BAB II
TINJAUAN PUSTAKA

2.1 Pengertian dan Perkembangan Hukum Pembuktian Tentang Data Elektronik

Seiring dengan perkembangan masyarakat dan teknologi, semakin lama manusia semakin banyak menggunakan alat teknologi digital, termasuk dalam berinteraksi antarsesamanya. Oleh karena itu, semakin lama semakin kuat desakan terhadap hukum, termasuk hukum pembuktian, untuk menghadapi kenyataan perkembangan masyarakat seperti itu. Sebagai contoh, untuk mengatur sejauh mana kekuatan pembuktian dari suatu tanda tangan digital/elektronik, yang dewasa ini sudah sangat banyak dipergunakan dalam praktik sehari-hari.[34]

Dalam hal ini, posisi hukum pembuktian seperti biasanya akan berada dalam posisi dilematis sehingga dibutuhkan jalan-jalan kompromistis. Di satu pihak, agar hukum selalu dapat mengikuti perkembangan zaman dan teknologi, perlu pengakuan hukum terhadap berbagai jenis perkembangan teknologi digital untuk benfungsi sebagai alat bukti di pengadilan. Akan tetapi, di lain pihak kecenderungan terjadi rnanipulasi penggunaan alat bukti digital oleh pihak-pihak yang tidak bertanggung jawab menyebabkan hukum tidak bebas dalam mengakui alat bukti digital tersebut.

[34] Munir Fuady, *Teori Hukum Pembuktian: Pidana dan Perdata*, (Bandung: PT. Citra Aditya Bakti, 2012), hlm 151.

Bahkan, mengikuti teori klasik dalam hukum pembuktian yang disebut dengan "hukum alat bukti terbaik "(*best evidence rule*), suatu alat bukti digital sulit diterima dalam pembuktian.

The best evidence rule[35] mengajarkan bahwa suatu pembuktian terhadap isi yang substansial dari suatu dokumen/ *photograph* atau rekaman harus dilakukan dengan membawa ke pengadilan dokumen/ *photograph* atau rekaman asli tersebut. Kecuali jika dokumen/ *photograph* atau rekaman tersebut memang tidak ada, dan ketidakberadaannya bukan terjadi karena kesalahan yang serius dari pihak yang harus membuktikan. Dengan demikian, menurut doktrin *best evidence* ini, fotokopi (bukan asli) dari suatu surat tidak mempunyai kekuatan pembuktian di pengadilan. Demikian juga dengan bukti digital, seperti *e-mail*, surat dengan mesin faksimile, tanda tangan elektronik, tidak ada aslinya atau setidak-tidaknya tidak mungkin dibawa aslinya ke pengadilan sehingga hal ini mengakibatkan permasalahan hukum yang serius dalam bidang hukurn pembuktian.[36]

Pemakaian internet dan bisnis melalui internet dewasa ini berkembang sangat pesat sehingga sektor hukum pun, termasuk hukum pembuktian, diminta untuk turun tangan sehingga bisnis melalui internet seperti itu dapat dicapai ketertiban dan kepastian, di samping tercapai pula unsure keadilan bagi para pihak. Berbisnis lewat internet (dengan menggunakan perangkat elektronik) ini sering disebut dengan *electronic commerce* (*e-commerce*) atau *electronic business* (*e-business*).

[35] *Ibid.*
[36] *Ibid,* hlm 152.

Menurut Munir Fuady, yang dimaksud dengan istilah *e-commerce* adalah suatu proses berbisnis dengan memakai teknologi elektronik yang menghubungkan antara perusahaan, konsumen, dan masyarakat dalam bentuk transaksi elektronik, dan pertukaran/ penjualan barang, servis, dan informasi secara elektronik. Dengan demikian, pada prinsipnya bisnis dengan *e-commerce* merupakan kegiatan bisnis tanpa warkat (*paperless trading*).[37]

Antara istilah *e-commerce* dan istilah *e-business* sering dipertukarkan meskipun sebenarnya terdapat perbedaan yang prinsipil di antara kedua istilah tersebut. Istilah e-commerce dalam arti sempit diartikan sebagai suatu transaksi jual beli atas suatu produk barang, jasa atau informasi antarmitra bisnis dengan memakai jaringan komputer yang berbasiskan pada internet. Adapun *e-commerce* dalam arti luas diartikan sama dengan istilah *e-business,* yakni tidak hanya mencakup transaksi online, tetapi juga termasuk layanan pelanggan, hubungan dagang dengan mitra bisnis, dan transaksi internal dalam sebuah organisasi.[38]

Kegiatan *e-commerce* dilakukan dengan orientasi-orientasi sebagai berikut:[39]

1. Pembelian *on line (on line transaction).*
2. Komunikasi digital (*digital communication*), yaitu suatu komunikasi secara elektronik.
3. Penyediaan jasa (*service*), yang menyediakan informasi tentang kualitas produk dan informasi instan terkini.

[37] *Ibid,* hlm 152.
[38] *Ibid.*
[39] *Loc.cit*

4. Proses bisnis, yang merupakan sistem dengan sasaran untuk meningkatkan otomatisasi proses bisnis.
5. *Market of one*, yang memungkinkan proses *customization* produk dan jasa untuk diadaptasikan pada kebutuhan bisnis.[40]

Apabila ditinjau dari sudut para pihak dalam bisnis *e-commerce*, yang merupakan jenis-jenis transaksi dari suatu kegiatan *e-commerce* adalah sebagai berikut:[41]

1. *Business to business* (B2B). (bisnis ke bisnis)
2. *Business to consumer* (B2C). (bisnis ke konsumen)
3. *Consumer to consumer* (C2C). (konsumen ke konsumen)
4. *Consumer to business* (C2B). (konsumen ke bisnis
5. *Non-business electronic commerce*. (bukan bisnis perdagangan elektronik)
6. *Intrabusiness (organizational) electronic commerce*. (organisasi perdagangan elektonik.

Berikut ini penjelasan dari masing-masing jenis transaksi *e-commerce* tersebut, yakni:

1. *Business to Business* (B2B) (bisnis ke bisnis)

Transaksi *business to business* (B2B) ini merupakan bisnis *e-commerce* yang paling banyak dilakukan. *Business to business* (B2B) ini terdiri atas:

a. Transaksi *inter-organizational systems* (IOS) (sistem antar organisasi), misalnya, *electronic funds transfer* (transfer dana elektronik), *electronic forms* (formulir elektronik), *integrated messaging* (pesan terpadu), *share data based*

[40] *Ibid,* hlm 153.
[41] *Ibid.*

(basis data saham), *supply chain management* (manajemen pasokan), dan lain-lain.

b. Transaksi pasar elektronik (*electronic market transaction*).

2. *Business to Consumer* (B2C)

Business to consumer (B2C) merupakan transaksi ritel dengan pembeli individual.

3. *Consumer to Consumer*(C2C)

Consumer to consumer (C2C) merupakan transaksi di mana konsumen menjual produk secara langsung kepada konsumen lainnya. Juga, seorang individu yang mengiklankan produk, baik berupa barang, jasa, pengetahuan, maupun keahliannya di salah satu situs lelang.

4. *Consumer to Business* (C2B)

Consumer to business (C2B) rnerupakan individu yang menjual produk atau jasa kepada organisasi dan individu yang mencari penjual dan melakukan transaksi.

5. Nonbusiness Electronic Commerce

Dalam hal ini, *nonbusiness electronic commerce* meliputi kegiatan nonbisnis, seperti kegiatan lembaga pendidikan, organisasi nirlaba, keagamaan, dan lain-lain.

6. Intrabusiness (Organizational) Electronic Commerce

Kegiatan ini meliputi semua aktivitas internal organisasi melalui internet untuk melakukan pertukaran barang, jasa dan informasi, menjual produk perusahaan kepada karyawan, dan lain-lain.[42]

Salah satu yang sangat menjadi masalah hukum tentang *e-commerce* adalah bahwa proses *e-commerce* belum dapat diakui, baik sebagai bukti oleh hukum secara konvensional, seperti yang diatur dalam KUH Perdata dan Undang-Undang Hukum Acara Perdata maupun pembuktian pidana dalarn Kitab Undang-Undang Hukum Acara Pidana (KUHAP).

Beberapa prinsip hukum yang bersentuhan dengan *e-commerce* yang mestinya diakui sektor hukum pembuktian adalah sebagai berikut:[43]

a. Semua informasi elektronik dalam bentuk data elektronik mestinya memiliki kekuatan hukum sehingga mempunyai kekuatan pembuktian. Dengan demikian, data elektronik mestinya mempunyai kekuatan pembuktian yang sama dengan dokumen kertas.
b. Kontrak yang dibuat secara elektronik mempunyai akibat hukum dan kekuatan pembuktian yang sama dengan kontrak yang dibuat secara tertulis di atas kertas.
c. Tanda tangan elektronik mestinya mempunyai kekuatan pembuktian yang sama dengan tanda tangan biasa.

[42] *Ibid,* hlm 154.
[43] *Ibid.*

Beberapa negara di dunia ini sudah mengadopsi perkembangan teknologi digital ke dalam hukum pembuktiannya, seperti:

a. Hong Kong telah memiliki Undang-Undang tentang Transaksi Elektronik sejak tanggal 7 Januari 2000.
b. Inggris telah memiliki *the Electronic Communication Bill* sejak tanggal 26 Januari 2000.
c. Jepang telah memiliki Undang-Undang tentang Tanda Tangan Elektronik dan Notarisasi Bisnis Nomor 102, tanggal 31 Mei 2000, yang mulai berlaku sejak tanggal 1 April 200l.[44]

Di samping berbagai negara yang telah mulai mengakui transaksi elektronik, termasuk cara pembuktiannya, maka Perserikatan Bangsa-Bangsa juga telah membuat *Uncitral Model Law* terhadap alat bukti komersil (*Uncitrat Model Law on Electronic Commerce*). *Uncitral Model Law* ini telah resmi dipublikasikan sejak tahun 1996, dengan bahasa aslinya dalam bahasa Arab, Cina, Inggris, Prancis, Rusia, dan Spanyol. *Model law* ini diharapkan dapat diterapkan pada setiap informasi dalam bentuk "data elektronik" (*data message*) yang digunakan dalam hubungannya dengan aktivitas komersil. Yang dimaksud dengan data elektronik (data message) dalam hal ini adalah setiap informasi yang dihasilkan, dikirim, diterima, atau disimpan dengan sistem elektronik, optikal, atau dengan cara-cara yang serupa, termasuk tetapi tidak terbatas pada sistem pertukaran data elektronik (*computer to computer*), surat elektronik, telegram, teleks, atau telekopi. Banyak ketentuan yang diatur dalam *model*

[44] *Ibid,* hlm 155.

law (model hukum) tersebut, baik yang bersentuhan secara langsung maupun yang tidak langsung dengan hukum pembuktian.[45]

Beberapa kriteria atau ketentuan dasar yang harus dipertimbangkan dalam hubungannya dengan pengakuan terhadap alat bukti digital adalah sebagai berikut:

1. **Perlakuan Hukum terhadap Data Elektronik**

   Dalam hal ini ditentukan bahwa siapa pun, termasuk pengadilan, tidak boleh menolak efek hukum, validitas hukum, dan pelaksanaan hukum semata-mata karena hal tersebut merupakan data elektronik. Di samping itu, pengadilan tidak boleh pula menolak efek hukum dari dokumen jika para pihak memang tidak rnungkin mendapatkan naskah asli dari dokumen tertentu.[46]

2. **Praduga Otentisitas**

   Prinsip praduga otentisitas (*presumption of authenticity*)[47] merupakan suatu ketentuan yang sering digunakan untuk membuktikan keaslian suatu dokumen/data digital atau keaslian tanda tangan digital. Dalam hal ini, yang dimaksud adalah bahwa hukum pembuktian beranggapan bahwa suatu dokumen/data digital atau tanda tangan digital dianggap asli, kecuali dapat dibuktikan sebaliknya.Yang dilakukan dalam hai ini adalah suatu pembuktian terbalik (*omkering van bewijslast*). Artinya, barang siapa yang menyatakan bahwa alat bukti tersebut palsu, dialah yang harus membuktikannya. Dengan demikian, sebagai konsekuensi dari prinsip praduga otentisitas ini adalah bahwa pengadilan

[45] *Ibid.*
[46] *Ibid,* hlm 156.
[47] *Ibid.*

tidak boleh menolak alat bukti digital hanya karena itu adalah bukti digital, tetapi jika mau ditolak, pihak yang berkeberatan atas bukti tersebut harus mengajukan alasan-alasan yang rasional, misalnya, dengan membuktikan bahwa alat bukti digital tersebut sebenarnya adalah palsu atau hasil rekayasa saja.

3. Notarisasi Bisnis

Notarisasi bisnis terhadap suatu alat bukti digital juga sering dipersyaratkan oleh hukum pembuktian. yang dirnaksud dengan notarisasi bisnis adalah pelibatan notaris atau petugas khusus untuk itu, yang setelah dilakukan penelaahan, pemeriksaan pemakaian standar tertentu, kemudian notaris atau petugas khusus tersebut menyatakan bahwa data atau tanda tangan digital tersebut adalah benar ditandatangani oleh pihak yang tertulis sebagai penandatangannya.

4. Perlakuan Hukum terhadap Tulisan Elektronik

Sebagaimana diketahui bahwa hukum di negara mana pun mensyaratkan transaksi tertentu dilakukan secara tertulis. Tujuan persyaratan tertulis bagi transaksi tertentu adalah sebagai berikut:[48]

a. Membantu para pihak untuk waspada dan sadar sepenuhnya akan isi dan konsekuensi dari kontrak yang ditandatanganinya.
b. Untuk mempermudah pernbuktian tentang maksud danr niat tertentu dari para pihak yang bertransaksi.
c. Untuk mendapatkan suatu kontrak atau dokumen yang tidak berubah-ubah.

[48] *Ibid,* hlm 156.

d. Untuk memperkuat keotentikan data tersebut dengan adanya pembubuhan tanda tangan dan meterai.
e. Agar kontrak tersebut dapat dibaca oleh semua pihak.
f. Agar dokumen tersebut dapat diterima oleh pihak yang berwenang atau pengadilan.
g. Untuk memungkinkan agar kontrak atau dokumen tersebut dapat digandakan lagi untuk kepentingan semua pihak yang berkepentingan.
h. Untuk memfinalisasi maksud para pihak dalam bentuk tulisan sekaligus menyediakan catatan bagi rnaksud tersebut.
i. Untuk menyimpan data dalam bentuk yang dapat terbaca.
j. Untuk memberikan hak dan kewajiban hukum bagi para pihak terhadap transaksi yang disyaratkan oleh undang-undang.

Tentang persyaratan dokumen terlulis sebagaimana banyak diharuskan untuk transaksi tertentu, maka dalam hubungannya dengan transaksi elektronik ditentukan bahwa persyaratan tertulis bagi data elektronik dianggap dipenuhi jika data tersebut berisi informasi yang dapat diakses langsung untuk digunakan pada kepentingan-kepentingan selanjutnya.

5. Persoalan Tanda Tangan pada Dokumen

Sebagaimana diketahui bahwa tanda tangan bagi suatu dokumen memainkan peranan yang sangat penting dalarn hukum pembuktian. Pada prinsipnya, akan sangat

tidak berarti bagi suatu Kontrak jika kontrak tersebut tidak pernah ditandatangani. Dalam hal ini, suatu tanda tangan akan berfungsi sebagai berikut:[49]

a. Sebagai identitas para pihak.
b. Untuk menghubungkan para pihak dengan isi dari dokumen yang bersangkutan.
c. Memberikan kepastian tentang telah terlibatnya para pihak secara nyata dalam dokumen tersebut.
d. Menunjukkan tempat keberadaan penandatangan pada saat itu.

Dalam hubungannya dengan persyaratan hukum yang menghendaki tanda tangan bagi suatu dokumen, dalam hubungan dengan data elektronik, persyaratan hukum dianggap cukup manakala:[50]

a. Digunakan metode tertentu yang mengidentifikasi orang dimaksud dan untuk mengindikasi bahwa orang dimaksud setuju dengan informasi dalam data elektronik.
b. Metode tersebut layak dan dapat dipercaya untuk maksud-maksud penggunaan data elektronik tersebut, dengan mempertimbangkan semua situasi dan kondisi, termasuk setiap perjanjian yang relevan.

[49] *Ibid*, hlm 157
[50] *Ibid*, hlm 158

Faktor-faktor yang harus dipertimbangkan untuk menentukan layak tidaknya suatu metode identifikasi tersebut, dalam arti layak secara hukum, komersil dan teknikal, adalah sebagai berikut:[51]

a. Tingkat kecanggihan peralatan yang dipakai dalam metode tersebut.
b. Jenis dan besaran dari transaksi tersebut.
c. Tingkat kelaziman dibuatnya transaksi komersil seperti itu di antara para pihak tersebut.
d. Hakikat dari aktivitas perdagangan tersebut.
e. Pemenuhan kebiasaan dalam perdagangan.
f. Maksud dari dipersyaratkannya tanda tangan oleh undang-undang yang bersangkutan.
g. Pemenuhan prosedur otentikasi yang ditetapkan oleh *intermediary*.
h. Tingkat kepentingan dan nilai informasi dalam data elektronik tersebut.
i. Tingkat penerimaan metode tersebut dalam industri yang relevan.
j. Ada atau tidaknya asuransi yang mengkaver data yang tidak diotorisasi.
k. Ketersediaan metode identifikasi yang alternatif dan biaya yang diperlukan.

6. Tidak Perlu Berhadapan Muka

Mengingat perkembangan teknologi digital yang semakin pesat, maka dewasa ini tidak sepantasnya lagi dipersyaratkan suatu tatap muka di antara pihak yang melakukan kontrak, tetapi cukup dengan memakai internet. Sekarang masih ada negara yang hukumnya mensyaratkan agar suatu kontrak, yang meskipun tidak

[51] *Ibid.*

tergolong kontrak khusus, masih memerlukan tatap muka. Sebagai contoh penjual polis asuransi atau penjual obat-obatan harus bertatap muka dengan pelanggannya dalam menjual produknya itu. Kewajiban tatap muka seperti ini tidak masanya lagi untuk dipertahankan, kecuali untuk kontrak yang sangat khusus, seperti kontrak tentang tanah.[52]

Oleh karena itu, terhadap suatu kontrak elektronik yang kontraknya dibentuk hanya melalui pengiriman data elektronik, kontrak tersebut tidak boleh ditolak hanya karena bahwa kontrak tersebut dibuat secara elektronik, yakni dibuat tanpa berhadapan muka, kecuali jika para pihak menentukan lain.

7. Tidak Memerlukan Konf irmasi Lewat Surat

Hukum pembuktian yang ortodok mensyaratkan jika penjual menjual barangnya melalui *e-commerce,* penjual diharuskan mengirimkan suatu dokumen yang berisikan konfirmasi tertulis melalui surat kepada para pelanggannya. Demikian juga jika suatu jual beli dilakukan dengan menggunakan faksimile, disyaratkan agar surat aslinya juga ikut dikirimkan. Ketentuan ortodoks tersebut sekarang sudah mulai ditinggalkan oleh hukum pembuktian yang modern, di mana pengiriman surat asli atau konfirmasi tertulis tersebut tidak dipersyaratkan lagi.

Di samping itu, jika hukum atau para pihak masih mensyaratkan adanya pengakuan atau konfirmasi penerimaan data atau tawaran tertentu, pengadilan tidak pantas lagi menolak suatu konfirmasi atas adanya kontrak karena alasan bahwa

[52] *Ibid,* hlm 160.

konfirmasi tersebut hanya dilakukan secara elektronik. Akan tetapi, konfirmasi tensebut dapat saja diberikan, misalnya, dalam bentuk-bentuk sebagai berikut:[53]

a. Komunikasi oleh penerima data dalam berbagai bentuk, baik secara otomatis maupun tidak.
b. Setiap tingkah laku penerima data, selama dapat mengindikasikan kepada pengirim data bahwa data sudah diterima oleh penerima data.
c. Jika sudah diterima konfirmasi penerimaan pengiriman data elektronik, hukum harus mempraduga bahwa data elektronik tersebut memang sudah diterima oleh penerima data tersebut.
d. Jika ada konfirmasi bahwa data elektronik telah memenuhi persyaratan teknis tertentu yang telah disetujui sebelumnya atau sesuai persyaratan undang-undang tertentu, harus dipraduga oleh hukum bahwa persyaratan teknis tersebut sudah dipenuhi.

8. Kewajiban Menyimpan Dokumen

Ada kalanya hukum mengharuskan pihak tertentu untuk menyimpan data atau dokumen untuk jangka waktu tertentu, misalnya, untuk keperluan akuntansi atau pajak. Akan tetapi, suatu data elektronik tidak selamanya dapat diharapkan disimpan dalam bentuknya yang asli mengingat acap kali data tersebut disimpan dalam bentuk yang sudah dipendekkan, atau diubah bentuk dan format, dan sebagainya.

[53] *Ibid.*

Oleh karena itu, jika data atau dokumen tersebut merupakan data elektronik, kewajiban menyimpan data atau dokumen tersebut harus dianggap telah memenuhi persyaratan hukum jika:[54]

a. Informasi dalam dokumen elektronik tersebut masih dapat diakses untuk masa-masa selanjutnya.
b. Informasi tersebut disimpan tetapi masih dapat diidentifikasi keasliannya dan tujuannya, dan dapat pula ditentukan waktu data tersebut diterima atau dikirim.
c. Informasi disimpan dalam format asli ketika disimpan, dikirim, atau diterima, atau dalam format yang dapat ditunjukkan bahwa data tersebut merepresentasi secara akurat terhadap informasi yang disimpan, dikirim, atau diterima tersebut.

Namun demikian, kewajiban menyimpan data tersebut tentunya tidak berlaku terhadap data atau informasi yang mempunyai tujuan hanya untuk dikirim atau diterima.

9. Hanya Berlaku terhadap Kontrak yang Dilakukannya Sendiri

Agar suatu kontrak elektronik dapat diterima sebagai suatu alat bukti, hukum di berbagai negara sering juga mempersyaratkan hal-hal sebagai berikut:[55]

a. Kontrak dikirimnya sendiri.

[54] *Ibid,* hlm 161.
[55] *Ibid.*

b. Kontrak dikirim oleh orang yang diberikan otorisasi, misalnya oleh sekretarisnya.
c. Dikirim melalui sistem informasi yang diprogram olehnya atau atas namanya untuk mengirimkan data elektronik secara otomatis.

10. Tidak Berlaku terhadap Kontrak-Kontrak Khusus

Bahwa seharusnya. ketentuan yang membolehkan pembuatan kontrak secara digital/elektronik tidak berlaku terhadap kontrak-kontrak khusus. Kekhususan itu, baik karena sangat berharganya benda yang menjadi objek dari kontrak tersebut maupun karena secara historis yuridis memang telah memerlukan prosedur khusus. Banyak variasi dari kontrak-kontrak yang dikecualikan/dikhususkan dari ketentuan tentang bukti digital/elektronik tersebut, tetapi biasanya adalah terhadap hal-hal sebagai berikut:[56]

a. Akta yang mensyaratkan harus dibuat di depan notaris, seperti akta pendirian perseroan terbatas, gosse akte pengakuan utang dan lain-lain.
b. Akta yang mensyaratkan harus dibuat di depan pejabat khusus, seperti akta yang berkenaan dengan berbagai model peralihan atas tanah, yang di Indonesia harus dibuat di depan Pejabat Pembuat Akta Tanah (PPAT)
c. Dokumen yang memerlukan suatu meterai, seperti akte yang melibatkan penerimaan sejumlah uang.
d. Surat kuasa.
e. Surat wasiat.

[56] *Ibid.*

f. Surat berharga komersil.

g. Sumpah.

h. Dokumen yang diproduksi oleh pengadilan.

i. Dan lain-lain.[57]

11. Ketegasan tentang Tempat dan Waktu Terjadinya Kata Sepakat

Sebagaimana diketahui bahwa dalam setiap kontrak, waktu, dan tempat dianggap terjadinya kontrak perlu ditentukan dengan tegas, terutama untuk mengetahui saat mulai berlakunya hak dan kewajiban para pihak, dan hukum mana yang berlaku dan pengadilan mana yang berwenang mengadilinya. Jika para pihak dalarn kontrak tersebut tidak nnenentukan dengan tegas kapan dan di mana kontrak dianggap dilakukan, hukurn harus menyediakan kaidahnya untuk itu.

Khusus terhadap kontrak-kontrak digital, untuk waktu terjadinya kontrak biasanya hukum akan mengaturnya sebagai berikut:[58]

a. Data elektronik dianggap sudah terkirim pada saat informasi tersebut sudah diterima oleh sistem informasi yang tidak lagi dikontrol oleh pengirim.

b. Data elektronik dianggap sudah diterima jika:

    1. Informasi tersebut sudah diterima oleh sistem informasi yang dirancang oleh penerimanya untuk menerima informasi seperti itu.

[57] *Ibid,* hlm 162.
[58] *Ibid,* hlm 163.

2. Tidak dirancang suatu sistem informasi untuk menerima informasi tersebut, informasi dianggap diterima manakala informasi tersebut sudah diketahui oleh penerimanya.

Adapun untuk tempat pengiriman dan penerimaan data elektronik dianggap di tempat-tempat sebagai berikut:[59]

a. Dianggap dikirirn pada tempat kedudukan bisnis dari pengirim dan dianggap diterirna pada tempat kedudukan bisnis penerima.
b. Jika terdapat lebih dari satu tempat kedudukan bisnis, dianggap di tempat yang paling dekat hubungannya dengan transaksi yang bersangkutan.
c. Jika tidak ada transaksi yang mendasarinya, di tempat kedudukan utama dari bisnisnya.
d. Jika tidak ada tempat kedudukan bisnisnya, di tempat para pihak biasanya berdomisili.

12. Display dalam Bentuk yang Dapat Dibaca

Agar suatu bukti digital dianggap sama seperti aslinya dan dapat diterima di pengadilan, sering juga dipersyaratkan agar diterima di pengadilan, sering juga dipersyaratkan agar informasi tersebut dapat dilakukan *display* di pengadilan dalam format yang asli.[60]

[59] *Ibid.*
[60] *Ibid.*

13. Integritas Informasi dan Keaslian Dokumen

Teori hukum pernbuktian sering rnensyaratkan agar suatu dokurnen yang dipakai sebagai bukti di pengadilan haruslah dokumen asli. Keaslian dari dokumen tertulis mudah ditentukan. Akan tetapi, keasliannya dari dokumen elektronik atau rekaman elektronik tidak mudah ditentukan. Dalam hal ini, di samping persyaratan dapat di-*display* seperti tersebut di atas, dokumen elektronik atau rekaman elektronik dianggap sebagai asli manakala ada jaminan yang wajar bahwa informasi dalam dokumen atau rekaman elektronik yang dibawa ke pengadilan tersebut masih tidak berubah, komplit, dan sama dengan pada waktu dokumen atau rekaman tersebut dilakukan secara final pertama kalinya.[61]

Standar terhadap realibilitas keaslian dokumen tersebut haruslah dikaji dari tujuan penyimpanan data tersebut (sehingga tidak berubah-ubah), dan dengan mengunakan kondisi yang relevan lainnya.

14. Pengakuan Hanya terhadap Cara dan Format Tertentu

Sebagaimana diketahui bahwa data elektronik ada berbagai jenis dan format. Tidak semua data elektronik tersebut *reliable* dan pantas diberlakukan sebagai alat bukti di pengadilan. Untuk itu, hukum pembuktian seyogianya membatasi dengan tegas data elektronik yang bagaimana dan dengan format yang bagaimana yang dapat diterima di pengadilan. Sebagai contoh, tentang *software* yang digunakan, cara dan

[61] *Ibid,* hlm 164.

alat untuk berkomunikasi, situs internet yang dipergunakan, dan lain-lain. Tentu saja ketentuan ini selalu berubah sesuai dengan perkembangan teknologi digital.[62]

15. Dapat Diterima jika Pihak Lawan Kontrak Tidak Menolaknya

Ketentuan hukum pembuktian yang modern sekarang dapat menerima kontrak elektronik dalam berbagai bentuk sebagai bukti adanya kontrak, asalkan sewaktu kontrak dibuat, pihak lawan kontrak tidak menyatakan keberatannya. Oleh karena itu, jika tidak ada yang berkeberatan pada waktu kontrak dibuat, suatu kontrak dapat saja dibuat lewat *e-mail*, *faksimile*, bahkan juga rnelalui telepon. rekaman suara, video atau SMS (*short message system*) pada telepon.[63]

16. *Electronic Commerce* untuk Bidang-Bidang Tertentu

Ketentuan-ketentuan pembuktian tentang data elektronik di bidang *e-commerce* sebagaimana tersebut di atas memang sering diberlakukan pada setiap kegiatan *electronic commerce*. Akan tetapi,dalam praktik sering juga diperlukan aturan khusus untuk suatu jenis *electronic commerce* khusus.[64] Sebagai contoh, *uncitral model law* tentang *electronic commerce* yang memberikan perlakuan khusus terhadap kegiatan pengiriman barang (*carriage of goods*) dengan memberikan aturan tambahan. Pengaturan untuk bidang-bidang khusus ini dapat dipahami mengingat bahwa ada kekhususan-kekhususan tertentu atau adanya pengaturan yang lebih detil di bidang yang bersangkutan.

[62] *Ibid.*
[63] *Ibid.*
[64] *Ibid,* hlm 165.

Salah satu bidang hukum yang banyak tersentuh oleh adanya transaksi via *e-commerce* adalah bidang hukum kontrak. Hal ini adalah wajar mengingat kebanyakan dari *deal* (kesepakatan) bisnis, termasuk bisnis lewat *e-commerce* didasari atas suatu kontrak bisnis. Oleh karena itu, membuktikan adanya suatu kontrak atau adanya suatu ketentuan dalam suatu kontrak, juga harus mengikuti kaidah-kaidah hukum kontrak tersebut.

Banyak bagian dari hukum kontrak yang harus mendapat kajian yang saksama rnanakala dihadapkan dengan transaksi *e-commerce* ini. Bidang-bidang dari hukum kontrak yang bersentuhan dengan bisnis *e-commerce* ini adalah sebagai berikut:[65]

1. Ada atau tidaknya penawaran (*offer*).
2. Ada atau tidaknya penerimaan (*acceptance*).
3. Ada atau tidaknya kata sepakat.
4. Jika ada kata sepakat, sejak kapan mulai ada.
5. Keharusan kontrak dan tanda tangan tertulis.
6. Masalah pembuktian perdata.
7. Bagaimana mengetahui para pihak dan kecakapan berbuat para pihak?
8. Perumusan kembali masalah wanprestasi.
9. Perumusan kembali masalah *force majeure*.
10. Ganti rugi yang bagaimana yang paling cocok untuk kontrak *e-commerce*?
11. Masalah kontrak berat sebelah dan kontrak baku.

[65] *Ibid,* hlm 166.

Masalah-masalah tersebut yang sebenarnya merupakan ruang lingkup hukum kontrak harus ada peraturan dalam undang-undang yang mengaturnya.

Kemudian, acap kali juga dalam proses *e-commerce* dilibatkan para pihak dari negara yang berbeda sehingga menimbulkan masalah, yaitu hukum yang berlaku di antara kedua negara tersebut jika ada persengketaan, pengadilan mana yang berwenang? Hal ini penting diketahui mengingat tentang *e-commerce* ini, hukum dari negara yang satu berbeda dengan hukum negara lain. Yang jelas, setiap tindakan yang membawa akibat hukum, seperti kegiatan *e-commerce* ini, haruslah ada hukum yang mengaturnya. Dalam hubungannya dengan hukum, mana yang berlaku dan pengadilan mana yang berwenang untuk kegiatan *e-commerce* ini? Untuk itu, berlakulah prinsip-prinsip hukum sebagai berikut:[66]

a. Jika para pihak melakukan pilihan hukum (*choice of law*) dan atau pengadilan yang berwenang dalam kontraknya, hukum dan pengadilan yang dipilih tersebutlah yang berlaku.
b. Jika terhadap bidang *e-commerce* yang sudah terdapat perjanjian internasional dan di negara yang bersangkutan berlaku perjanjian internasional tersebut, ketentuan dalam perjanjian internasional tersebut haruslah dianggap berlaku.
c. Jika tidak ada pilihan hukum dan atau pengadilan, dan tidak ada pula perjanjian internasional, berlakulah prinsip-prinsip hukum perdata internasional dari kedua negara tersebut.

[66] *Ibid,* hlm 167.

Di samping itu, transfer dana secara elektronik merupakan transfer dana yang satu atau lebih bagian dalam transfer dana yang dahulu menggunakan warkat (secara fisik) kemudian diganti dengan menggunakan teknik elektronik. Bagian-bagian dalam transfer dana yang dahulunya memakai paper based, kemudian diganti dengan sistem elektronik adalah sebagai berikut:[67]

1. Pengiriman pesan elektronik di antara bank pengirim dengan bank penerima, misalnya, model lama tersebut diganti dengan instruksi pembayaran via *telex, the Society for Worldwide Interbank Financial Telecommuncations* (SWIFT), (komunitas masyarakat untuk telekomunikasi keuangan antar bank di seluruh dunia) atau hubungan *computer to computer*.
2. Data-data penting yang dahulunya dibuat dengan *paper based* di ganti dengan sistem data yang terekam dengan mesin seperti *Magnetic Ink Character Recognition* (MIGR) (pengenalan karakter internasional) atau *Optical Character Recognition* (IOCR) (karakter pengakuan).
3. Penggunaan data, terminologi, dan dokumentasi pengiriman yang standar. Dalam hal ini, berbagai aspek dari operasional bank telah distandardisasi oleh *the Banking committee of International Organization for Standardization* (lSO, TC 68) (komite perbankan organisasi internasional untuk standarisasi), dan ISO tersebut telah menyediakan suatu *Draft International Standard* (DIS 7982) dalam bahasa Inggris dan Prancis untuk pemakaian *Computer to Computer Telecommunications Networks* (jaringan telekomunikasi). Disamping itu,

[67] *Ibid,* hlm 167.

disediakan pula Dls 7746 terhadap format *telex* untuk *Interbank Funds Transfer Messages* (pesan transfer dana antar bank) dan hasil revisi dalam bentuk *draft bank* data *Elements Directory* (ISO/TC 68/N 265) (rancangan direktori elemen data besok).

4. Pembuatan instruksi transfer dengan komputer.
5. Menciptakan system elektronik baru yang tidak sekadar menggantikan sistem lama yang berdasarkan *paper based*.

Selanjutnya, pengiriman uang via elektronik (seperti lewat komputer atau internet) atau lewat telepon akan tidak mempunyai bukti tertulis sama sekali. Hal ini tentu akan rentan terhadap timbulnya kerawanan-kerawanan dan timbul disputes di kemudian hari, di samping dapat terjadi pula penipuan/ pemalsuan. Oleh karena itu, biasanya bank yang menggunakan teknik ini akan menggunakan sistem konfirmasi tertulis yang dilakukan segera setelah dilakukan transfer. Di samping itu, tersedia pula beberapa model pengamanan yang lain, seperti pemberian contoh tanda tangan, penentuan terhadap yang disebut dengan istilah *test key* (kunci tes) merekam suara percakapan telepon, dan lain-lain.

2.2 *Cyberspace* (dunia virtual) & *Cybercrime* (kejahatan dunia maya)

a. *Cyberspace* (dunia virtual)

Cyberspace merupakan dunia virtual yang terbentuk dari hasil penyatuan antara manusia dan teknologi, yaitu dari perkembangan teknologi informasi dan

kornunikasi (*information and communication technology* - ICT). Teknologi informasi dan komunikasi merupakan gabungan dari teknologi komputer, telekomunikasi serta jaringan kornputer dan telekomunikasi, seperti yang digambarkan oleh Koops :[68]

> *"technologies that store, transmit, and/ or process information and communication ... the term is generally used to indicate "modern" or "high" technology, in particular electronic data-processing technologies. Thus, ICT focuses on computers, telecommunications, and computer and telecommunication networks. The term is sometimes used as a virtual synonym for the Internet."*
>
> Teknologi yang menyimpan, mengirimkan, dan/ atau informasi proses dan komunikasi istilah "modern" atau teknologi " tinggi", teknologi pengolahan data elektronik tertentu. Dengan demikian, ICT berfokus pada computer, telekomunikasi jaringan. Istilah kadang-kadang digunakan sebagai sinonim virtual untuk internet.

Lebih lanjut, *cyberspace* (dunia virtual) merupakan "*bioelectronic environment that is literally universal: It exists everywhere there are telephone wires, coaxial cables, fiber-optic lines or electromagnetic waves."* (lingkungan bioelektronik yang secara harfiah yang universal : Itu ada dimana-mana kabel telepon, kabel koaksial, jalur kabel optik atau gelombang elektromagnetik).[69] Kehadiran *cyberspace* (dunia virtual) merupakan tonggak dimulainya peradaban informasi (*information age*) dimana informasi dapat diperoleh dan dikirimkan serta disebarkan dengan mudah ke banyak orang dalam waktu yang cepat. Setiap orang

[68] Josua Sitompul, *Cyberspace Cybercrimes Cyberlaw: Tinjauan Aspek Hukum Pidana*, (Jakarta: Tetanusa, 2012), hlm 33.

[69] Esther Dyson, *A Magna Carta for the Knowledge Age*, http://www.pff.org/, diakses tanggal 15 Desember 2014.

juga dapat mengirimkan atau menerima informasi secara etektronik dalam berbagai bentuk dalam jumlah yang sangat banyak.

Cyberspace (dunia virtual) terbentuk dari berbagai macam jaringan computer dan telekomunikasi yang saling terhubung dan berinterasi yang disebut "*electronic nervous system"* (sistem elektronik). Jaringan ini bahkan rnembentuk "*global village*" (secara global)[70], suatu tempat yang dimiliki oleh semua orang, dan dalam tempat tersebut tersimpan berbagai macam informasi yang mungkin tidak dapat dihitung lagi; "*cyberspace is the land of knowledge*" (dunia virtual adalah tempat pengetahuan). Dunia ini bersifat *borderless* dan *ubiquitous* (batas dan dimana-mana). Setiap orang dari mana saja dan kapan saja dapat memasuki dan dapat saling berkomunikasi di dunia ini tanpa perlu berada di dalamnya secara fisik.

Karakteristik tersebut mendorong munculnya pandangan bahwa seperti di dunia nyata, dalam *cyberspace* (dunia virtual) sebagai dunia baru juga harus ada "hak asasi manusia". Tiap manusia dalam dunia cyber memiliki kebebasan mendasar, yang salah satunya ialah hak untuk tidak menggunakan identitas asli mereka. Sebaliknya mereka dapat menggunakan identitas secara anonim atau alias (*pseudo*) dalam melakukan transaksi dengan pihak lain. Tidak hanya itu, ideologi kebebasan dalam

[70] Pemikiran Marshall McLuhan, http://www.livinginternet.com/, diakses tanggal 15 Desember 2014.

dunia cyber pun berkembang, dan ideologi ini disebut Langdon Winner sebagai "*cyberlibertarianism*", yaitu:[71]

> *"a collection of ideas that links ecstatic enthusiasm for electronically mediated forms of living with radical, right wing libertarian ideas about the proper definition of freedom, social life, economics, and politics in the years to come."*
>
> Kumpulan ide-ide yang menghubungkan untuk bentuk elektronik dimediasi dengan radikal, ide libertarian tentang definisi yang tepat dari kebebasan, kehidupan sosial,ekonomi, dan politik di tahun-tahun mendatang.

Penggagas ideologi ini melihat bahwa internet adalah milik bersama dan oleh karena itu setiap orang memiliki hak penuh untuk berada dan melakukan interaksi di dalamnya. Dengan demikian, pemerintah tidak perlu turut campur dengan membuat regulasi yang membatasi kebebasan mereka. Teknologi akan berkembang apabila pemerintah tidak mengontrol teknologi, dan apabila halangan-halangan terhadap *free-market competition* (persaingan pasar bebas) dihilangkan. Permasalahan yang timbul seharusnya diselesaikan oleh para pengguna internet sendiri. Apabila mereka tidak dapat menyelesaikannya, barulah pemerintah turun tangan untuk mengatur.

[71] Langdon Winner, *Cyberlibertarian Myths and the Prospects for Community*, http://www.rpi.edu/, diakses tanggal 15 Desember 2014.

b. *Cybercrime* (kejahatan dunia maya)

Sama seperti di dunia konvensional yang penuh dengan permasalahan hukum, *cybersurfers* juga semakin melihat adanya masalah-masalah hukum dalam di dunia cyber. Kebebasan untuk menggunakan identitas anonim atau alias membutuhkan kepercayaan yang kuat antara para pihak yang melakukan transaksi. Risiko akan semakin besar dalam hal jumlah dan nilai transaksi semakin banyak dan besar. Tidak adanya saki yang melihat secara langsung terjadinya transaksi tersebut dapat memperbesar risiko.

Hal yang lebih buruk dari masalah ialah timbulnya kejahatan seperti yang terjadi dalam dunia fisik. Para penjahat melihat karakteristik internet sebagai kesempatan atau sarana bagi mereka untuk melaksanakan niat jahat melalui berbagai perbuatan yang lebih dikenal dengan *cybercrimes*. Kebebasan menggunakan identitas dimanfaatkan untuk menipu, kebebasan untuk berekspresi digunakan untuk menyebarkan informasi yang berisi fitnah, kebebasan untuk mengembangkan teknologi dan kreativitas digunakan untuk merusak website atau menyebarkan virus.

Brenner membagi *cybercrimes* menjadi tiga kategori:[72]

"cybercrimes are often described os falling into three categories: crimes in which the computer is the target of the criminal activity, crimes in which the computer is a tool used to commit the crime, and crimes in which the use of the computer is on incidental aspect of the commission of the crime."

[72] Josua Sitompul, *Op.Cit*, hlm 36.

kejahatan dimana komputer adalah target dari kegiatan kriminal, kejahatan dimana komputer adalah alat yang digunakan untuk melakukan kejahatan, dan kejahatan dimana penggunaan komputer adalah aspek insidental kejahatan tersebut.

Sedangkan Nicholson menggunakan terminologi *computer crimes* dan mengkategorikan *computer crimes* menjadi:[73]

> *first, a computer may be the 'object' of a crime: the offender targets the computer itself. This encompasses theft of computer processor time and computerized services. Second, a computer may be the 'subject' of a crime: a computer is the physical site of the crime, or the source of , or reasan for, unique forms of asset loss. This includes the use of 'viruses' , 'worms', 'Trojan horses' , 'logic bombs', and 'sniffers.' Third, a computer may be an 'instrument' used to commit traditional crimes in a more complex manner. For example, a computer might be used to collect credit card informotion to moke fraudulent purchases.*
> Pertama, komputer mungkin 'objek' kejahatan : pelaku menargetkan diri sendiri. Komputer meliputi pencurian waktu prosesor komputer dan layanan komputerisasi.
>
> Kedua, komputer mungkin sebagai 'subjek' kejahatan : komputer adalah situs fisik kejahatan, atau sumber, atau alas an, bentuk unik kehilangan asset. Ini termasuk penggunaan virus cacing, Trojan horse, logika bom, dan sniffer.
>
> Ketiga, komputer mungkin menjadi 'alat' yang digunakan untuk melakukan kejahatan dengan cara yang lebih kompleks sebagai contoh, sebuah komputer dapat digunakan untuk mengumpulkan informasi kartu kredit untuk penipuan.

Menurut Walden (2007), cybercrimes adalah bagian dari computer crimes. Walden melihat bahwa pengktasifikasian computer crimes dapat didasarkan pada teknologi (*technology-based*), motivasi (*motivation-based*), hasil (*outcome-based*), dan

[73] *Ibid,* hlm 37.

komunikasi (*communication-based*), serta informasi (*information-based*)." Walden mengkategorikan tindak pidana menjadi tiga, yaitu: *computer-related crime, content-related crime, dan computer integrity offences*. Berikut penjelasannya.

> *"The first category is traditional types of criminal offence that may be committed using computers as the instrument of the crime, such as fraud. The second cotegory, content based cybercrimes, such as criminal copyright infringement and child pornography, concern reliance on the use of computer and communications technoloqies to facilitate the distribution of unlawful content or illegal data. The distinction being made between computer related and content-related crime is primarily one of focus. In both, computers are a tool or instrument for the commission of a crime, rather than the target itself. However, in computer-related crime, the data or information being processed is also a tool or instrument for committing a criminal act; while in content-related crime, the data or information is the crime, not a tool or instrument. The third category is offences that have been established to specifically address activities that attack the integrity of computer and communications systems, such as distributing computer viruses"*[74]
>
> Kategori pertama adalah jenis tindak pidana yang dapat dilakukan dengan mengunakan komputer sebagai alat kejahatan, penipuan seperti itu. Kategori kedua, kejahatan cyber konten berbasis, seperti pelanggaran pidana hak cipta dan pornografi anak, kekhawatiran ketergantungan pada penggunaan komputer dan teknologi komunikasi untuk memfasilitasi distribusi konten yang melanggar hukum atau data illegal. Perbedaan yang dibuat antara komputer adalah alat untuk kejahatan dari pada target itu sendiri. Namun dalam kejahatan terkait komputer, data atau informasi yang diproses juga merupakan alat untuk melakukan tindak pidana; sedangkan dalam kejahatan terkait konten, data atau informasi adalah kejahatan bukan alat.

Berbicara mengenai motivasi melakukan tindak pidana cyber, Grabosky ef al menyimpulkan bahwa yang memotivasi pelaku rnelakukan tindak pidana tersebut adalah *"greed, lust, power, revenge, adventure, and the desire to taste 'forbidden*

[74] Ian Walden, *Computer Crimes and Digital investigations,* (New York: Oxford University Press, 2007), hlm 19.

fruit' (keserakahan, nafsu, kekuasaan, balas dendam, petualangan, dan keinginan). Sedangkan Kingler menyimpulkan bahwa motivasi pelaku tindak pidana cyber dapat dibagi menjadi MEECES yaitu: "*money, entertainment, ego, cause, entrance to social groups, and status* (uang, hiburan, ego, asal, pintu masuk ke kelompok sosial dan status)."[75]

Dalam *Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders* (kongres 10 negara bersatu pada pencegahan kejahatan dan perawatan pelaku yang diselenggarakan di Vienna, 10-17 April 2000, dibahas kategori *cyber crime* (kejahatan dunia maya). *Cyber crime* (kejahatan dunia maya) dapat dilihat secara sempit maupun secara luas, yaitu :[76]

(a) Cyber crime in a narrow sense ("computer crime"): any illegal behavior directed by means of electronic operotions that targets the security of computer systems and the data processed by them;
(b) Cyber crime in a broader sense ("computer-related crime"): any illegal behaviour committed by means of , or in relation to, a computer system or network, including such crimes as illegal possession , offering or distributing information by means of a computer system or network.

(a) Kejahatan *cyber* dalam arti sempit (kejahatan komputer) : setiap perilaku illegal diarahkan dengan cara operasi elektronik yang menargetkan keamanan sistem komputer dan data diproses oleh mereka.
(b) *Cyber crime* dalam arti luas (kejahatan terkait komputer) : setiap perilaku illegal yang dilakukan dengan cara, atau berhubungan dengan sistem komputer atau jaringan, termasuk kejahatan seperti kepemilikan illegal, menawarkan atau mendistribusikan informasi melalui sistem komputer atau jaringan.

[75] Josua Sitompul, *Op.Cit*, hlm 38.
[76] *Ibid.*

Dari penjelasan-penjelasan tersebut, *cyber crime* dapat berupa kejahatan baru yang tidak diatur dalam undang-undang pidana konvensional, dan juga dapat berupa kejahatan konvensional yang menggunakan sarana komputer atau sistem komputer.

2.3 Keabsahan Alat Bukti Elektronik

Undang-Undang Nomor 11 Tahun 2008 tentang ITE telah mengatur bahwa upaya paksa yang dapat digunakan aparat penegak hukurn untuk memperoleh alat bukti elektronik ialah melalui penggeledahan dan penyitaan Sistem Elektronika atau melalui intersepsi atau penyadapan. Aparat penegak hukurn menggunakan cara penggeledahan dan penyitaan apabila penyidik sudah mengetahui secara jelas sumber alat bukti elektronik tersebut (lokasi komputer, laptop, USB, server milik tersangka, korban, atau saksi). Sedangkan berdasarkan batasan-batasan yang diatur dalam perundang-undangan, intersepsi atau penyadapan dapat digunakan oleh aparat penegak hukum sebagai cara mengumpulkan informasi dan keterangan terkait dengan suatu tindak pidana (tersangka, tindak pidana yang dipersangkakan, saksi, lokasi tindak pidana); inforrnasi tersebut dapat dijadikan alat bukti.[77]

Seperti yang telah dijelaskan sebelumnya bahwa dalam sistem pembuktian di Indonesia, kesalahan terdakwa ditentukan oleh minimal dua alat bukti yang sah dan keyakinan hakim. Keabsahan alat bukti didasarkan pada pemenuhan syarat dan ketentuan baik segi formil maupun materil. prinsip ini juga berlaku terhadap pengumpulan dan penyajian alat bukti elektronik baik yang dalam bentuk original rnaupun hasil cetaknya, yang diperoleh baik melalui penyitaan maupun intersepsi.

[77] Josua Sitompul, *Op.Cit*, hlm 282.

KUHAP telah memberikan pengaturan yang jelas mengenai upaya paksa penggeledahan dan penyitaan secara umum, tetapi belum terhadap Sistem Elektronik.[78]Akan tetapi, KUHAP belum mengatur mengenai intersepsi atau penyadapan; hal ini diatur di dalam berbagai undang-undang yang lebih spesifik. Oleh karena itu, ketentuan dan persyaratan formil dan materil mengenai alat bukti etektronik harus mengacu kepada KUHAP, Undang-Undang Nomor 11 Tahun 2008 tentang ITE, dan undang-undang lain yang mengatur secara spesifik mengenai alat bukti etektronik tersebut. Tulisan ini membatasi hanya kepada ketentuan dan persyaratan yang di atur dalam Undang-Undang Nomor 11 Tahun 2008 tentang ITE saja. Yang dimaksud dengan persyaratan materil ialah ketentuan dan persyaratan yang dimaksudkan untuk menjamin keutuhan data (*integrity*), ketersediaan, (*availability*), keamanan (*security*), keotentikan (*authenticity*), dan keteraksesan (*accessibility*) informasi atau Dokumen Elektronik dalam proses pengumpulan dan penyimpanan dalam proses penyidikan dan penuntutan, serta penyampaiannya di sidang pengadilan. Dalam hal ini dibutuhkan suatu cabang disiplin ilmu di bidang forensic komputer (*computer forensic*) atau forensik digital (*digital forensic*) yaitu *"a branch of forensic science pertaining to legal evidence found in computers and digital storage media."*[79]

Cabang ilmu ini penting mengingat:

> *Electronic evidence is, by its very nature, fragile. It can be altered, damaged, or destroyed by improper handling or improper examination. For this reason,*

[78] Pasal 31 UU ITE.
[79] http://en.wikipedia.org/, diakses pada tanggal 20 Januari 2015.

> *special precautions should be taken to document, collect, preserve, and examine this type of evidence. Failure to do so may render it unusable or lead to an inaccurate conclusion.*[80]
> Bukti elektronik adalah, pada dasarnya rapuh. Hal ini dapat diubah, rusak, atau hancur karena penanganan yang tidak tepat atau pemeriksaan yang tidak benar. Untuk alasan ini, tindakan pencegahan khusus harus diambil untuk mendokumentasikan, mengumpulkan, melestarikan, dan memeriksa jenis bukti. Kegagalan untuk melakukannya dapat membuat itu tidak dapat digunakan atau menyebabkan kesimpulan yang tidak akurat.

Persyaratan materil alat bukti etektronik diatur dalam Pasal 5 ayat (3) Undang-Undang Nomor 11 Tahun 2008 tentang ITE, yaitu Informasi atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik sesuai dengan ketentuan yang diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang ITE. Lebih lanjut, Sistem Etektronik diatur dalam Pasal 15 s.d. 16 Undang-Undang Nomor 11 Tahun 2008 tentang ITE dan dari kedua pasal ini, dapat diperoleh persyaratan yang lebih rinci, yaitu bahwa Sistem Elektronik:[81]

1. andal, aman, dan bertanggung jawab;
2. dapat menampilkan kembali Informasi atau Dokumen Elektronik secara utuh;
3. dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan Informasi Elektronik;
4. dilengkapi dengan prosedur atau petunjuk dan dapat beroperasi sesuai prosedur atau petunjuk yang telah ditetapkan tersebut;

[80] Josua Sitompul, *Op.Cit*, hlm 284.
[81] Pasal 15 s.d. 16 Undang-Undang Nomor 11 Tahun 2008 tentang ITE

Selain itu, Pasal 6 Undang-Undang Nomor 11 Tahun 2008 tentang ITE juga memberikan persyaratan materil mengenai keabsahan alat bukti etektronik, yaitu bahwa informasi atau dokumen elektronik dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan. Undang-Undang Nomor 11 Tahun 2008 tentang ITE tidak mengatur perihal cara atau metode yang digunakan untuk mengumpulkan, mengamankan, menampilkan atau menjamin keutuhan informasi alat bukti elektronik karena pada dasarnya, Undang-Undang Nomor 11 tahun 2008 tentang ITE menganut asas netral teknologi. Maksudnya, cara atau metode pengumpulan dan pengamanan alat bukti elektronik dapat menggunakan teknologi yang tersedia sepanjang dapat memenuhi persyaratan keabsahan alat bukti elektronik.[82]

Sedangkan persyaratan formil alat bukti elektronik diatur dalam Pasal 5 ayat (4) dan Pasal 43 Undang-Undang Nomor 11 Tahun 2008 tentang ITE, yaitu:[83]

1. Informasi atau Dokumen Elektronik tersebut bukanlah:
    a. Surat yang menurut undang-undang harus dibuat dalam bentuk tertulis;
    b. Surat beserta dokumennya yang menurut undang-undang harus dibuat dalam bentuk akta notaril atau akta yang dibuat oleh pejabat pembuat akta.
2. penggeledahan atau penyitaan terhadap Sistem Elektronik harus dilakukan atas izin ketua pengadilan negeri setempat;

[82] Josua Sitompul, *Op.Cit*, hlm 285.
[83] Pasal 5 ayat (4) dan Pasal 43 Undang-Undang Nomor 11 Tahun 2008 tentang ITE

3. penggeledahan atau penyitaan dan (2) tetap menjaga terpeliharanya kepentingan pelayanan umum;

Dalam hal Sistem Elektronik yang digunakan telah memenuhi persyaratan tersebut, maka kualitas alat bukti elektronik dalam bentuk originalnya (Informasi Elektronik atau Dokumen Elektronik) dan hasil cetak dari Informasi atau Dokumen Elektronik adalah sama. Dengan kata lain, polisi, jaksa, dan hakim dapat menggunakan keduanya atau salah satunya. Akan tetapi, perlu diingat pula bahwa dalam kasus-kasus tertentu, ada kalanya penggunaan alat bukti elektronik lebih tepat dibanding penggunaan hasil cetak dari Informasi atau Dokumen Elekronik karena Informasi atau Dokumen Elektronik tersebut dapat memberikan informasi yang tidak dapat diberikan apabila Informasi atau Dokumen Elektronik tersebut dicetak.

Alat bukti elektronik yang mana yang digunakan? Apakah yang dalam bentuk originalnya ataukah yang telah dicetak? Hal ini tentunya dapat dilihat kasus per kasus. Salah satu contoh ialah dalam kasus perampokan yang terekam dalam cctv maka dokumen elektronik yung terekam oleh cctv sebaiknya disajikan dalam bentuk originalnya. Video dapat berisi gambar bergerak dan bersuara. Penggunaan alat bukti dalam bentuk originalnya ini akan memudahkan aparat penegak hukum dalam memahami fakta hukum yang terekam dalam video tersebut. Aparat penegak hukum juga dapat mencetak setiap gerakan pelaku waktu melakukan aksi perampokan yang

terekam tetapi ini tentunya akan membutuhkan kertas yang sangat banyak sehingga tidak efektif.[84]

Akan tetapi, dalam kasus-kasus tertentu penggunaan hasil cetak dari Informasi atau Dokumen Elektronik lebih memudahkan aparat penegak hukum dalam menyajikannya di persidangan. Salah satu contohnya ialah dalam tindak pidana pemerasan yang dikirimkan lewat SMS atau email. Dalam kasus seperti ini, penggunaan dan penyajian hasil cetak dari SMS atau email yang diperoleh dari suatu telepon genggam (*handphone*) atau komputer lebih memudahkan aparat penegak hukum dalam menilai fakta hukum. Pada prinsipnya SMS atau email sama dengan tulisan,tetapi dalam bentuk elektronik. Oleh karena itu, sepanjang SMS dalam handphone yang dimaksud sudah diperiksa integritas, ketersediaan, dan keotentikan atau keoriginalan serta relevansinya dengan kasus yang diperkara-kan, maka hasil cetak SMS itupun sudah cukup sebagai alat bukti.[85] Polisi atau jaksa tidak perlu membawa, memperagakan serta menunjukkan SMS dalam handphone tersebut di persidangan karena membutuhkan waktu dan biaya yang lebih besar.

a. Urgensi Pengaturan yang Lebih Spesifik

Sama halnya dengan persyaratan dan ketentuan alat bukti yang diatur dalam KUHAP, alat bukti elektronik harus memenuhi persyaratan baik secara formil dan materil sehingga alat bukti tersebut dapat dinyatakan sah dan dipergunakan di persidangan. Ketentuan dan persyaratan tersebut adalah untuk menjamin kepastian

[84] *Ibid,* hlm 286.
[85] *Ibid.*

hukum dan berfungsi sebagai alat penguji dalam menentukan keabsahan alat bukti sehingga hakim dapat yakin dengan fakta-fakta hukum yang dihadirkan melalui alat bukti elektronik.[86]

Alat bukti elektronik memiliki cakupan yang luas dan jenis yang beragam, seperti *email, websites*, *short message service* (SMS), *video, dan electronically stored information* (ESI),[87] foto digital, *computer-generated documents and data files*, termasuk hasil, cetak dari informasi atau dokumen elektronik lainnya. Tiap jenis alat bukti elektronik tersebut memiliki karakteristik secara teknis yang memerlukan penanganan tersendiri dalam menentukan keabsahannya secara hukum. Oleh karena itu, perlu adanya kesepahaman di antara kalangan aparat penegak hukum mengenai prinsip-prinsip pengumpulan, penganalisaan, serta penyajian alat bukti elektronik yang beragam itu. Dalam hal diperlukan, dapat ditetapkan peraturan dan putusan yang lebih spesifik yang dijadikan pedoman dalam memeriksa alat bukti elektronik baik ditingkat penyidikan, penuntutan, maupun di persidangan. Pengaturan atau patokan tersebut dapat melalui pembentukan peraturan dibawah undang-undang, penafsiran hakim (*wetintepretarie*) dan penemuan hukum (*rechtsvinding*) oleh hakim. Peraturan yang dimaksud juga dapat berupa peraturan bersama antara instansi aparat penegak hukum yang dapat digunakan sebagai pedoman baik di pusat maupun di daerah di seluruh Indonesia. Pedoman atau pengaturan yang dimaksud harusnya

[86] *Ibid,* hlm 287.
[87] http://www.law.northwestern.edu/, diakses pada tanggal 15 Desember 2014.

didasarkan pada best practices yang berlaku yaitu metode digital forensik. Perihal digital forensik akan dijelaskan pada bagian selanjutnya.[88]

Perihal kekuatan dan nilai pembuktian tidak perlu lagi dibahas mengingat esensi keduanya sama dengan alat bukti yang diatur dalam Pasal 184 KUHAP, yaitu kekuatan pembuktian dari alat bukti elektronik bersifat bebas (*volledig bewijskracht*) dan bersifat tidak mengikat atau menentukan (*beslissende beweijskracht*). Nilai pembuktian dari seluruh alat bukti didasarkan pada penilaian hakim.

b. Digital Forensik

Sebagaimana disebutkan dalam bagian sebelumnya bahwa salah satu syarat materil alat elektronik dapat diterima di pengadilan ialah bahwa informasi atau dokumen elektronik harus dapat dijamin ketersediaan, keutuhan, keotentikan, dan keteraksesannya. Dengan dipenuhinya persyaratan materil dan juga persyaratan formil elektronik dalam bentuk original maupun hasil cetak dari alat bukti elektronik memiliki nilai yang sama. Untuk menjamin terpenuhinya persyaratan tersebut diperlukan suatu metode ilmiah yang didukung teknologi khusus untuk memeriksa alat bukti elektronik. Dalam bagan ini akan dipaparkan secara singkat peranan forensik yang diterapkan untuk mengumpulkan, mengolah, serta menyajikan alat bukti elektronik untuk kepentingan penegakan hukum. Mengingat luasnya pembahasan digital forensik dalam penyidikan, dalam bagian ini hanya dibatasi pada prinsip-prnsip dalam digital forensik.[89]

[88] Josua Sitompul, *Op.Cit,* hlm 288.
[89] *Ibid.*

Dalam satu transaksi elektronik akan ada begitu banyak informasi yang tercatat atau terekam di banyak alat dan perangkat. Semakin banyak transaksi maka akan semakin banyak informasi. Apabila seseorang melakukan *hacking* terhadap *website* satu instansi pemerintah melalui laptop dengan menggunakan *mobile modem*, aktivitas pelaku sebenarnya tercatat di banyak tempat- mulai laptop pelaku, SIM card modem yang digunakan penyelenggara telekomunikasi yang menyediakan layanan jasa internet, dan server website yang diserang bersama dengan catatan aktivitas-aktivitas lainnya. Oleh karena itu, seperti mencari jarum di tumpukan jerami, aparat penegak hukum harus mencari informasi yang relevan dengan tindak pidana diantara informasi yang terekam: informasi yang menunjukkan adanya tindak pidana dan menunjukkan pelaku tindak pidana. Informasi elektronik atau dokumen elektronik, bila tidak ditangani dengan benar, dapat berubah, rusak, atau hilang.

Jika informasi tersebut hilang dan tidak dapat ditemukan kembali maka aparat penegak hukum tidak dapat memperoleh alat bukti elektronik; jika informasi tersebut berubah atau rusak maka informasi yang dimaksud tidak dapat dijadikan alat bukti di persidangan. Oleh karena itu, aparat penegak hukum harus mencari, mengumpulkan, dan menganalisa informasi dengan cepat dan tepat.[90]

Associotion of Chief Police Officers (ACPO) memberikan empat prinsip dalam penanganan alat bukti elektronik.[91] *Pertama,* semua penanganan terhadap alat bukti elektronik (yaitu data yang diperoleh dari komputer atau media penyimpanan,

[90] *Ibid,* hlm 289.
[91] Good Practice Guide for Computer-Based Electronic Evidence, hlm 4.

atau alat dan perangkat elektronik lain) yang dilakukan oleh aparat penegak hukum tidak boleh mengakibatkan adanya perubahan atau kerusakan terhadap data agar dapat diterima di pengadilan. Dengan demikian, data yang diperoleh pada waktu penyidikan sama dengan data yang dihadirkan dipersidangan. Penanganan yang tidak tepat terhadap data dapat merusak, rnenghilangkan, mengubah data. Sama seperti dalam penyidikan tindak pidana konvensional, ketika memasuki tempat kejadian perkara (TKP), penyidik perlu, misalnya, menggunakan sarung tangan agar sidik jarinya tidak menempel pada gelas atau kaca yang berada di TKP. Penyidik juga perlu memasukkan barang bukti yang mudah pecah dalam tempat yang aman sehingga tidak rusak. Demikian juga dengan data, ketika komputer dalam keadaan hidup, penyidik perlu melakukan forensik dalam keadaan hidup karena apabila komputer dimatikan, data-data yang bersifat *volatile* (mudah menguap) dapat hilang.[92]

Kedua, dalam keadaan-keadaan dimana seseorang harus mengakses data original yang terdapat dalam komputer atau media penyimpanan, orang yang dimaksud harus memiliki kompetensi untuk melakukannya, dan harus mampu memberikan penjelasan mengenai relevansi tindakannya terhadap data dan akibat dari perbuatannya itu. Dalam penyidikan konvensional, tidak semua penyidik dapat masuk ke dalam TKP dan memeriksa serta mengumpulkan barang bukti, hanya orang yang memiliki kompetensi yang dapat melakukan tindakan-tindakan tersebut. Misalnya, ketika ditemukan mayat dalam keadaan telungkup, penyidik yang tidak

[92] *Ibid.*

memiliki kompetensi dibidang kedokteran forensik seharusnya tidak memindahkan mayat, tetapi menunggu ahli kedokteran forensik untuk memeriksanya, termasuk menentukan waktu dan penyebab kematian.[93]

Prinsip ketiga adalah bahwa harus ada prosedur dan proses yang jelas yang diterapkan untuk mengumpulkan dan menganalisa alat bukti elektronik. Prosedur yang dimaksud memuat penanganan alat bukti elektronik mulai dari penemuan barang bukti (komputer, telepon genggam, USB, *router*, atau laptop) yang mengandung alat bukti elektronik, pembungkusan barang bukti, pemeriksaan, analisa, dan pelaporan. Dengan demikian, setiap pihak yang berkepentingan dapat memeriksa proses dan prosedur yang dimaksud dan memperoleh hasil yang sama. Terakhir, harus ada pihak atau pejabat yang bertanggung jawab untuk memastikan pelaksanaan kegiatan agar sesuai dengan peraturan perundang-undangan serta keseluruhan proses dan prosedur yang dimaksud.[94]

Hal lain yang perlu diperhatikan dalam pengumpulan barang bukti yang menyimpan alat bukti elektronik ialah bahwa ada begitu banyak jenis alat dan media yang menyimpan informasi. Tidak hanya komputer, laptop, handphone, atau USB, tetapi juga router, modem, kamera digital, harddisk eksternal, CD atau DVD, serta PDA. Mengingat ada begitu banyak jenis media penyimpanan informasi dan

[93] Josua Sitompul. *Op.Cit,* hlm 290.
[94] *Ibid.*

teknologi, penanganannya pun memiliki karakteristiknya masing-masing. Secara umum, digital forensic dapat dibagi menjadi:[95]

1. komputer forensik,yaitu forensik yang dilakukan terhadap komputer, laptop, atau harddisk dan media penyimpanan sejenis;
2. *mobile forensic*, yaitu forensik yang dilakukan terhadap telepon genggam;
3. *network forensic*, yaitu forensik yang dilakukan terhadap jaringan komputer;
4. *audio forensik*, yaitu forensik yang dilakukan terhadap suara;
5. *image forensik*, yaitu forensik yang dilakukan terhadap gambar;
6. *video forensik*, yaitu forensik yang dilakukan terhadap video dan cctv.

Seperti yang disebutkan sebelumnya bahwa bukan tujuan buku ini membahas masing-masing karakteristik forensik. Akan tetapi, untuk memberikan gambaran umum dalam bagian ini dijelaskan secara ringkas tahap-tahap digital forensic. Berdasarkan prinsip ACPO yang telah disebutkan di atas. Berdasarkan prinsip ini, prosedur digital forensik terbagi tiga tahap besar, yaitu:[96]

1. Pengambilan (*acquisition*);

   Mengingat sifatnya yang dapat diubah, dirusak, atau dihilangkan apabila tidak ditangani dengan tepat, pengambilan Informasi atau Dokumen Elektronik harus dilakukan dengan menjaga dan melindungi keutuhan atau integritasnya. Tahap ini dimaksudkan untuk mengambil dan mengamankan alat bukti elektronik asli (original). Cara atau prosedur pengambilan alat bukti elektronik original dapat

[95] Muhammad Nuh Al-Azhar, *Digital Forensic: Panduan Praktis Investigasi Komputer*, hlm 25-26.

[96] Josua Sitompul, *Op.Cit*, hlm 291.

didasarkan pada kondisi awal ditemukannya alat bukti elektronik atau alat/perangkat yang menyimpan alat bukti elektronik tersebut. Untuk memberikan gambaran, sebagai contoh, ACPO memberikan prosedur penanganan terhadap komputer yang ditemukan dalam keadaan menyala dan dalam keadaan mati, antara lain sebagai berikut:[97]

Tabel 2
Prosedur Penanganan Terhadap Komputer yang Ditemukan dalam Keadaan Menyala dan dalam Keadaan Mati.

Terhadap computer yang ditemukan dalam keadaan menyala:	Terhadap komputer yang ditemukan dalam eadaan mati:
1. mengamankan area tempat komputer berada; 2. memindahkan orang-orang dari komputer dan dari lokasi Power supply; 3. mengambil gambar atau video dari sistem komputer dan semua komponen-komponennya; jika tidak ada kamera, dapat membuat sketsa komputer dan sistem; 4. memeriksa adanya catatan mengenai password disekitar komputer; 5. dapat bertanya kepada pengguna komputer mengenai sistem komputer termasuk password dan mencatat semua keterangannya; 6. mencatat tampilan yang ada dilayar monitor komputer; 7. jangan menekan tombol keyboard atau mouse jika	1. Memastikan bahwa computer dalam keadaan mati (bukan dalam keadaan standby atau sleep); ada kemungkinan laptop yang tertutup sebenarnya tidak dalam keadaan mati, jika laptop dibuka, proses akan berjalan lancar kembali; 2. mengamankan area tempat komputer berada; 3. memindahkan orang-orang dari komputer dan dari lokasi power supply; 4. mengambil gambar atau video dari sistem komputer dan semua komponen-komponennya; jika tidak ada kamera, dapat membuat sketsa komputer dan sistem; 5. memberikan label terhadap semua komponen, termasuk port dan kabel;

[97] Muhammad Nuh Al-Azhar, *Op.Cit*, hlm 8-9.

komputer terlihat mati, dapat menggerak-gerakkan mouse, setelah itu dicatat tindakan menggerakkan mouse; 8. selama dimungkinkan, kumpulkan data yang dapat hilang ketika sumber listrik dicabut; terhadap tindakan ini harus dilakukan pencatatan; 9. membiarkan printer menyelesaikan pencetakan terhadap dokumen yang diperintahkan komputer; 10. mencatat seluruh proses dan tindakan secara detail.	6. jangan menyalakan computer, apapun kondisinya; 7. memindahkan baterai (sumber listrik) dari komputer; 8. cabut sumber listrik serta alat dan perangkat lain dari soket komputer; 9. memeriksa adanya catatan mengenai password disekitar computer; 10. memberikan label terhadap port dan kabel sehingga computer dapat dikonstruksikan di kemudian hari baik oleh ahli forensic maupun berdasarkan kebutuhan pengadilan; 11. mencatat seluruh proses dan tindakan secara detail.

Sumber: Muhammad Nuh Al-Azhar

2. Pemeriksaan dan Analisa;

Pemeriksaan terhadap alat bukti elektronik original umumnya menggunakan perangkat keras dan perangkat lunak yang khusus dibuat untuk kepentingan digital forensik. Pada tahap ini, pemeriksa rnelakukan ekstraksi, yaitu mengambil seluruh data dari media dimana data tersebut tersimpan, termasuk data yang telah terhapus sebelumnya. Pemeriksa juga perlu menggunakan *write blocker* (penulisan bloker), yaitu alat yang digunakan untuk mencegah penulisan terhadap data original. Selain itu, dalam melakukan pengambilan data, pemeriksa juga perlu menentukan nilai dari keseluruhan data yang diambil (*hash*). Nilai (*hash*) dari data onginal akan sama dengan nilai dari hasil ekstraksi. Sehingga, apabila diperlukan pemeriksaan ulang oleh pemeriksa yang berbeda (misalnya pemeriksa dari advokat tersangka), nilai dari alat bukti elektronik tersebut akan

sama. Setelah alat bukti elektronik original diperoleh, pemeriksaan terhadap alat bukti elektronik harus dilakukan dengan membuat salinan (*copy*) dari informasi atau dokumen elektronik yang asli (*original*).[98]

Setelah pengambilan informasi atau dokumen elektronik dilakukan, tahap selanjutnya ialah pemeriksaan dan analisa terhadap alat bukti elektronik. Pemeriksaan dilakukan terhadap salinan dari alat bukti elektronik yang asli. Pemeriksa juga dapat membuat salinan dari salinan alat bukti elektronik sebagai bahan kerja. Pada tahap ini pemeriksa juga melakukan analisa, yaitu adalah mengintepretasikan informasi yang telah diekstraksi dan menentukan informasi atau data yang relevan dengan tindak pidana.[99] Tergantung dari jenis tindak pidana, dalam tahap ini, pemeriksa mencari informasi elektronik atau dokumen elektronik yang menunjukkan adanya tindak pidana atau menunjukkan pelaku tindak pidana. Misalnya, dalam tindak pidana penyebaran pornografi, pemeriksa harus menemukan adanya file-file pornografi dalam komputer, laptop, atau USB pelaku. Untuk membuktikan adanya penyebaran, pemeriksa dapat mencari rekaman email yang masih tersimpan dalam komputer pelaku; dari rekaman email tersebut, pemeriksa dapat mengetahui penerimaan email. Dalam tindak pidana akses ilegal, harus menemukan adanya rekaman aktivitas transaksi elektronik (*log file*) yang menunjukkan bahwa pelaku, dengan menggunakan IP tertentu, berhasil mengakses suatu website secara illegal.

[98] Josua Sitompul, *Op.Cit,* hlm 293.
[99] *Ibid.*

3. Dokumen dan presentasi

Setiap tindakan yang dilakukan dalam pengumpulan dan pemeriksaan alat bukti elektronik harus didokumentasikan secara akurat dan menyeluruh. Tidak hanya tindakan dalam melakukan digital forensik, tetapi juga tindakan yang terkait dengannya, misalnya serah terima komputer dari petugas yang mengambil barang di tempat kejadian perkara kepada pemeriksa forensik.[100]

Laporan dapat memuat proses dan tahapan yang dilakukan dalam pemeriksaan, termasuk alat dan perangkat yang dilakukan dalam pemeriksaan, termasuk alat dan perangkat yang digunakan. Selain itu, laporan juga perlu memuat informasi mengenai keseluruhan data yang diperoleh serta data yang relevan dengan tindak pidana.

Penanganan yang tidak tepat terhadap komputer yang menyala dapat menghilangkan informasi elektronik yang sifatnya *volatile* (mudah menguap). Tidak diberinya label terhadap komponen serta kabel atau port dari alat dan perangkat yang telah dipreteli ditempat kejadian perkara dapat menyulitkan analis digital forensik untuk menyusun kembali perangkat tersebut di laboratorium forensik. Demikian juga pencatatan yang tidak lengkap dapat menimbulkan keraguan hakim atau pengacara terhadap hasil forensik yang dilakukan.

Dalam pengumpulan alat bukti elektronik, penyidik akan menemukan berbagai informasi, baik yang relevan dengan tindak pidana, maupun yang tidak relevan. Terkait dengan hal ini, penyidik harus menjaga kerahasiaan informasi,

[100] *Ibid*, hlm 294.

khususnya informasi terkait privasi seseorang yang tidak relevan dengan tindak pidana. Semua informasi yang tidak relevan tidak boleh diungkap di pengadilan.[101]

Dalam pengumpulan dan pemeriksaan alat bukti elektronik, dalam banyak kasus di Indonesia, penyidik memerlukan kerjasama dengan penyelenggara telekomunikasi. Kembali kepada contoh yang disebutkan sebelumnya tentang *hacking* terhadap *website* satu instansi pemerintah melalui laptop dengan menggunakan mobile modem. Penyidik mungkin masih dapat menemukan jejak-jejak pelaku, seperti *Internet Protocol* (IP) yang digunakan pelaku untuk mengakses website dan waktu pengaksesan website. IP pelaku yang tercatat adalah IP publik. Pengguna IP publik dapat dicari melalui layanan *whois* dan dari layanan tersebut penyidik dapat mengetahui pemilik *IP publik*. Mengingat pelaku menggunakan *mobile modem*, pelaku penyidik hanya dapat mengetahui dari layanan whois penyelenggara telekomunikasi yang menggunakan IP publik tersebut. Berdasarkan informasi yang ia peroleh, penyidik harus menghubungi penyelenggara telekomunikasi yang dimaksud untuk memperoleh rekaman transaksi etektronik (*log file*) dan modem yang digunakan. Selain itu, penyelenggara juga dapat memberikan informasi mengenai identitas yang diberikan oleh pengguna layanan telekomunikasi pada waktu mendaftar SIM card untuk kali pertama.[102]

[101] *Ibid.*
[102] *Ibid*, hlm 295.

2.4 Perkembangan Hukum Pembuktian Elektronik di Indonesia.

Di Indonesia ada perkembangan dalam sistem hukum pembuktian khususnya yang menyangkut dengan pembuktian elektronik, setelah keluarnya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Jika sebelumnya paling jauh bukti elektronik hanya dipakai dalam hukum acara perdata sebagai bukti "persangkaan" atau dalam hukum acara pidana hanya dipakai sebagai bukti "petunjuk", maka dengan keluarnya Undang-Undang tentang Informasi dan Transaksi Elektronik tersebut, alat bukti elektronik berupa informasi elektronik, dokumen elektronik, dan hasil cetaknya dengan tegas diakui sebagai alat bukti yang sah dan penuh di pengadilan asalkan memenuhi persyaratan-persyaratan tertentu sebagaimana yang ditentukan dalam undang-undang. Dengan demikian, undang-undang ini diharapkan dapat menjawab berbagai hak yang bekaitan dengan hukum (termasuk hukum pembuktian) yang berkenaan dengan dunia maya (*cyber law*, *virtual world law*), hukum tentang teknologi informasi dan komunikasi (*law of technology of information and communication*), dan hukum tentang perdagangan dengan memakai elektronik (*e-commerce*).[103]

Menurut Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, maka yang dimaksud teknologi informasi adalah suatu teknik mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan menyebarkan informasi. Sedangkan yang dimaksud dengan sistem elektronik adalah serangkaian perangkat, dan prosedur erektronik yang berfungsi

[103] Munir Fuady, *Op.Cit*, hlm 168.

mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirim, atau menyebarkan informasi elektronik.

Selanjutnya, yang dimaksud dengan "informasi elektronik" adalah suatu atau sekumpulan data elektronik termasuk, tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI) (pertukaran data elektronik), surat elektronik (*electronic mail*), angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.[104]

Kemudian, yang dimaksud dengan transaksi elektronik adalah setiap perbuatan hukum yang dilakukan dengan menggunakan perangkat komputer, jaringan komputer, atau media elektronik lainnya.

Adapun yang dimaksud dengan dokumen elektronik adalah setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam. bentuk analog, digital, elektromagnetik, optikal, atau yang 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 yang sejenisnya, huruf, tanda, angka, kode akses, symbol, atau peforasi, yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

Penggunaan alat bukti elektronik dalam sistem hukum pembuktian didasari atas asas-asas sebagai berikut:[105]

---

[104] *Ibid.*
[105] *Ibid*, hlm 169.

1. Asas kepastian hukum;
2. Asas manfaat;
3. Asas kehati-hatian;
4. Asas itikad baik; dan
5. Asas kebebasan memilih teknologi atau netral teknologi.

Selanjutnya, pengakuan hukum pembuktian terhadap penggunaan dan pemanfaatan alat bukti elektronik dari teknologi informasi dan transaksi elektronik di Indonesia adalah sebagai berikut:[106]

1. Mencerdaskan kehidupan bangsa sebagai bagian dari masyarakat informasi dunia.
2. Meningkatkan perdagangan dan perekonomian nasional melalui bisnis dengan menggunakan *e-commerce*.
3. Meningkatkan efektivitas dan efisiensi pelayanan publik.
4. Memajukan pemikiran dan kemampuan masyarakat di bidang pemanfaatan teknologi informasi.
5. Memberikan rasa aman, keadilan, dan kepastian hukum bagi pengguna jasa teknologi informasi.

Telah disebutkan bahwa alat bukti elektronik berupa informasi elektronik, dokumen elektronik, dan hasil cetaknya dengan tegas diakui sebagai alat bukti yang sah dan penuh di pengadilan, baik dalam proses peradilan perdata, peradilan pidana maupun dalam peradilan-peradilan lainnya. Dengan demikian, penggunaan alat bukti elektronik ini merupakan bahkan merupakan tambahan atau perluasan dari alat bukti

[106] *Ibid.*

alat bukti yang telah ada dan diakui oleh hukum acara perdata ataupun hukum acara pidana.

Beberapa persyaratan yuridis di Indonesia agar suatu informasi elektronik, dokumen elektronik, dan hasil cetaknya dapat diakui sebagai alat bukti yang sah dan penuh adalah sebagai berikut:[107]

1. Para pihak yang melakukan transaksi elektronik harus beritikad baik dan dapat menuangkan transaksi elektronik tersebut dalam suatu kontrak elektronik.
2. Pernbuktian dengan sistem alat bukti elektronik tidak berlaku terhadap:
    a. Pembuktian yang oleh undang-undang disyaratkan dalam bentuk tertulis.
    b. Pembuktian yang oleh undang-undang disyaratkan dalam bentuk akta notaris atau akta yang dibuat oleh pejabat pembuat akta.
3. Menggunakan sistem elektronik sebagaimana yang ditentukan oleh undang-undang, yakni sistem elektronik yang berupa serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyirnpan, menampilkan, mengumumkan, mengirim, atau menyebarkan informasi elektronik.
4. Informasi yang terdapat dalam informasi elektronik atau dokumen elektronik dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan.
5. Jika digunakan "sertifikat elektronik" untuk mendukung suatu tanda tangan elektronik, penanda tangan harus memastikan kebenaran dan keutuhan semua

[107] *Ibid*, hlm 170.

informasi yang terkait dengan sertifikat elektronik tersebut. Sertifikat elektronik ini diberikan oleh Penyelenggara Sertifikat Elektronik yang diakui secara sah dengan tujuan untuk memastikan keabsahan suatu tanda tangan atau keterkaitan suatu tanda tangan elektronik dengan pemiliknya.

6. Tanda tangan elektronik baru mempunyai kekuatan hukum jika:[108]
   a. Data pembuatan tanda tangan elektronik hanya terkait dengan pihak penanda tangannya.
   b. Pada saat proses penandatanganan elektronik, maka data pembuatan tanda tangan elektronik hanya berada dalam kuasa pihak penanda tangan.
   c. Segala perubahan terhadap tanda tangan elektronik atau perubahan terhadap informasi elektronik yang terkait dengan tanda tangan elektronik tersebut, yang terjadi setelah waktu penandatanganan, dapat diketahui.
   d. Tersedianya cara-cara tertentu yang dipakai untuk mengidentifikasi siapa pihak penandatangannya.
   e. Tersedia cara-cara tertentu untuk menunjukkan bahwa penandatangan telah memberikan persetujuan terhadap informasi elektronik yang terkait.

[108] *Ibid*