instansi strategis lainnya tanpa hak atau secara tidak sah dengan menggunakan sandi akses palsu, melakukan pembongkaran atau perusakan dengan atau tanpa maksud merugikan instansi yang dituju, dipidana penjara paling singkat 7 (tujuh) tahun dan paling lama 12 (dua belas) tahun atau denda sedikit – dikitnya Rp. 700.000.000,- (tujuh ratus juta

Formatted: Bullets and Numbering

rupiah) dan sebanyak-banyaknya Rp. 1.500.000.000,- (satu milyar lima ratur juta rupiah).

~~1.~~2. Apabila ~~-~~pelaku kejahatan ~~-~~dimaksud ~~-~~ayat (1) ~~–~~terbukti telah ~~-~~menyebarkan dan atau mengumumkan informasi yang harus dilindungi kepada pihak yang tidak berwenang, dipidana penjara sesuai Ayat (1), ditambah 2 (dua) tahun.

Pasal 13~~2~~

Pemalsuan Identitas

1. Barangsiapa ~~Setiap orang yang~~ dengan sengaja terbukti memanm~~m~~faatkan T~~t~~eknologi I~~i~~nformasi untuk melakukan transaksi elektronik, dengan menggunakan identitas palsu, atau identitas milik orang lain, dipidana penjara paling singkat 6 (enam) bulan dan paling lama 3 (tiga) tahun , dan dikenakan denda sedikit- sedikitnya Rp 50.000.000,- (lima puluh juta rupiah).
2. Apabila ~~-~~transaksi elektronik dimaksud A~~a~~yat (1) pasal ini ~~-~~dilakukan untuk ~~-dengan~~ transaksi ekonomi dengan menggunakan alat pembayaran berupa kartu kredit, atau kartu debit atau alat pembayaran lainnya yang bukan miliknya sah, dipidana penjara paling singkat ~~-~~7 ~~-~~(tujuh) tahun, ~~-~~dan dikenakan ~~-~~denda sebesar 2 (dua) kali dari nilai kerugian yang ditimbulkannya~~:~~.

Pasal ~~13~~ 14

Mengubah dan Memalsukan Data

Barangsiapa~~Setiap orang yang~~ dengan sengaja ~~–~~dan ~~–~~melawan hukum ~~–~~mengubah, menghapus, atau menghilangkan sebagian data komputer asli, yang mengakibatkan hilangnya keaslian data dan menggunakan data yang tidak asli untuk melakukan ~~kegiatan~~ kegiatan dan atau ~~/~~keperluan lain yang sah, dikategorikan sebagai tindak pemalsuan, dan dipidana penjara paling singkat minimal 2 (dua) tahun dan paling lama 5 (lima) tahun.

Pasal 15~~4~~

Mengubah Data Yang Merugikan Orang Lain

Barangsiapa ~~Setiap orang yang~~ dengan sengaja ~~-~~dan dan melawan hukum, memasukkan, mengubah, menghapus, atau menghilangkan sebagian data komputer atau mengganggu sistem komputer, yang menimbulkan kerugian bagi orang lain, dipidana penjara paling singkat 3 (tiga) tahun dan paling lama 7 (tujuh) tahun, dan dikenakan denda sedikit-dikitnya 3 (tiga) kali dari nilai kerugian yang ditimbulkan.

Pasal 16

Perbuatan Asusila~~5~~

Barangsiapa~~Setiap orang yang~~ dengan sengaja dan secara melawan hukum memanfaatkan teknologi informasi untuk menyebarkan gambar, tulisan atau secara bersamaan dari keduanya yang mengandung sifat – sifat pornografi, melakukan tindakan sebagaimana dimaksud pasal 281, 282 dan pasal 283 Kitab Undang-Undang Hukum Pidana, sehingga memenuhi ketentuan Pasal 281, 282, 283 KUHP, dipidana penjara paling singkat 3 (tiga) tahun dan paling lama 7 (tujuh) tahun.

Pasal 17~~6~~

Pornografi Anak - anak

Barangsiapa~~Setiap orang yang~~ dengan sengaja ~~—~~dan secara melawan hukum memanfaatkan ~~-~~T~~t~~eknologi I~~i~~nformasi untuk menyimpan, memproduksi, menyebarkan, atau menawarkan bahan – bahan atau informasi yang bersifat pornografi dengan menggunakan anak – anak sebagai model dan atau sasarannya, dipidana penjara paling singkat 5 (lima) tahun dan paling lama 15 (lima belas) tahun.~~.~~

Pasal 18~~7~~

Bantuan Kejahatan

Barangsiapa~~Setiap orang yang~~ dengan sengaja ~~-~~memanfaatkan ~~-~~T~~t~~eknologi I~~i~~nformasi untuk membantu terjadinya percobaan, atau persekongkolan yang menjurus pada kejahatan, dipidana penjara 2 (dua) tahun dan paling lama 5 (lima) tahun, atau denda sedikit-dikitnya Rp. 200.000.000,- (dua ratus juta rupiah) dan sebanyak-banyaknya Rp. 1.000.000.000,- (satu milyar rupiah).

Pasal 1~~9~~8

Mengakses Tanpa Hak Terhadap Komputer Yang Dilindungi

Barangsiapa~~Setiap orang yang~~ dengan sengaja dan secara melawan hukum ~~-~~melakukan akses melalui komputer tertentu yang statusnya dilindungi oleh pihak yang berwenang atau melanggar hak akses yang diberikan atau tidak diberikan kepadanya, dengan maksud untuk mencuri atau memperoleh sesuatu yang bukan merupakan haknya, dipidana penjara paling singkat 5 (lima) tahun dan paling lama 12 (dua belas) tahun atau denda sedikit – dikitnya Rp. 1.000.000.000,- (satu milyar rupiah) dan sebanyak-banyaknya Rp. 2.500.000.000,-(dua milyar lima ratus jut arupiah).

Pasal 20~~19~~

Teror

Barangsiapa~~Setiap orang yang~~ dengan sengaja dan secara melawan hukum memanfaatkan ~~-~~Tteknologi Iinformasi untuk melakukan teror, sehingga memenuhi ketentuan tindak pidana terorisme dimaksud dalam Undang-Undang Pemberantasan Tindak Pidana Terorisme, dipidana penjara paling singkat 10 (sepuluh) tahun dan paling lama 30 (tiga puluh) tahun, atau setidak-tidaknya dipidana sesuai Ketentuan yang berlaku dalam Undang-Undang Pemberantasan Tindak Pidana Terorisme.

Bab VI~~-~~I

Tindak Pidana Yang Berkaitan Dengan Teknologi Informasi Sebagai Sasarannya

Pasal 21~~0~~

Intersepsi

Barangsiapa~~Setiap orang yang~~ dengan sengaja dan melawan hukum melakukan intersepsi tanpa hak, secara tidak sah, atau ilegal, dipidana penjara paaling singkat 2 (dua) tahun dan paling lama 5 (lima) tahun.

Pasal 2~~2~~1

Merusak Situs Internet

1. Barangsiapa~~Setiap orang yang~~ dengan sengaja ~~-~~terbukti merusak situs Internet milik orang atau badan hukum lain, yang menimbulkan kerugian material bagi orang atau badan hukum lain tersebut dipidana penjara paling ~~-~~singkat ~~-~~1 (satu) tahun dan paling lama 5 (lima) tahun.
2. Apabila situs Internet yang dirusak dimaksud ayat (1) pasal ini, milik pemerintah, militer atau situs Internet lain yang termasuk dilindungi oleh pihak yang berwenang, dipidana penjara paling singkat 5 (lima) tahun dan paling lama 7 (tujuh) tahun.

Pasal 2~~3~~2

Penyadapan Terhadap Jaringan Komunikasi Data

Barangsiapa~~Setiap orang yang~~ dengan sengaja dan melawan hukum ~~-~~terbukti ~~-~~melakukan penyadapan terhadap jaringan komunikasi data atau sistem komputer yang terhubung dalam jaringan komputer lokal maupun global (Internet), yang selanjutnya digunakan untuk kepentingan sendiri atau untuk kepentingan pihak ~~orang~~ lain~~-~~, dipidana penjara paling singkat ~~-~~2 ~~-~~(dua) tahun dan paling lama 5 (lima) tahun..

Pasal 2~~4~~3

Pemalsuan Nomor Internet Protocol

Barangsiapa~~Setiap orang yang~~ dengan sengaja memalsukan nomor Internet Protocol yang digunakan untuk berkomunikasi dengan orang atau badan hukum lain~~lain~~, yang menimbulkan kerugian material bagi orang atau badang hukum lain dipidana penjara paling singkat 2 (dua) tahun dan paling lama 5 (lima) tahun.~~.~~

Pasal 2~~5~~4

Merusak Database atau Enkripsi

Barangsiapa~~Setiap orang yang~~ dengan sengaja mengacaukan atau membuat sistem komputer tidak dapat berfungsi sebagaimana mestinya dengan cara merusak data base

atau teknologi enkripsi, pada sistem komputer tersebut, dipidana penjara paling singkat 3 (tiga) tahun dan paling lama 7 (tujuh) tahun.

.

Pasal 2~~6~~5

Penggunaan Nama Domain Tidak Sah

Barangsiapa~~Setiap orang yang~~ dengan sengaja dan secara melawan hukum menggunakan nama domain milik orang atau badan hukum lain, yang menimbulkan kerugian material bagi orang atau badan hukum lain atau bagi pemiliknya yang sah, ~~–~~dipidana penjara paling singkat 2 (dua) tahun dan paling paling lama 5 (lima) tahun.

Pasal 2~~7~~6

Penyalah-gunaan Surat Elektronik

1. Barangsiapa~~Setiap orang yang~~ dengan sengaja dan melawan hukum menggunakan surat elektronik untuk mengumumkan, menawarkan atau menjual barang dan atau jasa yang sifatnya melanggar hukum atau dilarang oleh Undang-Undang, dipidana penjara paling singkat 1 (satu) tahun dan paling lama 3 (tiga) tahun.
2. Barangsiapa~~Setiap orang yang~~ dengan sengaja dan melawan hukum memalsukan atau menggunakan alamat surat elektronik milik orang atau badang hukum lain tanpa seijin dari orang atau badan hukum tersebut, dipidana penjara paling singkat 1(satu) tahun dan paling lama 5 (lima) tahun..

Pasal 2~~8~~

Pelanggaran Hak Cipta~~7~~

Barangsiapa~~Setiap orang yang~~ dengan sengaja ~~–~~dan melawan hukum ~~–~~memanfaatkan T~~t~~eknologi I~~i~~nformasi yang dimaksudkan untuk melanggar hak cipta ~~-~~sebagaimana diatur dalam Undang – Undang Hak Cipta, dipidana penjara paling singkat 5 (lima) tahun dan paling lama 10 (sepuluh) tahun atau setidak-tidaknya sesuai ketentuan yang berlaku dalam Undang-Undang Hak Cipta.

Pasal 29

Pelanggaran Hak Privasi~~8~~

Barangsiapa~~Setiap orang yang~~ dengan sengaja dan melawan hukum memanfaatkan T~~t~~eknologi I~~i~~nformasi untuk mengganggu hak privasi individu dengan cara menyebarkan data pribadi tanpa seijin yang bersangkutan, dipidana penjara paling singkat 3 (tiga) tahun dan paling lama 7 (tujuh) tahun.

~~**Pasal 29**~~

~~Setiap orang yang dengan sengaja menyalah gunakan peralatan teknologi informasi di luar peruntukkannya, yang dapat menimbulkan kerugian bagi orang lain, dipidana penjara paling singkat 2 (dua) tahun dan paling lama 5 (lima) tahun..~~

Bab VII~~I~~

Penyidikan, Penuntutan dan Pemeriksaan di Sidang Pengadilan

Pasal 30

1. Penyidikan, penuntutan dan pemeriksaan di sidang Pengadilan dalam tindak pidana pemanfaatan T~~t~~eknologi I~~i~~nformasi, dilakukan berdasarkan Hukum Acara yang berlaku, kecuali ditentukan lain dalam Undang-Undang ini.
2. Untuk kepentingan penyidikan dan penuntutan, penyidik diberi wewenang untuk melakukan penahanan terhadap tersangka paling lama 6 (enam) bulan.
3. Dalam kasus ayat (2) di atas jika dipandang perlu penyidik dapat meminta ekstradisi tersangka pelaku tindak pidana kepada negara di mana tersangka berdomisili

Formatted: Bullets and Numbering

Pasal 31

~~1.~~Untuk memperoleh bukti yang cukup, penyidik dapat menggunakan setiap laporan intelijen dari kepolisian, kejaksaan, Direktorat Jendral Imigrasi, Direktorat Jendral Bea Cukai, Tentara Nasional Indonesia, Badan Intelijen Negara, Departemen Luar Negeri, Departemen Dalam Negeri atau Instansi lain yang terkait

Formatted: Bullets and Numbering

~~2.Dalam kasus ayat (3) di atas jika dipandang perlu penyidik dapat meminta ekstradisi tersangka pelaku tindak pidana kepada negara di mana tersangka berdomisili.~~

Pasal 32

1. Selain Penyidik Pejabat Polisi Negara Republik Indonesia, Pejabat Pegawai Negeri Sipil tertentu di lingkungan Departemen atau Kementrian yang lingkup tugas dan tanggung jawabnya di bidang Tteknologi Iinformasi diberi kewenangan khusus sebagai Penyidik Pegawai Negeri Sipil sebagaimana dimaksud dalam Undang – Undang Hukum Acara Pidana. Untuk melakukan penyidikan tindak pidana pemanfaatan Tteknologi Iinformasi
2. Penyidik sebagaimana dimaksud dalam ayat (1) pasal ini mempunyai wewenang:
   a. menerima laporan atau pengaduan dari seseorang atau badan hukum tentang adanya tindak pidana pemanfaatan Tteknologi Iinformasi;
   b. melakukan pemeriksaan atas kebenaran laporan atau keterangan berkenaan dengan tindak pidana pemanfaatan Tteknologi Iinformasi;
   c. melakukan penangkapan terhadap orang, badan usaha atau badan hukum yang diduga melakukan tindak pidana di bidang Tteknologi Iinformasi;
   d. melakukan pemeriksaan terhadap alat dan atau sarana yang berkaitan dengan pemanfaatan Tteknologi Iinformasi yang diduga digunakan untuk melakukan tindak pidana pemanfaatan ~~teknologi~~ Teknologi Iinformasi;
   e. menghentikan penggunaan alat dan atau sarana kegiatan pemanfaatan Tteknologi Iinformasi yang menyimpang dari ketentuan yang berlaku;
   f. meminta keterangan dan menetapkan barang bukti sehubungan dengan tindak pidana pemanfaatan Tteknologi Iinformasi;
   g. memanggil orang untuk didengar dan atau diperiksa sebagai tersangka atau saksi sehubungan dengan tindak pidana pemanfaatan Tteknologi Iinformasi;
   h. melakukan pemeriksanaan terhadap tempat tertentu yang diduga digunakan sebagai tempat untuk melakukan tindak pidana pemanfaatan Tteknologi Iinformasi;
   i. menyegel atau menyita alat dan atau sarana yang diduga digunakan untuk melakukan tindak pidana pemanfaatan Tteknologi Iinformasi;

j. meminta bantuan ahli yang diperlukan dalam penyidikan terhadap tindak pidana pemanfaatan Tteknologi Iinformasi;
k. mengadakan penghentian penyidikan tindak pidana pemanfaatan Tteknologi Iinformasi;
l. mengadakan tindakan lain menurut hukum yang bertanggung jawab.

3. Penyidik Pegawai Negeri Sipil sebagaimana dimaksud dalam ayat (1) dalam melaksanakan tugasnya memberitahukan dimulainya penyidikan dan melaporkan hasil penyidikannya kepada Penyidik Pejabat Polisi Negara Republik Indonesia.
4. Kewenangan penyidikan sebagaimana dimaksud dalam ayat (2) dilaksanakan sesuai dengan ketentuan Undang – Undang tentang Hukum Acara Pidana.

Pasal 33

1. Selain alat bukti yang sudah diatur dalam Undang-Undang Hukum Acara Pidana, catatan elektronik yang tersimpan dalam sistem komputer merupakan alat bukti yang sah.
2. Catatan elektronik dalam ayat (1), yang akan dijadikan alat bukti sah di pengadilan wajib dikumpulkan oleh penyidik dengan mengikuti prosedur sesuai ketentuan yang berlaku.
3. Selain catatan elektronik dimaksud ayat (2), maka dapat digunakan sebagai alat bukti meliputi :
   a. Informasi yang diucapkan, dikirimkan, diterima atau disimpan secara elektronik atau yang serupa dengan itu.
   b. Data, rekaman atau informasi yang dapat dilihat, dibaca dan atau didengar, yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang di atas kertas, benda fisik apapun selain kertas, atau yang terekam secara elektronik, termasuk tetapi tidak terbatas pada :
      1). -Tulisan, suara atau gambar;
      2). -Peta, rancangan, foto atau sejenisnya;
      3).– Huruf, tanda, angka, simbol atau perforasi yang memiliki makna atau dapat dipahami oleh orang yang mampu membaca atau memahaminya;

c. Alat bukti elektronik, khususnya yang berwujud perangkat lunak diperoleh dengan cara penggandaan dari lokasi asalnya dengan cara tertentu tanpa merusak struktur logika program.

4. Prosedur pengumpulan dan perolehan alat bukti elektronik ditetapkan dengan Peraturan Pemerintah.

Pasal 34

Penyidik dapat melakukan penangkapan terhadap setiap orang yang diduga keras melakukan tindak pidana pemanfaatan Tteknologi Iinformasi berdasarkan bukti permulaan -yang cukup .

Pasal 35

1. Penyidik, penuntut umum atau hakim berwenang memerintahkan kepada bank dan lembaga jasa keuangan untuk melakukan pemblokiran terhadap rekening bank dan atau harta kekayaan setiap orang yang diketahui atau patut diduga merupakan hasil tindak pidana Tteknologi Iinformasi.
2. Perintah penyidik, penuntut umum atau hakim sebagaimana dimaksud dalam ayat (1) harus dilakukan secara tertulis dengan menyebutkan secara jelas mengenai :
   a. Nama -dan jabatan penyidik, penuntut umum atau hakim;
   b. Identitas setiap orang yang telah dilaporkan oleh bank dan lembaga jasa keuangan kepada penyidik, tersangka atau terdakwa;
   c. Alasan pemblokiran;
   d. Tindak pidana yang disangkakan atau didakwakan, dan
   e. Tempat harta kekayaan berada;
3. Bank dan lembaga jasa keuangan setelah menerima perintah penyidik, penuntut umum, atau hakim sebagaimana dimaksud dalam ayat (2) wajib melaksanakan pemblokiran sesaat setelah surat perintah pemblokiran diterima;
4. Bank dan lembaga jasa keuangan wajib menyerahkan Berita Acara pelaksanaan pemblokiran kepada penyidik, penuntut umum atau paling lambat 1 (satu) hari kerja terhitung sejak tanggal pelaksanaan pemblokiran;

5. Harta kekayaan yang diblokir harus tetap berada pada bank dan atau lembaga jasa keuangan yang bersangkutan.
6. Bank dan atau lembaga jasa keuangan yang melanggar ketentuan sebagaimana dimaksud dalam ayat (3) dan ayat(4) dikenakan sanksi administratif sesuai dengan peraturan perundang-undangan yang berlaku..

Pasal 36

1. Untuk kepentingan pemeriksaan dalam perkara tindak pidana pemanfaatan Ttekhnologi Iinformasi; penyidik, penuntut umum atau hakim berwenang untuk meminta keterangan dari bank dan atau lembaga jasa keuangan mengenai harta kekayaan setiap orang yang diketahui atau patut diduga melakukan tindak pidana pemanfaatan tekhnologi informasi.
2. Dalam meminta keterangan sebagaimana dimaksud dalam ayat (1) terhadap penyidik, penuntut umum atau hakim tidak berlaku ketentuan Undang-Undang yang mengatur tentang rahasia bank dan kerahasiaan transaksi keuangan lainnya.
3. Permintaan keterangan harus diajukan secara tertulis dengan menyebutkan secara jelas mengenai:
   a. Nama dan jabatan penyidik, penuntut umum atau hakim;
   b. Identitas setiap orang yang ddiketahui atau patut diduga melakukan tindak pidana pemanfaatan tekhnologi informasi.
   c. Tindak pidana yang disangkakan atau didakwakan;
4. Surat permintaan untuk memperoleh keterangan sebagaimana dimaksud dalam ayat (1) dan ayat (2) harus ditandatangani oleh :
   a. Kepala Kepolisian Daerah dalam hal permintaan diajukan oleh penyidik;
   b. Kepala Kejaksaan Tinggi dalam hal permintaan diajukan oleh penuntut umum;
   c. Hakim Ketua majelis yang memeriksa perkara yang bersangkutan;

Pasal 37

1. Berdasarkan bukti yang cukup sebagaimana dimaksud pasal 34, penyidik berhak :

a. Membuka, memeriksa dan menyita surat dan kiriman melalui pos atau jasa pengiriman lainnya yang mempunyai hubungan dengan perkara tindak pidana pemanfaatan Tteknologi Iinformasi yang sedang diperiksa;
b. Menyadap pembicaraan melalui telepon atau alat komunikasi lain yang diduga digunakan untuk mempersiapkan, merencanakan dan melakukan tindak pidana pemanfaatan Tteknologi Iinformasi;
c. Menyita perangkat elektronik yang diduga digunakan untuk mempersiapkan, merencanakan dan melakukan tindak pidana pemanfaatan Tteknologi Iinformasi;

2. Tindakan penyadapan sebagaimana dimaksud ayat (1) butir b, hanya dapat dilakukan atas perintah Ketua Pengadilan Negeri untuk jangka waktu paling lama 60 (enam puluh) hari;

Pasal 38

1. Dalam pemeriksaan, saksi memberikan keterangan terhadap apa yang dilihat dan dialami sendiri dengan bebas dan tanpa tekanan.
2. Dalam penyidikan dan pemeriksaan di sidang pengadilan, saksi dan orang lain yang bersangkutan dengan tindak pidana pemanfaatan Tteknologi Iinformasi, dilarang menyebutkan nama atau alamat pelapor atau hal-hal lain yang memberikan kemungkinan dapat diketahuinya identitas pelapor.
3. Sebelum pemeriksaan dilakukan, larangan sebagaimana dimaksud dalam ayat (2) diberitahukan kepada saksi dan orang lain tersebut.

Pasal 39

1. Apabila terdakwa telah dipanggil secara sah dan patut, namun tidak hadir di sidang pengadilan tanpa alasan yang sah, maka perkara dapat diperiksa dan diputus tanpa hadirnya terdakwa;

2. Dalam hal terdakwa hadir pada sidang berikutnya sebelum putusan dijatuhkan, maka terdakwa wajib diperiksa, dan segala keterangan saksi dan surat-surat yang dibacakan dalam sidang sebelumnya dianggap sebagai diucapkan dalam sidang sekarang;
3. Putusan yang dijatuhkan tanpa kehadiran terdakwa diumumkan oleh penuntut umum pada pengumuman pengadilan, atau diberitahukan kepada kuasanya.
4. Terdakwa atau kuasanya dapat mengajukan banding atas putusan dimaksud dalam ayat (1).
5. Apabila terdakwa meninggal dunia sebelum putusan dijatuhkan dan terdapat bukti yang cukup kuat bahwa yang bersangkutan telah melakukan tindak pidana pemanfaatkan teknologi informasi, maka hakim atas tuntutan penuntut umum menetapkan penyitaan terhadap harta kekayaannya;
6. Penetapan penyitaan sebagaimana dimaksud ayat (5) tidak dapat dimohonkan upaya hukum;
7. Setiap orang atau badan hukum yang berkepentingan dapat mengajukan keberatan kepada Pengadilan yang telah menjatuhkan penetapan dimaksud ayat (5), dalam waktu 30 (tiga puluh) hari terhitung sejak tanggal pengumuman sebagaimana dimaksud dalam ayat (3).

BAB ~~V~~IX~~H~~
Ganti rugi dan Rehabilitasi

Pasal 40

1. Setiap korban akibat tindak pidana pemanfaatan teknologi informasi ~~–~~berhak memperoleh ~~ndapatkan~~ ganti rugi sepanjang diatur dalam Undang – Undang atau ketentuan lain yang sah;
2. Ganti rugi sebagaimana dimaksud ayat (1) dibebankan kepada pelaku tindak pidana;
3. Ganti rugi dimaksud diberikan dan dicantumkan dalam amar putusan Pengadilan.

Pasal 41

1. Setiap orang berhak memperoleh rehabilitasi apabila oleh pengadilan diputus bebas atau diputus lepas dari segala tuntutan hukum yang putusannya telah mempunyai kekuatan hukum tetap.
2. Rehabilitasi tersebut diberikan dan dicantumkan sekaligus dalam putusan pengadilan sebagaimana dimaksud ayat (1).

Pasal 42

1. Pengajuan ganti rugi dilakukan oleh korban atau kuasanya kepada pelaku atau pihak ketiga atau kepada Pengadilan Negeri sesuai prosedur yang berlaku dan berdasarkan amar putusan.
2. Pengajuan rehabilitasi dilakukan oleh korban kepada Menteri Kehakiman dan Hak Asasi Manusia;

Pasal 43

1. Pelaku sebagaimana dimaksud pasal 42 ayat (1) wajib melaksanakan pemberian ganti rugi, paling lambat 60 (enam puluh) hari kalender terhitung sejak penerimaan permohonan.
2. Pelaksanaan pemberian ganti rugi dilaporkan oleh pelaku kepada Ketua Pengadilan yang memutuskan perkara, disertai dengan tanda bukti pelaksanaan pemberian ganti rugi tersebut.
3. Salinan tanda bukti pelaksanaan pemberian ganti rugi sebagaimana dimaksud ayat (1) disampaikan kepada korban atau keluarga korban yang merupakan ahli waris.
4. Setelah Ketua Pengadilan menerima tanda bukti sebagaimana dimaksud ayat(1), Ketua Pengadilan mengumumkan pelaksanaan tersebut pada papan pengumuman pengadilan yang bersangkutan;
5. Apabila pelaksanaan pemberian ganti rugi kepada pihak korban melampaui batas waktu sebagaimana dimaksud dalam ayat (1), korban atau keluarga korban yang merupakan ahli warisnya dapat melaporkan hal tersebut kepada pengadilan.

6. Pengadilan sebagaimana dimaksud ayat (1) segera memerintahkan pelaku untuk melaksanakan putusan tersebut paling lambat 30 (tiga puluh) hari kalender terhitung sejak tanggal perintah tersebut diterima.

Pasal 44

Apabila ganti rugi dilakukan secara bertahap, maka setiap tahapan pelaksanaan atau keterlambatan pelaksanaan harus dilaporkan kepada Pengadilan.

Bab ~~I~~X

Ketentuan Penutup

Pasal 45

Undang – undang ini berlaku mulai pada tanggal diundangkan. Agar supaya setiap orang mengetahuinya, memerintahkan pengundangan undang – undang ini dengan penempatannya dalam Lembaran Negara Republik Indonesia.

Ditetapkan di Jakarta
Pada tanggal : …….
PRESIDEN REPUBLIK INDONESIA
Ttd
……..

Diundangkan di Jakarta
Pada tanggal : ……..
SEKRETARIS NEGARA REPUBLIK INDONESIA
Ttd
…….

LEMBARAN NEGARA REPUBLIK INDONESIA TAHUN ……. NOMOR……

Penjelasan Atas Rancangan Undang – Undang

Nomor Tahun

Tentang

Tindak Pidana Di Bidang Teknologi Informasi

Umum

Pembangunan nasional berupaya mewujudkan masyarakat adil dan makmur yang merata material dan spiritual berdasarkan Pancasila dan Undang – Undang Dasar 1945. Salah satu sarana untuk mewujudkan masyarakat sejahtera sebagaimana diamanatkan dalam Pancasila dan Undang – Undang Dasar 1945 adalah pemanfaatan tteknologi khususnya ~~teknologi~~ Teknologi Iinformasi secara aman, optimal, merata dan menyebar ke seluruh lapisan warga negara Indonesia.

Kemajuan Tteknologi Iinformasi di samping telah memberikan kemaslahatan terhadap masyarakat di sisi lain juga menimbulkan kekhawatiran karena adanya penggunaan yang menyimpang dari tujuan sebenarnya. Agar peluang kerugian yang ditimbulkan oleh adanya pemanfaatan teknologi informasi yang tidak semestinya, dibutuhkan perangkat peraturan dan perundangan yang membatasi sekaligus menghukum penggunaan Tteknologi Iinformasi untuk kejahatan.

Kejahatan dalam bidang Tteknologi Iinformasi secara umum terdiri dari dua kelompok. Pertama, kejahatan biasa yang menggunakan teknologi informasi sebagai alat bantunya. Dalam kejahatan ini, terjadi peningkatan modus dan operandi dari semula menggunakan peralatan biasa, sekarang telah memanfaatkan Tteknologi Iinformasi. Dampak dari kejahatan biasa yang telah menggunakan Tteknologi Iinformasi ternyata cukup serius, terutama bila dilihat dari jangkauan dan nilai kerugian yang ditimbulkan oleh kejahatan tersebut. Pencurian uang atau pembelian barang menggunakan kartu kredit curian melalui media Internet dapat menelan korban di wilayah hukum negara lain, suatu hal yang jarang terjadi dalam kejahatan konvensional. Kedua, kejahatan yang muncul setelah adanya Internet, di mana sistem komputer sebagai korbannya. Jenis kejahatan

dalam kelompok ini makin bertambah seiring dengan kemajuan teknologi informasi itu sendiri. Salah satu contoh yang termasuk dalam kejahatan kelompok kedua adalah perusakan situs Internet, pengiriman virus atau program – program komputer yang tujuannya merusak sistem kerja komputer tujuan.

Kesulitan yang banyak dihadapi dengan perangkat perudangan yang selama ini berlaku antara lain ada pada penindakan terhadap kejahatan jenis kedua, yang ternyata belum diatur dalam KUHP. Kesulitan berikutnya adalah pada pengumpulan dan penyajian barang bukti yang sah di pengadilan. Sistem hukum harus dapat mengakui catatan transaksi elektronik sebagai alat bukti yang sah di pengadilan.

Pasal 1

Cukup jelas

Pasal 2

Undang – undang ini dimaksudkan sebagai pendamping KUHP ketika terjadi tindak pidana di bidang teknologi informasi yang penyidikan, pembuktian, dan penuntutannya tidak dapat sepenuhnya menggunakan KUHP. Lebih khusus, undang – undang ini digunakan untuk menghukum tindak pidana konvensional di mana penggunaan teknologi informasi cukup menonjol dalam kejahatan tersebut, atau tindak pidana dengan teknologi informasi sebagai sasarannya.

Pasal 3

Butir 1. s.d. 8 : Cukup jelas.

Butir 9: dengan berlakunya undang – undang ini, perusahaan penyelenggara akses Internet, atau penyelenggara layanan teknologi informasi baik yangmelayani keperluan sendiri maupun keperluan komersial diwajibkan memelihara catatan transaksi elektronik dalam suatu data base atau *transaction log file* secara periodik, sekurang – kurangnya untuk masa dua tahun yang telah lewat. Pemeliharaan *transaction log file* ini dimaksudkan untuk memudahkan bagi penyidik untuk memperoleh bukti – bukti elektronik, ketika terjadi tindak pidana yang terjadi pada atau secara tidak sengaja

melibatkan perusahaan penyelenggara akses Internet, atau penyelenggara layanan teknologi informasi.

Pasal 4

Cukup jelas

Pasal 5

Pasal ini adalah pasal koneksitas, jika pencurian yang diancam dengan pasal 362 KUHP terbukti menggunakan teknologi informasi, maka terhadap pencurian tersebut dapat dituntut dengan pasal ini.

Pasal 6

Cukup jelas

Pasal 7

Sistem informasi dan peralatan teknologi informasi milik atau yang dioperasikan oleh instansi pemerintah, militer, perbankan, dan instansi lain yang tergolong strategis adalah termasuk sistem informasi dan peralatan teknologi informasi yang dilindungi (*protected computers*). Status sebagai sistem informasi yang dilindungi diberikan oleh pemerintah melalui Peraturan Pemerintah.

Pasal 8

Cukup jelas

Pasal 9

Cukup jelas

Pasal 10

Cukup jelas

Pasal 11

Pasal ini adalah pasal koneksitas, jika pidana pornografi yang dilakukan terbukti menggunakan teknologi informasi, maka terhadap pidana pornografi tersebut diancam menggunakan undang – undang ini.

Pasal 12

Cukup jelas

Pasal 13

Cukup jelas

Pasal 14

Cukup jelas

Pasal 15

Cukup jelas

Pasal 16

Cukup jelas

Pasal 17

Cukup jelas

Pasal 18

Cukup jelas

Pasal 19

Cukup jelas

Pasal 20

Cukup jelas

Pasal 21

Cukup jelas

Pasal 22

Cukup jelas

Pasal 23

Cukup jelas

Pasal 24

Cukup jelas

Pasal 25

Cukup jelas

Pasal 26

Cukup jelas

Pasal 27

Cukup jelas

Pasal 28

Cukup jelas

Pasal 29

Cukup jelas

Pasal 30

Cukup jelas

Pasal 31

Cukup jelas

Pasal 32

Cukup jelas

Pasal 33

Cukup jelas

Pasal 34

Cukup jelas

Pasal 35

Cukup jelas

Pasal 36

Cukup jelas

Pasal 37

Cukup jelas

Pasal 38

Cukup jelas

Pasal 39

Cukup jelas

Pasal 40

Cukup jelas

Pasal 41

Cukup jelas

Pasal 42

Cukup jelas

Pasal 43

Cukup jelas

Pasal 44

Cukup jelas

Pasal 45

Cukup jelas

*****