BAB III

CONTOH KASUS TINDAK PIDANA *SKIMMING*

A. Kasus Tindak Pidana *Skimming* Berdasarkan Putusan Nomor 5/Pid.Sus/2021/PN Dps

Berawal dari Petugas Kepolisian Direktorat Reskrimsus Polda Bali memperoleh informasi dari pihak PT. Bank BNI, Tbk Denpasar terkait adanya informasi dari masyarakat bahwa terdapat beberapa transaksi mencurigakan yang dilakukan oleh orang asing dengan menggunakan kartu lain menyerupai kartu ATM (kartu putih yang berisi *Magnetic stripe*) di beberapa mesin ATM Bank BNI yang terdapat di seputaran Denpasar.

Pada hari Rabu, tanggal 28 Oktober 2020, melaksanakan patroli di seputaran kota Denpasar dan sekitar pukul 10.35, melihat adanya 1 (satu) orang asing mencurigakan datang dan masuk ke dalam mesin ATM Bank BNI kode mesin S1ERNN12PP Pertokoan Darma, yang beralamat di Jl. Hasanudin No. 59 Denpasar dengan ciri-ciri perawakan tinggi dan badan kekar, menggunakan helm *full face* warna hitam, jaket warna hitam, celana straight panjang warna Hitam dan sepatu.

Hasil penelusuran yang dilakukan oleh pihak BNI yaitu saksi I Nengah Ariyasa dan saksi Wawan Setiawan diperoleh jika kartu ATM tersebut dan diketahui bahwa memang benar telah terjadi sebanyak 3 (tiga) kali transaksi tertanggal 28 Oktober 2020 dengan menggunakan 2 (dua) buah kartu yaitu sebanyak 2 (dua) kali menggunakan kartu nomor 6725722400486476067 dan 1 (satu) kali menggunakan kartu nomor 6725512500054022716.

Pihak BNI melakukan pengecekan terhadap data rekaman CCTV yang terdapat pada mesin ATM BNI Berdasarkan data hasil rekaman CCTV yang terpasang di mesin ATM tersebut dapat diketahui bahwa pada tanggal 28 Oktober 2020, sekitar pukul 11.03 wita, terdapat 1 (satu) orang yang telah melakukan transaksi pada mesin ATM tersebut dengan ciri-ciri perawakan tinggi dan badan kekar, menggunakan *helm full face* warna hitam, jaket warna hitam dan sepatu, yang mana menurut saksi bahwa waktu yang tercatat pada hasil rekaman CCTV tersebut lebih cepat selama 24 (dua puluh empat) menit dari waktu yang sesungguhnya (*real time*) sesuai yang tercatat pada data Elektrik Jurnal, sehingga dapat dipastikan bahwa yang melakukan semua transaksi sesuai data tersebut diatas diantaranya yaitu transaksi penarikan tunai sebesar Rp. 2.500.000, - pukul 10:39:10 dengan menggunakan kartu nomor 6725722400486476067 adalah seseorang yang terlihat pada hasil rekaman CCTV tersebut.

Hasil penelusuran tersebut selanjutnya saksi I Komang Metro Adi Putra dan saksi I Kadek Reka Octa Jayantara dari Dit.Reskrimsus Polda Bali melakukan penangkapan terhadap terdakwa Bojidar Petrov Popov, pada hari Kamis, tanggal 29 Oktober 2020, sekira pukul 08.15 wita bertempat di depan Hotel Canggu *Dream Village* Jalan Banjar Kangin, Tibubeneng, Kecamatan Kuta Utara, Badung.

Saat dilakukan penggeledahan terhadap Terdakwa Bojidar Petrov Popov ditemukan 1 (satu) buah celana *straight* panjang warna Hitam merk *Under Armour,* 1 (satu) pasang sepatu merk *nike airmax* warna Hitam, 1 (satu) hp merk iphone 7 warna Hitam model A1778, IMEI 353070092725320, 1 (satu) buah

harddisk eksternal warna Hitam merk *Seagate,* 20 (dua puluh) lembar uang tunai pecahan Rp 100.000,- , 1 (satu) buah laptop merk ASUS tipe Vivobook 14 warna Ungu dengan model A412D beserta charger.

Dilakukan pengecekan secara digital forensik oleh Ahli I Made Dwi Aritanaya, S.H., CCPA, CCLA, dimana ditemukan ada aplikasi MSRX yang terinstal didalam 1 (satu) buah Laptop ASUS tipe *Vivobook* 14 warna ungu dengan model A412D dengan path This PC/OS (C:)/Program Files (x86) terhadap 1 (satu) buah kartu warna hitam BDD dengan nomor kartu 4565 5214 6214 1410 dapat Ahli jelaskan berdasarkan hasil pengecekan yang Ahli lakukan dengan menggunakan perangkat berupa pembaca kartu *Magnetic stripe (magnetic card reader)* dengan nomor seri *cardteck* MSR230U terhadap kartu tersebut, dapat diketahui jika terdapat data rekening bank tertentu pada pita *magnetic (Magnetic stripe)* yang termuat pada 1 (satu) buah kartu hitam BDD dengan nomor kartu 4565 5214 6214 1410 yaitu data kartu perbankan dengan nomor 6725722400486476067 yang merupakan kartu *Mastercard Debit* yang dikeluarkan oleh Cirrus, Germany.

Terdakwa Bojidar Petrov Popov membawa kartu *Magnetic Strip* serta alat pembaca dan penulis kartu merk MSR X6 dari negara terdakwa, Bulgaria. Terdakwa mengaku alat pembaca dan penulis kartu merk MSR X6 berfungsi untuk membaca dan menulis data perbankan pada kartu *Magnetic Strips* sedangkan kartu *Magnetic Strip* warna Hitam berfungsi untuk menyimpan data perbankan. Cara menggunakan alat pembaca dan penulis kartu merk MSR X6 adalah dengan menghubungkannya dengan Laptop milik terdakwa tersebut yang

sudah terpasang aplikasi MSRX, maka terdakwa mengetik angka - angka perbankan pada aplikasi tersebut.

Terdakwa Bojidar Petrov Popov menekan menu *"Write"* kemudian terdakwa menggesekan kartu *Magnetic Strips* pada alat pembaca dan penulis kartu merk MSR X6. Selanjutnya kartu *Magnetic Strips* siap digunakan, dimana Terdakwa memperoleh data perbankan tersebut dari internet pada *website* www.sendsface.com, yang mana pada *website* tersebut sudah terdapat data perbankan yang sebelumnya telah diunggah (*upload*) oleh seseorang (namun terdakwa tidak tahu namanya dan darimana yang bersangkutan mengunggahnya).

Data tersebut diunduh *(download)* oleh terdakwa dengan menggunakan HP miliknya merk Iphone 7 warna hitam. Kartu hitam BDD dengan nomor kartu 4565 5214 6214 1410 tersebut sudah memuat data perbankan yang dibeli oleh terdakwa di internet. Terdakwa sendiri yang memasukkan data tersebut dengan menggunakan laptop dan *card reader* MSRX miliknya tersebut. Namun terdakwa belum sempat menggunakan kartu tersebut.

Hasil transaksi yang dilakukan Terdakwa dengan kartu hasil *Skimming* tersebut tujuannya untuk memperoleh uang. Akibat perbuatan Terdakwa Bojidar Petrov Popov tersebut mengakibatkan kerugian Pihak Bank secara materiil dimana kewajiban pihak Bank harus melakukan pergantian terhadap kerugian nasabah tersebut dan juga pihak Bank mengalami kerugian secara *immateriil* dimana ATM yang digunakan untuk ilegal akses adalah mesin ATM Bank dan hal tersebut dapat merusak nama baik dan kridibiltas keamanan transaksi terhadap bank yang ada di Indonesia karena digunakan sebagai tempat melakukan

kejahatan, selain itu data-data nasabah Bank yang bertransaksi di ATM yang semestinya sangat rahasia dan tidak boleh diketahui oleh orang lain, datanya dicopy dan digunakan bertransaksi. Perbuatan Terdakwa Bojidar Petrov Popov sebagaimana diatur dan diancam pidana dalam Pasal 30 ayat (1) Jo. Pasal 46 ayat (1) Undang-Undang No. 19 tahun 2016 tentang Perubahan atas Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.[50]

B. Kasus Tindak Pidana *Skimming* Berdasarkan Putusan Nomor 1045/Pid.B/2020/PNJKT.TIM.

Terdakwa I Haerullah Ceylan, Terdakwa II Ufuk Kemaneci dan Terdakwa III Hakan Batal pada hari Kamis tanggal 14 Mei 2020 sekira pukul 05.30 WIB sampai pukul 06.30 WIB atau setidaknya pada waktu lain masih di bulan Mei tahun 2020 bertempat di ATM Bank Mandiri Raden Intan Jakarta Timur atau setidaknya pada tempat lain yang masih termasuk dalam daerah hukum Pengadilan Negeri Jakarta Timur mengambil uang Rp. 11.000.000,- (sebelas juta rupiah) milik orang lain dengan maksud untuk dimiliki secara melawan hukum yang dilakukan oleh dua orang atau lebih dengan bersekutu yang dilakukan para Terdakwa.

Pada waktu dan tempat sebagaimana tersebut di atas berawal ketika tanggal 12 Mei 2020 Terdakwa III mengajak Terdakwa II bertemu di *We Stay Coliving* Hotel Jakara Selatan dan membawakan alat-laat yang akan digunkan untuk *skimming*, kemudian Terdakwa III bersama Terdakwa II menuju sebuah ATM Bank Mandiri di Jalan Raden Intan Jakarta Timur untuk memasang alat *skimming* di Mesin

[50] www.mahkamahagung.co.id/diakses 22 Mei 2022

ATM tersebut dengan maksud agar data para nasabah yang melakukan transaksi di ATM tersebut tersalin dalam alat *skimming*.

Pada tanggal 13 Mei 2020 sekira pukul 22.00 Terdakwa III dan Terdakwa II kembali mendatangi ATM Bank Mandiri di Jalan Raden Intan untuk mencabut alat *skimming* yang sudah dipasang sebelumnya, selanjutnya alat *skimming* tersebut dibawa menuju tempat tinggal Terdakwa I di Apartemen Semanggi Jakarta Selatan dan diserahkan kepada Terdakwa I untuk memindahkan data nasabah bank yang ada dalam alat *skimming* tersebut ke kartu lain yang berbentuk seperti kartu.

Data nasabah yang masuk dalam alat *skimming* yang dipasang Terdakwa II dan Terdakwa III adalah data nasabah Bank Mandiri atas nama Bayu Satria dengan nomor kartu 4097662884869036 dan Daria Hilmah, dengan nomr kartu 4616993249998240. Bahwa setelah data para nasabah tersebut berhasil dipindahkan oleh Terdakwa I ke kartu-kartu lain yang menyerupai kartu ATM, kemudian kartu-kartu tersebut diserahkan kembali kepada Terdakwa II dan Terdakwa III dengan maksud untuk dapat dilakukan transaksi tarik tunai di mesin ATM.

Pada tanggal 14 Mei 2020 sekira pukul 05.45 WIB sampai pukul 06.15 WIB Terdakwa II dan Terdakwa III dengan menggunakan kartu yang serupa ATM tersebut melakukan transaksi penarikan tunai di sebuah Mesin ATM CIMB Niaga di daerah Kemang Jakarta Selatan dan berhasil menarik tunai uang sejumlah Rp. 10.000.000,-(sepuluh juta rupiah) dari rekening atas nama Bayu Satria dan Rp. 1.000.000,-(satu juta rupiah) dari rekening atas nama Daria Hilmah. Bahwa

setelah itu uang hasil penarikan tunai tersebut dibagi untuk Terdakwa I Rp. 5.000.000,- (lima juta rupiah), untuk Terdakwa II dan Terdakwa III masing-masing Rp. 3.000.000,- (tiga juta upiah).

Putusan Nomor 1045/Pid.B/2020/PNJKT.TIM, menyatakan :

Mengadili:

1. Menyatakan Terdakwa I Hayrullah Ceylan, Terdakwa II Ufuk Kemaneci dan Terdakwa III hakan battal terbukti secara sah dan meyakinkan besalah melakuka Tindak Pidana Pencurian Dengan Pemberatan sebagaimana Surat Dakwaan Tunggal Penuntut Umum.
2. Menjatuhkan pidana kepada Terdakwa I Hayrullah Ceylan, Terdakwa II Ufuk Kemaneci dan Terdakwa III Hakan Battal oleh karena itu dengan pidana penjara masing-masing selama 2 (dua) Tahun.

C. Data Kasus *Skimming* di Indonesia

Indonesia menjadi salah satu surga kejahatan perbankan. Salah satu modusnya adalah *skimming*. Indikasinya, sepertiga kasus *skimming* di dunia terjadi di Indonesia. Dalam tiga tahun terakhir, ada 5.500 kasus *skimming* di dunia. Sebanyak 1.549 kasus di antaranya terjadi di Indonesia. salah satu alasan para penjahat melakukan modus *skimming* di Tanah Air adalah karena Indonesia merupakan negara yang sangat nyaman untuk ditinggali.[51]

[51] https://nasional.tempo.co/read/680461/sepertiga-kasus-skimming-di-dunia-terjadi-di-indonesia/diakses 26 Agustus 2022

BAB IV

ANALISIS PENEGAKAN HUKUM

TERHADAP UPAYA PENCEGAHAN *SKIMMING*

A. Penegakan Hukum Tindak Pidana Terhadap Pelaku *Skimming*

Skimming merupakan suatu bentuk kejahatan menurut hukum di Indonesia dapat dilihat berdasarkan Pasal 363 ayat (1) ke-4e dan ke-5e KUHP, Pasal 378 KUHP, Pasal 30 ayat (1) dan ayat (2) Undang-Undang RI No. 19 tahun 2016 tentang perubahan atas Undang-Undang RI No. 11 tahun 2008 tentang informasi dan transaksi elektronik, Pasal 3 Undang-Undang No. 8 tahun 2010 (2) Terhadap pembuktian kejahatan *skimming* saat ini belum ada hukum acara khusus yang mengatur sehingga dalam hal ini pembuktian terkait kejahatan *skimming* masih mengacu pada KUHAP.

Adanya bukti elektronik sebagai perluasan bukti Pasal 184 ayat (1) KUHAP saat ini sudah diakui berdasarkan dasar Pasal 5 ayat (1), ayat (2) dan Pasal 44 huruf b Undang-Undang ITE dan putusan MK Nomor 20/Undang-Undang-XIV/2016. Penegakan hukum kejahatan *skimming* yaitu peningkatan jumlah SDM terkait penyidik kejahatan siber, penambahan alat dan perlengkapan investigasi, mengikutkan para penyidik terkait pelatihan khusus kejahatan siber dalam rangka peningkatan kemampuan penyidik terhadap kejahatan siber lebih khususnya dalam hal ini kejahatan *skimming*, membangun mekanisme yang lebih baik terkait pelaporan viktimisasi dan pengumpulan data penangkapan, peningkatan

kerjasama dengan berbagai pihak yang terkait dengan kejahatan siber khususnya dalam hal ini kejahatan *skimming*.

Kemajuan teknologi merupakan sesuatu yang tidak bisa kita hindari dalam kehidupan ini, karena kemajuan teknologi akan berjalan sesuai dengan kemajuan peradaban, teknologi dan ilmu pengetahuan. Teknologi membantu manusia mampu berinteraksi dengan manusia lain tanpa adanya batasan ruang dan waktu. Setiap inovasi diciptakan untuk memberikan manfaat positif bagi kehidupan manusia. Memberikan banyak kemudahan, serta sebagai cara baru dalam melakukan aktifitas manusia.

Khusus dalam bidang teknologi masyarakat sudah menikmati banyak manfaat yang dibawa oleh inovasi-inovasi yang telah di hasilkan dalam dekade terakhir ini, Berbagai teknologi seperti radio, majalah, koran, televisi merupakan teknologi yang diciptakan manusia untuk dapat mengirimkan informasi dari suatu tempat ke tempat lain, namun kurangnya dari teknologi tersebut konsep komunikasinya masih bersifat satu arah, tidak adanya kemampuan untuk memberikan dan mendapatkan *feedback* antara source dan *receiver messages*.

Struktur masyarakat dirubah oleh kemajuan teknologi dari yang bersifat lokal menuju ke arah masyarakat yang bersifat global. Perubahan ini disebabkan oleh kehadiran teknologi informasi yang terus berkembang. Perkembangan teknologi informasi itu berpadu dengan media dan komputer, yang kemudian melahirkan piranti baru yang di sebut internet dalam mengirimkan informasi. Sehingga, internet sangat membantu manusia dalam menyelesaikan masalahnya.

Website sebagai salah satu aplikasi dari internet merupakan media yang sangat membatu dalam perkembangan teknologi komunikasi dalam masa kini. *Website* juga merupakan media untuk mendapatkan informasi dan promosi di dunia internet seperti personal, profil sekolah, profil perusahaan, berita pendidikan, bisnis, berita terkini dan semua hal yang dibutuhkan manusia dapat diakses melalui internet. Dengan *website* mudah menyebarkan dan mendapatkan informasi yang dibutuhkan.

Website berfungsi sebagai media promosi, media pemasaran, media informasi, media pendidikan, dan media komunikasi. Meskipun demikian, dengan melihat banyak sekali manfaat seperti manfaat *website* tersebut, kehadiran internet telah memunculkan paradigma baru dalam kehidupan manusia. Kehidupan berubah dari yang hanya bersifat nyata (*real*) ke realitas baru yang bersifat maya *(virtual*). Realitas yang kedua ini biasa dikaitkan dengan internet dan ruang di dunia maya (*cyberspace*).

Internet dengan kelebihan-kelebihannya mempunyai sisi kelemahan dan memiliki dampak buruk jika dipergunakan orang yang tidak bertanggungjawab. Adanya *cyberspace* memberi peluang terjadinya kejahatan atau lebih dikenal dengan *cybercrime* (kejahatan dunia maya), banyak sekali jenis *cybercrime* salah satunya adalah *defacing*.

Defacing yang merupakan salah satu kejahatan dunia maya yaitu kegiatan merubah tampilan suatu *website* orang lain tanpa izin baik halaman utama atau *index* filenya ataupun halaman lain yang masih terkait dalam satu URL dengan *website* tersebut (bisa di *folder* atau di *file*). *Defacing* terdiri dari dua tahap, yaitu

mula-mula menerobos sistem orang lain atau kedalam *web server* dan tahap kedua adalah mengganti halaman *website* (*web page*).

Hacking dan *defacing* tidak dapat terpisahkan satu sama lain, karena *defacing* merupakan salah satu kegiatan *hacking* yaitu, kegiatan menerobos program komputer milik orang atau pihak lain tanpa izin. Pada awalnya *hacking* tidak selalu berkonotasi negatif, karena sebenarnya tujuan *hacking* adalah untuk mengetahui sistem keamanan milik orang tertentu dan memberi tahu celahnya. Tetapi dalam perkembangannya di masyarakat *hacking* di nilai dan di anggap kata yang mewakili sebuah kejahatan dunia maya, dan pada kenyataanya memang *hacking* dilakukan tanpa izin.

Dibentuknya Undang-undang Nomor 11 Tahun 2008 jo Undang-undang Nomor 19 tahun 2016 tentang Informasi dan Transaksi Elektronik oleh pemerintah yang disahkan pada tanggal 28 April 2008 dan perubahannya pada tanggal 25 November 2016, diharapkan agar semua kejahatan mayantara dapat terakomodir oleh Undang-undang tersebut, termasuk *defacing* yang telah diatur di dalamnya.

Undang-undang tersebut *defacing* telah diatur pada Pasal 30:

1. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau Sistem Elektronik milik orang lain dengan cara apapun
2. 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.

3. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengkases komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengaman.

Pasal di atas dari ayat (1) sampai ayat (3) menerangkan tentang *illegal acces* karena langkah awal *deface* yaitu memasuki sistem orang lain atau melakukan *hacking*, dan berikutnya *defacing* diatur pada Pasal 32 ayat (1) yang berbunyi: (1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambahkan, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik. Adapun Pasal tersebut di atas menerangkan larangan melakukan modifikasi terhadap suatu *website* atau masuk dalam kategori data *interference* pada bab tentang perbuatan dilarang, seperti yang dijelaskan sebelumnya bahwa *defacing* dilakukan dengan dua tahap, pertama melakukan *hacking* dan selanjutnya memodifikasi *website*.

Terlihat dengan jelas bahwa *defacing* merupakan suatu tindak pidana yang tentunya ada sanksi hukumnya. Salah satunya yang merugikan masyarakat adalah kejahatan mayantara dalam hal ini *defacing* tentu menjadi salah satu perbuatan yang dilakukan sehingga terwujudnya sebuah keadilan. Adapun dalam Undang-Undang No.19 Tahun 2016 berkaitan dengan tindak pidana *Defacing* merupakan perbuatan dilarang yang telah diatur pada Pasal 30 dalam hal *illegal acces* dan pada Pasal 32 ayat (1) dalam hal data *interference* mengingat langkah awal dalam *defacing* adalah melakukan *hacking* kemudian memodifikasi dari *website* tersebut. Mengenai Perundangan dunia maya (*defacing*) yang masuk ranah tindak kejahatan

dunia maya (*cyber crime*) diatur dalam BAB VII mengenai perbuatan yang dilarang dalam Undang-Undang No.11 Tahun 2008 jo Undang-Undang No.19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik.

Penegakan terhadap *cyber crime* di Indonesia masih belum mencerminkan penegakan hukum yang efektif meski Indonesia telah memiliki Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Undang-Undang *a quo* belum bisa mengakomodir *cyber crime* yang semakin marak di Indonesia yang mana meliputi penipuan kartu kredit, penipuan perbankan, *defacing, cracking*, transaksi seks, pornografi, judi *online*, penyebaran berita bohong melalui internet dan terorisme. Hal tersebut terjadi karena *cyber crime* tidak dibatasi oleh teritorial suatu negara, sehingga menunjukkan penyelarasan dibidang informasi, media, dan informatika berkembang tanpa dapat di bendung.

Penyalahagunaan kartu kredit milik orang lain di internet merupakan kasus *cyber crime* terbesar yang berkaitan dengan dunia bisnis internet di Indonesia. Penyalahgunaan kartu kredit milik orang lain memang tidak terlalu rumit dan bisa dilakukan secara fisik atau *online*. Nama dan kartu kredit orang lain yang diperoleh di berbagai tempat (restoran, hotel, atau segala tempat yang melakukan transaksi pembayaran dengan kartu kredit) di masukkan di aplikasi pembelian barang di Internet. Hal tersebut lah yang kemudian membuka peluang untuk para *hacker* dapat memasuki, memodifikasi, atau merusak *homepage (hacking)* sehingga kasus *hacking* atau peretasan semakin lama sering terjadi Kasus

peretasan umumnya bertujuan untuk mengambil data-data tertentu yang dimiliki target. Tapi ada juga peretasan yang bertujuan menghancurkan data atau sistem tertentu sehingga berdampak seperti kerusakan digital. Dalam peraturan juga disebutkan bahwa kasus *cyber crime* terkait dengan pengambilan data atau sistem elektronik. Kasus pembobolan ATM yang sering terjadi pada korban *cyber crime hacker* bisa dikatakan tindakan peretasan data dan pencurian uang milik korban.

Perkembangan ilmu pengetahuan dan teknologi saat ini tidak hanya mampu memberikan dampak yang positif saja namun perkembangan tersebut ternyata disalahgunakan sebagai sarana kejahatan. Hal tersebut sangat penting untuk di antisipasi bagaimana kebijakan hukumnya, sehingga *cyber crime* yang terjadi dapat dilakukan upaya penanggulangannya dengan hukum pidana, termasuk dalam hal ini adalah mengenai sistem penegakannya. Indonesia sendiri sudah memiliki aturan hukum *cyber crime* yang tertuang dalam Undang-Undang Nomor 19 tahun 2016 tentang Informasi dan Transaksi Elektronik yaitu atas perubahan undang-undang nomor 11 tahun 2008.

Penegak hukum merupakan salah satu komponen dalam penegakan hukum. Penegak hukum merupakan mereka yang secara langsung atau tidak langsung berkontribusi di dalam suatu proses penegakan hukum. Pada dasarnya penegak hukum akan menggabungkan antara nilai, kaidah, dan perilaku. Penegak hukum pada umumnya sering melakukan tindakan dan pemeliharaan dalam tercapainya tujuan keadilan. Sikap dari penegak hukum di dalam melaksanakan tugas-tugasnya, tidak jarang melakukan diskresi yang merupakan suatu pengambilan putusan dalam mengatasi masalah yang dihadapi tetapi didalam pengambilan

putusan penegak hukum harus tetap berpegang teguh terhadap peraturan, walaupun tidak menutup kemungkinan adanya diskresi yang tanpa berpegang pada peraturan, karena peraturan mengenai masalah tersebut belum ada.

B. Upaya Pencegahan Tindak Pidana Terhadap Pelaku *Skimming*

Kendala yang menyebabkan terjadinya pencurian uang menggunakan skimmer tidak lepas dikarenakan kelalaian dari pemilik kartu ATM itu sendiri. Pada kejahatan pembobolan ATM dengan cara *skimming*, korban biasanya tanpa sadar telah direkam video pada saat memasukkan pin ATM dan pita magnetik sudah pula direkam melalui alat khusus. Upaya hukum yang dilakukan terhadap tindak pidana pencurian uang dengan menggunakan *skimmer* adalah upaya kepolisian merupakan bagian integral dari kebijakan sosial (*social policy*). Kebijakan sosial dapat di artikan sebagai usaha yang rasional untuk mencapai kesejahteraan masyarakat (*social welfare policy*) dan sekaligus mencakup perlindungan masyarakat (*social defence policy*).

Hambatan yang di hadapi dalam melakukan penegakan hukum terhadap pelaku tindak pidana pencurian menggunakan *skimmer* adalah Aspek Internal yaitu Subtansi Hukum, Aspek penegak hukum (*law enforcement factor*), aspek fasilitas, aspek hambatan informasi, aspek kerahasian perbankan. Sedangkan aspek eksternal yaitu aspek masyarakat dan aspek kebudayaan.

Era globalisasi seperti saat ini, majunya perkembangan teknologi informasi dan komunikasi menciptakan berbagai macam hal kemajuan dalam bidang pemerintahan, bisnis, perbankan, Pendidikan, Kesehatan, dan kehidupan pribadi seseorang dalam menjalani kehiupan bersosialisasi dalam masyarakat. Namun,

tidak menutup kemungkinan ada beberapa oknum yang menjadikan kemajuan tersebut sebagai sarana dan/atau peluang untuk melakukan hal-hal negative atau kejahatan. Salah satu contohnya yaitu kejahatan siber (*cyber crime*). Sehingga dapat dikatakan bahwa kemajuan teknologi infomasi dan komunikasi ini dapat diumpamakan sebagai pedang bermata dua, karena selain memberikan kontribusi yang positif, juga menjadi sarana potensial dan sarana efektif untuk melakukan perbuatan melawan hukum.

Contoh kasus Putusan Nomor 1045/Pid.B/2020/PNJKT.TIM. Pada tanggal 13 Mei 2020 sekira pukul 22.00 Terdakwa III dan Terdakwa II kembali mendatangi ATM Bank Mandiri di Jalan Raden Intan untuk mencabut alat *skimming* yang sudah dipasang sebelumnya, selanjutnya alat *skimming* tersebut dibawa menuju tempat tinggal Terdakwa I di Apartemen Semanggi Jakarta Selatan dan diserahkan kepada Terdakwa I untuk memindahkan data nasabah bank yang ada dalam alat *skimming* tersebut ke kartu lain yang berbentuk seperti kartu.

Data nasabah yang masuk dalam alat *skimming* yang dipasang Terdakwa II dan Terdakwa III adalah data nasabah Bank Mandiri atas nama Bayu Satria dengan nomor kartu 4097662884869036 dan Daria Hilmah, dengan nomr kartu 4616993249998240. Bahwa setelah data para nasabah tersebut berhasil dipindahkan oleh Terdakwa I ke kartu-kartu lain yang menyerupai kartu ATM, kemudian kartu-kartu tersebut diserahkan kembali kepada Terdakwa II dan Terdakwa III dengan maksud untuk dapat dilakukan transaksi tarik tunai di mesin ATM.

Terdakwa II dan Terdakwa III dengan menggunakan kartu yang serupa ATM tersebut melakukan transaksi penarikan tunai di sebuah Mesin ATM CIMB Niaga di daerah Kemang Jakarta Selatan dan berhasil menarik tunai uang sejumlah Rp. 10.000.000,- (sepuluh juta rupiah) dari rekening atas nama Bayu Satria dan Rp. 1.000.000,-(satu juta rupiah) dari rekening atas nama Daria Hilmah. Bahwa setelah itu uang hasil penarikan tunai tersebut dibagi untuk Terdakwa I Rp. 5.000.000,- (lima juta rupiah), untuk Terdakwa II dan Terdakwa III masing-masing Rp. 3.000.000,- (tiga juta upiah).

Di Indonesia pada umumnya pemanfaatan perkembangan teknologi dan informasi sangatlah berkembang, banyaknya orang yang memanfaatkan teknologi untuk meraup keuntungan finansial seperti menjadi Youtuber, selebgram, programmer, dan lain. Dalam perkembangannya juga masalah kriminalitas semakin berkembang karena ruang lingkup teknologi yang luas Berbagai kejahatan dapat timbul dalam dunia maya misalnya penghinaan, pornografi, kejahatan terhadap keamanan negara, seperti pembocoran rahasia Negara serta perbuatan yang menimbulkan kerugian secara finasial bagi para korbannya seperti berita palsu, penipuan dan juga peretasan kartu kredit (*carding*).

Fenomena *cyber crime* memang harus diwaspadai karena kejahatan ini berbeda dengan kejahatan lain pada umumnya. *Cyber crime* dapat dilakukan tanpa mengenal batas teritorial dan tanpa interaksi langsung antara pelaku dengan korban kejahatan. Bisa dipastikan dengan sifat global internet, semua negara yang melakukan kegiatan internet hampir pasti akan terkena akibat dari perkembangan tindak pidana komputer ini.

Tindak pidana peretasan kartu kredit/ carding salah satu jenis kejahatan siber yang sering terjadi dewasa ini. *Carding* adalah kejahatan dengan menggunakan data kartu kredit. Perbuatan tersebut dapat dikategorikan dalam 2 (dua) bentuk yaitu transaksi konvensional atau *offline* dan transaksi maya atau online. Tindak pidana *carding* telah berkembang pesat di Indonesia, sementara itu pengaturan sistem hukum di Indonesia masih memberikan celah dan lemahnya sistem pengawasan atas kejahatan ini.

Kemajuan teknologi informasi terutama pada bidang komputer dan internet terbukti telah memberikan dampak positif bagi kemajuan kehidupan manusia. Perlu digaris bawahi, dibalik kelebihan dan kemudahan yang ditawarkan oleh komputer dan internet, ternyata memiliki sisi gelap yang dapat menghancurkan kehidupan dan budaya manusia itu sendiri. Perkembangan teknologi informasi mengubah pola pemikiran mengenai batas wilayah, waktu, nilai-nilai, wujud benda, logika berfikir, pola kerja, dan batas perilaku sosial dari yang bersifat manual menjadi komputerisasi/digital.

Informasi sudah dianggap sebagai "*power"* yang diartikan sebagai kekuatan dan kekuasaan yang sangat menentukan nasib manusia itu sendiri. Saat ini ketergantungan masyarakat akan teknologi informasi semakin tinggi sehingga semakin tinggi pula resiko yang dihadapi. Teknologi informasi saat ini menjadi "pedang bermata dua" karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum termasuk tindak pidana (kejahatan). Berbagai bentuk tindak pidana (kejahatan) inilah yang kemudian dikenal dengan *cybercrime*.

Banyaknya masyarakat yang menggunakan media elektronik sebagai alat komunikasi memiliki potensi untuk terjadinya pelanggaran terhadap privasi khususnya adalah penyalahgunaan berupa pembobolan atau pencurian data pribadi. Hal tersebut dipengaruhi oleh perilaku atau budaya masyarakat yang senang membagi bagi data serta informasi. Contohnya dari media elektronik seperti telepon seluler yang mengharuskan mengisi data pribadi atau registrasi sebelum menggunakan kartu telepon seluler atau bahkan melalui media elektronik internet di setiap profil pada akun jejaring sosial (seperti *facebook, twitter, friendster, myspace,* dan lain-lain) individu yang bersangkutan selalu mencantumkan data-data pribadinya secara relatif lengkap dan jujur. Informasi pribadi, seperti tanggal lahir, nomor telepon, tempat tinggal, foto-foto pribadi dan lainnya tentu saja secara sengaja maupun tidak sengaja, dipicu dengan karakteristik internet yang terbuka dan bebas, data informasi ini mudah sekali mengalir dari satu tempat ke tempat lainnya tanpa terkendali.

Urgensi pemberian perlindungan hukum kepada data pribadi ini mulai menguat seiring dengan meningkatnya jumlah pengguna telepon seluler dan internet. Sejumlah kasus yang mencuat, terutama yang memiliki keterkaitan dengan kebocoran data pribadi seseorang dan bermuara kepada aksi penipuan atau tindak kriminal pornografi, menguatkan wacana pentingnya pembuatan aturan hukum untuk melindungi data pribadi. Pelindungan terhadap data pribadi berkaitan dengan konsep privasi, konsep privasi sendiri adalah merupakan sebuah gagasan untuk memelihara integritas dan martabat setiap orang secara pribadi.

Privasi adalah istilah lain yang kemudian digunakan oleh negara-negara maju yang berkaitan dengan data pribadi sebagai hak yang harus dilindungi, yaitu hak seseorang untuk tidak diganggu kehidupan pribadinya. membahas privasi berarti membahas tentang hak untuk menikmati hidup. Meskipun privasi diakui sebagai hak asasi manusia, sebagai sebuah konsep, sangat sulit untuk mendefinisikan dan bervariasi sesuai dengan konteks, bangsa, dan budaya.

Hak privasi melalui pelindungan data merupakan elemen kunci bagi kebebasan dan harga diri individu. Pelindungan data menjadi pendorong bagi terwujudnya kebebasan politik, spiritual, keagamaan bahkan kegiatan yang bersifat privat. Hak untuk menentukan nasib sendiri, kebebasan berekspresi dan privasi adalah hak-hak yang penting untuk menjadikan kita sebagai manusia.

Penindakan kasus *cyber crime* sering mengalami hambatan terutama dalam penangkapan tersangka dan penyitaan barang bukti. Dalam penangkapan tersangka sering kali 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.

Salah satu kasus Putusan Nomor 5/Pid.Sus/2021/PN Dps, sekitar pukul 11.03 wita, terdapat 1 (satu) orang yang telah melakukan transaksi pada mesin ATM

tersebut dengan ciri-ciri perawakan tinggi dan badan kekar, menggunakan *helm full face* warna hitam, jaket warna hitam dan sepatu, yang mana menurut saksi bahwa waktu yang tercatat pada hasil rekaman CCTV tersebut lebih cepat selama 24 (dua puluh empat) menit dari waktu yang sesungguhnya (*real time*) sesuai yang tercatat pada data Elektrik Jurnal, sehingga dapat dipastikan bahwa yang melakukan semua transaksi sesuai data tersebut diatas diantaranya yaitu transaksi penarikan tunai sebesar Rp. 2.500.000, - pukul 10:39:10 dengan menggunakan kartu nomor 6725722400486476067 adalah seseorang yang terlihat pada hasil rekaman CCTV tersebut.

Hasil penelusuran tersebut selanjutnya saksi I Komang Metro Adi Putra dan saksi I Kadek Reka Octa Jayantara dari Dit.Reskrimsus Polda Bali melakukan penangkapan terhadap terdakwa Bojidar Petrov Popov, pada hari Kamis, tanggal 29 Oktober 2020, sekira pukul 08.15 wita bertempat di depan Hotel Canggu Dream Village JalanBanjar Kangin, Tibubeneng, Kecamatan Kuta Utara, Badung.

Saat dilakukan penggeledahan terhadap Terdakwa Bojidar Petrov Popov ditemukan 1 (satu) buah celana straight panjang warna Hitam merk Under Armour, 1 (satu) pasang sepatu merk nike airmax warna Hitam, 1 (satu) hp merk iphone 7 warna Hitam model A1778, IMEI 353070092725320, 1 (satu) buah *harddisk* eksternal warna Hitam merk *Seagate,* 20 (dua puluh) lembar uang tunai pecahan Rp 100.000,- , 1 (satu) buah laptop merk ASUS tipe *Vivobook* 14 warna Ungu dengan model A412D beserta *charger.*

Dilakukan pengecekan secara digital forensik oleh Ahli I Made Dwi Aritanaya, S.H., CCPA, CCLA, dimana ditemukan ada aplikasi MSRX yang

terinstal didalam 1 (satu) buah Laptop ASUS tipe Vivobook 14 warna ungu dengan model A412D dengan path This PC/OS (C:)/Program Files (x86) terhadap 1 (satu) buah kartu warna hitam BDD dengan nomor kartu 4565 5214 6214 1410 dapat Ahli jelaskan berdasarkan hasil pengecekan yang Ahli lakukan dengan menggunakan perangkat berupa pembaca kartu *Magnetic stripe (magnetic card reader)* dengan nomor seri *cardteck* MSR230U terhadap kartu tersebut, dapat diketahui jika terdapat data rekening bank tertentu pada pita magnetic *(Magnetic stripe)* yang termuat pada 1 (satu) buah kartu hitam BDD dengan nomor kartu 4565 5214 6214 1410 yaitu data kartu perbankan dengan nomor 6725722400486476067 yang merupakan kartu *Mastercard Debit* yang dikeluarkan oleh Cirrus, Germany.

Terdakwa Bojidar Petrov Popov membawa kartu Magnetic Strip serta alat pembaca dan penulis kartu merk MSR X6 dari negara terdakwa, Bulgaria. Terdakwa mengaku alat pembaca dan penulis kartu merk MSR X6 berfungsi untuk membaca dan menulis data perbankan pada kartu *Magnetic Strips* sedangkan kartu Magnetic Strip warna Hitam berfungsi untuk menyimpan data perbankan.

Pertanggungjawaban pidana peretasan (*hacking*) di dasarkan pada ketentuan Pasal 30 Undang-Undang ITE. Di dalam Pasal 30 Undang-Undang ITE, seseorang dapat dipidana apabila orang tersebut mengakses sistem elektronik atau komputer korban dan juga dalam Pasal ini menentukan bahwa cara yang dilakukan adalah dengan cara apapun (termasuk peretasan) selama hal tersebut dilakukan dengan cara tanpa haknya. Apabila suatu *website* di retas oleh *hacker*, maka si penyedia

layanan *web hosting* tidak dapat dimintai pertanggungjawaban pidana. Penyedia layanan *web hosting* hanya sebagai media penyedia saja, tetapi pemilik penyedia layanan *web hosting* tidak dapat mengelak untuk dimintai pertanggungjawaban pidana apabila pemilik membuat layanan-nya semata-mata untuk memfasilitasi tindak pidana. Sama halnya dengan seorang penyedia bangunan apartemen tidak dapat dimintakan pertanggungjawaban apabila pemilik apartemen dimasuki oleh kawanan pencuri.

Pemidanaan di Indonesia seharusnya merujuk pada pendekatan norma yang bersifat menghukum penjahat sehingga dapat membuat efek jera. Eksistensi penegakan hukum dalam hal visi dan misi penegakan hukumnya, baik di tingkat penyidik, penuntut sampai tingkat pengadilan, harusnya memiliki presensi yang sama sesuai tuntutan hukum dan keadilan masyarakat.

Analisis yang didapat dari kasus tersebut mengenai *cyber crime hacker*, merupakan salah satu perbuatan melanggar hukum, sebagaimana sudah diatur dalam Pasal 32 ayat (1) jo Pasal 48 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana diubah dengan Undang-undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Karena perbuatan kejahatan menggunakan media elektronik yang sudah diatur secara khusus di Undang-Undang ITE sehingga Pasal yang terdapat didalam KUHP dikesampingkan sesuai dengan asas pidana *lex specialis derogate legi generali* yang berbunyi “Jika suatu tindakan masuk dalam suatu ketentuan pidana umum,

tetapi termasuk juga dalam ketentuan pidana khusus, maka hanya yang khusus itu yang diterapkan".

Kendala yang dihadapi oleh aparat kepolisian dalam upaya penanggulangan *cyber crime* dapat dibagi ke dalam 4 (empat) aspek, yaitu: aspek penyidik (Tingkat kemampuan dan *skill* penyidik), alat bukti (data yang rentan untuk diubah dan dihapus), fasilitas *(laboratorium forensic computer*) dan jurisdiksi. Banyak kendala yang di hadapi oleh aparat penegak hukum dalam memberantas *cyber crime*. Kendala tersebut tentu akan mempengaruhi penegakan hukum terhadap *cyber crime* sehingga tidak dapat di atasi dengan maksimal. Kepolisian sebagai salah satu penegak hukum tidak luput dari kendala tersebut.

Beberapa kendala yang menghambat upaya penanggulangan *cyber crime* dari pihak kepolisian, dapat dilihat dari empat aspek yaitu:

1. Aspek Penyidik

Penyidik kepolisian memiliki peran penting dalam upaya penanggulangan *cyber crime*, dimana kemampuan penyidik sangat dibutuhkan untuk mengungkap kasus-kasus *cyber crime*. Adanya unit *cyber crime* di lingkungan kepolisian membuktikan bahwa dibutuhkannya penyidik khusus yang memiliki kemampuan di bidang informasi dan transaksi elektronik guna menangani kejahatan-kejahatan di dunia maya. Pendidikan khusus untuk memberikan pengetahuan terkait *cyber* kepada para penyidik yang khusus menangani masalah *cyber crime* sangat penting untuk dilakukan agar dapat mengakomodir kebutuhan penyidik dalam mengungkap kasus *cyber crime*.

2. Aspek Alat Bukti

Proses penyidikan kasus *cyber crime*, alat bukti elektronik memiliki peran penting dalam penanganan kasus. Alat bukti dalam kasus *cyber crime* berbeda dengan alat bukti kejahatan lainnya dimana sasaran atau media *cyber crime* merupakan data-data atau sistem komputer / internet yang sifatnya mudah diubah, dihapus, atau disembunyikan oleh pelaku kejahatan. Terutama jika melihat dalam pengaturan alat bukti dalam Pasal 184 KUHAP yang tidak mengenal istilah bukti elektronik/digital *(digital evidence)* sebagai bukti yang sah menurut undang-undang. Sering kali juga di dapati alat bukti elektronik sudah dilakukan modifikasi, di ubah bahkan di hapus, meski hal tersebut tidak berlaku bagi pelaku yang tertangkap tangan dalam melakukan aksi nya karena alat bukti dapat langsung diamankan oleh pihak kepolisian.

3. Aspek Fasilitas

Mengungkap kasus-kasus *cyber crime* dibutuhkan fasilitas yang mampu menunjang kinerja aparat kepolisian. Salah satunya adalah dengan memaksimalkan kemampuan digital forensik. Digital forensik ini dapat bekerja dalam laboratorium komputer forensik. Laboratorium komputer forensik di gunakan untuk mengamankan dan menganalisis bukti digital sehingga diperoleh fakta atas suatu kasus yang terjadi. Digital forensik ini dapat bekerja dengan mengungkap data-data yang bersifat digital serta merekam dan menyimpan bukti-bukti yang berupa *soft copy* (gambar, program, html, suara, dan lain sebagainya). Sayangnya belum semua kantor polisi memiliki laboratorium komputer forensik tersebut, padahal laboratorium tersebut sangat penting digunakan dalam mengungkap kasus *cyber crime*.

4. Aspek Jurisdiksi

Asas-asas berlakunya hukum pidana menurut tempat yang konvensional / tradisional (jurisdiksi fisik) tentunya menghadapi tantangan sehubungan dengan masalah pertanggungjawaban *cyber crime*. Penanganan *cyber crime* tidak akan berhasil jika aspek jurisdiksi diabaikan. Karena pemetaan yang menyangkut kejahatan dunia maya menyangkut juga hubungan antar kawasan, antar wilayah, dan antar negara. Penetapan jurisdiksi diperlukan dan diatur dalam Pasal 2 undang-undang informasi dan transaksi elektronik nomor 11 tahun 2008, yaitu: "Undang-undang ini berlaku untuk setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam undang-undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau diluar wilayah hukum indonesia dan merugikan kepentingan Indonesia".

Upaya penanganan *cyber crime* dalam klasifikasi *hacker* dibutuhkan keseriusan seluruh pihak mengingat teknologi informasi telah dijadikan sarana berbudaya komunikasi. Keberadaan undang- undang yang mengatur *cyber crime* terutama dalam klasifikasi *hacker* diperlukan, akan tetapi jika pelaksanaanya tidak memiliki kemampuan dan keahlian dalam bidang tersebut dan masyarakat terus menjadi sasaran, tujuan pembentukan undang-undang tersebut tidak akan tercapai.

Menurut ketentuan Pasal 30 dan Pasal 46 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan atau sistem elektronik milik orang

lain dengan cara apapun untuk memperoleh informasi elektronik dan atau dokumen elektronik dikenakan sanksi pidana penjara antara 6 (enam) sampai 8 (delapan) tahun dan atau denda sekitar Rp 1.000.000.000,- (satu miliar rupiah) sampai dengan Rp 2.000.000.000,- (dua miliar rupiah).

Pembentuk Undang-Undang telah merumuskan ketentuan pidana seperti dalam ketentuan peraturan diatas, namun pada kenyataannya penegakan hukum pada *cyber crime hacker* ini di rasa masih sangat kurang. Salah satu penyebabnya adalah tidak semua korban mempunyai keinginan untuk melaporkan meski korban sudah menderita kerugian secara materil. Selain itu kurangnya kompetensi aparat penegak hukum dalam memberantas *cyber crime hacker* juga membawa pengaruh terhadap penegakan hukumnya.

Solusi untuk mencegah kejahatan dengan menggunakan teknologi informasi adalah sebagai berikut:

1. Pencurian dan penggunaan *account* internet milik orang lain solusinya adalah Penggunaan enkripsi yaitu dengan mengubah data-data yang dikirimkan sehingga tidak mudah disadap (*plaintext* diubah menjadi *chipertext*). Untuk meningkatkan keamanan *authentication* (pengunaan user_id dan *password*), penggunaan enkripsi dilakukan pada tingkat *socket*. Hal ini akan membuat orang tidak bias menyadap data atau transaksi yang dikirimkan dari/ke server WWW.
2. Kejahatan kartu kredit yang dilakukan lewat transaksi online di Yogyakarta solusinya adalah Perlu adanya *cyberlaw*: *Cybercrime* belum sepenuhnya terakomodasi dalam peraturan / Undang-undang yang ada, penting adanya

perangkat hukum khusus mengingat karakter dari *cybercrime* ini berbeda dari kejahatan konvensional.

3. Pornografi solusinya adalah di Swedia, perusahaan keamanan internet, *NetClean Technology* bekerjasama dengan *Swedish National Criminal Police Department* dan *Ngoecpat*, mengembangkan program *software* untuk memudahkan pelaporan tentang pornografi anak. Setiap orang dapat mendownload dan menginstalnya ke komputer. Ketika seseorang meragukan apakah material yang ada di internet itu legal atau tidak, orang tersebut dapat menggunakan *software* itu dan secara langsung akan segera mendapat jawaban dari Ecpat Swedia.
4. Penipuan Melalui Situs Internet solusinya adalah meningkatkan pengetahuan dan kesadaran masyarakat tentang masalah *cybercrime*, sehingga masyarakat tidak mudah terpengaruh dengan iklan dalam situs.
5. Penipuan Lewat Email solusinya adalah Adanya kesadaran masyarakat yang sudah menjadi korban untuk melaporkan kepada polisi, sehingga korban email itu dapat dikurangi atau bahkan pengirim email dapat segera ditangkap.
6. Kejahatan yang berhubungan dengan nama domain solusinya adalah Meningkatkan sistem pengamanan jaringan komputer nasional sesuai dengan standar internasional.
7. Terjadinya perubahan dalam *website* KPU solusinya adalah Penggunaan *Firewall.* Tujuan utama dari *firewall* adalah untuk menjaga agar akses dari orang tidak berwenang tidak dapat dilakukan. Program ini merupakan perangkat yang diletakkan antara internet dengan jaringan internal. Informasi

yang keluar dan masuk harus melalui atau melewati *firewall*. Firewall bekerja dengan mengamati paker *Intenet Protocol* (IP) yang melewatinya *Denial of Service (DoS*) dan *Distributed DoS (DDos*) *attack* solusinya adalah Perlunya Dukungan Lembaga Khusus: Lembaga ini diperlukan untuk memberikan informasi tentang *cybercrime*, melakukan sosialisasi secara intensif kepada masyarakat, serta melakukan riset-riset khusus dalam penanggulangan *cybercrime*.