

BAB II

TINJAUAN PUSTAKA

Bab ini menerangkan secara khusus mengenai perlindungan data pribadi dan Transaksi *e-commerce*, baik secara teori-teori dan doktrin secara umum maupun pengaturannya dalam beberapa peraturan perUndang-Undangan yang berlaku diluar daripada Undang-Undang Informasi dan Transaksi Elektronik. Kemudian diuraikan mengenai keamanan dan kerahasiaan data dalam komputer dan internet.

A. Tinjauan Umum Tentang Perlindungan Data Pribadi

Pada zaman sekarang, informasi merupakan hal yang penting dan menentukan perkembangan ekonomi suatu negara baik negara berkembang maupun negara maju. Informasi mengenai individu selalu dikelola oleh pemerintah dan swasta, tetapi munculnya era komputer menciptakan ancaman yang lebih besar bagi privasi individu tersebut, serta kemungkinan individu menderita kerugian sebagai akibat dari ketidaktelitian atau pembocoran informasi jauh lebih besar (Shinta Dewi, 2009:53). Era digital telah memicu ledakan pertumbuhan data pribadi yang dibuat, disimpan dan ditransmisikan pada komputer dan perangkat mobile, broadband dan situs internet dan media (Cammeron G Shilling, 2011:1). Kemajuan teknologi

juga menimbulkan ancaman serius bagi privasi pribadi dan keamanan informasi.

Konsep hukum telematika, mengemukakan bahwa data merupakan representasi formal suatu konsep, fakta, atau instruksi. Pada penggunaan sehari-hari data berarti suatu pernyataan yang diterima secara apa adanya (Purwanto 2007:13)

Pada *Data Protection Act* Pasal 1 ayat 1, data ialah setiap informasi yang diproses melalui peralatan yang berfungsi secara otomatis menanggapi perintah-perintah yang diberikan bagi tujuannya dan disimpan dengan maksud untuk dapat diproses. Data juga termasuk informasi yang merupakan bagian tertentu dari catatan-catatan kesehatan, kerja sosial, pendidikan, atau yang disimpan sebagai bagian dari suatu sistem yang relevan.

Menurut Purwanto data merupakan bahan baku informasi, yang didefinisikan sebagai kelompok teratur simbol-simbol yang mewakili kuantitas, tindakan, benda, dan sebagainya. Data terbentuk dari karakter yang dapat berupa alfabet, angka, maupun simbol khusus. Data disusun untuk diolah dalam bentuk struktur data, struktur file, dan data base (Purwanto, 2007:13)

Data dan juga informasi merupakan sumber daya yang sangat penting bagi jalannya suatu organisasi. Pada zaman sekarang ini organisasi yang mampu menggunakan data dan informasi secara cepat, benar, tepat dan lengkap yang mampu bersaing dengan rivalnya. Pengambilan keputusan

sebagai bagian dari kegiatan manusia tidak lepas dari adanya data dan informasi ini. Pengambilan keputusan tidak terjadi bila mana tidak ada data dan informasi.

Pada tahun 1970 Swedia dan Jerman telah mengeluarkan Undang-Undang mengenai perlindungan data. Undang-Undang ini dikeluarkan dikarenakan banyaknya telah di temukan penggunaan komputer dalam pemrosesan dan penyimpanan data, sehingga di perlukannya Undang-Undang untuk melindungi data tersebut. (Shinta Dewi, 2009:37).

Setiap Negara menggunakan istilah yang berbeda antara informasi pribadi dan data pribadi, tetapi secara substansif kedua istilah tersebut mempunyai pengertian yang hampir sama sehingga kedua istilah tersebut sering kali digunakan bergantian (Shinta Dewi, 2009:37).

Data pribadi terdiri dari fakta-fakta, pendapat atau komunikasi yang berkaitan dengan individu yang merupakan informasi sangat pribadi atau sensitif sehingga individu yang bersangkutan ingin menyimpan atau membatasi orang lain untuk mengoleksi, menggunakan, atau menyebarkan kepada pihak orang lain. Menurut Jerry Kang, data pribadi menggambarkan suatu informasi yang erat kaitannya dengan seseorang yang membedakan karakteristik masing-masing individu (Jerry Kang, 1998:5). Pada dasarnya perlindungan data di bagi atas 2 (dua) jenis yaitu bentuk perlindungan data yang berupa perlindungan fisik data, baik data yang terlihat maupun tidak terlihat (Shinta Dewi, 2009:9). Bentuk perlindungan

data yang berikutnya adalah sisi regulasi yang mengatur mengenai penggunaan data oleh orang lain yang tidak berhak, penyalahgunaan data untuk kepentingan tertentu, dan perusakan terhadap data itu sendiri (Shinta Dewi, 2009:10).

Pada berbagai Negara maju, digunakan istilah *privacy*/privasi sebagai hak yang harus dilindungi, yaitu hak seseorang untuk tidak di ganggu kehidupan pribadinya. Konsep privasi untuk pertama kalinya dikembangkan oleh warren dan Brandheis yang menulis sebuah artikel dalam jurnal ilmiah sekolah hukum Universitas Harvard yang berjudul “*The Right to Privacy*” atau hak untuk tidak diganggu. Dalam jurnal tersebut menurut Warren dan Brandheis dengan adanya perkembangan dan kemajuan teknologi maka timbul suatu kesadaran masyarakat bahwa ada hak seseorang untuk menikmati hidup. Hak untuk menikmati hidup tersebut diartikan sebagai hak untuk seseorang tidak diganggu kehidupan pribadinya baik oleh orang lain atau oleh Negara, oleh karena itu hukum harus mengakui dan melindungi hak privasi tersebut (Shinta Dewi, 2009:10).

Alasan privasi harus dilindungi yaitu (Shinta Dewi, 2009:10): Pertama, dalam membina hubungan dengan orang lain, seseorang harus menutup sebagian kehidupan pribadinya sehingga dia dapat mempertahankan posisinya pada tingkat tertentu. Kedua, seseorang di dalam kehidupannya memerlukan waktu untuk dapat menyendiri (*solitude*) sehingga privasi sangat diperlukan oleh seseorang. Ketiga, privasi adalah

hak yang berdiri sendiri dan tidak bergantung kepada hal lain tetapi hak ini hilang apabila orang tersebut mempublikasikan hal-hal yang bersifat pribadi kepada umum. Keempat, privasi juga termasuk hak seseorang untuk melakukan hubungan domestik termasuk bagaimana seseorang membina perkawinan, membina keluarganya dan orang lain tidak boleh mengetahui hubungan pribadi tersebut sehingga kemudian Warren menyebutnya sebagai *the right against the word*. Kelima, alasan lain mengapa privasi patut mendapat perlindungan hukum karena kerugian yang diderita sulit untuk dinilai dimana kerugiannya dirasakan jauh lebih besar dibandingkan dengan kerugian fisik, karena telah mengganggu kehidupan pribadinya sehingga bila ada kerugian yang diderita maka pihak korban wajib mendapat kompensasi.

Privasi merupakan suatu konsep yang sangat sulit didefinisikan karena setiap orang memberi batasan yang berbeda tergantung dari sisi mana orang menilainya.

B. Keamanan dan Kerahasiaan Data Pribadi Dalam Teknologi Informasi.

Seiring dengan pesatnya perkembangan di bidang teknologi dan informasi, data menjadi suatu komoditi yang eksklusif. Perlindungan data saat ini menjadi fenomena yang menarik karena itu tindakan-tindakan preventif atas pencurian, pembobolan dan kerusakan data dan informasi perlu untuk mendapatkan pemikiran mengenai perlindungannya. Keamanan dan

kerahasiaan data pada jaringan komputer saat ini menjadi isu yang sangat penting dan terus berkembang.

Beberapa kasus menyangkut sistem keamanan saat ini menjadi suatu garapan yang membutuhkan biaya penanganan dan pengamanan yang sedemikian besar. Sistem-sistem vital seperti sistem pertahanan, sistem perbankan, sistem *e-commerce* dan sistem-sistem setingkat itu membutuhkan tingkat keamanan yang sedemikian tinggi. Hal ini lebih disebabkan oleh kemajuan bidang jaringan komputer dengan konsep *open system*-nya sehingga siapapun, dimanapun, dan kapanpun mempunyai kesempatan untuk mengakses kawasan-kawasan vital tersebut.

Untuk menjaga keamanan dan kerahasiaan data dalam suatu jaringan komputer, diperlukan beberapa jenis enkripsi agar data tidak dapat dibaca atau dimengerti oleh sembarangan orang kecuali untuk penerima yang berhak. Pengamanan data tersebut selain bertujuan untuk meningkatkan keamanan data, juga berfungsi untuk:

1. Melindungi data agar tidak dapat dibaca oleh orang/pihak yang tidak berhak
2. Mencegah agar orang/pihak yang tidak berhak tidak menyisipkan, menghapus, dan merubah data.

Selain keamanan dan kerahasiaan data dalam jaringan komputer, konsep ini juga berlaku untuk keamanan dan kerahasiaan data pada internet. Hal ini mengingat bahwa kemajuan yang dicapai dalam bidang

pengembangan sistem operasi komputer sendiri dan utilitasnya sudah sedemikian jauh dimana tingkat performansi, kehandalan, dan fleksibilitas *software* menjadi kriteria utama dan berharganya informasi tersebut dan ditunjang oleh kemampuan pengembangan *software* tentunya menarik minat para pembobol (*hacker*) dan penyusup (*intruder*).

Masalah keamanan dan kerahasiaan data merupakan salah satu aspek paling penting dari suatu sistem informasi. Hal ini terkait dengan begitu pentingnya informasi tersebut dikirim dan diterima oleh orang yang berkepentingan. Informasi tidak berguna lagi apabila di tengah jalan informasi itu disadap atau dibajak oleh orang tidak berhak. Oleh karena itu, pengamanan dalam sistem informasi telah menjadi isu hangat ketika transaksi elektronik mulai diperkenalkan. Tanpa pengamanan yang ketat dan canggih, perkembangan teknologi informasi tidak memberikan manfaat yang maksimal kepada masyarakat.

Terhubungnya sebuah sistem informasi dengan Internet membuka peluang adanya kejahatan melalui jaringan komputer. Hal ini menimbulkan tantangan bagi penegak hukum. Hukum dari sebagian besar negara di dunia belum menjangkau daerah *cyberspace*. Saat ini hampir semua negara di dunia berlomba-lomba untuk menyiapkan landasan hukum bagi internet. Terkait dengan masalah yang terjadi dan perlunya pengamanan terhadap data yang ada dalam komputer, lingkup keamanan data dari suatu sistem komputer mencakup hal-hal yang tidak saja berkaitan dengan keamanan

fisik, keamanan akses, keamanan file dan data, keamanan jaringan, tetapi terdapat hal-hal lainnya (Purwanto, 2007:49). Ancaman paling signifikan terhadap keamanan dari sistem komputer pada saat ini bukan berupa ancaman terhadap keamanan fisik, tetapi juga ancaman terhadap keamanan non-fisik yang dapat dibagi dalam 2 (dua) kategori yaitu (Purwanto, 2007:50): *Intruders* dan *Malicious Program*.

Perlindungan data dalam sistem keamanan komputer di kenal dengan nama metodologi keamanan komputer. Keamanan komputer memiliki cabang yang sangat banyak, dalam masalah keamanan pertimbangan-pertimbangan untuk mengamankan sistem harus di perhatikan seperti keamanan database, keamanan data, keamanan komputer, keamanan perangkat komputer, keamanan aplikasi, keamanan jaringan dan keamanan informasi. Metodologi keamanan komputer merupakan sesuatu yang sangat penting dalam masalah keamanan komputer karena semua elemen saling berkaitan. (Ariyus Dony, 2006:6).

Menurut Dony Ariyus, (Dony Ariyus, 2006:7) keamanan dasar dari komputer terdiri dari 4 level yang terdiri dari:

1. Keamanan level 0

Merupakan keamanan fisik yang merupakan keamanan tahap awal dari komputer *security*. Jika keamanan fisik tidak terjaga dengan baik maka data-data, bahkan hardware komputer sendiri tidak dapat diamankan.

2. Keamanan level 1

Terdiri dari keamanan pc itu sendiri, *device*, *application* yang di gunakan untuk mengamankan sebuah *database*. Contohnya, jika kita ingin *database* aman, maka kita harus memperhatikan dahulu apakah aplikasi yang di pakai untuk membuat desain *database* tersebut merupakan aplikasi yang sudah di akui keamanannya, seperti *oracle*. Selain itu kita harus memperhatikan sisi lain yaitu data security. Data security adalah cara mendesain *database* tersebut. Selanjutnya *device security* adalah ala-alat apa yang dipakai supaya keamanan dari komputer terjaga dan tidak kalah pentingnya adalah keamanan dari komputer itu sendiri. Keamanan komputer disini adalah keamanan fisik dari orang-orang yang tidak berhak mengakses komputer tempat *database* tersebut disimpan.

3. Keamanan level 2

Keamanan level 2 adalah *network security*. Komputer yang terhubung dengan jaringan, baik itu *LAN (Local Area Network)*, *WAN (Wide Area Network)*, maupun Internet, sangat rawan dalam masalah keamanan karena komputer server bisa diakses menggunakan komputer *client*, baik itu untuk merusak data, mencuri data, maupun melakukan perbuatan-perbuatan lainnya.

Oleh karena itu, setelah keamanan level 1 selesai dikerjakan maka keamanan level 2 harus dirancang supaya tidak terjadi kebocoran jaringan, akses ilegal, dan perbuatan-perbuatan yang dapat merusak keamanan data tersebut.

4. Keamanan level 3

Keamanan level 3 adalah *information security*. Keamanan informasi yang dimaksud disini adalah keamanan informasi-informasi yang kadang kala tidak begitu diperdulikan oleh administrator atau pegawai, seperti memberikan *password* kepada teman, kertas-kertas bekas transaksim dan lain sebagainya. Hal tersebut bisa menjadi sesuatu yang dianggap fatal. Jika informasi-informasi tersebut diketahui oleh orang yang tidak bertanggung jawab, maka mereka dapat mengakses data-data penting yang ada di dalam komputer.

5. Keamanan level 4

Keamanan level 4 admerupakan keamanan secara keseluruhan dari komputer. Jika level 0-3 sudah dapat dikerjakan dengan baik, maka otomatis keamanan untuk level 4 sudah terpenuhi tetapi jikalau salah satu dari level tersebut belum bisa terpenuhi, maka masih ada lubang keamanan yang bisa diakses. (Dony Ariyus, 2006:7)

Meskipun level 4 sudah memenuhi syarat, tetapi tidak menutup kemungkinan adanya penyusupan oleh *user* ilegal.

Setelah langkah keamanan tersebut telah dijalankan maka ada tiga langkah selanjutnya yang dikerjakan yaitu mendeteksi, mencegah, dan mempertahankan.

Untuk mengenali sebuah serangan yang dilakukan oleh *hacker* atau *cracker*, digunakan data yang telah diperoleh. Pendekatan yang sering digunakan untuk mengenali serangan tersebut antara lain adalah:

1. *Anomaly detection* (deteksi penyimpangan).

Anomaly detector mengidentifikasi perilaku tak lazim yang terjadi dalam host atau network. Detektor berfungsi dengan asumsi bahwa serangan itu dapat dideteksi dengan sistem yang mampu mengidentifikasi perbedaan tersebut. *Anomaly detector* menyusun profil-profil yang merepresentasikan kebiasaan *user* yang normal, *host*, atau koneksi jaringan. Profil-profil tersebut dibangun atas data-data historis yang di kumpulkan dalam periode operasi normal. Selanjutnya, detektor mengumpulkan data-data peristiwa dan menggunakan langkah-langkah beragam ketika aktivitas yang diamati menyimpang dari normal.

2. *Misuse detection*

Detektor yang melakukan analisis terhadap aktivitas sistem, mencari *event* atau set *event* yang cocok dengan pola perilaku yang dikenali sebagai serangan. Pola perilaku serangan itu disebut *signatures*. Oleh karena itu, *misuse detection* banyak dikenal sebagai *signature based detection*.

C. Regulasi mengenai Ketentuan Perlindungan Data Pribadi di Indonesia

Sampai sejauh ini Indonesia belum memiliki kebijakan atau regulasi mengenai perlindungan data pribadi dalam satu peraturan khusus. Pengaturan mengenai hal tersebut masih termuat secara terpisah di beberapa perUndang-Undangan dan hanya mencerminkan aspek perlindungan data

pribadi secara umum. Adapun pengaturan tersebut antara lain terdapat dalam Undang-Undang Informasi dan Teknologi, Undang-Undang nomor 7 tahun 1971 tentang Ketentuan-Ketentuan Pokok Kearsipan, Undang-Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan, Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 2 tahun 1992 tentang Perbankan, Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan, Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi dan Undang-Undang Nomor 24 Tahun 2013 tentang perubahan Atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan.

Menurut Peraturan Pemerintah Nomor 52 Tahun 2000 tentang Penyelenggaraan Telekomunikasi yang merupakan peraturan pelaksana dari Undang-Undang Telekomunikasi, internet dimasukkan dalam jenis jasa multimedia, yang diidentifikasi sebagai penyelenggara jasa komunikasi yang menawarkan layanan berbasis teknologi informasi. Hal tersebut menunjukkan bahwa pengaturan internet termasuk kedalam peraturan tentang telekomunikasi. Undang-Undang Telekomunikasi mengatur beberapa hal yang berkenaan dengan kerahasiaan informasi antara lain dalam Pasal 22 dinyatakan, bahwa setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau manipulasi: (a) akses ke jasa telekomunikasi; dan/atau (b) akses ke jasa telekomunikasi; dan atau (c) akses ke jaringan telekomunikasi khusus.

Pengaturan mengenai perlindungan terhadap data pribadi pengguna internet lebih lanjut terdapat dalam Undang-Undang Informasi dan Transaksi Elektronik. Undang-Undang ini memang belum memuat aturan perlindungan data pribadi secara khusus. Meskipun demikian, secara Implisit Undang-Undang ini memunculkan pemahaman baru mengenai perlindungan terhadap keberadaan suatu data atau informasi elektronik baik yang bersifat umum atau pribadi.

Perlindungan data pribadi dalam sebuah sistem elektronik di Undang-Undang ITE Nomor 19 Tahun 2016 meliputi perlindungan dari penggunaan tanpa izin, perlindungan oleh penyelenggara sistem elektronik, dan perlindungan dari akses dan intervensi *illegal*. Terkait dengan perlindungan data pribadi dari penggunaan tanpa izin, Pasal 26 Undang-Undang ITE mensyaratkan bahwa penggunaan setiap data pribadi dalam sebuah media elektronik harus mendapat persetujuan pemilik data bersangkutan. Setiap orang yang melanggar ketentuan ini dapat digugat atas kerugian yang di timbulkan.

Bunyi Pasal 26 Undang-Undang Nomor 19 Tahun 2016 Tentang ITE adalah sebagai berikut:

- 1. Penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan.*

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

Penjelasan Pasal 26 Undang-Undang Nomor 19 Tahun 2016 Tentang ITE menyatakan bahwa data pribadi merupakan salah satu bagian dari hak pribadi seseorang. Sedangkan definisi Pasal 1 Peraturan Pemerintah No 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik yaitu data perorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya.

Penjelasan Pasal 26 ayat (1) Undang-Undang Nomor 19 Tahun 2016 Tentang ITE juga menerangkan lebih jauh tentang pengertian hak pribadi. Isi penjelasan itu adalah sebagai berikut:

Dalam pemanfaatan teknologi informasi, perlindungan data pribadi merupakan salah satu bagian dari hak pribadi. Hak pribadi mengandung pengertian sebagai berikut:

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

Bila ditarik penafsiran secara umum, maka perlindungan data sebenarnya telah diatur kedapalm Pasal-Pasal selanjutnya dalam Undang-

Undang ITE, yaitu Pasal 30-33 dan Pasal 35 yang masuk kedalam BAB VII mengenai Perbuatan yang Dilarang. Secara tegas, Undang-Undang ITE melarang adanya akses secara melawan hukum kepada data pribadi milik orang lain melalui sistem elektronik untuk memperoleh informasi dengan cara menerobos sistem pengaman. Selain itu juga Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik menyatakan bahwa penyadapan (*interception*) adalah termasuk perbuatan yang dilarang kecuali dilakukan oleh pihak yang memiliki kewenangan untuk itu dalam rangka upaya hukum. Setiap orang yang merasa dirugikan akibat dilakukannya perbuatan yang dilarang tersebut dapat mengajukan gugatan ganti kerugian, dan pelaku pun mempunyai tanggung gugat atas apa yang dilakukannya.

D. Transaksi *E-commerce* dan Manfaatnya

Perdagangan Elektronik (*E-commerce = Electronic commerce*) adalah bagian dari *e-lifestyle* yang memungkinkan transaksi jual beli dilakukan secara online dari sudut tempat mana pun (Hidayat Taufik, 2010:5). *E-commerce* juga dapat diartikan sebagai suatu proses berbisnis dengan menggunakan teknologi elektronik yang menghubungkan antara perusahaan, konsumen dan masyarakat dalam bentuk transaksi elektronik dan pertukaran/penjualan barang, servis, dan informasi secara elektronik (Munawar, Kholil. 2009: *E-commerce*. <http://staff.uns.ac.id>)

Sedangkan pengertian *E-commerce* (Perdagangan Elektronik) menurut Jony Wong (Wong Jony, 2010:33) adalah pembelian, penjualan dan pemasaran barang serta jasa melalui sistem elektronik. Seperti televisi, radio dan jaringan komputer atau internet.

Menurut Vermaat (Varmaat, Shelly Cashman, 2007: 83.) *E-commerce* merupakan transaksi bisnis yang terjadi dalam jaringan elektronik seperti internet. Siapapun yang mempunyai jaringan internet dapat berpartisipasi dalam kegiatan *E-commerce*.

E-commerce memiliki beberapa manfaat, baik itu organisasi, perusahaan dan masyarakat itu sendiri, berikut beberapa manfaat dari *E-commerce* (Suyanto, 2003:50-51):

a. Bagi organisasi pemilik *E-commerce*

- 1) Memperluas market place hingga ke pasar nasional dan internasional.
- 2) Dengan capital outlay yang minim, sebuah perusahaan dapat dengan mudah menemukan lebih banyak pelanggan, supplier yang lebih baik dan partner bisnis yang paling cocok dari seluruh dunia.
- 3) *E-commerce* menurunkan biaya pembuatan, pemrosesan, pendistribusian, penyimpanan, dan pencarian informasi yang menggunakan kertas.
- 4) *E-commerce* mengurangi waktu antara outlay modal dan penerimaan produk dan jasa.

b. Bagi konsumen

- 1) *E-commerce* memungkinkan pelanggan untuk berbelanja atau melakukan transaksi selama 24 jam sehari sepanjang tahun dari hampir setiap lokasi.
- 2) *E-commerce* memberikan lebih banyak pilihan kepada pelanggan, mereka bisa memilih berbagai produk dari banyak vendor.
- 3) *E-commerce* menyediakan produk dan jasa yang tidak mahal kepada pelanggan dengan mengunjungi banyak tempat dan melakukan perbandingan secara cepat.
- 4) Pelanggan bisa menerima informasi yang relevan secara detil dalam hitungan detik, bukan lagi hari atau minggu.

Perdagangan dalam dunia elektronik juga mempunyai beberapa tahapan agar dapat terjadinya suatu proses perdagangan antara pembeli dan pelaku usaha tersebut, proses tersebut mencakup tahap-tahap yang dapat diuraikan sebagai berikut (Suyanto, 2003:46):

1. *Show*. Penjual menunjukkan produk atau layanannya di situs yang dimiliki, lengkap dengan detail spesifikasi produk dan harganya.
2. *Register*. Konsumen melakukan register untuk memasukkan data-data identitas, alamat pengiriman dan informasi *login*.
3. *Order*. Setelah konsumen memilih produk yang diinginkan, konsumen pun selanjutnya melakukan order pembelian.
4. *Payment*. Konsumen melakukan pembayaran.

5. *Verification*. Verifikasi data konsumen seperti data-data pembayaran (No. rekening atau kartu kredit).
6. *Deliver*. Produk yang dipesan pembeli kemudian dikirimkan oleh penjual ke konsumen.

Setelah melihat tahapan proses dari perdagangan *e-commerce*, maka kita juga perlu melihat apa perbedaan yang mencolok antara perdagangan dalam *e-commerce* sangat berbeda dengan perdagangan konvensional. Perdagangan *e-commerce* identik dengan mempertemukan penjual serta pembeli melalui media internet/telekomunikasi. Berikut ini merupakan karakteristik *e-commerce* yang membedakannya dengan perdagangan konvensional:

1. Karakteristik *E-commerce*
 - a. Transaksi yang dilakukan tidak hanya dalam lingkup nasional, melainkan dapat mencapai lingkup internasional;
 - b. Transaksi yang dilakukan tidak mengenal siapa penjual dan siapa pembeli;
 - c. Terjadinya transaksi antara dua belah pihak;
 - d. Adanya pertukaran barang, jasa, atau informasi;
 - e. Internet merupakan medium utama dalam proses atau mekanisme perdagangan tersebut;

Bisnis *e-commerce* mulai bertumbuh dengan cepat sejak tahun 1998. Pada awal pertumbuhannya tipe bisnis ini hanya melingkupi bidang

business to consumer. Namun pada perkembangannya bisnis ini mulai melingkupi hal yang lain, berikut penjabarannya (Adi Sulisty, 2016: 13-23):

1. Jenis-jenis *E-commerce*

Jenis-jenis *e-commerce* yang sering dilakukan:

a. B2B (*Business to Business*)

B2B adalah transaksi secara elektronik antara entitas atau obyek bisnis yang satu ke obyek bisnis lainnya.

b. B2C (*Business to Consumer*)

B2C adalah kegiatan *E-Businesses* dalam pelayanan secara langsung kepada konsumen melalui barang atau jasa, dengan penjualan langsung di internet dan pemesanan dapat langsung dilakukan oleh konsumen karena biaya sudah tercantum.

c. C2C (*Consumer to Consumer*)

C2C merupakan sistem komunikasi dan transaksi bisnis antara konsumen untuk memenuhi kebutuhan tertentu pada saat tertentu.

d. C2B (*Consumer to Bussines*)

C2B adalah suatu model bisnis dimana seorang konsumen dapat menjadi seorang konsumen yang menawarkan berbagai produk maupun pengembangan produk itu sendiri atau menawarkan jasa kepada perusahaan tertentu yang nantinya perusahaan membayar jasa atau produk tersebut, konsep ini kebalikan dari B2C.

Melihat jenis-jenis *e-commerce* yang sering dilakukan kita tidak boleh melupakan bagaimana metode pembayaran yang digunakan dalam suatu transaksi *e-commerce*. Metode pembayaran dalam transaksi *e-commerce* sangat penting untuk di perhatikan karena kerap kali dalam metode pembayaran inilah terdapat celah bagi orang-orang yang tidak bertanggung jawab untuk mencuri data dari seorang konsumen. Berikut ini merupakan metode pembayaran yang dilakukan dalam sebuah transaksi *e-commerce*:

1. Kartu magnetik (*Magnetic Stripe Card*).

Kartu magnetik adalah kartu plastik kecil yang memiliki pita termagnetisasi di permukaannya. Kartu magnetik digunakan secara luas untuk aplikasi-aplikasi seperti kartu debit, kartu kredit, kartu telpon, kartu ATM, kartu yang digunakan untuk masuk ke gedung-gedung yang memiliki perangkat keamanan tertentu, dan sebagainya. Dalam hal ini, kartu magnetik dapat diperluas fungsinya menjadi kartu yang dapat digunakan untuk melakukan transaksi-transaksi pembelian barang dan/atau jasa dalam kaitannya dengan perdagangan elektronik.

Kartu magnetik biasanya memiliki pita magnetik yang mengandung 2 atau 3 jalur informasi. Pengkodean informasi biasanya dilakukan mengikuti standar ISO (*international standar Organization*). kemudian, mesin pembaca kartu magnetik yang bersangkutan biasanya dapat membaca dan mengkodekan informasi-informasi yang ada pada kartu magnetik tersebut. Data-data pada kartu itu juga dapat disandikan

(enkripsi), sehingga aman bagi para pencuri yang mampu menyalang informasi-informasi di kartu tersebut ke kartu yang lainnya.

2. Kartu Kredit

Transaksi dalam menggunakan kartu kredit, konsumen memberikan nomor kartu kreditnya ke pedagang. Pedagang kemudian dapat memverifikasi nomor itu ke bank penerbit dan kemudian pedagang tersebut dapat membuat slip pembelian bagi konsumen untuk disetujui. Pedagang kemudian dapat menggunakan slip pembelanjaan itu untuk mendapatkan uang dari bank. Terdapat dua fitur yang melindungi keamanan transaksi di internet serta perangkat lunak pengelola yang di butuhkan saat menggunakan kartu kredit. 2 cara tersebut adalah mengirimkan kartu kredit yang tidak tersandikan lewat jaringan internet, atau menyandikan nomor kartu kredit sebelum transaksi yang bersangkutan ditransmisikan. Jika transmisi terbatas antara konsumen dan pedagang disandikan, pedagang harus mengembalikan data tersandikan tadi ke bentuk semula sehingga data tadi dapat digunakan untuk melengkapi proses pembelian.

3. Cek Elektronik

Sistem pembayaran menggunakan kartu kredit tidak dapat disangkal lagi merupakan sistem pembayaran yang paling populer dalam perdagangan di internet, tetapi ia bukan satu-satunya metode pembayaran di internet. Hingga saat ini ada 2 sistem yang dikembangkan oleh *Financial Service Technology Corporation*, yang lainnya oleh *Cybercash* yang

memungkinkan konsumen menggunakan cek elektronik untuk membayar secara langsung kepada pedagang di Web.

4. *Digital Cash*

Pada sistem *digital cash*, nilai uang terbentuk tidak lebih dari untaian bit-bit. Bank dapat mendebit rekening kita dengan sejumlah penarikan yang nilainya sama dengan nilai uang (sering disebut token) yang digunakan. Bank dapat melakukan validasi masing-masing token dengan penanda digital (*digital stamp*) sebelum mentransmisikannya ke komputer pribadi kita, dan mentransmisikan sejumlah *token* ke penjual, yang kemudian melakukan verifikasi kebank dan menarik dananya. Untuk kebanyakan sistem, masalah terbesar yang harus dihadapi adalah masalah keamanan. Dalam hal ini kita harus memberi perlindungan yang memadai pada setiap token yang di kirimkan dari konsumen ke pedagang. Skema-skema penyandian (enkripsi canggih seperti yang di usulkan *Netcash* mungkin dapat digunakan dengan resiko penurunan kinerja transaksi (dalam hal kecepatannya).

5. Kartu Pintar (*Smart Card*)

Kartu pintar adalah kartu plastik kecil yang bentuk dan tampilannya mirip dengan kartu magnetik biasa, tetapi didalamnya mengandung suatu mikroprosesor dan tempat penyimpanan (memori). Teknologi kartu pintar merupakan inovasi yang mengatasi keterbatasan-keterbatasan yang dimiliki oleh kartu magnetik yang kita bahas di subbab sebelumnya, yang relatif mudah rusak oleh goresan-goresan di

bagian pita magnetiknya. Data-data yang tersimpan di kartu pintar relatif tahan terhadap kerusakan-kerusakan yang biasa terjadi pada kartu magnetik, seperti goresan, pemberian medan magnetik, dan sebagainya, biasanya kartu pintar lebih tahan 100 kali dari kartu magnetik. Kartu pintar pertama kali ditemukan di Eropa, tetapi penggunaannya berkembang di Amerika Serikat, sebelum akhirnya digunakan di seluruh dunia. Dalam hal ini, kartu pintar dapat dikelompokkan menjadi 2 kategori yaitu *memory smart card* dan *intelligent smart card*. *Memory smart card* memiliki kemampuan pemrosesan dan kapasitas memori yang lebih rendah/kecil dibandingkan *intelligent smart card* untuk melakukan pemrosesan tambahan yang dibutuhkan. Penggunaan kartu pintar seringkali lebih aman, karena kartu pintar memiliki mikroprosesor didalamnya dan data-data pada kartu pintar juga dapat disandikan menggunakan protokol SET (*Secure Electronic Transaction*)(Nugroho Adi, 2006:90).