PENGATURAN TINDAK PIDANA MAYANTARA (*CYBER CRIME*) DALAM SISTEM HUKUM INDONESIA

M Syukri Akub
Fakultas Hukum Universitas Hasanuddin
email : syukri.akub@ymail.com

Abstract

Cyber crime is a crime by using computers and internet access that knows no national borders. Losses that can arise from cyber crime also surpass the harm caused by conventional crime. Cyber crime prevention encountered many difficulties, one of them in the legal arrangement because the form of cyber crime always experience the development along with the progress of information technology.

Keywords: legal arrangement; Cyber crime;

Abstrak

Kejahatan dunia maya adalah kejahatan dengan menggunakan komputer dan akses internet yang tidak mengenal batas negara. Kerugian yang dapat timbul dari kejahatan dunia maya juga melampaui kerugian yang disebabkan oleh kejahatan konvensional. Pencegahan kejahatan dunia maya menemui banyak kesulitan, salah satunya dalam pengaturan hukum karena bentuk kejahatan dunia maya selalu mengalami perkembangan seiring dengan kemajuan teknologi informasi.

Kata kunci: Pengaturan; Kejahatan Siber;

A. PENDAHULUAN

Teknologi informasi mengalami perkembangan yang sangat pesat di berbagai negara termasuk di Indonesia.Kemajuan teknologi informasi membawa pengaruh baik dalam perkembangan ekonomi serta perolehan informasi yang cepat dari seluruh dunia.Namun disamping membawa pengaruh yang baik, perkembangan teknologi informasi juga membawa pengaruh buruk. Salah satu akibat buruk yang timbul dari kemajuan teknologi informasi adalah maraknya tindak pidana mayantara (yang selanjutnya akan disebut *cyber crime*).

Meningkatnya kasus*cyber crime* merupakan masalah yang dihadapi oleh semua Negara-negara di dunia. Buktinya, dengan dijadikannya *cyber crime*sebagai salah satu topik pembahasan pada Kongres PBB mengenai *The Prevention of Crime and the Treatment of Offender* ke-8 tahun 1990 di Havana, Kuba dank e-10 di Wina, Austria.

Jumlah kasus cyber crime atau kejahatan di dunia maya yang terjadi di Indonesia merupakan yang tertinggi di dunia, antara lain, karena banyaknya aktivitas para hacker di

Tanah Air.Kasus cyber crime di Indonesia adalah nomor satu di dunia. *Cyber crime* pada anak disebutkan telah menjadi tren baru di banyak negara, termasuk Indonesia.Penggunaan internet yang nyaris tanpa kendali menyebabkan anak-anak rentan menjadi korban dari berbagai tindak kejahatan di dunia maya. Kejahatan seksual, pornografi, *trafficking*, *bullying* dan bentuk kejahatan lain yang dilakukan secara online menjadi ancaman yang semakin besar mengintai generasi penerus bangsa. Menurut data yang dipublikasikan KPAI, sejak tahun 2011 hingga 2014, jumlah anak korban pornografi dan kejahatan online di Indonesia telah mencapai jumlah 1.022 anak. Secara rinci dipaparkan, anak-anak yang menjadi korban pornografi online sebesar 28%, pornografi anak online 21%, prostitusi anak online 20%, objek cd porno 15% serta anak korban kekerasan seksual online 11%. Jumlah itu diprediksi akan terus meningkat bila tidak ditanggulangi secara optimal. Pertumbuhan angka anak korban kejahatan online itu bertumbuh pesat seiring meningkatnya jumlah pengguna internet di Tanah Air. (https://circlenewssite. wordpress.com/ 2016/ 11/11/ kasus-cybercrime-di-indonesia-selama-5-tahun-terakhir-tahun-2010-2015/).

Pada bulan maret 2016, Direktorat Cyber crime Bareskrim Polri menangkap tiga tersangka pembobol situs layanan penjualan tiket pesawat Tiket.com.Ketiganya membobol dengan meretas situs Tiket.com yang mengakibatkan kerugian mencapai Rp 4 miliar dan Citilink rugi hampir Rp 2 milyar.Para tersangka diduga pernah meretas 4600 situs yang berpotensi menghasilkan uang jika berhasil mereka retas. (https: //elshinta.com/news/ 103295/2017/03/30/hacker-lulusan-smp-bobol-situs-penjualan-tiket).

Dari kasus tersebut di atas, memberikan gambaran kejahatan yang timbul akibat penyalahgunaan kemajuan teknologi informasi sangat besar dampak buruknya.Oleh karena diperlukan upaya-upaya pencegahan dan pemberantasan terhadap *cyber crime*, khususnya mengenai pengaturan hukumnya.

B. ANALISIS DAN PEMBAHASAN

1. Pengertian *Cyber crime*

Cyber crime merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapatkan perhatian luas di dunia internasional.Vodymyr Golubev menyebutnya sebagai *the new form of anti-social behavior*. Beberapa julukan/sebutan lainnya yang cukup keren diberikan kepada jenis kejahatan baru ini di dalam berbagai tulisan, antara lain, sebagai kejahatan dunia maya (*cyber space/virtual space offence*) dimensi baru dari *high tech crime*, dimensi baru dan *transnasional crime*, dan dimensi baru dari *white collar crime*(Barda Nawawi Arief, 2007;1).

Cyber crime merupakan bentuk-bentuk kejahatan yang ditimbulkan karena pemanfaatan teknologi internet. Dapat juga didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan internet yang berbasis pada kecanggihan teknologi komputer dan telekomunikasi.

Dalam “Background paper” Kongres PBB X untuk Workshop on crimes related to the computer network, dokumen A/CONF.187/10,3-2200, halaman 5 dijelaskan bahwa cyber crime dibagi dua kategori yaitu:

1. *Cybercrime* dalam arti sempit disebut *computer crime*, yaitu prilaku ilegal / melanggar yang secara langsung menyerang sistem keamanan komputer dan data yang diproses oleh komputer.
2. *Cybercrime* dalam arti luas disebut *computer related crime*, yaitu prilaku ilegal/ melanggar yang berkaitan dengan sistem komputer atau jaringan.

Dari beberapa pengertian di atas, *cybercrime* dirumuskan sebagai perbuatan melawan hukum yang dilakukan dengan memakai jaringan komputer sebagai sarana / alat komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain.

2. Bentuk *Cyber crime*

*Cyber crime*merupakan tindak pidana yang timbul akibat penyalahgunaan teknologi informasi yang ditandai dengan lahirnya internet yang membentuk ruang *cyber*. Dalam Draft Convention on Cyber crime (Draf No. 19 dan No.25 Rev.5)th.2000 dan Draft Explanatory Memorandum ti the Draft Convention on Cyber crime th 2001, yang dipersiapkan oleh European Committee on Crime Problems.

Ada berbagai kategori dari *cyber crime*(Agus Raharjo,2002;203-205) yaitu sebagai berikut:

a. Joy Computing, yaitu pemakaian komputer orang lain tanpa izin. Hal ini termasuk pencurian waktu operasi computer
b. Hacking, yaitu mengakses secara tidak sah atau tanpa izin dengan alat suatu terminal.
c. The Trojan Horse, yaitu manipulasi data atau program dengan jalan mengubah data atau instruksi pada sebuah program, menghapus, menambah, menjadikan tidak terjangkau dengan tujuan untuk kepentingan pribadi atau orang lain.
d. Data Leakage, yaitu menyangkut bocornya data ke luar terutama mengenai data yang harus dirahasiakan. Pembocoran data komputer itu bisa berupa rahasia negara, perusahaan, data yang dipercayakan kepada seseorang dan data dalam situasi tertentu.
e. Data Diddling, yaitu suatu perbuatan yang mengubah data valid atau sah dengan cara tidak sah, mengubah input data, atau output data.
f. To Frustate data communication atau penyia-nyiaan komputer.
g. Software Piracy, yaitu pembajakan perangkat lunak terhadap hak cipta yang dilindungi HAKI.
h. Cyber Espionage, merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (computer network system) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu sistem yang computerized.Biasaynya si penyerang menyusupkan sebuah program mata-mata yang dapat kita sebut sebagai spyware.
i. Infringements of Privacy, kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan

terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara computerized, yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materil maupun immateril, seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.

j. Data Forgery, merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai scriptless document melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen e-commerce dengan membuat seolah-olah terjadi "salah ketik" yang pada akhirnya akan menguntungkan pelaku.

k. Unauthorized Access to Computer System and Service, kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan (hacker) melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun begitu, ada juga yang melakukan hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Kejahatan ini semakin marak dengan berkembangnya teknologi internet/intranet.bagi yang belum pernah dengar, ketika masalah Timor Timur sedang hangat-hangatnya dibicarakan di tingkat internasional, beberapa website milik pemerintah RI dirusak oleh hacker.Kisah seorang mahasiswa fisipol yang ditangkap gara-gara mengacak-acak data milik KPU.dan masih banyak contoh lainnya.

l. Cyber Sabotage and Extortion, merupakan kejahatan yang paling mengenaskan.Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu logic bomb, virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku. Dalam beberapa kasus setelah hal tersebut terjadi, maka pelaku kejahatan tersebut menawarkan diri kepada korban untuk memperbaiki data, program komputer atau sistem jaringan komputer yang telah disabotase tersebut, tentunya dengan bayaran tertentu. Kejahatan ini sering disebut sebagai cyber-terrorism.

m. Offense against Intellectual Property, kejahatan ini ditujukan terhadap Hak atas Kekayaan Intelektual yang dimiliki pihak lain di internet. Sebagai contoh adalah peniruan tampilan pada web page suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.Dapat kita contohkan saat ini.Situs mesin pencari bing milik microsoft yang konon di tuduh menyerupai sebuah situs milik perusahaan travel online.

n. Illegal Contents, merupakan kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Sebagai contohnya adalah pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau

harga diri pihak lain, hal-hal yang berhubungan dengan pornografi atau pemuatan suatu informasi yang merupakan rahasia negara, agitasi dan propaganda untuk melawan pemerintahan yang sah, dan sebagainya.

Dari bentuk*cyber crime* tersebut di atas, nampak bahwa pada dasarnya *cyber crime* adalah penyerangan pada *content*, *computersystem* dan *communicationsystem* milik orang lain atau umum di dalam *cyberspace*.

3. Bentuk *cyber crime* berdasarkan motif terbagi menjadi 2 yaitu :

a. *Cyber crime* sebagai tindak kejahatan murni : dimana orang yang melakukan kejahatan yang dilakukan secara di sengaja, dimana orang tersebut secara sengaja dan terencana untuk melakukan pengrusakkan, pencurian, tindakan anarkis, terhadap suatu system informasi atau system computer.

b. *Cyber crime* sebagai tindakan kejahatan abu-abu : dimana kejahatan ini tidak jelas antara kejahatan criminal atau bukan karena dia melakukan pembobolan tetapi tidak merusak, mencuri atau melakukan perbuatan anarkis terhadap sistem informasi atau sistem komputer tersebut.

Dari berbagai macam kategori*cyber crime* di atas, bentuk *cyber crime* yang sering terjadi di Indonesia adalah kejahatan pemalsuan kartu kredit dengan cara melacak nama, nomor kartu kredit dilengkapi expire date-nya (tanggal jatuh tempo) seseorang untuk dimiliki dan digunakan sebagai sarana untuk melakukan kejahatannya dengan melakukan transaksi-transaksi atau pemesanan barang melalui internet dengan perusahaan-perusahaan tertentu yang menyediakan fasilitas pembelian dan pengiriman barang melalui internet. Selain itu, hacking situs juga termasuk cyber crime yang sering terjadi di Indonesia, bahkan tak jarang situs Polri pun diretas oleh para hackers seperti yang dilakukan oleh Naufal cs.

4. Pengaturan cyber crime melalui Hukum Pidana

Kongres PBB telah menghimbau Negara anggota untuk menanggulangi cyber crime dengan sarana penal.Walaupun kenyataannnya tak mudah, namun karena kasus *cybercrime* yang terjadi dewasa ini telah menimbulkan keresahan bagi masyarakat, khususnya mereka yang menggunakan sarana-sarana komputer dan informasi, maka perlindungan hukum bagi mereka yang dirugikan tersebut adalah merupakan sebuah kebutuhan yang harus segera dibuat oleh Negara.

Pengaturan *cyber crime* didasarkan pada sumber hukum yang berlaku saat ini baik dalam KUHP maupun undang-undang di luar KUHP.

Pengaturan bentuk cyber crime di dalam KUHP dapat dilihat pada pasal-pasal sebagai berikut:

a. Pasal 362 KUHP tentang pencurian;

b. Pasal 369 KUHP tentang Pemerasan dan Pengancaman;

c. Pasal 372 KUHP tentang Penggelapan;

d. Pasal 386 KUHP tentang Perbuatan Curang;

e. Pasal 506 KUHP tentang Pelanggaran Ketertiban Umum;

f. Pasal 382 bis KUHP;

g. Pasal 383 KUHP.

Berikut ini adalah beberapa kategori kasus *Cybercrime* yang telah ditangani dalam UU Informasi dan Transaksi Elektronik (Pasal 27 sampai dengan Pasal 35) :

a. Pasal 27 Illegal Contents

- muatan yang melanggar kesusilaan (Pornograph);
- muatan perjudian (Computer-related betting);
- muatan penghinaan dan pencemaran nama baik;
- muatan pemerasan dan ancaman (Extortion and Threats).

b. Pasal 28 Illegal Contents

- berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik. (Service Offered fraud)
- informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan (SARA).

c. Pasal 29 Illegal Contents

Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancamankekerasan atau menakut-nakuti yang ditujukan secara pribadi.

d. Pasal 30 Illegal Access

- Dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.
- 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.
- 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.

e. Pasal 31 Illegal Interception

- Intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain.
- 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.

f. Pasal 32 Data Leakage and Espionag

Mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.

g. Pasal 33 System Interferenc

Melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.

h. Pasal 34 Misuse Of Device

Memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki: perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi cybercrime, sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi cybercrime.

i. Pasal 35 Data Interference

- Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.
- Dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.
- 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.
- 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.

j. Pasal 31 Illegal Interception

- Intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain.
- 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.

k. Pasal 32 Data Leakage and Espionag

Mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.

l. Pasal 33 System Interferenc

Melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.

m. Pasal 34 Misuse Of Device

Memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki: perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi cybercrime, sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi cybercrime.

n. Pasal 35 Data Interference

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.

C. PENUTUP

Tindak pidana mayantara (*cyber crime)* adalah tindak pidana yang menggunakan computer dan internet sebagai sarana.Bentuk tindak pidana mayantara (*cyber crime)* dapat dibedakan berdasarkan aktifitas dan motif pelakunya.Pengaturan hukum pidana mengenai tindak pidana mayantara (*cyber crime)* melalui KUHP dan undang-undang khusus di luar KUHP.

DAFTAR PUSTAKA

Abdul Wahid dan Mohammad Labib.2005. Kejahatan Mayantara (Cyber Crime), PT. Rafika Aditama, Bandung.

Ahmad M.Ramli. 2004. *Cyber Law dan HAKI dalam Sistem Hukum Indonesia*. PT.Refika Aditama, Bandung.

Agus Raharjo. 2002. *Cybercrime, Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*. PT.Citra Aditya Bakti, Bandung.

Barda Nawawi Arief. 2007. *Tindak Pidana Mayantara, Perkembangan kajian Cyber Crime di Indonesia*. PT.Rajagrafindo Persada, Jakarta.

Djanggih, H., Thalib, H., Baharuddin, H., Qamar, N., & Ahmar, A. S. 2018. The effectiveness of law enforcement on child protection for cybercrime victims in Indonesia. In *Journal of Physics: Conference Series* (Vol. 1028, No. 1, p. 012192). IOP Publishing.

Hambali Thalib, Farid Yusuf, 2016. Cyber Crime Tantangan dan Penanggulangannya Studi Kasus pada Polrestabes Makassar.

Thalib, H., Rahman, S., & Semendawai, A. H. 2017. The Role Of Justice Collaborator In Uncovering Criminal Cases In Indonesia. *Diponegoro Law Review*, *2*(1), 27-39.

Undang-Undang RI No. 19 Tahun 2016 tentang Perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Kitab Undang-Undang Hukum Pidana Indonesia