BAB I

PENDAHULUAN

A. Latar Belakang

Perkembangan ilmu pengetahuan dan teknologi, terutama teknologi informasi seperti internet sangat menunjang setiap orang mencapai tujuan hidupnya dalam waktu singkat, baik legal maupun illegal dengan menghalalkan segala cara karena ingin memperoleh keuntungan. Dampak buruk dari perkembangan dunia maya ini tidak dapat dihindarkan dalam kehidupan masyarakat modern saat ini dan masa depan. Berkembangnya teknologi informasi menimbulkan kekhawatiran pada perkembangan tindak pidana di bidang teknologi informasi yang berhubungan dengan *cybercrime* atau kejahatan mayantara.

> Kemajuan teknologi informasi dan komunikasi sudah semakin cepat sehingga mempengaruhi setiap aspek kehidupan manusia, tanpa disadari produk teknologi sudah menjadi kebutuhan sehari-hari, penggunaan televisi, telepon, fax, *cellular (handphone)* dan internet sudah bukan hal yang aneh dan baru khususnya di kota-kota besar.[1]

Informasi yang dapat diakses secara cepat dan efektif melalui telepon rumah, telepon genggam, televisi, komputer, jaringan internet dan berbagai media elektronik, telah menggeser cara manusia bekerja, belajar, mengelola perusahaan, menjalankan pemerintahan, berbelanja ataupun melakukan kegiatan perdagangan. Kenyataan demikian sering disebut sebagai era globalisasi ataupun revolusi informasi, untuk menggambarkan

[1] Dikdik M Arief Mansur dan Elisatris Gultom, ***Cyber Law Aspek Hukum Teknologi Informasi, Repika*** Aditama, Bandung, 2015, h. 121

betapa mudahnya berbagai jenis informasi dapat di akses, dicari, dikumpulkan serta dapat dikirimkan tanpa lagi mengenal batas-batas geografis suatu negara.

Teknologi informasi memegang peran yang penting baik di masa kini, maupun di masa yang akan datang.[2] Menurut Didik J. Rachbini, "teknologi informasi dan media elektronika dinilai sebagai simbol pelopor, yang akan mengintegrasikan seluruh sistem dunia, baik dalam aspek sosial, budaya, ekonomi dan keuangan".[3] "Era globalisasi yang dilalui menjadi tanda perkembangan teknologi itu sendiri. Globalisasi telah menjadi pendorong lahirnya era perkembangan teknologi informasi."[4] Sehingga dampak dari globalisasi dan perkembangan teknologi saat ini dapat kita lihat sendiri yaitu maraknya anak-anak kecil yang sudah memainkan alat-alat elektronik yang canggih. Dimana melalui alat-alat elektronik tersebut dapat memasuki dunia yang seolah nyata melalui jaringan internet yang lebih sering dikenal dengan dunia maya.

Perkembangan teknologi informasi yang sedemikian rupa, membuat dunia telah memasuki era baru komunikasi. Dengan demikian, teknologi informasi ini telah mengubah perilaku masyarakat global. Di samping itu perkembangan teknologi informasi telah menyebabkan dunia menjadi tanpa batas *(borderless)* dan menyebabkan perubahan sosial secara

---

[2]Agus Raharjo, ***Cybercrime - Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi***Citra Aditya Bakti, Bandung, 2012, h. 1

[3]Dikdik M. Arief Mansur dan Elisatris Gultom, ***Op.Cit,*** h. 1.

[4]Budi Suharyanto, ***Tindak Pidana Teknologi Informasi (Cyber Crime), Urgensi Pengaturan dan Celah Hukumnya***, Rajawali Pers, Jakarta, 2013, h. 1.

signifikan berlangsung demikian cepat. “Teknologi informasi saat ini telah menjadi pedang bermata dua, karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi sarana efektif bagi terjadinya perbuatan-perbuatan melawan hukum”.[5] Dengan terjadinya perbuatan melawan hukum tersebut, maka ruang lingkup hukum harus diperluas untuk dapat menjangkau perbuatan-perbuatan tersebut.

> Akibat perkembangan teknologi informasi lahirlah suatu era baru yang dikenal dengan hukum telematika. Hukum telematika dapat juga disebut dengan hukum siber. Hal ini didasari pada argumentasi bahwa hukum siber (*cyber crime*) merupakan kegiatan yang memanfaatkan komputer sebagai media yang didukung oleh sistem telekomunikasi baik itu *dial up system*, menggunakan jalur telepon, maupun *wireless system* yang menggunakan antena khusus nirkabel.[6]

Seiring dengan perkembangan tersebut, ternyata teknologi informasi yang berkembang dalam jaringan internet juga menyebabkan terjadinya kejahatan pada dunia internet itu sendiri. Permasalahan hukum yang yang sering kali kita hadapi adalah ketika terkait dengan penyampaian informasi, komunikasi dan/atau transaksi secara elektronik, khususnya dalam hal pembuktian dan hal yang terkait dengan perbuatan hukum yang dilaksanakan melalui sistem elektronik.

> Teknologi dan Hukum merupakan dua unsur yang saling mempengaruhi dan keduanya juga mempengaruhi masyarakat. Di satu sisi teknologi dapat dilihat sebagai sarana untuk mencapai tujuan tertentu, akan tetapi, di sisi lain teknologi juga dapat dilihat sebagai aktivitas manusiawi. Pada dasarnya, setiap teknologi dikembangkan untuk memenuhi kebutuhan tertentu dan melalui teknologi itu diberikan

---

[5] ***Ibid***, h. 2.

[6] Judhariksawan, ***Pengantar Hukum Telekomunikasi*** Raja Grafindo Persada, Jakarta, 2015, h. 12.

> suatu manfaat dan layanan bagi manusia termasuk meningkatkan keefisienan dan keefektivitasan kerja.[7]

Pemanfaatan teknologi dan informasi dapat dirasakan manfaatnya baik di bidang pendidikan dan perekonomian dan lain-lain, hal-hal yang berkaitan dengan perkembanagan ilmu pengetahuan, sains dan lain sebagainya yang dengan mudah dapat di akses. Perkembangan teknologi dan informasi ini tidak saja memberikan manfaat melainkan juga mengakibatkan masalah yang dapat merugikan masyarakat, seperti halnya penyalahgunaan data, pencurian data pribadi, penjualan data pribadi, penipuan dan lain-lain.

> Pelaku usaha atau penyelenggara sistem elektronik dapat mengumpulkan data pribadi dari pelanggan atau calon pelanggan secara *daring*, dimana data digital dapat diperjualbelikan tanpa sepengetahuan dan seizin pemilik data atau disalahgunakan (untuk tujuan di luar pemberian, penyerahan data pribadi digital), bisa juga terjadi data pribadi yang terkoneksi dibajak, dicuri *(hack)* oleh pihak ketiga. [8]

Penyalahgunaan data pribadi merupakan perbuatan yang memenuhi unsur-unsur perbuatan pidana seperti unsur tindak pidana pencurian dan unsur tindak pidana penipuan serta tindak pidana lainnya baik dari sisi unsur objektif maupun unsur subjektif. Dengan adanya penyalahgunaan data pribadi, maka dapat terlihat adanya kelemahan sistem, kurangnya pengawasan, sehingga data pribadi dapat disalahgunakan dan mengakibatkan kerugian bagi pemilik data tersebut. Penyalahgunaan,

---

[7]Josua Sitompul, ***Cyberspace, Cybercrimes, Cyberlaw : Tinjauan Aspek Hukum Pidana*****,** Tatanusa, Jakarta, 2012, h. 31

[8] Sahat Maruli Tua Situmeang, "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber", *Jurnal* Sasi, Volume 27 Nomor 1, Januari-Maret 2021, h.39.

pencurian, penjualan data pribadi merupakan suatu pelanggaran hukum dalam bidang teknologi informasi dan juga dapat dikategorikan sebagai pelanggaran atas hak asasi manusia, karena data pribadi merupakan bagian dari hak asasi manusia yang harus dilindungi.

Persaingan yang sangat ketat dihadapi oleh para pelaku usaha operator dalam menarik minat para konsumennya. Banyak produk yang ditawarkan dengan harga-harga menarik, bahkan ada operator yang menawarkan SMS (*Short Message Service*) gratis atau biaya percakapan gratis. Hal ini dimanfaatkan konsumen untuk memilih produk yang akan digunakan sehingga banyak konsumen yang sering melakukan ganti nomor telepon selulernya hanya untuk memanfaatkan promosi harga yang murah. Pemanfaatan konsumeris itu diindikasikan menjadi peluang bagi pihak pemilik *provider* untuk mengambil keuntungan sebesar-besarnya.

Seiring dengan lajunya perkembangan informasi dan teknologi, maka tidak luput dari masalah terutama mengenai penyalahgunaan Nomor Induk Kependudukan (NIK) dan nomor Kartu Keluarga (KK) untuk melakukan registrasi kartu prabayar. Penyalahgunaan NIK hingga potensi timbulnya kejahatan itu muncul akibat belum ada regulasi yang jelas mengenai penggunaan NIK pada saat melakukan registrasi kartu prabayar, meski Kominfo telah mengeluarkan Permenkominfo No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik, namun belum adanya regulasi perlindungan data privasi yang komprehensif, menjadikan rentannya data-data pribadi yang dikumpulkan. Termasuk regulasi yang

mampu mengikat seluruh kementerian/lembaga, juga swasta dalam berbagai sektor, serta adanya sanksi dan pemulihan jika terjadi pelanggaran penyalahgunaan data pribadi.

Tindakan kejahatan akibat penyalahgunaan NIK untuk registrasi prabayar ini, merupakan dampak dari pengaturan yang tidak teratur, karena banyaknya tindak pidana yang menggunakan handphone dengan kartu prabayar yang didaftarkan menggunakan NIK yang tidak sah tersebut.

Adanya Surat Edaran Badan Regulasi Telekomunikasi Indonesia (BRTI) Nomor 01 Tahun 2018 tentang larangan penggunaan data kependudukan tanpa hak atau melawan hukum untuk keperluan registrasi pelanggan jasa telekomunikasi, membuat kepolisian memiliki landasan untuk menjerat para pelaku penyalahgunaan NIK itu dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE).

Apabila ada pihak-pihak yang turut serta membantu tindak pidana penyalahgunaan NIK untuk registrasi prabayar akan diancam Pasal 55 Kitab Undang-Undang Hukum Pidana (selanjutnya disebut KUHP) sehingga jika ditemukan *dealer, provider* bahkan regulator yang ikut serta dalam penyalahgunaan NIK untuk registrasi prabayar ini akan diancam dengan hukuman pidana.

Tindak pidana penyalahgunaan data kependudukan dengan cara mengaktifkan kartu prabayar *Global Sytem For Mobile* (GSM) dengan NIK

secara illegal melanggar Pasal 51 ayat (1) UU ITE seperti dalam putusan Nomor 461/Pid/Sus/2020/PN. Sda dengan terdakwa Vinna Primakusuma Dewi dan Yogi Budi Dharma. Berdasarkan putusan di atas menjelaskan bahwa kejahatan manipulasi informasi elektronik dilakukan oleh para terdakwa dengan melakukan tindak pidana dengan sengaja tanpa hak dan melawan hukum bersama-sama manipulasi informasi elektronik dengan tujuan agar informasi elektronik tersebut dianggap sebagai data yang otrentik.

Berdasarkan latar belakang di atas, maka penulis memilih judul skripsi tentang "**Analisis Yuridis Penjualan Kartu Perdana Gsm Dengan Memanipulasi Data Orang Lain (Studi Putusan Nomor 461/Pid.Sus/2020/PN.Sda)".**

B. Rumusan Masalah

Rumusan masalah dalam penulisan skripsi ini adalah:

1. Bagaimana pengaturan hukum tentang penjualan kartu perdana GSM dengan memanipulasi data orang lain dalam Putusan No.461/Pid.Sus/2020/ PN.Sda ?
2. Bagaimana penerapan sanksi penjualan kartu perdana GSM dengan memanipulasi data orang lain dalam Putusan No.461/Pid.Sus/2020/ PN.Sda ?
3. Bagaimana pertimbangkan hukum hakim penjualan kartu perdana GSM dengan memanipulasi data orang lain dalam Putusan Nomor. 461/Pid.Sus/2020/ PN.Sda ?

C. Tujuan Penelitian

Tujuan penelitian dalam penulisan skripsi ini adalah :

1. Untuk mengetahui pengaturan hukum tentang penjualan kartu perdana GSM dengan memanipulasi data orang lain dalam Putusan No.461/Pid.Sus/2020/ PN.Sda.
2. Untuk mengetahui penerapan sanksi penjualan kartu perdana GSM dengan memanipulasi data orang lain dalam Putusan No.461/Pid.Sus/2020/ PN.Sda.
3. Untuk mengetahui pertimbangkan hukum hakim penjualan kartu perdana GSM dengan memanipulasi data orang lain dalam Putusan Nomor. 461/Pid.Sus/2020/ PN.Sda.

D. Manfaat Penelitian

Manfaat penelitian dalam penulisan skripsi ini adalah :

1. Secara teoritis diharapkan menjadi bahan untuk pengembangan wawasan dan memperkaya khasanah ilmu pengetahuan, menambah dan melengkapi perbendaharaan dan koleksi ilmiah serta memberikan kontribusi pemikiran yang menyoroti dan membahas mengenai tindak pidana penjualan kartu perdana GSM dengan memanipulasi data orang lain.
2. Secara praktis :
   a. Sebagai pedoman atau masukan bagi aparat penegak hukum maupun praktisi hukum dalam menentukan kebijakan menangani

dan menyelesaikan tindak pidana penjualan kartu perdana GSM dengan memanipulasi data orang lain.

b. Memberikan sumbangan pemikiran dan informasi ilmiah bagi masyarakat khususnya mengenai tindak pidana penjualan kartu perdana GSM dengan memanipulasi data orang lain.

E. Definisi Operasional

Definisi operasional dalam penelitian ini adalah:

1. Analisis adalah sudut pandangan, mempertimbangkan sesuatu hendaknya dari berbagai, pemunculan atau penginterpretasian gagasan, masalah, situasi, dan sebagainya sebagai pertimbangan yang dilihat dari sudut pandang tertentu.[9] Yuridis adalah hal yang diakui oleh hukum, suatu kaidah yang dianggap hukum atau dimata hukum dibenarkan keberlakuannya, baik yang berupa peraturan-peraturan, kebiasaan, etika bahkan moral yang menjadi dasar penilaiannya. [10]
2. Penjualan adalah proses kegiatan menjual, yaitu dari kegiatan penetapan harga jual sampai produk didistribusikan ke tangan konsumen (pembeli).[11]
3. Kartu perdana *Global Sytem For Mobile* (GSM) adalah sebuah kartu yang harus dimiliki oleh konsumen untuk mendapatkan layanan dari masing-masing kartu *Subscriber Identity Module* (SIM) prabayar.[12]

---

[9]WJS. Poerwadarminta, ***Kamus Umum Bahasa Indonesia***, PN. Balai Pustaka, Jakarta, 2008, h.170.

[10]***Ibid***, h.481.

[11]Sofjan Assauri, ***Manajemen Pemasaran***, Rajawali Pers, Jakarta, 2017, h.23.

[12]Yitno Pranoto, "Analisis Brand Switchingpada Kartu Prabayar GSMSimpati, As, Mentari, IM3-Smart, XL bebas dan Xl jempol Berdasarkan Atribut Produk", *Jurnal Ekonomi*, Volume 1 Nomor 2 Tahun 2019, h. 48.

4. Memanipulasi adalah sebuah proses rekayasa dengan melakukan penambahan, pensembunyian, penghilangan atau pengkaburan terhadap bagian atau keseluruhan sebuah realitas, kenyataan, fakta-fatkta ataupun sejarah yang dilakukan berdasarkan sistem perancangan sebuah tata sistem nilai.[13]
5. Putusan adalah putusan yang di ucapkan oleh hakim karena jabatannya dalam persidangan perkara pidana yang terbuka untuk umum setelah melalui proses dan prosedural hukum acara pidan pada umumnya berisikan amar pemidanaan atau bebas atau pelepasan dari segala tuntutan hukum dibuat dalam bentuk tertulis dengan tujuan menyelesaikan perkara.[14]

[13] Sudarsono, ***Kamus Hukum**,* Rineka Cipta Jakarta, 2016, h, 418.

[14]Lilik Mulyadi, ***Kompilasi Hukum Pidana Dalam Perspektif Teoritis Dan Prakter Pradilan*****,** Mandar Maju, Bandung, 2017, h.127.

BAB II

TINJAUAN PUSTAKA

A. Gambaran Umum Tindak Pidana Teknologi Informasi dan Transaksi Elektronik

1. Pengertian Tindak Pidana Teknologi Informasi dan Transaksi Elektronik.

Ketentuan umum Pasal 1 UU ITE disebutkan, bahwa informasi elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, elektronic data interchange (EDI), surat elektronik (elektronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya sedangkan transaksi elektronik adalah perbuatan hukum yang dilakukan menggunakan komputer, jaringan komputer, dan atau media elektronik lainnya.

Teknologi selain membawa keuntungan berupa dipermudahnya hidup manusia, juga membawa kerugian-kerugian berupa semakin dipermudahkannya penjahat dalam melakukan kejahatannya. Teknologi juga memberikan pengaruh yang signifikan dalam pemahaman mengenai kejahatan terutama terhadap aliran-aliran kriminologi yang memberatkan pada faktor manusia,baik secara lahir maupun psikologis.

> Perkembangan teknologi merupakan salah satu faktor yang dapat menimbulkan kejahatan, sedangkan kejahatan itu sendiri telah ada dan muncul sejak permulaan zaman sampai sekarang dan masa yang

> akan datang. Bentuk-bentuk kejahatan yang ada pun semakin hari semakin bervariasi. Suatu hal yang patut untuk diperhatikan bahwa kejahatan sebagai gejala sosial sampai sekarang belum diperhitungkan dan diakui untuk menjadi suatu tradisi atau budaya, padahal jika dibandingkan dengan berbagai budaya yang ada, usia kejahatan tentulah lebih tua.[15]

Kejahatan pada dasarnya tumbuh dan berkembang dalam masyarakat, tidak ada kejahatan tanpa masyarakat atau seperti ucapan bahwa masyarakat mempunyai penjahat sesuai dengan jasanya. Banyak tentang faktor kejahatan yang ada dalam masyarakat, namun yang pasti adalah bahwa kejahatan merupakan salah satu bentuk perkembangan perilaku manusia yang perkembangannya terus sejajar dengan perkembangan masyarakat itu sendiri. “Kejahatan telah diterima sebagai suatu fakta, baik pada masyarakat yang paling sederhana (primitif) maupun pada masyarakat yang modern, yang merugikan masyarakat”.[16]

Begitu eratnya pengaruh perkembangan teknologi dengan kejahatan terkadang membuat hukum seakan terpana melihat pesatnya perkembangan tersebut. Sehingga terkadang hukum terlambat untuk mengimbangi perkembangan teknologi. Dalam tindak pidana teknologi informasi ini juga, hukum seakan sempat tertinggal dalam pesatnya kemajuan internet. Sehingga seperti telah diuraikan di awal bab I dimana dunia internet atau dunia maya akan menjadi hutan belantara yang tak bertuan bila terus dibiarkan tanpa hukum yang mengatur secara khusus. Karena memang meskipun dunia tersebut virtual, tetap ada suatu

---

[15] Merry Magdalena dan Maswigrantoro Roes Setyadi, ***Cyberlaw Tidak Perlu Takut*****,** Andi, Yogyakarta, 2007,h.46.

[16] Agus Raharjo, ***Op. Cit***., h. 29

kehidupan di dalamnya yang sempat belum ada aturan yang mengatur di dalamnya.

Mulanya terdapat dua pendapat mengenai perlu tidaknya undang-undang yang mengatur mengenai kejahatan teknologi informasi, diantaranya :

a. Kelompok pertama yang mengatakan bahwa sampai hari ini belum ada perundangan yang mengatur masalah *cybercrime*. Karena itu jika terjadi tindakan kriminal di dunia *cyber*, sangat sulit bagi aparat hukum untuk menjerat pelakunya. Pendapat ini diperkuat dengan banyaknya kasus *cybercrime* yang tidak dapat dituntaskan oleh sistem peradilan. Persoalannya berdasar pada sulitnya aparat mencari pasal-pasal yang dapat dipakai sebagai landasan tuntutan di pengadilan.
b. Kelompok kedua adalah mereka yang beranggapan bahwa tidak ada kekosongan hukum. Mereka yakin, walau belum ada perundangan yang mengatur masalah tersebut, para penegak hukum dapat menggunakan ketentuan hukum yang sudah ada. Untuk melaksanakannya diperlukan keberanian hakim menggali Undang-Undang yang ada dan membuat ketetapan hukum (yurisprudensi) sebagai landasan keputusan pengadilan.[17]

UU ITE terdapat dua muatan besar yang diatur di dalamnya yaitu :

b. Pengaturan tentang transaksi elektronik
c. Pengaturan tentang tindak pidana teknologi informasi.

Materi tersebut merupakan implementasi dari beberapa prinsip ketentuan internasional, yaitu *Uncitral Model Law on Electronic Commerce, Uncitral Model Law on Electronic Signature, Convention on Cybercrime, EU Directives on Electronic Commerce, dan EU Directives on Electronic Signature*. Ketentuan-ketentuan tersebut adalah instrument internasional dan regional yang banyak diterapkan oleh negara-negara Eropa, Amerika, dan Asia.[18]

Substansi pengaturan dalam tindak pidana teknologi informasi dalam UU ITE mencakup hukum pidana materiil, yaitu kriminalisasi

[17] Merry Magdalena dan Maswigrantoro Roes Setyadi, ***Op.Cit***., h. 82
[18] ***Ibid***, h. 136.

perbuatan-perbuatan yang termasuk kategori tindak pidana teknologi informasi. Pedoman yang digunakan adalah *Convention on Cybercrime*. “Undang-undang ini juga memuat hukum pidana formil yang khusus untuk menegakkan hukum pidana di bidang teknologi informasi ini”.[19]

Berkaitan dengan perumusan delik yang mempunyai beberapa elemen, diantara para ahli mempunyai jalan pikiran yang berlainan. Sebagian besar berpendapat membagi elemen perumusan delik secara mendasar saja, dan ada juga yang berpendapat yang membagi elemen perumusan delik secara terperinci, diantaranya unsur subjektif dan objektif.

Unsur objektif dalam perumusan delik tindak pidana teknologi informasi ini mengalami beberapa terobosan dari sifat-sifat umum KUHP. Hal ini disebabkan kegiatan pada dunia maya meskipun bersifat virtual tetapi dikategorikan sebagai tindakan dan perbuatan hukum yang nyata. Secara yuridis untuk ruang *cyber* sudah tidak ada tempatnya lagi untuk mengkategorikan sesuatu dengan ukuran dan kualifikasi konvensional untuk dapat dijadikan objek dan perbuatan, sebab jika cara ini yang ditempuh akan terlalu banyak kesulitan dan hal-hal yang lolos dari jerat hukum. Kegiatan *cyber* adalah kegiatan virtual, tetapi berdampak sangat nyata meskipun alat bukti elektronik, dengan subjek perlakunya harus dikualifikasikan pula sebagai telah melakukan perbuatan hukum secara nyata.

---

[19] ***Ibid***.

> Dunia hukum sebenarnya sudah sejak lama memperluas penafsiran asas dan normanya ketika menghadapi persoalan benda tidak berwujud, misalnya dalam kasus pencurian listrik sebagai perbuatan pidana. Dalam keyataan kegiatan *cyber* tidak lagi sederhana karena kegiatannya tidak lagi dibatasi oleh wilayah suatu negara, yang mudah diakses kapan pun dan dari mana pun. Kerugian dapat terjadi baik pada pelaku transaksi maupun pada orang lain yang tidak pernah melakukan transaksi, misalnya pencurian kartu kredit melalui pembelanjaan internet.[20]

Tindak pidana yang diatur dalam UU ITE mengatur tentang perbuatan yang dilarang. Perbuatan-perbuatan tersebut dapat dikategorikan menjadi beberapa kelompok sebagai berikut :

a. Tindak pidana yang berhubungan dengan aktivitas ilegal, yaitu:
   a. Distribusi atau penyebaran, transmisi, dapat diaksesnya konten *illegal,* yang terdiri dari:
      a) Kesusilaan
      b) Perjudian
      c) Penghinaan atau pencemaran nama baik
      d) Pemerasan atau pengancaman
      e) Berita bohong yang menyesatkan atau merugikan konsumen
      f) Menimbulkan rasa kebencian berdasarkan SARA
      g) Mengirimkan informasi yang berisi ancaman kekeasan atau menakut-nakuti yang ditujukan secara pribadi.
   b. Dengan cara apapun melakukan akses ilegal;
   c. Intersepsi ilegal terhadap informasi atau dokumen elektronik dan sistem elektronik;

a. Tindak pidana yang berhubungan dengan gangguan (interfensi), yaitu:
   1) Gangguan terhadap informasi atau dokumen elektronik (*data interference*)
   2) Gangguan terhadap sistem elektronik (*system interference*)
b. Tindak pidana memfasilitasi perbuatan yang dilarang.
c. Tindak pidana pemalsuan informasi atau dokumen elektronik
d. Tindak pidana tambahan (*accesoir*);
e. Perberatan-perberatan terhadap ancaman pidana.[21]

Secara konsep tindak pidana teknologi informasi dapat dilihat secara sempit maupun luas. Secara sempit tindak pidana teknologi informasi ini ialah perbuatan yang dikategorikan tindak pidana yang ditujukan terhadap integritas, ketersediaan, dan kerahasiaan data, termasuk terhadap sistem.

---

[20] Budi Suhariyanto, ***Op. Cit***., h 103
[21] Josua Sitompul, ***Op. Cit***., h. 147

Tindak pidana ini dalam arti luas merupakan perbuatan pidana yang dilakukan dengan menggunakan atau melalui sarana komputer sistem atau jaringan, termasuk tindak pidana konvensional dengan menggunakan komputer atau sistem elektronik. Tindak pidana teknologi informasi diatur dalam UU ITE sebagaimana diatur dalam BAB VII dan BAB XI. Hampir semua ketentuan perbuatan yang dilarang dalam UU ITE telah mengakomodir *substantive law* dari *Convention on Cybercrime.*

2. Unsur-Unsur Tindak Pidana Informasi dan Transaksi Elektronik

Kemajuan teknologi akhir-akhir ini menimbukan banyak kemajuan di segala bidang, termasuk dalam kontak seseorang dengan pihak lainnya. Aktivitas dunia maya merupakan salah satu contoh dari perkembangan teknologi yang sedemikian pesat. Sebenarnya aktivitas dunia maya sangat luas menyangkut banyak hal dari berbagai bidang. Melalui media elektronik ini kita memasuki dunia maya yang bersifat abstrak universal, lepas dari keadaan, tempat dan waktu.

Istilah media sosial adalah salah satu bentuk perkembangan internet yang paling fenomenal dewasa ini. Semua mengenal *facebook, twitter, plruk* dan banyak lagi situs-situs media sosial di internet. Kemunculan berbagai situs media sosial memberikan kemudahan bagi setiap orang dan berbagai belahan dunia untuk berinteraksi satu dengan yang lain. Media sosial juga melahirkan masalah-masalah baru diantaranya, muncul kejahatan baru yang lebih canggih dalam bentuk *cyber crime*.

Pasal 27 ayat (4) UU ITE berbunyi : setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau

membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan pemerasan dan/atau pengancaman.

> Ketentuan Pasal 27 UU ITE merupakan ketentuan yang mengatur tindak pidana yang diatur dalam KUHP yaitu mengenai tindak pidana kesusilaan (Pasal 282 dan Pasal 283 KUHP), perjudian (Pasal 303 KUHP), penghinaan atau pencemaran nama baik (Pasal 310 dan Pasal 311 KUHP), dan pemerasan atau pengancaman (Pasal 368 dan Pasal 369 KUHP). Perumusan perbuatan dalam Pasal 27 Undang-Undang RI Nomor 11 tahun 2008 pada dasarnya merupakan reformulasi tindak pidana yang terdapat dalam pasal-pasal KUHP tersebut.[22]

Perumusan ketentuan Pasal 27 ayat (4) UU ITE yang menggabungkan tindak pidana pemerasan dan/atau pengancaman dalam satu ketentuan padahal dalam KUHP tindak pidana pemerasan diatur dalam Pasal 368 sedangkan pengancaman diatur dalam Pasal 369 KUHP.

> Perumusan ketentuan Pasal 27 ayat (4) UU ITE yang menggabungkan tindak pidana pemerasan dengan pengancaman dalam satu ketentuan tetap menimbulkan masalah karena kedua tindak pidana tersebut jenis deliknya berbeda. Ketentuan tindak pidana pemerasan sebagaimana diatur dalam Pasal 368 KUHP adalah delik biasa sedangkan tindak pidana pengancaman dalam Pasal 369 KUHP adalah delik aduan.[23]

Ketentuan Pasal 27 UU ITE mensyaratkan perbuatan mendistribusikan, mentransformasikan dan/atau membuat dapat diaksesnya konten yang dilarang tersebut dilakukan dengan sengaja dan tanpa hak.[24]

---

[22] Sigit Suseno, ***Yurisdiksi Tindak Pidana Siber**,* Refika Aditama, Bandung, 2012, h. 166

[23]Sigit Suseno, ***Op.Cit*****,** .h71.

[24]Asri Sitompul, ***Hukum Internet Pengenalan Mengenai Masalah Hukum Cyberspace*****,** Citra Adiyta Bakti, Bandung, 2011, h. 38

Pasal 28 Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik:

(1) Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik.
(2) Setiap orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA).

Sanksi terhadap perbuatan tersebut diatur dalam Pasal 45 ayat (2) Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yaitu hukuman pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp.1.000.000.000,00 (satu miliar rupiah).

Pasal 29 UU ITE menentukan setiap orang dengan sengaja dan tanpa hak mengirimkan informasi elektronik dan/atau dokumen elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi. Secara pribadi yang dimaksud adalah orang perseorang (manusia atau *natural* person) sehingga dengan demikian tidak termasuk korporasi. “Tindak pidana tersebut hanya dapat dipertanggungjawabkan secara pidana kepada pelakunya apabila sasaran atau korban tindak pidana tersebut adalah orang perseorangan karena yang dapat merasa takut adalah manusia.

Pasal 30 ayat (1) UU ITE yaitu: Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apapun. Sanksi perbuatan tersebut

diatur dalam Pasal 46 ayat (1) UU ITE yaitu: Hukuman pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp.600.000.000,00 (enam ratus juta rupiah).

Pasal 30 ayat (2) UU ITE yaitu: Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apa pun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik.

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

a. Melakukan komunikasi, mengirimkan, memancarkan atau sengaja berusaha mewujudkan hal-hal tersebut kepada siapa pun yang tidak berhak untuk menerimanya; atau
b. Sengaja menghalangi agar informasi dimaksud tidak dapat atau gagal diterima oleh yang berwenang menerimanya di lingkungan pemerintah dan/atau pemerintah daerah.

Sanksi perbuatan tersebut sebagaimana diatur dalam Pasal 46 ayat (2) UU ITE yaitu: Hukuman pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp.700.000.000,00 (tujuh ratus juta rupiah).

Pasal 30 ayat (3) UU ITE yaitu: Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan. Sistem pengamanan adalah sistem yang membatasi akses Komputer atau melarang akses ke

dalam Komputer dengan berdasarkan kategorisasi atau klasifikasi pengguna beserta tingkatan kewenangan yang ditentukan. Sanksi diatur dalam Pasal 46 ayat (3) UU ITE yaitu: Hukuman pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp.800.000.000,00 (delapan ratus juta rupiah)".

Pasal 31 UU ITE yaitu:

(1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas informasi elektronik dan/atau dokumen elektronik dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain. Yang dimaksud dengan "intersepsi atau penyadapan" adalah kegiatan untuk mendengarkan, merekam, membelokkan, mengubah, menghambat, dan/atau mencatat transmisi informasi elektronik dan/atau dokumen elektronik yang tidak bersifat publik, baik menggunakan jaringan kabel komunikasi maupun jaringan nirkabel, seperti pancaran elektromagnetis atau radio frekuensi.
(2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi informasi elektronik dan/atau dokumen elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian informasi elektronik dan/atau dokumen elektronik yang sedang ditransmisikan.
(3) Kecuali intersepsi sebagaimana dimaksud pada ayat (1) dan ayat (2), intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang
(4) Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.

Sanksi pelanggaran Pasal 31 diatur dalam Pasal 47 UU ITE yaitu: Hukuman pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp.800.000.000,00 (delapan ratus juta rupiah).

Pasal 32 ayat (1) UU ITE yaitu: setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah,

menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu informasi elektronik dan/atau dokumen elektronik milik orang lain atau milik publik. Sanksinya diatur dalam Pasal 48 ayat (1) Pasal 31 UU ITE yaitu: Hukuman pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp.2.000.000.000,00 (dua miliar rupiah).

Pasal 32 ayat (1) UU ITE yaitu: setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer informasi elektronik dan/atau dokumen elektronik kepada sistem elektronik orang lain yang tidak berhak. Sanksinya diatur dalam Pasal 48 ayat (2) Pasal 31 UU ITE yaitu: Hukuman pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp.3.000.000.000,00 (tiga miliar rupiah).

Pasal 32 ayat (3) UU ITE yaitu: Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu informasi elektronik dan/atau dokumen elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya. Sanksinya diatur dalam Pasal 48 ayat (2) Pasal 31 UU ITE yaitu: Hukuman pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp.5.000.000.000,00 (lima miliar rupiah).

Pasal 33 UU ITE yaitu: setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya sistem elektronik dan/atau mengakibatkan sistem elektronik menjadi tidak bekerja sebagaimana mestinya. Sanksinya diatur dalam

Pasal 49 Pasal 31 UU ITE yaitu: Hukuman pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp.10.000.000.000,00 (sepuluh miliar rupiah).

3. Jenis-Jenis Tindak Pidana Teknologi Informasi dan Transaksi Elektronik.

Sesungguhnya banyak perbedaan diantara para ahli dalam mengklasifikasiakan kejahatan komputer (*computer crime*). Ternyata dari klasifikasi tersebut terdapat kesamaan dalam beberapa hal. Memudahkan klasifikasi tindak pidana teknologi informasi tersebut, maka dari beberapa klasifikasi dapat disilmpulkan :

a. Kejahatan-kejahatan yang menyangkut data atau informasi komputer.
b. Kejahatan-kejahatan yang menyangkut program atau perangkat lunak komputer.
c. Pemakaian fasilitas-fasilitas komputer tanpa wewenang untuk kepentingan-kepentingan yang tidak sesuai dengan tujuan pengelolaan atau operasinya.
d. Tindakan-tindakan yang mengganggu operasi komputer.
e. Tindakan merusak peralatan komputer atau peralatan yang berhubungan dengan komputer atau sarana penunjangnya.[25]

Berdasarkan klasifikasi tersebut kejahatan computer tidak hanya berbatas pada penggunaan komputer yang menyimpang daru tujuan penggunaannya, tetapi juga menyangkut pada informasi yang terkait pada alat-alat lain yang berhubungan dengan komputer seperti jaringan internet, informasi yang didapat pada jaringan internet dan lain sebagainya.

[25] Abdul Wahid dan M. Labib, ***Kejahatan Mayantara (Cybercrime),*** Refika Aditama, Bandung, 2005, h. 67

Melihat bentuk-bentuk kejahatan yang berhubungan erat dengan penggunaan teknologi informasi yang berbasis utama komputer dan jaringan telekomunikasi, dalam beberapa literatur dan praktiknya dikelompokkan dalam beberapa bentuk. Dari beberapa pengelompokan yang ada dapat dilihat secara umum bentuk dari kejahatan teknologi informasi ini antara lain :

a. *Unauthorized acces to computer system and service*
   Kejahatan yang dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya.
b. *Illegal content*
   Merupakan kejahatan dengan memasukkan data atau informasi ke internet tentang suatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum.
c. *Data forgery*
   Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* melalui internet.
d. *Cyber spionage*
   Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain dengan meamasuki sistem jaringan komputer (*network system*) pihak sasaran.
e. *Cyber sabotage and exortion*
   Kejahatan ini dilakukan dengan membuat gangguan, perusakan, atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.
f. *Offense against intellectual property*
   Kejahatan ini ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di internet. Sebagai contoh adalah peniruan terhadap tampilan pada suatu laman (*web page*) pada situs milik orang lain secara illegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.
g. *Infregments of privacy*
   Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan seseorang pada formulir data pribadi yang tersimpan secara komputerisasi (*computerized*), yang apabila diketahui oleh orang lain akan dapat merugikan korbannya secara materiil maupun immaterial seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi, dan sebagainya.[26]

[26] ***Ibid***, h. 70.

Berdasarkan kriteria bentuk-bentuk kejahatan teknologi informasi di atas, maka dapat diklasifikasikan lebih sederhana, bentuk-bentuk kejahatan teknologi informasi ini dapat dikelompokkan dalam dua golongan (besar): penipuan data dan penipuan program.

B. Manipulasi Data

Istilah memanipulasi data ini dikenal dengan sebutan *The Trojan horse* yang mempunyai pengertian sebagai suatu perbuatan yang bersifat mengubah data atau instruksi pada sebuah program, menghapus, menambah, membuat data atau pada sebuah program menjadi tidakterjangkau dengan tujuan kepentingan pribadi/kelompok.[27] Manipulasi informasi elektronik merupakan suatu tindakkan dengan cara merekayasa atau merubah suatu informasi elektronik dan/atau dokumen elektronik. Manipulasi elektronik merupakan salah satu dari banyaknya bentuk kejahatan yang terjadi di dalam sistem informasi elektronik.[28]

Pelaku manipulasi data dapat dimungkinkan dilakukan secara *online* (melalui sistem jaringan). Hal tersebut memungkinkan bagi seseorang untuk melakukan tindak pidana pemalsuan dengan sasaran sistem *database* perusahaan maupun perbankan yang menggunakan teknologi jaringan. Pelaku dalam tindak pidana ini memanfaatkan fungsi internet

[27]Yusuf Randi, ***Proteksi Terhadap Kriminalitas Dalam Bidang Komputer*****,** Refika Aditama, Bandung, 2016, h.80.

[28]Budi Suhariyanto, ***Op.Cit***, h.56.

sebagai salah satu media publiksi yang disalahgunakan untuk kepentingan sendiri atau golongannya. Teknologi informasi tersebut saat ini sangat memungkinkan pihak-pihak melakukan delik ini. Penggunaan *website* sebagai salah satu alat publikasi diinternet tergolong sangat efektif. Bahkan dimasa mendatang bukan tidak mungkin fungsi publikasi dari internet akan menjadi mediator terpenting dari suatu informasi.

Tindak pidana manipulasi informasi elektronik merupakan bagian dari kejahatan dunia maya atau biasa dikenal dengan *cybercrime*, *cybercrime* merupakan perkembangan lebih lanjut dari kejahatan komputer (*computer crime*).

> Pengertian *cybercrime* sendiri telah diungkapkan dalam berbagai literatur yang terus berkembang, diantaranya dalam kebijakan *US Departement of Justice* yang menyatakan bahwa *cybercrime* adalah setiap perbuatan melawan hukum dimana penngetahuan komputer diperlukan untuk pelaksanaan penyidikan dan penuntutan, dan dalam pendapat *organization of european community development* yang menyatakan bahwa *cybercrime* adalah setiap perbuatan yang melawan hukum, tidak etis atau tanpa hak sehubungan dengan proses otomatis dan transmisi data. Sedangkan dalam dokumen PBB tentang *The Prevention of Crime and the treatment of offlenderes* di Havana, Cuba pada Tahun 1999 dan di Wina, Austria tahun 2000, menyebutkan ada 2 (dua) istilah yang dikenal *cybercrime* dan computer related crime. Khusus dalam dokumen kongres di Wina, istilah *cybercrime* lebih lanjut dibagi menjadi 2 (dua) kategori yaitu :
>
> 1. *Cybercrime* adalah arti sempit yang disebut *computer crime* adalah tindakan ilegal apapun yang terarah dengan maksud untuk ekploitasi elektronik yang menargetkan keamanan dari sistem computer dan data yang telah diolah.
> 2. *Cybercrime* dalam arti luas yang disebut *computer related crime* adalah tindakan ilegal apapun yang telah dilakukan sehubungan dengan penawaran sistem komputer atau sistem atau jaringan yang mencakup kepemilikan, penawaran atau distribusi informasi ilegal yang ditujukan untuk sistem komputer atau jaringan. [29]

[29] Nudirman Munir, ***Pengantar Hukum Siber Indonesia***. RajaGrafindo Persada, Depok, 2017, h.63.

Perkembangan selanjutnya pengertian cybercrime menurut *convention on cybercrime* di Budapest tanggal 23 November 2001, dibagi menjadi 4 (empat) kategori yaitu :

1. *Offences againts the condicentiality, integrity and availability of computer data and systems*, (kejahatan terhadap kerahasiaan, integritas, dan ketersediaan data dan sistem komputer) yang meliputi:
   a. *Illegal access* (mengakses tanpa hak).
   b. *Illegal intereption* (tanpa hak menyadap).
   c. *Data interference* (merusak data).
   d. *Systems interference* (menggangg sistem).
   e. *Misuse of devices* (menyalahgunakan perlengkapan).
2. *Computer related offences* (kejahatan yang berhubungan dengan komputer), yang meliputi:
   a. *Computer related forgery* (yang berhubungan dengan pemalsuan).
   b. *Computer related fraud* (yang berhubungan dengan penipuan).
3. *Content related offences* yang meliputi *offences related to child pornography* (kejahatan yang bermuatan pornografi anak).
4. *Offences related to infringements of copyrights and related rights* (kejahatan yang berhubungan dengan HAKI).[30]

Cybercrime dirumuskan sebagai perbuatan melawan hukum yang dilakukan dengan memakai jaringan komputer sebagai sarana atau alat atau komputer sebagai objek baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. Sebagaimana lazimnya pembaruan teknologi pada umumnya, teknologi informasi *in casu internet* selain memberi manfaat juga menimbulkan implikasi-implikasi negatif (baik dalam ranah hukum perdata maupun hukum pidana), yaitu dengan terbukanya peluang timbulnya berbagai bentuk penyalahgunaan teknologi tersebut. Dalam ranah hukum pidana, dipahami bahwa di dalam jaringan komputer

[30] *Ibid*, h. 64.

seperti internet, masalah kriminaltias menjadi semakin kompleks karena ruang lingkupnya yang luas. Kriminalitas di internet atau *cybercrime* pada dasarnya adalah suatu tindakan pidana yang terjadi di ruang maya (*cyberspace*), baik yang menyerang fasilitas umum di dalam cyberspace ataupun kepemilikan pribadi.

Jenis-jenis kejahatan di internet terbagi dalam berbagai versi. Salah satu versi menyebutkan bahwa kejahatan ini terbagi dalam dua jenis, yaitu kejahatan dengan motif intelektual. Biasanya jenis yang pertama ini tidak menimbulkan kerugian dan dilakukan untuk kepuasan pribadi. Jenis kedua adalah kejahatan dengan motif politik, ekonomi atau kriminal yang berpotensi menimbulkan kerugian bahkan perang informasi.

Fenomena *cybercrime* memang harus diwaspadai karena kejahatan ini agak berbeda dengan kejahatan lain pada umumnya. *Cybercrime* dapat dilakukan tanpa mengenal batas teritorial dan tidak diperlukan interaksi langsung antara pelaku dengan korban kejahatan. Karakter internet yang bersifat global, semua negara yang melakukan kegiatan internet hampir pasti akan terkena imbas perkembangan *cybercrime* ini..

Danrivanto Budhijanto memperinci kasus-kasus *cybercrime* yang sering terjadi di Indonesia menjadi lima, yaitu :

1. Pencurian nomor kartu kredit;
2. Pengambilalihan situs web milik orang lain;
3. Pencurian akses internet yang sering dialami oleh ISP;
4. Kejahatan nama domain;

5. Persaingan bisnis dengan menimbulkan gangguan bagi situs saingannya.[31]

Khusus mengenai *cybercrime* dalam *e-comerce* didefinisikan sebagai “segala tindakan yang menghambat dan mengatasnamakan orang lain dalam perdagangan melalui internet”.[32] Modus baru seperti jual beli data konsumen dan penyajian informasi yang tidak benar dalam situs bisnis sering terjadi dalam *e-comerce.*

Selain itu jenis-jenis kejahatan dunia maya sebagaimana telah diuraikan di atas, diyakini bahwa jenis kejahatan dunia maya atau *cybercrime* akan terus berkembang seiring dengan teknologi dan alat yang marak digunakan oleh orang di seluruh dunia. Jika kejahatan dunia maya yang lazim dijumpai pada beberapa tahun belakangan ini antara lain berupa penipuan secara online, pemalsuan cek, penipuan kartu kredit, *confidence fraud*, penipuan identitas, pornografi anak dan lain sebagainya.

C. Kajian Hukum Islam Tentang Penjualan Kartu Perdana GSM Dengan Memanipulasi Data Orang Lain

Al-Quran secara tegas melarang perbuatan tindak pidana manipulasi. Adapun dalil yang melarang tindak pidana manipulasi sebagaimana dalam surat An-Nahl ayat 116 Allah SWT berfirman: Artinya: “Dan janganlah kamu mengatakan terhadap apa yang disebut-sebut oleh lidahmu secara Dusta "Ini halal dan ini haram", untuk mengada-adakan

---

[31] Danrivanto Budhijanto, ***Revolusi Cyberlaw Indonesia* (*Pembaruan dan Revisi UU ITE 2016*)**, Reflika Aditama, Bandung, 2018, h.16.

[32] ***Ibid*,** h.17

kebohongan terhadap Allah. Sesungguhnya orang-orang yang mengada-adakan kebohongan terhadap Allah Tiadalah beruntung".[33]

Berdasarkan dalil tersebut, Islam sangat melarang keras terhadap penipuan (manipulasi) baik itu berupa perbuatan, perkataan, dan lain sebagainya karena hal tersebut dapat merugikan bagi dirinya sendiri maupun orang lain. Dengan demikian, dapat dikemukakan bahwa manipulasi adalah sifat tercela dan sangat berbahaya, termasuk dalam konteks pemalsuan data yang berarti berbohong dalam memberikan keterangan yang sebenarnya di dalam isi data tersebut.

[33]Kementerian Agama RI. *Alquran dan Terjemahannya*, Jakarta: Direktorat Jenderal Haji Republik Indonesia, Jakarta, 2016, h.261.