Jurist-Diction
Volume 4 No. 2, Maret 2021

Pertanggungjawaban Pidana Tindak Pidana Pemerasan Dengan Modus Operandi Penyebaran *Ransomware Cryptolocker*

Nur Syamsi Tajriyani
nur-syamsi-tajriyani-2017@fh.unair.ac.id
Universitas Airlangga

How to cite:
Nur Syamsi Tajriyani, 'Pertanggungjawaban Pidana Tindak Pidana Pemerasan Dengan Modus Operandi Penyebaran *Ransomware Cryptolocker*' (2021) Vol. 4 No. 2 Jurist-Diction.

Histori artikel:
Submit 9 Januari 2021;
Diterima 18 Februari 2021;
Diterbitkan 1 Maret 2021.

DOI:
10.20473/jd.v4i2.25785

p-ISSN: 2721-8392
e-ISSN: 2655-8297

Abstract

Cyber sabotage and extortion through electronic systems in the case of cryptolocker ransomware's spread is something new in Indonesia. This can be seen from the absence of a court decision regarding the case for the distribution of cryptolocker ransomware. The modus operandi of ransomware cryptolocker's spread is quite complex because it is something that must be considered in terms of its legal application because these acts covers several criminal acts, namely extortion and threats, destruction, and disruption of electronic systems. Because the perpretators of this act are people who have more knowledge about technology, it caused difficulties because of the lack of information about the perpretators that can be obtained. This research has a target in the form of how the modus operandi and criminal responsibility of the perpetrators of blackmail through electronic systems in the case of ransomware cryptolocker's spread.

Keywords: *Criminal Liability, Cryptolocker Ransomware, Extortion.*

Abstrak

Tindak pidana pemerasan melalui sistem elektronik dalam kasus penyebaran ransomware cryptolocker merupakan hal yang baru di Indonesia. Hal ini terlihat dari belum adanya putusan pengadilan mengenai kasus penyebaran ransomware cryptolocker. Modus operandi penyebaran ransomware cryptolocker yang cukup kompleks merupakan sesuatu yang harus diperhatikan dalam hal penerapan hukumnya oleh karena serangkaian perbuatan tersebut melingkupi beberapa tindak pidana yaitu pemerasan dan pengancaman, perusakan, dan mengakibatkan terganggunya sistem elektronik. Pelaku yang merupakan orang yang memiliki ilmu lebih tentang teknologi juga menjadi kesulitan tersendiri karena minimnya informasi mengenai pelaku yang bisa didapatkan. Penelitian ini memiliki sasaran berupa bagaimana modus operandi dan pertanggungjawaban pidana pelaku tindak pidana pemerasan melalui sistem elektonik dalam kasus serangan ransomware cryptolocker.

Kata Kunci: Pertanggungjawaban Pidana; *Ransomware Cryptolocker*; Pemerasan.

Pendahuluan

Perkembangan teknologi saat ini yang begitu pesat menjadikan dunia sekarang ini makin sempit, batas-batas negara menjadi semakin buram. Ada pandangan, dunia kini tidak lagi terbagi-bagi oleh ideologi, tetapi teknologi.[1] Berbicara mengenai teknologi, maka tak lepas pula dari ilmu pengetahuan. Teknologi kini tidak dapat dipisahkan dengan ilmu pengetahuan karena ilmu pengetahuan tidak sekedar berinteraksi dengan teknologi, bahkan fungsinya telah menjadi inovator di dalam kegiatan teknologi canggih. Pertumbuhan ilmu pengetahuan semakin menyatu sehingga kedua hal tersebut disebut IPTEK.[2]

Teknologi Informasi dan Komunikasi mengandung pengertian yaitu segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, dan pemindahan informasi antar media. Teknologi informasi dan komunikasi merupakan peralatan elektronik yang terdiri dari perangkat keras dan perangkat lunak serta segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengolahan, dan transfer atau pemindahan informasi antar media (Rusman, dkk. 2012:89). Berkembangnya teknologi informasi, media, dan komunikasi juga menyebabkan hubungan dunia menjadi tanpa batas (*borderless*) sehingga menyebabkan terjadinya perubahan sosial, ekonomi, dan budaya secara signifikan dalam waktu cepat. Namun, teknologi informasi dan telekomunikasi yang tanpa batas selain menuai dampak positif, juga menimbulkan dampak negatif oleh karena pemanfaatan teknologi informasi dan telekomunikasi yang disalahgunakan dapat menjadi media yang efektif untuk melakukan perbuatan melawan hukum, salah satunya adalah penyalahgunaan teknik *cryptovirology* yang seharusnya digunakan untuk mengenkripsi data-data penting yang bersifat rahasia yang disalahgunakan untuk melakukan tindak pidana pemerasan melalui *ransomware cryptolocker*. Sebagaimana sebuah teori mengatakan "*crime is product of society itself*".[3]

---

[1] Didik Endro Purwoleksono, *Hukum Pidana Untaian Pemikiran* (Airlangga University Press 2019).[49]. Selanjutnya disebut Didik Endro 1.

[2] *ibid.*

[3] Ari Juliano Gema, 'Cybercrime : Sebuah Fenomena di Dunia Maya' (hukumonline 2000) <www.hukumonline.com> dikunjungi pada pada 05-05-2020.

Perkembangan internet yang pesat juga berbanding lurus dengan modus operandi kejahatan yang muncul. Pada 2017, dunia digemparkan dengan menyebarnya sebuah *Malicious Software* (*Malware*) yang berjenis *Ransomware Cryptolocker* yang bernama *Wanna Decryptor*. *Ransomware Wanna Decryptor* atau dikenal dengan *WannaCry* bekerja dengan cara mengunci sistem komputer. Pada 14 Mei 2017, Europol memperkirakan ada lebih dari 200.000 korban *ransomware WannaCry* yang tersebar di 150 negara. *Ransomware WannaCry* meminta uang tebusan agar file yang 'dibajak' dengan proteksi enkripsi bisa dikembalikan dan diakses kebali. Uang tebusan yang diminta harus dibayarkan dengan instrumen *cryptocurrency* yaitu *bitcoin* yang jika dikurskan 1 *bitcoin* setara Rp. 4.000.000,- (empat juta rupiah). Uang tebusan ini akan semakin tinggi apabila uang tebusan tidak segera dibayarkan.[4]

Berdasarkan latar belakang tersebut di atas, penulis tertarik untuk melakukan penelitian yang bertujuan untuk mengetahui pertanggungjawaban pidana tindak pidana pemerasan dengan modus operandi *ransomware cryptolocker* mengingat kasus penyebaran *ransomware cryptolocker* merupakan kasus dengan modus operandi yang unik dengan cara melakukan enkripsi terhadap data korban.

Metode Penelitian

Dalam penelitian ini, penulis menggunakan metode penelitian hukum doktrinal (*doctrinal research*). Penelitian doktrinal (*doctrinal research*) dalam penelitian ini membahas mengenai pengertian, prinsip-prinsip, konsep hukum, dan peraturan perundang-undangan yang terkait, serta melakukan analisis terhadap aturan hukum satu dengan lainnya yang relevan dengan permasalahan yang dibahas pada penelitian ini. Penulis juga menggunakan dua pendekatan dalam penelitian ini yaitu pendekatan perundang-undangan dan pendekatan konseptual. Pendekatan perundang-undangan dilakukan dengan menelaah semua undang-undang dan regulasi yang bersangkut paut dengan isu hukum yang sedang ditangani. Sedangkan

[4] Fauzan Jamaludin, 'Begini Dampak dari Serangan Malware WannaCrypt' (merdeka 2017) <www.merdeka.com> dikunjungi pada 05-05-2020.

untuk pendekatan konseptual dilakukan dengan cara mempelajari pandangan-pandangan dan doktrin-doktrin yang berkembang dalam ilmu hukum sehingga penulis akan menemukan ide-ide yang melahrikan pengartian-pengertian hukum, konsep-konsep hukum, dan asas-asas hukum yang relevan dengan isu hukum yang dihadapi, yaitu konsep tindak pidana pemerasan, konsep sistem elektronik, dan konsep pertanggungjawaban pidana. Adapun sumber bahan hukum yang digunakan adalah sumber hukum primer dan sumber hukum sekunder. Sumber hukum primer berupa ketentuan hukum nasional yang berkaitan dengan penegakan hukum terkait kesehatan dan narkotika seperti beberapa diantaranya adalah Undang-Undang Nomor 1 Tahun 1946 tentang Peraturan Hukum Pidana (KUHP), Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), dan Putusan pengadilan yaitu : Putusan No. 272/Pid.Sus/2019/PN.Mtr. Sedangkan sumber hukum sekunder berupa buku-buku literatur, doktrin para ahli, jurnal hukum, berita, serta artikel hukum, yang relevan dengan topik penelitian ini.

Pengertian *Ransomware Cryptolcker*

Malicious Software atau lebih dikenal dengan istilah *Malware* adalah perangkat lunak komputer yang sengaja dirancang untuk merusak sistem, jaringan atau server tanpa sepengetahuan atau tanpa izin pemiliknya. Istilah Malware berasal dari kata *Malicious* yang berarti "berniat jahat" dan *software* yang berarti "perangkat lunak". Tujuan diciptakannya *Malware* sendiri adalah untuk mencuri data atau informasi dari perangkat elektronik yang terkena, serta dapat menyerang komputer dan mengakibatkan terganggunya sistem elektronik. Seiring berjalannya waktu, diciptakan pula beragam jenis malware dengan tujuan yang berbeda-beda. Berikut adalah jenis-jenis malware yang umum ditemukan dalam kehidupan sehari-hari:[5]

[5] Awan Setiawan & Erwin Yulianto, *Keamanan dalam Media Digital* (Informatika Bandung 2020).[60-62].

1. *Virus* : *Virus* merupakan sebuah program yang dapat menduplikasi dirinya sendiri untuk kemudian menyebar ke sebuah sistem jaringan dengan tujuan untuk melakukan pengerusakan komputer dan/atau jaringan komputer.
2. *Trojan* : *Trojan* merupakan program yang berpura-pura sebagai program yang tidak berbahaya padahal sejatinya merusak dan *trojan* akan masuk ke dalam sistem dan merusak sistem tersebut. *Trojan* dapat memberikan akses remote kepada penggunanya sehingga ketika akses tersebut terbuka, si pengguna *trojan* dapat melakukan akses terhadap komputer korban dari jarak jauh.
3. *Worm* : *Worm* merupakan program jahat yang masuk ke dalam komputer atau sistem jaringan komputer dengan tujuan untuk menyebarkan kode yang bersifat merusak dengan cara berpindah ke komputer lain pada jaringan yang sama secara otomatis dan tanpa bisa dicegah oleh pemilik komputer tersebut.
4. *Spyware* : *Spyware* bekerja dengan memonitor aktivitas korban tanpa diketahui oleh korban. Dengan hal demikian, pengguna *spyware* mendapatkan banyak informasi rahasia dari korban seperti login data, password, dan juga informasi kartu kredit.
5. *Ransomware* : *Ransomware* diciptakan untuk menghalangi korban mengakses sistem komputer miliknya dengan tujuan untuk memeras korban yang komputernya terinfeksi untuk memberikan tebusan sejumlah uang. *Ransomware* akan melakukan enkripsi terhadap file yang terdapat dalam suatu sistem komputer terkena.
6. *Rootkits* : *Rootkits* merupakan kumpulan perangkat lunak yang berfungsi untuk menyembunyikan (meng-*hide*) proses, file dan data sistem yang sedang berjalan pada *Operating System*. *Rootkits* memiliki kemampuan untuk mengubah pengaturan keamanan, mencuri informasi penting, dan dapat pula melakukan kontrol terhadap komputer korban untuk menyerang komputer lainnya.

Salah satu jenis malware yang sering digunakan dalam tindak pidana pemerasan adalah *ransomware*. *Ransomware*, sesuai dengan namanyam *ransom* = tebusan (dalam Bahasa Inggris), sehingga dapat dikatakan bahwa ransomware sengaja diciptakan sebagai media efektif tindak pidana pemerasan dengan objek serangannya adalah perangkat elektronik. *Ransomware* terdiri dari banyak jenis atau varian dengan jumlah mencapai ratusan atau bahkan ribuan dengan karakteristik yang berbeda-beda. Namun, secara umum ada dua jenis *ransomware* yaitu sebagai berikut:

- *Locker Ransomware* (Non-Enkripsi). *Locker ransomware* menginfeksi korban dengan menutup akses (*lock-screen*) ke dalam *resources* yang ada di komputernya. Setelah layar terkunci, pelaku akan meminta sejumlah tebusan kepada korban, agar hak akses korban dapat diberikan kembali.[6]

[6] '*Reveton Worm Ransomware'* (KnowBe4) <https://www.knowbe4.com/reveton-worm> dikunjungi pada 07-11-2020.

- *Ransomware Cryptolocker* (Enkripsi). *Ransomware Cryptolocker* atau *Crypto Ransomware* merupakan jenis yang paling sering digunakan oleh pelaku kejahatan siber. *Ransomware Cryptolocker* akan mengenkripsi dokumen elektronik pada komputer, lalu pelaku akan meinta uang tebusan untuk mendapatkan kunci dekripsinya.[7]

Modus Operandi Tindak Pidana Pemerasan dengan *Ransomware Cryptolocker*

Sebelum membahas mengenai proses-proses yang digunakan oleh pelaku dalam penyebaran *ransomware cryptolocker*, perlu dipaparkan terlebih dahulu mengenai apa itu modus operandi. M. Sholehuddin memaparkan modus operandi sendiri mempunyai pengertian sebagai sebagai metode operasional suatu perbuatan yang mungkin saja terdiri dari satu atau lebih kombinasi dari beberapa perbuatan.[8] Dalam hal ini modus operandi merupakan cara, metode, atau teknik yang digunakan oleh seseorang untuk melakukan suatu kejahatan, dalam hal ini adalah pelaku penyebaran *ransomware cryptolocker.* Berikut ini merupakan alur modus operandi tindak pidana pemerasan dalam kasus penyebaran *ransomware cryptolocker*:

1. *Ransomware cryptolocker* biasanya disebarkan oleh pelaku melalui situs web, server, atau dapat juga melalui surat elektronik (*e-mail*)[9] yang mengatasnamakan instansi resmi yang isinya meminta korban untuk membuka *file attachment* yang berisi *ransomware cryptolocker* yang pada umumnya berupa sebuah file Portable Executable (.exe).
2. Setelah *file attachment* tersebut ter-download, maka *ransomware cryptolocker* akan secara otomatis melakukan instalasi dan akan melakukan koneksi ke server milik pelaku yang kemudian akan mengirimkan kunci RSA[10] 2048 bit yang akan digunakan untuk melakukan enkripsi terhadap data pada komputer korban.

---

[7] Nur Fajar, 'Pengertian dan Jenis *Malware Ransomware*' (it-jurnal 2017) <*https://www.it-jurnal.com/pengertian-dan-jenis-malware-ransomware/*> dikunjungi pada 05-05-2020.

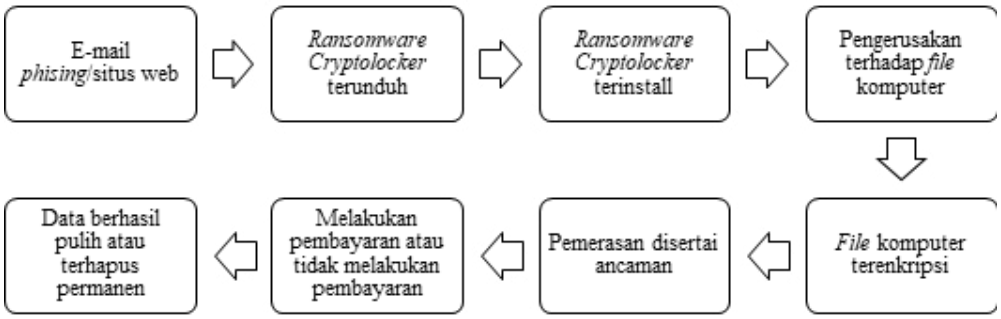
[8] M. Sholehuddin, *Tindak Pidana Perbankan* (PT. Raja Grafindo Persada 1997).[11].

[9] Ferdiansyah, 'Analisis Aktivitrtas dan Pola Jaringan Terhadap E*ternal Blue & Wannacry Ransomware*' (Juni 2018), Volume 4 Nomor 1 Jurnal Sistem Informasi.

[10] RSA, akronim dari Revest Shamir Adleman, adalah salah satu teknik kriptografi dimana kunci untuk melakukan enkripsi berbeda dengan kunci untuk melakukan dekripsi. Kunci untuk melakukan enkripsi disebut sebagai kunci publik, sedangkan kunci untuk melakukan dekripsi disebut sebagai kunci privat.

3. Setelah *ransomware cryptolocker* berhasil mengambil alih sebuah sistem, kemudian *ransomware cryptolocker* tersebut menggunakan kunci RSA bekerja dengan menyisipkan kode yang berupa angka ke dalam file-file dalam komputer korban yang tersusun dari kode binari, dimana apabila kode tersebut bertambah atau berkurang bahkan hanya satu angka, maka akan dapat mengakibatkan sistem komputer menjadi rusak atau terganggu.
4. Awalnya *ransomware cryptolocker* hanya akan mengunci sistem komputer korbannya dengan programnya yang akan menutupi seluruh layar komputer, dan komputer tersebut tidak akan bisa dibuka hingga *user* memasukan *password* yang tepat.
5. Setelah itu pada layar komputer korban akan informasi-informasi sebagai berikut:
   a. Terdapat pesan bahwa komputer telah terinfeksi *ransomware cryptolocker.*
   b. Jangka waktu data terhapus permanen.
   c. Jangka waktu pembayaran dinaikkan.
   d. Cara pembayaran untuk ditukarkan dengan kode dekripsi.
6. Korban harus memiliki kode dekripsi yang hanya diketahui oleh pembuat *ransomware cryptolocker* tersebut dengan cara melakukan pembayaran sejumlah uang untuk ditukarkan dengan kode dekripsi. Dalam hal ini, korban memiliki opsi untuk melakukan pembayaran atau tidak melakukan pembayaran.
7. Konsekuensi atas pilihan korban untuk melakukan pembayaran atau tidak melakukan pembayaran adalah dapat dilakukannya pemulihan data dengan kode dekripsi atau terhapusnya data secara permanen. Namun, terkadang korban tidak pula menerima kode dekripsi meskipun telah melakukan pembayaran sejumlah uang kepada pelaku.

Secara singkat, alur modus operandi tindak pidana pemerasan melalui sistem elektronik dalam kasus penyebaran *ransomware cryptolocker* diuraikan dalam bagan berikut:



Pengertian dan Unsur-Unsur Tindak Pidana Pemerasan dan Pengancaman

Sebelum membahas pengertian tindak pidana, maka perlu terlebih dahulu dijabarkan mengenai apa itu hukum pidana. Van Hamel memberikan definisi hukum pidana sebagai suatu aturan yang dianut suatu Negara sebagai kewajiban dalam menegakkan hukum dengan cara melarang sesuatu yang bertentangan dengan hukum (*onrecht*), dan barangsiapa yang melanggarnya akan dikenakan hukuman berupa nestapa.[11] Moeljatno mamandang hukum pidana sebagai bagian dari keseluruhan hukum yang berlaku di suatu negara, dengan dasar-dasar dan aturan-aturan untuk menentukan perbuatan mana yang tidak boleh dilakukan, dilarang, dan disertai ancaman atau sanksi berupa pidana tertentu bagi barangsiapa yang melanggarnya; kapan dan dalam kondisi seperti apa sanksi yang diancamkan dapat dijatuhkan kepada barangsiapa yang melaggar larangan-larangan tersebut; cara yang digunakan dalam hal pelaksanaan pengenaan sanksi apabila ada yang disangka telah melanggar larangan tersebut.[12] Berdasarkan pendapat beberapa sarjana yang telah diuraikan, hukum pidana adalah aturan-aturan mengenai perbuatan apakah yang dapat digolongkan sebagai tindak pidana.

Istilah tindak pidana berdasarkan kajian etimologis berasal dari kata '*strafbaar feit'*. Dalam KUHP memang tidak ditemui mengenai definisi dari '*strafbaar feit'* itu sendiri, namun berdasarkan pendapat sarjana, diantaranya adalah Simons yang memberikan arti dari kata '*stafbaar feit'* sebagai kelakuan (*handeling*) yang diancam dengan pidana, yang bersifat melawan hukum, yang berhubungan dengan kesalahan dan yang dilakukan oleh orang yang mampu bertanggung jawab.[13] Sedangkan Van Hamel menguraikan tindak pidana (*strafbaar feit*) sebagai perbuatan manusia yang diatur oleh undang-undang, melawan hukum, *strafwardig* (patut atau bernilai untuk dipidana), dan dapat dicela karena kesalahan (*en aan schuld te witjen*).[14] Sehingga, dapat diambil poin bahwa tindak pidana yaitu perbuatan yang dilarang oleh hukum

[11] Didik Endro Purwoleksono, *Hukum Pidana* (Airlangga University Press 2014).[4]. Selanjutnya disebut Didik Endro 2.

[12] *ibid*.[3].

[13] Moeljatno, *Asas-Asas Hukum Pidana* (Rineka Cipta Jakarta 2000).[56].

[14] Zainal Abidin Farid, *Hukum Pidana 1* (Sinar Grafika Jakarta 2007).[225].

suatu negara dan dapat diancam dengan sanksi pidana. Didik Endro Purwoleksono dalam bukunya menjabarkan unsur tindak pidana diuraikan sebagai berikut:[15]

1. Kelakuan dan akibat;
2. Hal ikhwal atau keadaan yang menyertai perbuatan;
3. Keadaan tambahan yang memberatkan pidana;
4. Unsur melawan hukum obyektif; dan
5. Unsur melawan hukum subyektif.

Berkembangnya modus operandi tindak pidana yang menggunakan sarana teknologi informasi dan telekomunikasi masa kini melatarbelakangi lahirnya hukum siber atau hukum telematika, hukum teknologi informasi (*law of information technology*), hukum dunia maya (*virtual world law*), hukum mayantara sebagai rezim hukum baru. Tindak pidana siber atau disebut juga sebagai *cyber crime* pada awalnya didefinisikan sebagai kejahatan komputer. Mengenai definisi kejahatan komputer sendiri, sampai sekarang para sarjana belum sependapat mengenai pengertian atau definisi dari kejahatan komputer. Namun, para sarjana pada waktu itu, pada umumnya lebih menerima pemakaian kata "*computer crime*" oleh karena dianggap lebih luas dan biasa dipergunakan dalam hubungan internasional.[16]

Pengertian Tindak Pidana dan Pertanggungjawaban Pidana

Setelah membahas mengenai tindak pidana, tentu tidak terlepas dari pertanggungjawaban pidananya yaitu dapat atau tidak dapat dipidananya pelaku tindak pidana.[17] Hukum pidana memberikan konsep pertanggungjawaban sebagai konsep sentral yang dikenal dengan ajaran kesalahan (*mens rea*), sehingga dalam hal pertanggungjawaban pidana menggunakan asas tiada pidana tanpa kesalahan (*geen straf zonder schuld*).[18] Dipidananya seseorang tidak cukup hanya bila seseorang tersebut telah melakukan perbuatan yang bertentangan dengan hukum atau bersifat melawan hukum, tetapi harus memenuhi syarat bahwa orang yang

[15] Didik Endro 2, *Op.Cit.*[44].
[16] Puslitbang Hukum dan Peradukan Mahkamah Agung RI 'Naskah Akademis Kejahatan Internet (*Cybercrimes*)', (2004).[4].
[17] Didik Endro 2, *Op.Cit.*[63].
[18] *ibid.*

melakukan perbuatan itu mempunyai kesalahan. Menurut Moeljatno, kesalahan adalah keadaan psikis yang tertentu pada orang yang melakukan perbuatan pidana dan adanya hubungan antara keadaan tersebut dengan perbuatan yang dilakukan yang sedemikian rupa, hingga orang itu dapat dicela karena melakukan perbuatan tadi.[19] Mengenai apakah seseorang dapat dimintai pertanggungjawaban pidana atau tidak, perlu diperhatikan hal-hal berikut:[20]

1. Melakukan tindak pidana. Apabila perbuatan, tindakan, kegiatan, atau aktivitas seseorang tersebut telah melanggar suatu aturan dalam suatu negara, maka orang tersebut telah melakukan tindak pidana.
2. Diatas umur tertentu dan mampu bertanggung jawab. Berdasarkan Pasal 45 Kitab Undang-Undang Hukum Pidana, batasan umur tertentu untuk dapat dimintai pertanggungjawaban pidana adalah minimal 16 (enam belas) tahun ketika melakukan suatu tindak pidana. Dalam UU SPPA, seseorang dikategorikan sebagai Anak adalah apabila ia telah berumur 12 (dua belas) tahun dan belum berumur 18 (delapan belas) tahun. Apabila mengacu pada peraturan perundang-undangan yang lebih baru, maka seseorang dapat dipertanggungjawabkan atas tindak pidana yang dilakukan apabila telah berumur 12 (dua belas) tahun. Selain berpatokan pada usia, seseorang dapat dimintai pertanggungjawaban apabila:
   a. Mampu menentukan niat, kehendak, dan rencana atas perbuatan yang akan dilakukan;
   b. Mengetahui atau menginsafi bahwa perbuatannya tersebut dipandang tidak patut oleh masyarakat;
   c. Mengetahui atau menginsafi arti, makna, hakikat dari perbuatan bahwa perbuatannya baik atau buruk.
3. Dengan kesengajaan atau kealpaan. Kesalahan (*schuld*) dalam perkara tindak pidana secara luas terdiri atas kesengajaan (*dolus*) dan kealpaan (*culpa*). Dalam *Memorie van Toelichting* (MvT) Menteri Kehakiman sewaktu pengajuan *Criminiel Wetboek* tahun 1881 (yang menjadi Kitab Undang-Undang Hukum

[19] Moeljatno, *Asas-Asas Hukum Pidana* (PT. Rineke Cipta 2002).[158].
[20] *ibid.*

Pidana Indonesia tahun 1915), dijelaskan bahwa "sengaja" diartikan sebagai "dengan sadar dari kehendak melakukan suatu kejahatan tertentu". Bentuk atau corak kesengajaan diklasifikasikan menjadi 3 (tiga) sebagai berikut:[21]

a. Kesengajaan sebagai maksud (*Dolus Als Oogmerk*): Bahwa pelaku tindak pidana memang memiliki tujuan atau kehendak atau bermaksud dan berkeinginan untuk melakukan suatu tindak pidana.
b. Kesengajaan sebagai kepastian (*Zekerheids Bewustzjin*): Bahwa pelaku memiliki kesadaran mengenai akibat yang menurut akal manusia pada umumnya pasti terjadi karena dilakukannya suatu perbuatan tindak pidana.
c. Kesengajaan sebagai kemungkinan (*Dolus Eventualis*) : Moeljatno menyebut kesengajaan sebagai kemungkinan sebagai teori apa boleh buat, yaitu bahwa pelaku tindak pidana mengetahui dan berkehendak untuk melakukan tindak pidana, serta ia tidak peduli siapa yang menjadi korbannya.

Kealpaan (*culpa*). Kealpaan sama halnya dengan kesengajaan yang merupakan salah satu bentuk kesalahan yang dilandasi oleh tidak hati-hati, dan tidak menduga-duga. Kealpaan dalam arti luas berarti kesalahan pada umumnya, sedangkan kealpaan dalam arti sempit adalah bentuk kesalahan yang berupa kealpaan.[22] Didik Endro memaknai kurang hati-hati dimana pelaku tidak mengadakan penelitian, kemahiran, atau usaha pencegahan yang nyata dalam keadaan-keadaan tertentu atau dalam caranya melakukan perbuatan.[23] Sedangkan unsur kurang menduga-duga terdiri dari 2 (dua) kemungkinan, yaitu:[24]

a. Kealpaan yang disadari (*Bewuste Culpa*): Dimaknai bahwa pelaku seharusnya menyadari adanya akibat atas tindakan yang dilakukan;
b. Kealpaan yang tidak disadari (*Onbewuste Culpa*): Dimaknai bahwa pada awalnya pelaku tindak pidana tidak menyadari adanya akibat atas perbuatan yang dilakukan, namun ternyata pada kenyataannya akibat atas perbuatan

[21] *Op.Cit*, Didik Endro 2.[70-71].
[22] Ernest Sengi, 'Konsep Culpa dalam Perkara Pidana Suatu Analisis Perbandingan Putusan Nomor 18/Pid.B/2017/PN.Tobelo' (Oktober 2019) Vol. 17 No. 2 Jurnal Era Hukum.[203].
[23] *ibid.*[74].
[24] *ibid.*[74-75].

tersebut malah terjadi.

4. Tidak ada alasan pemaaf. Alasan pemaaf yang diatur dalam KUHP diuraikan sebagai berikut:
   a. Pasal 44: Seseorang yang jiwanya cacat atau terganggu karena penyakit;
   b. Pasal 49 ayat (2): Melakukan pembelaan terpaksa karena ada serangan atau ancaman serangan terhadap kehormatan kesusilaan atau harta benda sendiri maupun orang lain;
   c. Pasal 51 ayar (2): Adanya itikad baik dalam melaksanakan perintah jabatan meskipun tanpa wewenang.

Kitab Undang-Undang Hukum Pidana (KUHP) yang saat ini berlaku di Indonesia adalah produk hukum Belanda yang diwariskan dan diberlakukan berdasarkan asas konkordansi di wilayah Hindia Belanda. KUHP mengatur aturan-aturan mengenai hukum pidana beserta sanksinya, yang dapat dikenakan terhadap barangsiapa melanggar aturan tersebut. Dalam hal ini KUHP tidak memberikan pengertian mengenai siapakah "Barangsiapa" itu. Namun, terdapat beberapa petunjuk mengenai siapa subyek hukum dalam KUHP. Dalam Pasal 55 KUHP tentang penyertaan dalam melakukan perbuatan pidana, yang dapat dimintai pertanggungjawaban pidana adalah pelaku yang menyuruhlakukan, dan yang turut serta melakukan perbuatan. Maka dapat dikatakan bahwa KUHP hanya mengenal subyek hukum natuurlijkepersoon. Sejalan dengan hal tersebut, Hoofgerechshof van Nedherland Indie dalam Arrest pada tanggal 5 Agustus 1925 terlebih dahulu menyatakan pendapatnya bahwa subyek hukum pidana dalam KUHP dilihat dalam sebagian besar ketentuan pidana yang diawali dengan kata "barangsiapa" yang merupakan terjemahan dari kata Belanda "*hij*" yang menunjukkan bahwa subyek hukum pidana dalam KUHP adalah *natuurlijkepersoon* (manusia).

Dengan berkembangnya zaman, muncul produk-produk hukum baru yang mengakui korporasi sebagai subyek hukum yang mampu bertanggungjawab, diantaranya adalah UU ITE. Dalam UU ITE menguraikan secara jelas mengenai subyek hukum dalam Pasal 1 angka 21 yang menerangkan bahwa orang adalah orang perseorangan maupun badan hukum. Sehingga yang dapat dimintai

pertanggungjawaban pidana berdasarkan UU ITE adalah orang perseorangan dan badan hukum.

Pertanggungjawaban Pidana Tindak Pidana Pemerasan dengan Modus Operandi *Ransomware Cryptolocker*

Pelaku tindak pidana pemerasan dengan modus operandi ransomware cryptolocker dapat dipertanggungjawabkan karena melanggar Pasal 27 ayat (4) jo. Pasal 45 ayat (4), Pasal 32 ayat (1) jo. Pasal 48 ayat (1) dan Pasal 33 jo. Pasal 49 UU ITE. Subjek hukum pada Kitab Undang-Undang Hukum Pidana (KUHP) yang mengatur aturan-aturan mengenai hukum pidana beserta sanksinya, yang dapat dikenakan terhadap barangsiapa melanggar aturan tersebut. Dalam hal ini KUHP tidak memberikan pengertian mengenai siapakah "Barangsiapa" itu. Namun, terdapat beberapa petunjuk mengenai siapa subyek hukum dalam KUHP. Dalam Pasal 55 KUHP tentang penyertaan dalam melakukan perbuatan pidana, yang dapat dimintai pertanggungjawaban pidana adalah pelaku yang menyuruhlakukan, dan yang turut serta melakukan perbuatan. Maka dapat dikatakan bahwa KUHP hanya mengenal subyek hukum *natuurlijkepersoon*. Sejalan dengan hal tersebut, *Hoofgerechshof van Nedherland Indie* dalam *Arrest* pada tanggal 5 Agustus 1925 terlebih dahulu menyatakan pendapatnya bahwa subyek hukum pidana dalam KUHP dilihat dalam sebagian besar ketentuan pidana yang diawali dengan kata "barangsiapa" yang merupakan terjemahan dari kata Belanda "*hij*" yang menunjukkan bahwa subyek hukum pidana dalam KUHP adalah *natuurlijkepersoon* (manusia). Dengan berkembangnya zaman, muncul produk-produk hukum baru yang mengakui korporasi sebagai subyek hukum yang mampu bertanggungjawab, diantaranya adalah UU ITE. Dalam UU ITE menguraikan secara jelas mengenai subyek hukum dalam Pasal 1 angka 21 yang menerangkan bahwa orang adalah orang perseorangan maupun badan hukum. Sehingga yang dapat dimintai pertanggungjawaban pidana berdasarkan UU ITE adalah orang perseorangan dan badan hukum.

Pasal 27 ayat (4) Jo. Pasal 45 ayat (4) UU ITE

Pengaturan mengenai tindak pidana pemerasan melalui sistem elektronik diatur dalam Pasal 27 ayat (4) UU ITE yang berbunyi "Setiap Orang dengan sengaja dan tanpa hak Mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 1.000.000.000,00 (satu miliar rupiah)." Dengan pembuktian unsur-unsur sebagai berikut:

1. Dengan sengaja. Dilihat dari tujuan penciptaan *ransomware cryptolocker* yang digunakan sebagai sarana melakukan pemerasan dengan cara mengenkripsi data pada komputer korban, maka pelaku memiliki unsur kesalahan berupa kesengajaan sebagai maksud. Maka perbuatan pelaku memenuhi unsur subyektif Pasal 27 ayat (4) UU ITE yaitu "dengan sengaja".
2. Tanpa hak. Unsur "tanpa hak" merupakan salah satu arti dari melawan hukum atau *wedderechtelijk*. Atas dasar itu, makna atau arti "tanpa hak" dapat dimaknai sebagai perbuatan yang bertentangan dengan hukum objektif, perbuatan yang bertentangan dengan hak orang lain, perbuatan yang dilakukan tanpa hak yang ada pada diri seseorang, atau perbuatan yang dilakukan tanpa kewenangan.
3. Mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik. Mengenai unsur ini pada penjelasan Pasal 27 ayat (1) UU ITE telah dijabarkan definisi sebagai berikut:
    a. Mendistribusikan : Adalah mengirimkan dan/atau menyebarkan Informasi Elektronik dan/atau menyebarkan Informasi Elektronik dan/atau Dokumen Elektronik kepada banyak Orang atau berbagai pihak melalui Sistem Elektronik.
    b. Mentransimikan : Adalah mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang ditujukan kepada satu pihak lain melalui Sistem Elektronik.
    c. Membuat dapat diakses : Adalah semua perbuatan lain selain

mendistribusikan dan mentransmisikan melalui Sistem Elektronik yang menyebabkan Informasi Elektronik dan/atau Dokumen Elektronik dapat diketahui pihak lain atau publik.

Oleh karena unsur mendistribusikan dan/atau mentransmisikan dan/ atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik dapat dimaknai kumulatif atau alternatif terlihat dari penggunaan kata 'dan/atau', maka terbuktinya salah satu dari ketiga frasa tersebut sudah memenuhi unsur ini. Namun harus dilihat terlebih dahulu bagaimana cara pelaku melakukan penyebaran *ransomware cryptolocker* apakah dengan cata mentransmisikan, mendistribusikan, atau membuat dapat diakses.

4. Yang memiliki muatan pemerasan dan/atau pengancaman. Mengenai unsur "pemerasan" sebagaimana dalam Penjelasan Pasal 27 ayat (4) UU ITE, harus mengacu pada tindak pidana pemerasan dalam Pasal 368 ayat (1) KUHP, dengan pemenuhan unsur sebagai berikut:
   a. Untuk menguntungkan diri sendiri atau orang lain: bahwa pelaku menyebarkan *ransomware cryptolocker* dengan maksud untuk mendapatkan keuntungan berupa uang tebusan yang dibayarkan oleh korban. Sebagaimana telah diuraikan pada sub-subab sebelumnya, unsur ini tidak perlu dibuktikan benar-benar terjadi, melainkan cukup dibuktikan bahwa pelaku memiliki niat untuk menguntungkan diri sendiri atau orang lain. Pelaku penyebaran *ransomware cryptolocker* tentunya menghendaki adanya keuntungan dari perbuatannya oleh karena *ransomware cryptolocker* memang dari awal penciptaan sudah ditujukan untuk melakukan pemerasan terhadap korban. Maka dengan ini, unsur ini telah terpenuhi.
   b. Secara melawan hukum. Oleh karena pemerasan disertai ancaman merupakan salah satu perbuatan yang dilarang oleh hukum sebagaimana diatur dalam Pasal 368 ayat (1) KUHP, maka pelaku yang melakukan pemerasan menggunakan *ransomware cryptolocker* adalah melawan hukum.
   c. Memaksa. Pelaku penyebaran *ransomware cryptolocker* melakukan

pemaksaan berupa adanya tekanan yang ada pada layar komputer korban yang berisi yang jangka waktu jumlah uang tebusan akan dinaikkan dan jangka waktu data pada komputer korban akan terhapus. Pelaku memanfaatkan ketidakberdayaan korban yang takut kehilangan data-datanya sehingga memaksa korban untuk melakukan pembayaran sejumlah uang sebagaimana diinginkan oleh pelaku.

d. Kekerasan atau Ancaman Kekerasan. Adanya enkripsi terhadap data korban dapat mengakibatkan kerugian materiil maupun immateriil berupa tidak bekerjanya sistem pada komputer korban. Selain itu pelaku menghendaki adanya pembayaran sejumlah uang sebagaimana yang ditampilkan pada layar komputer korban dengan jangka waktu yang telah ditentukan sehingga korban terpaksa melakukan pembayaran untuk mengembalikan data-datanya. Salahuddien Manggalanny dalam putusan Nomor 272/Pid. Sus/2019/PN.Mtr memberikan pendapat bahwa ancaman itu dapat berupa pemerasan serta telah menimbulkan gangguan dan/atau kerugian yang nyata bagi orang lain serta keluarganya maupun berupa kekhawatiran akan keselamatan jiwa dan harta benda. Sehingga dapat disimpulkan bahwa ancaman dapat berupa pemerasan yang telah menimbulkan gangguan dan/ atau kerugian materiil dan immateriil. Unsur ini mensyaratkan bahwa dengan adanya kekerasan atau ancaman kekerasan ini, pemilik barang menyerahkan barang tersebut kepada pelaku. Sepanjang dapat dibuktikan adanya kerugian baik materiil maupun immateriil yang dialami oleh korban, maka unsur ini terpenuhi.

e. Untuk memberikan atau menyerahkan sesuatu barang. Penyerahan suatu barang dianggap telah ada apabila barang yang diminta oleh pelaku tersebut telah dilepaskan dari kekuasaan orang yang diperas, tanpa melihat apakah barang tersebut sudah benar - benar dikuasai oleh orang yang memeras atau belum. Pemerasan dianggap telah terjadi, apabila korban yang komputernya terinfeksi *ransomware cryptolocker* itu telah menyerahkan tebusan sejumlah uang yang dimaksudkan pelaku sebagai akibat pemerasan

terhadap dirinya. Sepanjang tujuan pelaku yaitu mendapatkan keuntungan berupa sejumlah uang dari korban tersebut telah tercapai, maka unsur ini telah terpenuhi.

Pasal 32 ayat (1) Jo. Pasal 48 ayat (1) UU ITE

Pengaturan mengenai proses cara kerja *ransomware cryptolocker* diuraikan dalam Pasal 32 ayat (1) Jo. Pasal 48 ayat (1) UU ITE yang berbunyi "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik Publik dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp. 2.000.000.000,00 (dua miliar rupiah)". Dengan penjabaran unsur-unsur sebagai berikut:

1. Dengan Sengaja. Dilihat dari tujuan penciptaan *ransomware cryptolocker* yang bekerja dengan cara menyisipkan kode binari melalui teknik enkripsi ke dalam file yang ada pada komputer korban sehingga menyebabkan komputer tersebut rusak, maka pelaku memenuhi unsur "dengan sengaja" dengan corak kesalahan berupa kesengajaan sebagai maksud.
2. Tanpa hak atau melawan hukum. Oleh karena mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik merupakan salah satu perbuatan yang dilarang oleh hukum sebagaimana diatur dalam Pasal 32 ayat (1) jo. Pasal 48 ayat (1) UU ITE, maka pelaku yang melakukan perbuatan tersebut menggunakan *ransomware cryptolocker* adalah melawan hukum.
3. Mengubah. Mengubah menurut KBBI memiliki arti menjadikan lain dari semula. Ransomware cryptolocker bekerja dengan cara mengubah susunan kode binari yaitu penambahan dalam file pada komputer korban menggunakan teknik enkripsi.
4. Menambah. Menambah menurut KBBI memiliki arti menjadikan (membubuhkan dan sebagainya) supaya lebih banyak (besar, hebat, dan sebagainya) . Penyisipan kode binari ke dalam file korban mengakibatkan adanya penambahan susunan file pada komputer korban.
5. Mengurangi. Mengurangi menurut KBBI memiliki arti mengambil (memotong) sebagian; menjadikan berkurang; menurunkan; menjadikan kurang. Ransomware cryptolocker dapat melakukan penghapusan data pada komputer korban secara permanen baik secara sekaligus, maupun secara bertahap apabila korban enggan melakukan pembayaran uang tebusan kepada pelaku untuk

ditukarkan dengan kode dekripsi.

6. Melakukan transmisi. Melakukan transmisi menurut KBBI memiliki arti melakukan pengiriman (penerusan) pesan dan sebagainya dari seseorang kepada orang (benda) lain; penularan, penyebaran, penjangkitan penyakit; bagian kendaraan bermotor yang memindahkan atau meneruskan tenaga dari mesin ke as belakang; persneling . Dalam penyebarannya ransomware cryptolocker dapat disebarkan oleh pelaku melalui situs web, server, maupun e-mail yang megatasnamakan instansi resmi.
7. Merusak. Merusak menurut KBBI memiliki arti sudah tidak sempurna (baik, utuh) lagi; luka-luka; bercalar-calar; calar balar; busuk; tidak dapat berjalan lagi (tentang mobil, mesin); tidak beraturan lagi (tentang bahasa, adat); tidak utuh lagi (perkawinan); terganggu (ingatannya); hancur; binasa; tidak baik . Adanya penyisipan kode binari ke dalam file pada komputer korban menggunakna teknik enkripsi tersebut mengakibatkan rusaknya sistem pada komputer korban sehingga komputer dan data yang ada di dalamnya tidak dalat digunakan sebagaimana mestinya.
8. Menghilangkan. Menghilangkan menurut KBBI memiliki arti melenyapkan; membuat supaya hilang; menghapus(kan); membersihkan; membuang supaya tidak ada lagi; meniadakan . Ransomware cryptolocker melakukan penghapusan data pada komputer korban secara permanen baik secara sekaligus, maupun secara bertahap apabila korban enggan melakukan pembayaran uang tebusan kepada pelaku untuk ditukarkan dengan kode dekripsi.
9. Memindahkan. Memindahkan menurut KBBI memiliki arti menempatkan ke tempat lain; membawa (ber)pindah; menyuruh (menggerakkan dan sebagainya) berpindah ke tempat lain; menerjemahkan; menularkan; menjangkitkan.
10. Menyembunyikan. Menyembunyikan menurut KBBI memiliki arti menyimpan (menutup dan sebagainya) supaya jangan (tidak) terlihat; sengaja tidak memperlihatkan (memberitahukan dan sebagainya); merahasiakan. Enkripsi terhadap data korban akibat serangan *ransomware cryptolocker* menyebabkan data pada komputer korban tidak dapat dibuka karena disandera atau disembunyikan.
11. Informasi Elektronik. Pasal 1 angka 1 UU ITE menjabarkan definisi mengenai informasi elektronik yaitu satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *Electronic Data Intercharge* (EDI), surat elektronik (*electronic mail*), telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.
12. Dokumen Elektronik. Pasal 1 angka 4 memberikan definisi mengenai dokumen elektronik yaitu setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang memiliki makna atau arti atau dapat

dipahami oleh orang yang mampu memahaminya.

Unsur Informasi Elektronik dan/atau Dokumen Elektronik bersifat alternatif terlihat dari penggunaan kata 'dan/atau'. Berdasarkan cara kerjanya, *ransomware cryptolocker* menggunakan kunci RSA yang disisipkan atau ditambahkan ke dalam dokumen elektronik pada komputer korban yang terdiri dari kode-kode binari yang berakibat terenkripsinya dokumen elektronik pada komputer terinfeksi sehingga tidak dapat dibuka. Maka, dalam hal ini unsur Tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik telah terpenuhi. Sehingga Pasal 32 ayat (1) Jo. Pasal 48 ayat (1) UU ITE ini dapat dikenakan kepada pelaku apabila perbuatan pelaku tersebut sudah sampai pada penyisipan kode binari ke dalam file-file pada komputer korban.

Pasal 33 jo. Pasal 49 UU ITE

Ransomware cryptolocker yang menginfeksi suatu komputer atau jaringan komputer mengakibatkan terganggungnya suatu sistem komputer, maka terhadap pelaku dapat dikenakan Pasal 33 Jo. Pasal 49 UU ITE yang berbunyi: "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp 10.000.000.000,00 (sepuluh miliar rupiah)." Dengan penjabaran unsur sebagai berikut:

1. Dengan Sengaja. Pelaku penyebaran *ransomware cryptolocker* bertanggungjawab atas terganggunya sistem elektronik orang lain yang diakibatkan oleh *ransomware cryptolocker* yang ia sebarkan, dimana *ransomware cryptolocker* ini mengakibatkan data yang ada pada komputer terinfeksi menjadi terenkripsi sehingga tidak dapat dibuka dan digunakan sebagaimana mestinya. Hal ini tentunya dikehendaki oleh pelaku penyebaran *ransomware cryptolocker* yang mengilhami cara kerja *ransomware cryptolocker*

yang mengenkripsi data pada komputer sehingga sistem elektronik menjadi terganggu dan tidak dapat digunakan sebagaimana mestinya, sehingga dalam hal ini pelaku memenuhi unsur "dengan sengaja" dengan corak kesalahan berupa kesengajaan sebagai maksud.

2. Tanpa hak atau melawan hukum. Oleh karena melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya merupakan salah satu perbuatan yang dilarang oleh hukum sebagaimana diatur dalam Pasal 33 jo. Pasal 49 UU ITE, maka pelaku yang melakukan perbuatan tersebut menggunakan *ransomware cryptolocker* adalah melawan hukum.
3. Melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.

Bahwa dilihat dari akibat yang ditimbulkan setelah *ransomware cryptolocker* berhasil melakukan enkripsi terhadap data-data pada komputer korban, yaitu tidak dapat digunakannya komputer beserta data yang ada pada komputer tersebut sebagaimana mestinya, maka unsur "tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya" telah terpenuhi. Sehingga Pasal 33 Jo. Pasal 49 UU ITE ini dapat dikenakan kepada pelaku apabila perbuatan pelaku telah menimbulkan akibat berupa terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.

Berdasarkan uraian di atas, maka pelaku penyebaran *ransomware cryptolocker* baik merupakan orang perseorangan maupun badan hukum dapat dipertanggungjawabkan karena melanggar Pasal 27 ayat (4) jo. Pasal 45 ayat (4), Pasal 32 ayat (1) jo. Pasal 48 ayat (1) dan Pasal 33 jo. Pasal 49 Undang-Undang Nomor Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sepanjang telah timbul akibat sebagaimana diuraikan dalam pasal-pasal tersebut di atas.

Perbarengan Perbuatan

Perbuatan pelaku penyebaran *ransomware cryptolocker* terdiri dari beberapa perbuatan sebagaimana dalam Pasal 27 ayat (4) Jo. Pasal 45 ayat (4) UU ITE dan Pasal 32 ayat (1) Jo. Pasal 48 ayat (1) UU ITE dan Pasal 33 Jo. Pasal 49 UU ITE, maka perlu digolongkan apakah perbuatan tersebut termasuk perbarengan perbuatan atau bukan. *Samenloop/concursus* dapat diterjemahkan dengan Gabungan atau Perbarengan. Perbarengan adalah terjadinya dua atau lebih tindak pidana oleh satu orang dimana tindak pidana yang pertama kali belum dijatuhi pidana, atau antara tindak pidana yang pertama dengan tindak pidana yang berikutnya belum dibatasi oleh suatu putusan hakim.[25] Istilah gabungan melakukan tindak pidana dalam KUHP diistilahkan dengan concursus atau samenloop, yaitu orang yang melakukan beberapa peristiwa pidana.[26] Ditinjau dari segi bentuknya, perbarengan perbuatan dibedakan menjadi:[27]

a. *Concursus Idealis*: Suatu perbuatan dikatakan sebagai *concursus idealis* apabila perbuatan atau kegiatan atau tindakan atau aktivitas tersebut melanggar beberapa undang-undang atau aturan atau beberapa pasal. *Concursus idealis* direpresentasikan dalam Pasal 63 KUHP dengan sistem pemidanaan *absorbtie* yaitu kepada pelaku hanya dikenakan terhadap tindak pidana yang diancam dengan pidana paling berat atau dikenakan aturan khusus.
b. *Concursus Realis*: Suatu tindak pidana merupakan *concursus realis* apabila ada seorang pelaku melakukan tindak pidana yang berdiri sendiri, dan semua tindak pidana diadili sekaligus. *Concursus realis* diatur dalam Pasal 65 KUHP dengan penjatuhan pidana tidak boleh lebih dari maksimum pidana terberat ditambah 1/3.
c. Perbuatan Berlanjut: Pebuatan berlanjut merupakan bentuk *concursus realis* yang khusus. Berdasarkan Pasal 64 KUHP, perbuatan berlanjut ada apabila seseorang melakukan beberapa perbuatan yang merupakan kejahatan atau

[25] Mahsur Ali, *Dasar*-dasar *Hukum Pidana* (Sinar Grafika 2011).[134].
[26] E. Utrecht, *Hukum Pidana II* (Pustaka Tinta Mas 1994).[137].
[27] Didik Endro 2, *Op.Cit.*[81].

pelanggaran yang berdiri sendiri, dan ada hubungannya sedemikian rupa sehingga harus dipandang sebagai satu perbuatan berlanjut.

Sebagaimana bentuk-bentuk perbarengan perbuatan dan modus operandi tindak pidana pemerasan dalam kasus penyebaran *ransomware cryptolocker* yang melanggar beberapa pasal yaitu Pasal 27 ayat (4) jo. Pasal 45 ayat (4), Pasal 32 ayat (1) jo. Pasal 48 ayat (1) dan Pasal 33 jo. Pasal 49 UU ITE, maka perbuatan tersebut merupakan *concursus idealis* oleh karena serangkaian perbuatan tersebut melanggar beberapa pasal dalam suatu aturan, sehingga apabila menggunakan sistem pemidanaan *absorbtie* maka dikenakan ancaman pidana terberat yaitu dalam Pasal 49 UU ITE dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp. 10.000.000.000,- (sepuluh miliar rupiah).

Cara Menghindari Serangan Ransomware Cryptolocker

Serangan ransomware tergolong berbahaya dan merugikan, maka perlu adanya langkah preventif untuk menghindari komputer terkena serangan ransomware, sebagai berikut:[28]

1. Pastikan komputer mendapat patch terbaru dan pembaruan terbaru melalui aktivasi fitur "Windows Update", dan usahakan untuk melakukan back-up atau pencadangan terhadap data penting sebelum melakukan pembaruan sistem untuk mencegah kerusakan, error, atau kehilangan data pada saat melakukan instalasi pembaruan sistem;
2. Lakukan scanning komputer menggunakan Anti-Virus terbaru secara berkala untuk membantu sistem komputer mengetahui keberadaan aplikasi tidak dikenal atau mempunyai signature malware;
3. Waspada pada setiap link yang diterima, terutama yang berasal dari e-mail spam atau e-mail phising;
4. Selalu aktifkan Windows Firewall yang berguna untuk membuat sebuah aturan/rules di dalam Windows Firewall sehingga program dapat melakukan pembaruan secara otomatis;
5. Aktifkan fitur "safe browsing" pada aplikasi (browser) yang digunakan, contohnya fitur safe browsing yang disediakan oleh Google untuk mendeteksi situs-situs yang tidak aman dan memiliki kemungkinan disusupi oleh malware. Apabila suatu situs diindikasi tidak aman, maka Google akan memberikan

[28] 'Penanganan dan Pencegahan Insiden Ransomware' (govcsirt) <https://govcsirt.bssn.go.id/penanganan-dan-pencegahan-insiden-ransomware/> dikunjungi pada 24-11-2020.

peringatan apabila situs yang hendak dikunjungi adalah situs berbahaya;
6. Lakukan back-up data penting secara berkala menggunakan penyimpanan eksternal atau media penyimpanan online seperti Google Drive dan iCloud.

Kesimpulan

Pertama, *ransomware cryptolocker* merupakan salah satu jenis perangkat lunak berbahaya (*malicious software*) yang ditujukan sebagai sarana melakukan pemerasan dengan tujuan untuk mendapatkan sejumlah uang dengan cara membuat gangguan atau pengerusakan terhadap data pada komputer korban dengan janji untuk mengembalikan kondisi data pada komputer setelah korban melakukan pembayaran sejumlah uang. *Ransomware cryptolocker* melakukan serangan terhadap sistem yang tidak terproteksi dari serangan *malware*. Kedua, modus operandi tindak pidana pemerasan dalam kasus penyebaran *ransomware cryptolocker* dimulai dari didistribusikannya atau ditransmisikannya aplikasi *ransomware cryptolocker* melalui e-mail, situs web, atau server yang di dalamnya sengaja disusupi *ransomware cryptolocker*. Setelah terunduh dan terinstal pada komputer korban, selanjutnya *ransomware cryptolocker* tersebut akan melakukan pengerusakan terhadap data pada komputer korban dengan cara menyisipkan kode-kode binari ke dalam data dan mengakibatkan terenkripsinya data-data pada komputer korban sehingga tidak dapat digunakan sebagaimana mestinya. Setelah itu, pada layar komputer korban akan muncul pesan pemerasan disertai ancaman yang pada pokoknya mengarahkan korban untuk membayar uang tebusan dengan jumlah tertentu kepada pelaku untuk ditukarkan dengan kode dekripsi yang akan mengembalikan keadaan data dan komputer korban seperti semula. Pelaku juga memanfaatkan pengancaman bahwa apabila dalam jangka waktu tertentu korban tidak melakukan pembayaran, maka data pada komputer korban akan secara otomatis terhapus permanen dan tidak dapat dipulihkan. Ketiga, pelaku dalam penyebaran *ransomware cryptolocker* memang menghendaki adanya enkripsi terhadap data-data yang diakibatkan oleh *ransomware cryptolocker* tersebut, dan apabila pemerasan tersebut berhasil, maka pelaku akan mendapatkan sejumlah uang dari hasil pembayaran yang dilakukan oleh korban. Maka berdasarkan hal tersebut pelaku dapat dimintai pertanggungjawaban karena

melanggar Pasal 27 ayat (4) jo. Pasal 45 ayat (4), Pasal 32 ayat (1) jo. Pasal 48 ayat (1) dan Pasal 33 jo. Pasal 49 Undang-Undang Nomor Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dengan ancaman pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp. 10.000.000.000,- (sepuluh miliar rupiah).

Daftar Bacaan

Buku

Awan Setiawan & Erwin Yulianto, *Keamanan dalam Media Digital* (Informatika Bandung 2020).

Didik Endro Purwoleksono, *Hukum Pidana* (Airlangga University Press 2014).

Didik Endro Purwoleksono, *Hukum Pidana Untaian Pemikiran* (Airlangga University Press 2019).

E. Utrecht, *Hukum Pidana II* (Pustaka Tinta Mas 1994).

M. Sholehuddin, *Tindak Pidana Perbankan* (PT. Raja Grafindo Persada 1997).

Mahsur Ali, *Dasar-dasar Hukum Pidana* (Sinar Grafika 2011).

Moeljatno, *Asas-Asas Hukum Pidana* (Rineka Cipta Jakarta 2000).

Moeljatno, *Asas-Asas Hukum Pidana* (PT. Rineke Cipta 2002).

Zainal Abidin Farid, *Hukum Pidana 1* (Sinar Grafika Jakarta 2007).

Jurnal

Ernest Sengi, 'Konsep Culpa dalam Perkara Pidana Suatu Analisis Perbandingan Putusan Nomor 18/Pid.B/2017/PN.Tobelo' (Oktober 2019) Jurnal Era Hukum.

Ferdiansyah, 'Analisis Aktivitas dan Pola Jaringan Terhadap *Eternal Blue* & *Wannacry Ransomware*' (Juni 2018) Jurnal Sistem Informasi.

Artikel

Puslitbang Hukum dan Peradukan Mahkamah Agung RI 'Naskah Akademis Kejahatan Internet (*Cybercrimes*)' (2004).

Laman

'Penanganan dan Pencegahan Insiden Ransomware' (govcsirt) <https://govcsirt.bssn.go.id/penanganan-dan-pencegahan-insiden-ransomware/>, dikunjungi pada 24-11-2020.

Ari Juliano Gema, 'Cybercrime : Sebuah Fenomena di Dunia Maya' (hukumonline 2000) <www.hukumonline.com>, dikunjungi pada pada 05-05-2020.

Fauzan Jamaludin, 'Begini Dampak dari Serangan Malware WannaCrypt' (merdeka 2017) <www.merdeka.com>, dikunjungi pada 05-05-2020.

KnowBe4*, 'Reveton Worm Ransomware'* (KnowBe4) <https://www.knowbe4.com/reveton-worm> dikunjungi pada 07-11-2020.

Nur Fajar*,* 'Pengertian dan Jenis Malware Ransomware' (it-jurnal 2017) <https://www.it-jurnal.com/pengertian-dan-jenis-malware-ransomware/> dikunjungi pada 05-05-2020.

Perundang-undangan

Undang-Undang Nomor 1 Tahun 1946 tentang Peraturan Hukum Pidana (Lembaran Negara Republik Indonesia Tahun 1958 Nomor 127).

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Tambahan Lembaran Negara Republik Indonesia Nomor 4843).

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Nomor 5952).

--halaman ini sengaja dibiarkan kosong--