ISSN 2541-6502

AKTUAL JUSTICE
JURNAL ILMIAH MAGISTER HUKUM
PASCASARJANA UNIVERSITAS NGURAH RAI

KEKHUSUSAN PROSES PENYIDIKAN TINDAK PIDANA CYBER CRIME

Renni Sartika[1], Sepuh A.I. Siregar[2], Ni Putu Riyani Kartika Sari[3]

[1]Kantor Hukum Legal Genesis Yogyakarta, E-mail: rennisartika17@gmail.com
[2] Inspektorat Pengawasan Polda Nusa Tenggara Timur ,
E-mail: sepuh.siregar64@gmail.com
[3]Fakultas Hukum Universitas Ngurah Rai, E-mail: riyani.ks@gmail.com

Abstract

The existence of the internet in human life is very supportive of all forms of human activity in today's digital era. However, technological advances with the use of the internet have resulted in the emergence of cybercrime or cyber crime. In its development, cyber crime requires special handling by the police in the process of investigation. For this reason, using normative juridical research, this study will examine the specificities of the cyber crime investigation process. In general, the process is almost the same as the criminal investigation process in general, except that it is carried out by cyber units or special units that have the task of carrying out cyber crime investigations. Apart from that, investigators of cybercrime will also use other special laws such as ITE, Consumer Protection, Banking, and so on.
Keyword: Investigation, Cybercrime, Information and Electronic Transactions.

Abstrak

Keberadaan internet dalam kehidupan manusia sangat mendukung segala bentuk aktivitas manusa di era digital saat ini. Namun adanya kemajuan teknologi dengan penggunaan internet tersebut salah satunya mengakibatkan munculnya cybercrime atau tindak pidana siber. Dalam perkembangannya tindak pidana siber memerlukan penanganan yang khusus oleh kepolisian dalam proses penyidikannya. Untuk itu dengan menggunakan penelitian yuridis normatif, penelitian ini akan mengkaji kehususan proses penyidikan tindak pidana siber. Adapun secara umum proses nya hampir sama seperti proses penyidikan tindak pidana pada umumnya hanya saja dilaksanakan oleh unit cyber atau unit khusus yang memiliki tugas melaksanakan penyidikan tindak pidana siber. Selain itu penjeratan yang dilakukan oleh penyidik atas tindak pidana siber (cybercrime) selain menggunakan KUHP juga menggunakan Undang-Undang Khusus lainnya seperti ITE, Perlindungan Konsumen, Perbankan, dan lain sebagainya.

Keyword : Penyidikan, Cybercrime, Informasi dan Transaksi Elektronik.

1. Pendahuluan

Perkembangan ilmu, pengetauan, teknologi, dan seni mengantarkan manusia memasuki "era digital" yang melahiran internet sebagai sebuah jaringan dengan mengkoneksi-kan antar subsistem jaringan menjadi satu jaringan superbesar yang dapat saling terhubungan (*online*) seluruh dunia. Bahkan teknologi internet mampu meng-konvergensi-kan data, informasi, audio, visual yang dapat berpengaruh pada kehidupan manusia. Saat ini, wujud komputer sebagai basis teknologi informasi, bukan hanya berwujud komputer konvensional (misalnya *personal computer*), melainkan sudah termasuk peralatan jinjing (*portable*) lain yang memiliki karakteristik sebagai komputer (misalnya *laptop, note-book, handphone, tablet*,dst).[1]

Kebutuhan dan penggunaan akan Internet dalam segala bidang seperti *e-banking*, *e-commerce*, *e-government*, *e-education* dan banyak lagi telah menjadi sesuatu yang lumrah. Bahkan apabila masyarakat terutama yang hidup di kota besar tidak bersentuhan dengan persoalan teknologi informasi dapat dipandang terbelakang atau "GAPTEK". Internet telah menciptakan dunia baru yang dinamakan *cyberspace*[2] yaitu sebuah dunia komunikasi berbasis komputer yang menawarkan realitas yang baru berbentuk virtual (tidak langsung dan tidak nyata). Walaupun dilakukan secara virtual, Internet mengubah konsep jarak dan waktu secara drastic sehingga seolah-olah dunia menjadi kecil dan tidak terbatas, dimana setiap orang bisa berhubungan, berbicara dan berbisnis dengan orang lain yang berada ribuan kilometer dari tempat di mana ia berada hanya dengan menekan tuts-tuts *keybord* dan *mouse* komputer yang ada di hadapannya.

[1] Widodo. (2013). *Hukum Pidana di Bidang Teknologi Informas Cybercrime Law : Telaah Teoritik dan Bedah Kasus*. Yogyakarta: Aswaja Pressindo. h. v.

[2] Raharjo, A.A. (2002). *Cyber Crime* : *Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi*. Bandung : Citra Aditya.

Internet atau jaringan komputer yang besar sesungguhnya tidak mengganggu manusia, malahan membantu manusia dalam mencapai tujuan-tujuan yang bersifat positif, seperti dalam bidang perbankan, yangmana kita dapat melakukan transaksi perbankan kapan saja dengan *e-banking* dan dengan *e-commerce* juga membuat kita mudah melakukan pembelian maupun penjualan suatu barang tanpa mengenal tempat. Mencari referensi atau informasi mengenai ilmu pengetahuan juga bukan hal yang sulit dengan adanya *e-library* dan banyak lagi kemudahan yang didapatkan dengan perkembangan Internet. Namun, Factor manusia yang menggunakan internet dengan tujuan jahat lah yang membuat pemakai internet tidak nyaman. Kejahatan inilah yang disebut *cyber crime* sedangkan manusianya dinamakan *hacker* hitam/*cracker. Hacker* secara harfiah berati mencincang atau membacok. *Hacker* dapat juga didefinisikan sebagai orang-orang yang gemar mempelajari seluk-beluk system komputer dan bereksperimen denganya.

Penggunaan istilah hacker terus berkembang seiring dengan perkembangan internet, tetapi terjadi pembiasan makna disini yang pertama *hacker* topi putih (*white hat hackers*), mereka masih memegang prinsip yang sama dengan perintis mereka yang mana masih memegang prinsip bahwa meng-*hack* adalah untuk tujuan meningkatkan keamanan jaringan internet. Sedangkan *hacker* dalam pengertian kedua adalah mereka yang dengan kemampuan yang dimiliki melakukan kejahatan, baik pencurian nomor kartu kredit sampai dengan perusakan situs atau website milik orang lain, mereka disebut dengan istilah *cracker* (*hacker* hitam).[3]

Bentuk-bentuk kejahatan siber (*cyber crime*) itu sendiri dapat dikelompokan menjadi tujuh yaitu : Unauthorized Access to Computer; System and Service; Illegal Contents; Data Forgery; Cyber Espionage; Cyber

[3] *Ibid*. h. 132.

Sabotage and Extortion; Offense against Intellectual Property; dan Infringements of Privacy.[4] Pengaturannya dengan KUHP, KUHAP dan UU RI No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Pasal 42 UU ITE memaparkan: " Penyidikan terhadap tindak pidana sebagaimana dimaksud dalam Undang-Undang ini, dilakukan berdasarkan ketentuan dalam Hukum Acara Pidana dan ketentuan dalam Undang-Undang ini. Sebagimana diatur dalam pasal 1 angka 2 KUHAP, Penyidikan adalah serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam undang-undang ini untuk mencari serta mengumpulkan bukti yang dengan bukti itu membuat terang tentang tindak pidana yang terjadi dan guna menemukan tersangkanya. sedangkan penyidik itu sendiri dalam ketentuan Pasal 1 angka 13 Undang-Undang No 2 Tahun 2002 tentang Kepolisian adalah pejabat polisi negara Republik Indonesia atau pejabat pegawai negeri sipil tertentu yang diberi wewenang khusus oleh undang-undang untuk melakukan penyidikan. Dalam hal ini Polri sebagai penyidik telah menyiapkan unit khusus untuk menangani kejahatan cyber ini yaitu UNIT V IT/CYBERCRIME Direktorat II Ekonomi Khusus Bareskrim Polri

2. Metode Penelitian

Kajian dalam tulisan ini menggunakan metode penelitian yuridis normatif atau penelitian hukum normatif. Menurut Mukti Fajar disampaikan bahwa, penelitian hukum normatif adalah suatu penelitian hukum yang melihat hukum sebagai suatu tatanan norma yang berkaitan mencakup asas-asas, norma, kaidah dari peraturan perundang-undangan, putusan pengadilan, perjanjian serta doktrin (ajaran)[5].

[4] Mansur, D.A.M., & Gultom E. (2005). *Cyber Law Aspek Hukum Teknologi Informasi*. Bandung: PT Refika Aditama. h. 9.

[5] Fajar, M & Ahmad Y. (2010). *Dualisme Penelitian Hukum Normatif dan Empiris*. Yogyakarta: Pustaka Pelajar. h. 34.

3. Hasil Dan Pembahasan

a. Proses Penyidikan Tindak Pidana Cyber Crime di Indonesia

Proses pnyidikan tindak pidana siber atau *cybercrime* pada umumnya hampir sama prosesnya dengan penanganan tindak pidana konvensional lain, hanya saja terdapat beberapa kekhususan seperti perangkat yang melaksanakannya adalah unit khusus yaitu unit cyber. Selain itu penanganan penyidikan cybercrime juga lebih rumit karena memerlukan kordinasi yang bersifat komprehensif dengan instansi-instansi lain yang berkaitan dengan tindak pidana tersebut. [6] Adapun rangkaian-rangkainan kegiatan penyidik dalam melakukan penyidikan adalah Penyelidikan, Penindakan, pemeriksaan dan penyelesaian berkas perkara.

a) Penyelidikan

serta tahap tersulit dalam proses penyidikan, karena dalam tahap ini penyidik harus dapat membuktikan tindak pidana yang terjadi serta bagaimana dan sebab-sebab tindak pidana tersebut untuk dapat menentukan bentuk laporan polisi yang akan dibuat. Informasi biasanya didapat dari NCB/Interpol yang menerima surat pemberitahuan atau laporan dari negara lain yang kemudian diteruskan ke Unit *cybercrime* satuan yang ditunjuk. Dalam penyelidikan kasus-kasus *cyber crime* yang modusnya seperti kasus *carding metode* yang digunakan hampir sama dengan penyelidikan dalam menangani kejahatan narkotika terutama dalam *undercover* dan *control delivery*.

[6] Agus, A.A., (2016), Penanganan Kasus CyberCrime di Kota Makasar (Studi Pada Kantor Kepolisian Resort Kota Besar Makasar). *Jurnal Supremasi.* Volume XI Nomor 1. April 2016, h.27.

Petugas setelah menerima informasi atau laporan dari *Interpol* atau *merchant* yang dirugikan melakukan koordinasi dengan pihakB*shipping* untuk melakukan pengiriman barang. Permasalahan yang ada dalam kasus seperti ini adalah laporan yang masuk terjadi setelah pembayaran barang ternyata ditolak oleh bank dan barang sudah diterima oleh pelaku, disamping adanya kerjasama antara *carder* dengan karyawan *shipping* sehingga apabila polisi melakukan koordinasi informasi tersebut akan bocor dan pelaku tidak dapat ditangkap sebab identitas yang biasanya dicantumkan adalah palsu. Untuk kasus *hacking* atau memasuki jaringan komputer orang lain secara ilegal dan melakukan modifikasi (*deface*), penyidikannya dihadapkan problematika yang rumit, terutama dalam hal pembuktian. Banyak saksi maupun tersangka yang berada di luar yurisdiksi hukum Indonesia, sehingga untuk melakukan pemeriksaan maupun penindakan amatlah sulit, belum lagi kendala masalah bukti-bukti yang amat rumit terkait dengan teknologi informasi dan kode-kode digital yang membutuhkan SDM serta peralatan komputer forensik yang baik.

Dalam hal kasus-kasus lain seperti situs porno maupun perjudian para pelaku melakukan hosting/ pendaftaran diluar negeri yang memiliki yuridiksi yang berbeda dengan negara kita sebab pornografi secara umum dan perjudian bukanlah suatu kejahatan di Amerika dan Eropa walaupun alamat yang digunakan berbahasa Indonesia dan operator daripada website ada di Indonesia sehingga kita tidak dapat melakukan tindakan apapun terhadap mereka sebab website tersebut bersifat universal dan dapat di akses dimana saja. Banyak rumor beredar yang menginformasikan adanya penjebolan bank-bank swasta secara online oleh *hacker* tetapi korban menutup-nutupi permasalahan tersebut. Hal ini berkaitan dengan kredibilitas bank bersangkutan yang takut apabila kasus ini tersebar akan merusak kepercayaan terhadap bank

tersebut oleh masyarakat. Dalam hal ini penyidik tidak dapat bertindak lebih jauh sebab untuk mengetahui arah serangan harus memeriksa server dari bank yang bersangkutan, bagaimana kita akan melakukan pemeriksaan jika kejadian tersebut disangkal oleh bank.

b) Penindakan

Penindakan kasus cybercrime sering mengalami hambatan terutama dalam penangkapan tersangka dan penyitaan barang bukti. Dalam penangkapan tersangka sering kali kita tidak dapat menentukan secara pasti siapa pelakunya karena mereka melakukannya cukup melalui komputer yang dapat dilakukan dimana saja tanpa ada yang mengetahuinya sehingga tidak ada saksi yang mengetahui secara langsung. Hasil pelacakan paling jauh hanya dapat menemukan IP Address dari pelaku dan komputer yang digunakan.

Hal itu akan semakin sulit apabila menggunakan warnet sebab saat ini masih jarang sekali warnet yang melakukan registrasi terhadap pengguna jasa mereka sehingga kita tidak dapat mengetahui siapa yang menggunakan komputer tersebut pada saat terjadi tindak pidana. Penyitaan barang bukti banyak menemui permasalahan karena biasanya pelapor sangat lambat dalam melakukan pelaporan, hal tersebut membuat data serangan di log server sudah dihapus biasanya terjadi pada kasus *deface*, sehingga penyidik menemui kesulitan dalam mencari log statistik yang terdapat di dalam server sebab biasanya secara otomatis server menghapus log yang ada untuk mengurangi beban server. Hal ini membuat penyidik tidak menemukan data yang dibutuhkan untuk dijadikan barang bukti sedangkan data log statistik merupakan salah satu bukti vital dalam kasus hacking untuk menentukan arah datangnya serangan.

c) Pemeriksaan

Penerapan pasal-pasal yang dikenakan dalam kasus *cyber crime* merupakan suatu permasalahan besar yang sangat merisaukan, misalnya apabila ada *hacker* yang melakukan pencurian data apakah dapat ia dikenakan Pasal 362 KUHP? Pasal tersebut mengharuskan ada sebagian atau seluruhnya milik orang lain yang hilang, sedangkan data yang dicuri oleh *hacker* tersebut sama sekali tidak berubah. Hal tersebut baru diketahui biasanya setelah selang waktu yang cukup lama karena ada orang yang mengetahui rahasia perusahaan atau menggunakan data tersebut untuk kepentingan pribadi. Pemeriksaan terhadap aksi dan korban banyak mengalami hambatan, hal ini disebabkan karena pada saat kejahatan berlangsung atau dilakukan tidak ada satupun saksi yang melihat (*testimonium de auditu*). Mereka hanya mengetahui setelah kejadian berlangsung karena menerima dampak dari serangan yang dilancarkan tersebut seperti tampilan yang berubah maupun tidak berfungsinya program yang ada, hal ini terjadi untuk kasus-kasus *hacking*.

Untuk kasus *carding*, permasalahan yang ada adalah saksi korban kebanyakan berada di luar negri sehingga sangat menyulitkan dalam melakukan pelaporan dan pemeriksaan untuk dimintai keterangan dalam berita acara pemeriksaan saksi korban. Apakah mungkin nantinya hasil BAP dari luar negri yang dibuat oleh kepolisian setempat dapat dijadikan kelengkapan isi berkas perkara? Mungkin apabila tanda tangan digital (*digital signature*) sudah disahkan maka pemeriksaan dapat dilakukan dari jarak jauh dengan melalui e-mailatau messanger. Internet sebagai sarana untuk melakukan penghinaan dan pelecehan sangatlah efektif sekali untuk "pembunuhan karakter".

Penyebaran gambar porno atau email yang mendiskreditkan seseorang sangatlah sering sekali terjadi. Permasalahan yang ada adalah, mereka yang menjadi korban jarang sekali mau menjadi saksi karena berbagai alasan. Apabila hanya berupa tulisan atau foto2 yang tidak

terlalu vulgar penyidik tidak dapat bersikap aktif dengan langsung menangani kasus tersebut melainkan harus menunggu laporan dari mereka yang merasa dirugikan karena kasus tersebut merupakan delik aduan (pencemaran nama baik dan perbuatan tidak menyenangkan). Peranan saksi ahli sangatlah besar sekali dalam memberikan keterangan pada kasus *cyber crime*,sebab apa yang terjadi didunia maya membutuhkan ketrampilan dan keahlian yang spesifik. Saksi ahli dalam kasus *cyber crime* dapat melibatkan lebih dari satu orang saksi ahli sesuai dengan permasalahan yang dihadapi, misalnya dalam kasus deface, disamping saksi ahli yang menguasai desain grafis juga dibutuhkan saksi ahli yang memahami masalah jaringan serta saksi ahli yang menguasai program.

d) Penyelesaian berkas perkara

Setelah penyidikan lengkap dan dituangkan dalam bentuk berkas perkara maka permasalahan yang ada adalah masalah barang bukti karena belum samanya persepsi diantara aparat penegak hukum, barang bukti digital adalah barang bukti dalam kasus *cyber crime* yang belum memiliki rumusan yang jelas dalam penentuannya sebab digital *evidence* tidak selalu dalam bentuk fisik yang nyata. Misalnya untuk kasus pembunuhan sebuah pisau merupakan barang bukti utama dalam melakukan pembunuhan sedangkan dalam kasus *cyber crime* barang bukti utamanya adalah komputer tetapi komputer tersebut hanya merupakan fisiknya saja sedangkan yang utama adalah data di dalam hard disk komputer tersebut yang berbentuk file, yang apabila dibuat nyata dengan print membutuhkan banyak kertas untuk menuangkannya, apakah dapat nantinya barang bukti tersebut dalam bentuk *compact disc* saja, hingga saat ini belum ada Undang-Undang yang mengatur mengenai bentuk dari pada barang bukti digital (*digital evidence*) apabila dihadirkan sebagai barang bukti di persidangan.

b. Penerapan aturan dalam Penjeratan Tindak Pidana Cyber Crime di Indonesia

Upaya yang dapat ditempuh untuk mengatasi kejahatan di masyarakat seperti cyber crime yakni menggunakan sarana hukum pidana yakni dengan menerapkan sanksi pidana kepada pelaku tindak pidana yang terkategori dalam cyber crime. [7] Pemidanaan terhadap yindak pidana siber atau cybercrime secara spesifik telah diatur rumusan pidananya dalam ketentuan Undang-Undang No 11 Tahun 2008 jo Undang-Undang No 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik serta beberapa peraturan perundangan-undangan lain yang memiliki konten cybercrime sebagai berikut:

a) Undang-Undang No 11 Tahun 2008 jo Undang-Undang No 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik

Sebagaimana diatur dalam ketentuan Pidana dalam BAB XI Undang-Undang ITE disebutkan bahwa perbuatan yang diancam pidana terhadap kejahatan cybercrime yang berkaitan dengan informasi dan transaksi elektronik antara lain sebagai berikut:

1) Pasal 45 ayat (1) UU ITE; Setiap orang yang tanpa hak mendistribusikan dan/atau membuat dapat diaksesnya informasi elektronik dan dokumen elektronik yang memuat konten kesusilaan dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 1.000.000.000 (satu miliar rupiah). Pasal 45 ayat (2) ; setiap orang yang tanpa hak menyebarkan berita bohong dan menyesatkan; menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian; dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 1.000.000.000 (satu miliar rupiah). Pasal 45 ayat (3) ;

[7] Antonie. (2017). Kejahatan Dunia Maya (Cyber Crime) dalam SIMAK Online. *Jurnal Nurani*. Vol.17, No. 2, Desember 2017. h. 273.

setiap orang yang secara tanpa hak mengirimkan / dokumen elektronik dan/atau informasi elektronik yang berisi ancaman kekerasan yang ditujukan secara pribadi pidana penjara paling lama 12 (duabelas) tahun dan/atau denda paling banyak Rp. 2.000.000.000 (dua miliar rupiah).

2) Pasal 46 Undang-Undang ITE; setiap orang yang secara tanpa hak mengakses jaringan komputer milik orang lain dipidana dengan pidana penjara paling lama 6 tahun dan/atau denda Rp. 600.000.000,- (ayat 1); pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp. 1.000.000.000 (ayat 2) dan pidana paling lama 12 tahun dan/atau denda paling banyak Rp. 2.000.000.000,-
3) Pasal 47 UU ITE; setiap orang yang tanpa hak melakukan intersepsi dipidana dengan pdiana penjara paling lama 10 tahun dan/atau denda paling banyak Rp800.000.000,-
4) Pasal 48 UU ITE; setiap orang yang secara melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan informasi elektronik dan/atau dokumen elektronik orang lain atau milik publik dipidana dengan pidana penjara paling lama 8 tahun dan/atau denda paling banyak Rp.2.000.000.000,- (ayat 1). Setiap orag yang secara melawan hukum dengan cara apapun memindahkan atau mentransfer informasi elektronik dan/atau dokumen elektronik kepada sistem elektronik orang lain yang tidak berhak dipidana dengan pidana penjara paling lama 9 tahun dan/atau denda paling banyak Rp. 3.000.000.000,- (ayat 2). Setiap orang yang melaksanakan tindakan sebagaimana dalam uraian diatas dan mengakibatkan terbukanya informasi yang bersifat rahasia atau pribadi dipidana dengan pidana penjara paling lama 10 tahun dan/atau denda paling banyak Rp. 5.000.000.000,-.

5) Pasal 49 UU ITE; setiap orang yang secara tanpa hak/ melawan hukum melakukan perbuatan yang mengakibatkan terganggunya sistem elektronik dipidana dengan pidana penjara paling lama 10 tahun dan/atau denda paling banyak Rp.10.000.000.000-
6) Pasal 50 UU ITE; setiap orang yang secara ilegal memproduksi dan/atau mendistribusikan perangkat keras atau perangkat lunak komputer dipidana dengan pidana penjara paling lama 10 tahun dan/atau denda Rp. 10.000.000,-
7) Pasal 51 UU ITE; setiap orang yang melaukan manipulasi terhadap sistem elektronik dan melakukan perbuatan yang dilarang oleh UU ITE dan menimbulkan kerugian bagi orang lain diancam dengan pidana penjara paling lama 12 tahun dan/atau denda paling banyak Rp. 12.000.000.000,-.

b) Kitab Undang-Undang Hukum Pidana (KUHP)

Dalam upaya menangani kasus-kasus yang terjadi para penyidik melakukan analogi atau perumpamaan dan persamaaan terhadap pasal-pasal yang ada dalam KUHP. Pasal-pasal didalam KUHP biasanya digunakan lebih dari satu Pasal karena melibatkan beberapa perbuatan sekaligus pasal - pasal yang dapat dikenakan dalam KUHP pada c*ybercrime* antara lain :

1) Pasal 362 KUHP yang dikenakan untuk kasus *carding* dimana pelaku mencuri nomor kartu kredit milik orang lain walaupun tidak secara fisik karena hanya nomor kartunya saja yang undang-undang tersebut sudah ada sejak tahun 2000 dan revisi terakhir dari rancangan undang-undang tindak pidana di bidang teknologi informasi sejak tahun 2004 sudah dikirimkan ke Sekretariat Negara RI oleh Departemen Komunikasi dan Informasi serta dikirimkan ke DPR namun dikembalikan kembali ke Departemen Komunikasi dan Informasi untuk diperbaiki. Tetapi, terdapat

beberapa hukum positif lain yang berlaku umum dan dapat dikenakan bagi para pelaku cybercrime terutama untuk kasuskasus yang menggunakan komputer sebagai sarana, antara lain: Kitab Undang Undang Hukum Pidana

2) Pasal 378 KUHP dapat dikenakan untuk penipuan dengan seolah olah menawarkan dan menjual suatu produk atau barang dengan memasang iklan di salah satu website sehingga orang tertarik untuk membelinya lalu mengirimkan uang kepada pemasang iklan. Tetapi, pada kenyataannya, barang tersebut tidak ada. Hal tersebut diketahui setelah uang dikirimkan dan barang yang dipesankan tidak datang sehingga pembeli tersebut menjadi tertipu.
3) Pasal 335 KUHP dapat dikenakan untuk kasus pengancaman dan pemerasan yang dilakukan melalui *e-mail* yang dikirimkan oleh pelaku untuk memaksa korban melakukan sesuatu sesuai dengan apa yang diinginkan oleh pelaku dan jika tidak dilaksanakan akan membawa dampak yang membahayakan. Hal ini biasanya dilakukan karena pelaku biasanya mengetahui rahasia korban.
4) Pasal 311 KUHP dapat dikenakan untuk kasus pencemaran nama baik dengan menggunakan media Internet. Modusnya adalah pelaku menyebarkan *email* kepada teman-teman korban tentang suatu cerita yang tidak benar atau mengirimkan *email* ke suatu *mailing list* sehingga banyak orang mengetahui cerita tersebut.
5) Pasal 303 KUHP dapat dikenakan untuk menjerat permainan judi yang dilakukan secara online di Internet dengan penyelenggara dari Indonesia.
6) Pasal 282 KUHP dapat dikenakan untuk penyebaran pornografi maupun website porno yang banyak beredar dan mudah diakses di Internet. Walaupun berbahasa Indonesia, sangat sulit sekali untuk menindak pelakunya karena mereka melakukan pendaftaran

domain tersebut diluar negri dimana pornografi yang menampilkan orang dewasa bukan merupakan hal yang ilegal.

7) Pasal 282 dan 311 KUHP dapat dikenakan untuk kasus penyebaran foto atau film pribadi seseorang yang vulgar di Internet.
8) Pasal 378 dan 262 KUHP dapat dikenakan pada kasus *carding*, karena pelaku melakukan penipuan seolah-olah ingin membeli suatu barang dan membayar dengan kartu kreditnya yang nomor kartu kreditnya merupakan curian.
9) Pasal 406 KUHP dapat dikenakan pada kasus *deface* atau *hacking* yang membuat sistem milik orang lain, seperti website atau program menjadi tidak berfungsi atau dapat digunakan sebagaimana mestinya.

c) Undang-Undang No 28 Tahun 2014 tentang Hak Cipta

Menurut Pasal 1 angka (9) UndangUndang No 28 Tahun 2014 tentang Hak Cipta, Program Komputer adalah seperangkat instruksi yang diekspresikan dalam bentuk bahasa, kode, skema,atau dalam bentuk apapun yang ditujukan agar komputer bekerja melakukan fungsi tertentu atau untuk mencapai hasil tertentu. Hak cipta untuk program komputer berlaku selama 50 tahun (Pasal 58 ayat (3)). Harga program komputer/ softwareyang sangat mahal bagi warganegara Indonesia merupakan peluang yang cukup menjanjikan bagi para pelaku bisnis guna menggandakan serta menjual software bajakan dengan harga yang sangat murah. Misalnya, program anti virus seharga $ 50 dapat dibeli dengan harga Rp20.000,00. Penjualan dengan harga sangat murah dibandingkan dengan software asli tersebut menghasilkan keuntungan yang sangat besar bagi pelaku sebab modal yang dikeluarkan tidak lebih dari Rp 5.000,00 perkeping. Maraknya pembajakan software di Indonesia yang terkesan "dimaklumi" tentunya sangat merugikan

pemilik hak cipta. Tindakan pembajakan program komputer tersebut juga merupakan tindak pidana sebagaimana diatur dalam Pasal 117 ayat (3) yaitu " Setiap Orang yang memenuhi unsur sebagaimana dimaksud pada ayat (2) yang dilakukan dalam bentuk Pembajakan dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau pidana denda paling banyak Rp4.000.000.000,00 (empat miliar rupiah).

d) Undang-Undang No 36 Tahun 1999 tentang Telekomunikasi

Menurut Pasal 1 angka (1) Undang-Undang No 36 Tahun 1999 tentang Telekomudikasi, Telekomunikasi adalah setiap pemancaran, pengiriman, dan/atau penerimaan dan setiap informasi dalam bentuk tanda-tanda, isyarat, tulisan, gambar, suara, dan bunyi melalui sistem kawat, optik, radio, atau sistem elektromagnetik lainnya. Dari definisi tersebut, maka Internet dan segala fasilitas yang dimilikinya merupakan salah satu bentuk alat komunikasi karena dapat mengirimkan dan menerima setiap informasi dalam bentuk gambar, suara maupun film dengan sistem elektromagnetik. Penyalahgunaan Internet yang mengganggu ketertiban umum atau pribadi dapat dikenakan sanksi dengan menggunakan UndangUndang ini, terutama bagi para hacker yang masuk ke sistem jaringan milik orang lain sebagaimana diatur pada Pasal 22, yaitu Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi:

1) Akses ke jaringan telekomunikasi
2) Akses ke jasa telekomunikasi
3) Akses ke jaringan telekomunikasi khusus

Apabila anda melakukan hal tersebut seperti yang pernah terjadi pada website KPU www.kpu.go.id, maka dapat dikenakan Pasal 50 yang berbunyi "Barang siapa yang melanggar ketentuan sebagaimanadimaksud dalam Pasal 22, dipidana dengan pidana penjara

paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah)".

e) Undang-Undang No 8 Tahun 1997 tentang Dokumen Perusahaan

Dengan dikeluarkannya Undang-Undang No. 8 Tahun 1997 tanggal 24 Maret 1997 tentang Dokumen Perusahaan, pemerintah berusaha untuk mengatur pengakuan atas mikrofilm dan media lainnya (alat penyimpan informasi yang bukan kertas dan mempunyai tingkat pengamanan yang dapat menjamin keaslian dokumen yang dialihkan atau ditransformasikan. Misalnya Compact Disk - Read Only Memory(CD - ROM), dan Write - Once - Read - Many (WORM), yang diatur dalam Pasal 12 Undang-Undang tersebut sebagai alat bukti yang sah.

f) Undang-Undang No 8 Tahun 2010 tentang Tindak Pidana Pencucian Uang

Undang-Undang ini merupakan Undang-Undang yang paling ampuh bagi seorang penyidik untuk mendapatkan informasi mengenai tersangka yang melakukan penipuan melalui Internet, karena tidak memerlukan prosedur birokrasi yang panjang dan memakan waktu yang lama, sebab penipuan merupakan salah satu jenis tindak pidana yang termasuk dalam pencucian uang (Pasal 2 Ayat (1) Huruf r). Penyidik dapat meminta kepada bank yang menerima transfer untuk memberikan identitas dan data perbankan yang dimiliki oleh tersangka tanpa harus mengikuti peraturan sesuai dengan yang diatur dalam Undang-Undang Perbankan. Dalam Undang-Undang Perbankan identitas dan data perbankan merupakan bagian dari kerahasiaan bank sehingga apabila penyidik membutuhkan informasi dan data tersebut, prosedur yang harus dilakukan adalah mengirimkan surat dari Kapolda ke Kapolri untuk diteruskan ke Gubernur Bank Indonesia. Prosedur tersebut

memakan waktu yang cukup lama untuk mendapatkan data dan informasi yang diinginkan. Dalam Undang-Undang Pencucian Uang proses tersebut lebih cepat karena Kapolda cukup mengirimkan surat kepada Pemimpin Bank Indonesia di daerah tersebut dengan tembusan kepada Kapolri dan Gubernur Bank Indonesia, sehingga data dan informasi yang dibutuhkan lebih cepat didapat dan memudahkan proses penyelidikan terhadap pelaku, karena data yang diberikan oleh pihak bank, berbentuk: aplikasi pendaftaran, jumlah rekening masuk dan keluar serta kapan dan dimana dilakukan transaksi maka penyidik dapat menelusuri keberadaan pelaku berdasarkan data– data tersebut. Undang-Undang ini juga mengatur mengenai alat bukti elektronik atau digital *evidence* sesuai dengan Pasal 73 huruf b yaitu alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu.

4. Kesimpulan

a. Proses penyidikan meliputi penyidikan, Penindakan, pemeriksaan dan penyelesaian berkas perkara. Tahap penyelidikan merupakan tahap pertama yang dilakukan oleh penyidik dengan adanya laporan atau informasi yang kemudain diteruskan ke Unit Cyber crime tertentu. Tahap Penindakan dalam hal ini penyidik melakukan penangkapan tersangka dan melakukan penyitaan. Tahap pemriksaan, dalam hal ini penyidik pelakukan pemerisaan saksi dan korban, dan Tahap terkahir apabila penyidikan lengkap maka dituangkan dalam bentuk berkas perkara.
b. Penerapan aturan untuk menjerat tindak pidana cyber crime secara spesifik diatur khusus dalam Undang-Undang No. 11 Tahun 2008 jo Undang-Undang No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, dan secara umum diatur dalam KUHP. Namun selain dua

ketentuan hukum tersebut terdapat ketentuan hukum yang digunakan untuk menjerat tindak pidana cybercrime dalam beberapa peraturan perundang-undangan diantaranya : Undang-Undang No 28 tahun 2014 tentang Hak cipta; Undang-Undang No 36 Tahun 1999 tentang Telekomunikasi; Undang-Undang No 8 Tahun 1997 tentang Dokumen Perusahaan; dan Undang-Undang No 8 Tahun 2010 tentang Tindak Pidana Pencucian Uang.

DAFTAR PUSTAKA

Agus, A.A., (2016), Penanganan Kasus *Cyber Crime* di Kota Makasar (Studi Pada Kantor Kepolisian Resort Kota Besar Makasar), *Jurnal Supremasi,* Volume XI Nomor 1, April 2016.

Antonie, (2017), Kejahatan Dunia Maya (Cyber Crime) dalam SIMAK Online, Jurnal Nurani, Vol.17, No. 2, Desember 2017.

Fajar, M & Ahmad Y, (2010), *Dualisme Penelitian Hukum Normatif dan Empiris,* Yogyakarta, Pustaka Pelajar.

Mansur, D.A.M., & Gultom E, (2005), *Cyber Law Aspek Hukum Teknologi Informasi*. Bandung. PT Refika Aditama.

Raharjo, A.A, (2002) *Cyber Crime* : *Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi.* Bandung : Citra Aditya.

Widodo, (2013) , *Hukum Pidana di Bidang Teknologi Informas, Cybercrime Law : Telaah Teoritik dan Bedah Kasus*. Yogyakarta. Aswaja Pressindo.

Undang-Undang No 11 Tahun 2008 jo Undang-Undang No 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia No 58 Tahun 2008m Tambahan Lembaran Negara Republik Indonesia Nomor 4843 Jo Lembaran Negara Republik Indonesia No 251 Tahun 2016 , Tambahan Lembaran Negara Republik Indonesia Nomor 5952).