PERLINDUNGAN HUKUM BAGI KORBAN SERANGAN RANSOMWARE

Oleh:
Desyanti Suka Asih K.Tus[1]
E-mail : desyanti@uhnsugriwa.ac.id
Dosen Prodi Hukum Hindu Fakultas Dharma Duta
Universitas Hindu Negeri I Gusti Bagus Sugriwa Denpasar

Abstract

Data is an important part of the need in today's Information Technology era. The data of every human individual in the world has a high level of sensitivity for anyone. Data that is currently developing both offline and online data, requires a certain level of security in its access. Good data security techniques are needed in ensuring the confidentiality of a data including from attacks of several types of malware viruses and ransomware.

Types of malware viruses and ransomware work with the concept of damaging, stealing and locking data with various purposes, one of which is to make a profit. Ransomware works by locking certain files that are targeted and encrypted so that the data is inaccessible. In the end, if you want to access the stored data, users are required to contact the contact of the creator of the ransoware by paying a certain amount of money in decrypting the locked data. Ransomware can be categorized as cyber extortion. Article 27 paragraph 4 of the ITE Law provides arrangements on the dissemination of information that has extortion content whose provisions are regulated in the Criminal Code. Ransomware meets the elements of the criminal act of extortion as stipulated in the provisions of Article 368 paragraph (1) of the Criminal Code. The perpetrator commits extortion coupled with acidification by closing the victim's access to his data. The government has made legal protection efforts for victims of ransomware among others through the arrangements contained in Article 27 Paragraph (4) of the ITE Law. As well as the application of criminal sanctions of confinement and fines for perpetrators of ransomware crimes. Protection of cyber space users can also be done by individuals (individuals) by building regulations in cyberspace and being vigilant in using the internet. In an effort to provide legal protection for ransomware victims, cooperation is needed between the government as a lawmaker and users (victims of ransomware) cyber space. More advanced and unconventional regulations are critical in dealing with cybercrime. Because all forms of cybercrime cannot be touched by the rule of law.

***Keywords**: Legal Protection, Victims, Ransomware*

Abstrak

Data merupakan bagian penting dari kebutuhan di era Teknologi Informasi saat ini. Data tiap individu manusia di dunia ini memiliki tingkat sensitifitas yang cukup tinggi bagi siapapun. Data yang saat ini berkembang baik data offline maupun online, memerlukan tingkat pengamanan tertentu dalam pengaksesannya. Teknik pengamanan data yang baik diperlukan dalam menjamin kerahasiaan suatu data termasuk dari serangan beberapa jenis virus malware maupun Ransomware.

Jenis virus malware maupun Ransomware bekerja dengan konsep merusak, mencuri hingga mengunci data dengan berbagai macam tujuan salah satunya untuk

mencari keuntungan. Ransomware bekerja dengan mengunci file-file tertentu yang diincar dan dienkripsi sehingga data tersebut tidak dapat diakses. Pada akhirnya, jika ingin mengakses data yang disimpan tersebut, pengguna diharuskan menghubungi kontak dari pembuat ransoware tersebut dengan membayar pada sejumlah uang dalam melakukan decrypt dari data yang terkunci tersebut. Ransomware dapat dikatagorikan sebagai pemerasan cyber. Pasal 27 ayat 4 UU ITE memberikan pengaturan tentang penyebaran informasi yang memiliki konten pemerasan yang ketentuan pemidanaanya diatur dalam KUHP. Ransomware memenuhi unsur-unsur tindak pidana pemerasan seperti yang diatur dalam ketentuan Pasal 368 ayat (1) KUHP. Pelaku melakukan pemerasan dibarengi dengan pengancaman dengan menutup akses korban atas data miliknya. Pemerintah telah melakukan upaya perlindungan hukum bagi korban Ransomware antar lain melalui pengaturan yang terdapat dalam Pasal 27 Ayat (4) UU ITE. Serta penerapan sanksi pidana kurungan dan denda bagi pelaku kejahatan Ransomware. Perlindungan terhadap pengguna ruang siber juga dapat dilakukan oleh perseorangan (pribadi) dengan membangun pertahana di ruang siber serta waspada dalam mempergunakan internet. Dalam upaya memberikan perlindungan hukum bagi korban Ransomware diperlukan adanya kerjasama antara pemerintah sebagai pembuat UU dengan pengguna (korban Ransomware) ruang siber. Pengaturan yang lebih maju dan tidak konvensional sangat penting dalam menangani tindak kejahatan siber. Karena segala bentuk kejahatan siber tidak dapat disentuh oleh aturan hukum konvensional.

Kata Kunci: Perlindungan hukum, Korban, Ransomware

PENDAHULUAN

Kemajuan teknologi merupakan awal dari kehadiran internet. Internet yang menjadi pembuka jalan bagi segala bentuk kemudahan di era digitalisasi saat ini. Kehadiran internet dengan segala manfaat baik yang dapat diperoleh penggunanya, tidak dapat dipungkiri memiliki sisi negatif. Bentuk kontribusi yang diperoleh dari penggunaan internet seperti peningkatan kesejahteraan, kemajuan dan peradaban manusia. Namun, di sisi lain internet juga merupakan wadah bagi kejahatan baru yang ada pada dunia hukum saat ini yang dikenal dengan istilah kejahatan siber atau cybercrime (Talinusa, 2015, p. 162).

Saat ini telah lahir suatu rezim hukum baru yang dikenal dengan hukum siber atau hukum telematika. Hukum siber atau cyber law, secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan teknologi informasi dan komunikasi. Permasalahan hukum yang seringkali dihadapi adalah ketika terkait dengan penyampaian informasi, komunikasi, dan/atau transaksi secara elektronik, khususnya dalam hal pembuktian dan hal yang terkait dengan perbuatan hukum yang dilaksanakan melalui sistem elektronik (Ramopolii, 2014, p. 6).

5 (lima) serangan siber yang sering terjadi antara lain:

Ransomware

Penyerang menginstal perangkat lunak untuk mematikan sistem bisnis atau membuat bisnis menjadi offline. Tebusan harus dibayar sebelum 'Ransomware' dihapus atau dinonaktifkan. Dalam variasinya, penyerang mengancam membuat data

korup sehingga tidak dapat digunakan jika uang tebusan tidak dibayarkan.

Pencurian data Penyerang mencuri data pelanggan dan menjualnya ke oknum lain yang kemudian melakukan pencurian identitas. Atau, mereka meminta pembayaran untuk mengembalikan data yang dicuri tadi.

Penyamaran sebagai CEO atau petinggi perusahaan lain

Pengintaian online atas data publik memungkinkan pelaku kejahatan menyamar sebagai CEO atau direktur keuangan. Pelaku kemudian dapat meminta perubahan detil pembayaran pada faktur dan mengalihkan pembayaran ke akun mereka sendiri.

Penambangan bitcoin

Bentuk kejahatan siber yang relatif baru tetapi semakin banyak terjadi. Penyerang memasang perangkat lunak pada sistem TI (Teknologi Informasi) perusahaan dan membajak prosesor untuk menghasilkan mata uang kripto. Sistem bisnis segera melambat atau berhenti.

Pencurian Intelectual Property

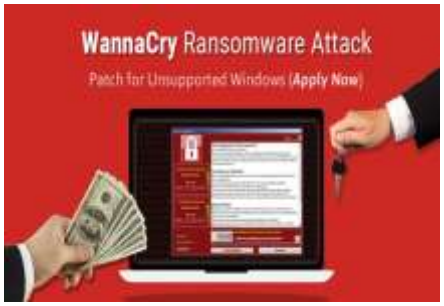
Spionase tidak terbatas pada aksi mata-mata di suatu negara. Spionase industri adalah ancaman nyata, dengan perusahaan ambisius yang menargetkan sistem perusahaan saingan untuk mencuri Intelectual Property (Roy, 2019).

Dari kelima bentuk kejahatan siber tersebut, kejahatan dengan bentuk Ransomware semakin meningkat. Laporan Dimension Data menunjukkan tahun 2017 terjadi peningkatan mengkhawatirkan terkait kejahatan Ransomware dan serangan siber. Pada tahun 2017, terjadi serangan Ransomware dengan kenaikan yang tinggi sekitar 350 persen, mewakili tujuh persen dari total serangan malware di seluruh dunia. Angka ini naik dari satu persen pada tahun 2016 dan diperkirakan akan berlanjut menyusul popularitas kampanye penanggulangan siber yang tengah berlangsung. Tercatat, 20 persen serangan itu menargetkan sektor bisnis dan layanan profesional, terutama di wilayah Eropa, Timur Tengah, dan Afrika (EMEA). Informasi tersebut berdasarkan laporan dari Dimension Data yang bertajuk "Executive Guide to the NTT Security 2018 Global Threat Intelligence Report". Dalam laporan tersebut, selama 2017 terjadi 150 juta serangan atau 40 ribu sampai 50 ribu serangan per hari (Alamsyah, 2018).

Kejahatan Ransomware tidak hanya menyerang negara maju seperti Amerika dan Uni Eropa. Indonesia sendiri menjadi negara yang rawan akan serangan ransomeware khususnya yang menyerang data milik pemerintah, BUMN maupun swasta. Pada tahun 2017, Rumah Sakit Kanker (RSK) Dharmais Jakarta menjadi sasaran malware pengunci akses ke komputer dan membuat seluruh data terenskripsi sejak Sabtu (13/5) pekan lalu. Akibatnya, pelayanan administrasi di rumah sakit terganggu dan harus dilakukan secara manual sehingga memperpanjang proses registrasi pasien (Putra, 2017).

Cara kerjasanya, serangan Ransomware ini terjadi di mana peretas mengirim email kepada calon korban yang berisi link (tautan) tertentu. Saat link itu di-klik, program jahat itu otomatis bekerja mengenkripsi folder, file, hingga drive di komputer. Sekalipun pengguna atau korban membersihkan komputernya dari virus, tetap saja file, folder atau drive yang terenkripsi tidak bisa digunakan kembali tanpa kunci yang digenggam peretas. Kepala Badan Intelijen Negera (BIN) Jenderal Budi Gunawan mengatakan serangan bermula dari bocornya tool yang

digunakan oleh National Security Agency (NSA), yakni sebuah kode pemprograman (exploit) yang memanfaatkan kelemahan sistem dari Microsoft Windows. Exploit tersebut digunakan sebagai satu cara menyebarkan virus secara cepat melalui software perusak yang bernama wannacry ke seluruh penjuru dunia (Putra, 2017).



Ilustrasi virus Wannacry Ransomware menyerang perangkat lunak komputer di berbagai negara – Istimewa (Ulun, 2019)

Kekhawatiran akan meningkatkan kejahatan Ransomware adalah sangat beralasan. Kejahatan ini dapat menimbulkan kerugian yang besar bagi korbannya. Contohnya serangan Ransomware ke kota Baltimore, Amerika Serikat. Pelaku kejahatan Ransomware meminta tebusan sekitar US$100 ribu. Tebusan tersebut tidak dibayar, sehingga menyebabkan kerugian sampai US$18 juta (Wibowo, 2019).

Kehadiran UU No. 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang No.11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE) diharapkan dapat menjadi pelengkap Kitab Undang-Undang Hukum Pidana (KUHP) dan solusi bagi tindak kejahatan yang terjadi di ruang siber. Dalam kasus yang tertangkapnya pelaku Ransomware di Sleman , DIY, terhadap pelaku dikenai ketentuan Pasal 49 Jo Pasal 33 dan Pasal 48 ayat (1) Jo Pasal 32 ayat (1) dan Pasal 45 ayat (4) Jo Pasal 27 ayat (4) dengan ancaman hukuman pidana 10 tahun penjara. Terhadap pelaku, keberadaan KUHP dan UU ITE adalah pedoman dalam memberikan penegakan hukum atas kejahatan yang dilakukan. Namun bagaimana perlindungan hukum bagi korban kejahatan Ransomware masih menjadi pertanyaan. Kerugian yang diderita korban tidak sedikit. Keenganan korban untuk membayar tebusan, kurang SDM yang profesional dan mahalnya biaya yang harus dikeluarkan untuk membangun pertahanan di ruang siber, kecerobohan pengguna internet yang memudahkan pelaku kejahatan siber dalam melancarkan aksinya, serta keadaan dimana korban tidak menyadari datanya dicuri menjadikan perlindungan terhadap korban kejahatan Ransomware menjadi semakin penting.

METODE

Pendekatan penelitian ini adalah pendekatan yuridis normative. Dalam penelitian hukum normative, maka jenis data yang digunakan adalah data sekunder atau disebut dengan bahan hukum. Bahan hukum terdiri dari bahan hukum primer dan bahan hukum sekunder. Teknik pengumpulan data yang digunakan dalam penelitian ini adalah melalui teknik studi kepustakaan. Teknik pengolahan data adalah kegiatan merapikan data hasil dari pengumpulan data sehingga siap dipakai untuk dianalisis secara kualitatif. Setelah melalui proses pengolahan yang selektif, kemudian data tersebut dijabarkan secara deskriptif analisis, yaitu dijabarkan dalam bentuk uraian–uraian yang nantinya dapat menjawab permasalahan yang dibahas.

PEMBAHASAN

1. Ransomware sebagai bentuk kejahatan di ruang siber

Ransomware merupakan jenis malware yang menyerang pengguna (*user*) dalam mengakses atau membatasi akses mereka ke dalam sistem maupun file, dengan mengunci layar atau mengenkripsi *file* sampai tuntutannya terpenuhi maupun dibayarkan (Everett, 2016, pp. 8-12). *Ransomware* memerlukan kunci enkripsi yang cukup sulit untuk memecahkan kode enkripsi tersebut karena tersimpan secara *remote* di *server* yang sudah diatur (Akbanoy, 2019, p. 15).

Ransomware termasuk dalam kualifikasi tindakan pemerasan dan/atau pengancaman sesuai dengan ketentuan Pasal 27 ayat (4) UU ITE. Tindakan ini dalam Pasal 368 ayat (1) KUHP disebutkan: "Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, memaksa seorang dengan kekerasan atau ancaman kekerasan untuk memberikan barang sesuatu, yang seluruhnya atau sebagian adalah kepunyaan orang itu atau orang lain, atau supaya membuat hutang maupun menghapuskan piutang, diancam karena pemerasan, dengan pidana penjara paling lama sembilan tahun."

Unsur-unsur yang ada dalam pasal ini adalah sebagai berikut:

a. Memaksa orang lain;
b. Untuk memberikan barang yang sama sekali atau sebagian termasuk kepunyaan orang itu sendiri atau kepunyaan orang lain, atau membuat utang atau menghapuskan piutang;
c. Dengan maksud hendak menguntungkan diri sendiri atau orang lain dengan melawan hak;
d. Memaksanya dengan memakai kekerasan atau ancaman kekerasan (Soesilo, 1988, p. 286).

Definisi kejahatan *Ransomware* memenuhi unsur-unsur Pasal 368 Ayat (1) KUHP tersebut diatas. Walaupun terjadi di ruang siber, tidak kasat mata, tindakan ini tetap dianggap nyata dan digolongkan kedalam tindakan pemerasan yang didalamnya terdapat unsur paksaan dan ancaman kekerasan. Paksaan dan ancaman yang di lakukan kepada korban *Ransomware,* bukan tindakan fisik secara nyata, tetapi dilakukan di ruang siber dengan mengunci data dan meminta uang tebusan melalui *email* korban. Apabila uang tebusan tidak dibayarkan, maka selamanya korban tidak dapat mengakses datanya. Kekerasan yang diderita korban bukan kekerasa fisik, tetapi kekerasan secara psikologis. Pelaku menekan korban untuk memenuhi tebusan yang diminta sebagai syarat untuk dapat membuka data korban yang telah terkunci.

2. Cara Kerja Ransomware

Cara kerja *Ransomware* dikutip dari carbonblack.com

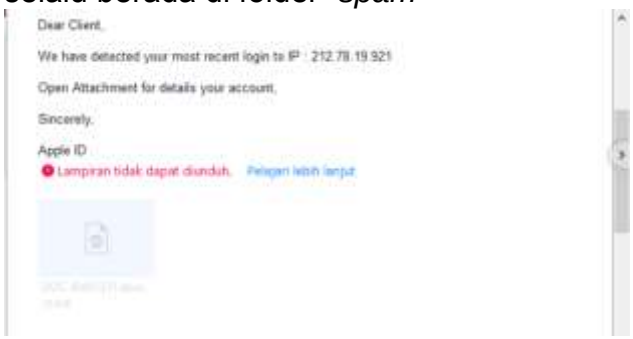
a. Pengguna menerima sebuah email yang seakan-akan seperti dari alamat email yang terkadang meyakinkan.
b. Link membuka sebuah window browser dan mengarahkan pengguna ke sebuah website yang tampak valid.
c. Saat membuka halaman, *web server* yang menyimpan *file* tertentu yang berbahaya serta mulai berkomunikasi dengan mesin (komputer) korban serta menyimpan *link* yang akan mengarahkan ke tempat *Ransomware* berada.
d. Ketika sebuah versi kerentanan terkonfirmasi, *exploit kit* mencoba untuk memanfaatkan kerentanan tersebut.
e. Dari tahap ini, biner tersebut melakukan proses

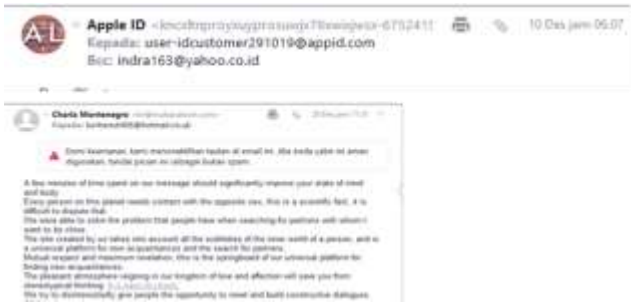
pengembangbiakan, termasuk vssadmin.exe (salinan bayangan), untuk menghapus bayangan yang sudah ada di mesin korban dan membuat yang baru untuk disembunyikan.

f. Setelah mengenkripsi *file* korban, *malware* mengirimkan kunci enkripsi
g. Kemudian *server* mengirimkan pesan ke korban.

Penanganan *Ransomware* saat ini cukup rumit dilakukan dalam mengatasi *Ransomware* yang sudah banyak beredar saat ini. Rumitnya ini dikarenakan kemudahan dalam membuat setiap jenis *Ransomware*. Kemudahan dalam mendapatkan *Ransomware* ini membuka peluang bagi penyerang dalam mencari target yang diinginkan.

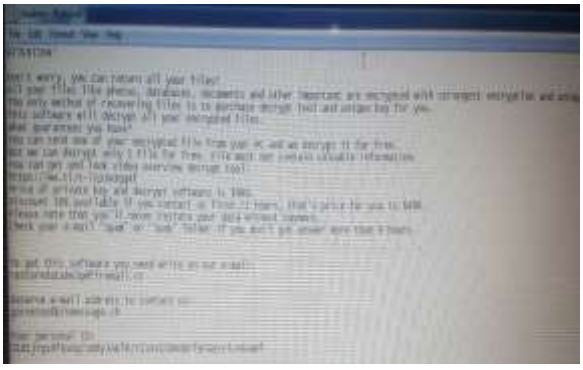
Contoh serangan *Ransomware* yang selalu berada di folder "*spam*"





Contoh serangan *Ransomware* yang menyerang file dokumen dengan ekstensi .lokf, yang sampai saat ini belum tersedia metode decryptnya

Contoh bentuk surat ancaman yang meminta tebusan dari *Ransomware*



3. Perlindungan Hukum Bagi Korban Serangan *Ransomware*

Peningkatan kemanan siber belum menjadi jaminan mutlak bagi masyarakat, pemerintah dan kalangan bisnis mendapatkan perlindungan dalam memanfaatkan ruang siber. Perlindungan bagi pengguna ruang siber masih harus menjadi prioritas. Pemerintah telah membentuk peraturan perundang-undangan dalam upaya memberikan perlindungan bagi pengguna ruang siber, akan tetapi memecahkan masalah di ruang siber bukan persoalan mudah, karena kejahatan di ruang siber dilakukan oleh sebuah komunikats (Maskun, 2013, p. 25). Salah satu cara untuk memberikan rasa aman kepada pengguna internet dengan adanya perkembangan teknologi adalah dengan mengetahui bagaimana tata cara perlindungan hukum yang tepat kepada pengguna internet sehingga pengguna internet dapat merasakan manfaatnya ketika berselancar di dunia maya ataupun melakukan transaksi *online* di dunia maya (Kusumawardani, 2019, p. 18). Mengingat saat ini informasi telah menjadi komoditi maka upaya untuk melindungi aset tersebut sangat

diperlukan. Salah satu upaya perlindungan adalah melalui hukum pidana, baik dengan bersaranakan penal maupun non penal (Arief, 2006).

Pasal 27 UU ITE mengatur perbuatan yang dilarang dilakukan di ruang siber.

(1) 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 yang melanggar kesusilaan.
(2) 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 perjudian.
(3) 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 penghinaan dan/atau pencemaran nama baik.
(4) 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.

Kejahatan *Ransomware* diatur dalam ketentuan Pasal 27 Ayat (4) “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”. *Ransomware* dikategorikan sebagai tindak pidana pemerasan. Kualifikasi perbuatan yang tergolong pemerasan dan/atau pengancaman dalam Pasal 368 ayat (1) KUHP.

Perumusan ketentuan Pasal 27 ayat (4) yang menggabungkan tindak pidana pemerasan dan/atau pengancaman dalam satu ketentuan padahal dalam KUHP tindak pidana pemerasan diatur dalam Pasal 368 sedangkan pengancaman diatur dalam Pasal 369 KUHP (Talinusa, 2015, p. 165).

Terhadap Informasi yang bersifat melawan hukum disiarkan atau disebarluaskan di internet hal tersebut tidak berarti sebagai hak asasi manusia dalam berkomunikasi, karena tidak dengan sendirinya internet dikategorikan hanya sebagai medium komunikasi khusus antar para pihak melainkan ia juga merupakan medium komunikasi global yang dapat diakses oleh semua pihak. Oleh karena itu dapat dikatakan bahwa internet bukanlah suatu media yang bebas hukum, ia tidak terlepas dari keberlakuan hukum terhadap para penciptanya, penggunanya dan pihak-pihak yang menyelenggarakannya sebagai infrastruktur publik dalam berkomunikasi dan berinformasi, baik dalam lingkup nasional maupun global (Makarim, 2003, pp. 50-51).

Berkaitan dengan perumusan perbuatan dalam ketentuan Pasal 27 ayat (1), ayat (2), ayat (3), dan ayat (4) dalam ketentuan Pasal 45 ayat (1) yang dinyatakan bahwa perbuatan-perbuatan tersebut diancam dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 1.000.000.000,- (satu miliar rupiah). Perumusan sanksi pidana demikian tidak tepat dan tidak proporsional karena sanksi pidananya menyamaratakan terhadap perbuatan-perbuatan dengan kualifikasi dan kualitas tindak pidana yang berbeda. Pasal 27 mengatur beberapa tindak

pidana yang berbeda baik dari luas tindak pidana yang diancamkan terhadap tindak pidana tersebut berbeda-beda. Dalam Pasal 45 ayat (1) sanksi pidananya disamaratakan untuk kesepakatan tindak pidana tersebut. Sanksi pidana terhadap suatu tindak pidana tidak boleh lebih buruk dari kejahatannya (Suhariyanto, 2013, p. 174). Keberadaan sanksi pidana yang diatur dalam UU ITE belum menjadi jaminan bahwa kejahatan *Ransomware* tidak akan terjadi lagi. Terlebih pengenaan sanksi ini bukan jaminan sebagai bentuk pelindungan hukum yang lebih pasti bagi pengguna ruang siber. Pidana penjara dan sanksi pidana bagi pelaku dirasa tidak sebanding dengan kerugian yang diderita oleh korban *Ransomware*.

Penegakan hukum terhadap pelaku tindak pidana mayantara merupakan suatu upaya perlindungan terhadap pengguna *cyberspace* (internet) dari para cracker yang menggunakan media internet dalam melakukan aksi kejahatannya. Meskipun belum terbentuknya hukum khusus siber (*cyber law*) di Indonesia yang berorientasi kepada kepentingan korban tapi diperlukan adanya upaya hukum melindungi kepentingan penduduk dunia maya (netizen) berikut privasinya dengan menggunakan hukum yang sudah ada sebelumnya meliputi perundang-undangan, yurisprudensi maupun konvensi-konvensi Internasional yang sudah diratifikasi oleh Indonesia (Tanthawi, 2014, p. 38).

Penanggulangan kejahatan tindak pidana internet dapat dilakukan dengan berbagai upaya diantaranya penanggulangan secara preemtif, preventif dan represif. Upaya preemtif dilakukan dengan meratifikasi konvensi-konvensi *cybercrime* internasional kedalam sistem perundang-undangan Indonesia. Penanggulangan *cybercrime* secara preventif dapat dilakukan dengan meningkatkan pengamanan, meningkatkan daya guna perangkat komputer, keahlian serta kedisplinan dalam menggunakan perangkat saat berselancar di dunia maya. Kegiatan tersebut dapat berupa tindakan-tindakan yang bisa dilakukan baik secara perorangan (pribadi), kebijakan nasional maupun global. Sedangkan Penanggulangan *cybercrime* secara represif dilakukan dengan menangkap para pelaku tindak pidana untuk diproses sesuai dengan hukum yang berorentasi pada kepentingan korban melalui pemberian restitusi, kompensasi maupun asistensi yang menjadi tanggung jawab pelaku dengan Negara sebagai fasilitatornya (Tanthawi, 2014, pp. 38-39).

Berdasarkan uarian diatas, keberadaan UU ITE dalam ketentuan Pasal 27 Ayat (4) secara tegas telah mengatur perbuatan yang dilarang dilakukan di ruang siber dan *Ransomware* adalah salah satu tindakan yang dilarang. *Ransomware* yang dikualifikasikan sebagai tindak pidana pemerasan yang dilakukan di ruang siber telah memenuhi unsur-unsur Pasal 368 ayat (1) KUHP yang dipidana dengan pemerasan. Keberadaan UU ITE dan KUHP adalah salah satu upaya negara dalam memberikan perlindungan kepada pengguna ruang siber. Ketentuan yang diatur dalam UU ITE dan KUHP adalah bentuk dari perlindungan hukum yang diberikan negara dalam bentuk pelindungan represif. Dengan memberikan sanksi pidana kepada pelaku, negara sebagai fasilitator, berusaha untuk memberikan keadilan kepada korban *Ransomware*. Walaupun pengaturan dalam UU ITE

dan KUHP masih harus direvisi dan diperbaharui agar dapat memberikan bentuk perlindungan hukum yang lebih maksimal. Hal ini karena kejahatan di ruang siber, khususnya *Runsomware* terus berkembang. Tidak berhenti pada jenis WannaCry, Locky, Petya, Not Petya. Kejahatan *Ransomware* yang biasanya dilakukan oleh kelompok dan terorganisir, menyebabkan pelaku dapat bergerak lebih cepat dari kapasitas negara membentuk peraturan perundang-undangan dalam memberikan perlindungan bagi pengguna ruang siber. Karena sifatnya yang terjadi di ruang siber tidak mengenal batas ruang dan waktu, kejahatan siber tidak dapat disentuh oleh aturan-aturan hukum konvensional. Maka diperlukan terobosan-terobosan yang lebih baik dalam menanggulangi sekaligus memberikan perlindungan hukum bagi korban.

Bentuk perlindungan yang dapat dipergunakan sebagai upaya pencegahan dapat dilakukan secara preventif. Bentuk perlindungan ini dapat dilakukan oleh perorangan secara pribadi maupun dengan kerjasama nasional dan global. Pengguna ruang siber dapat meninggkatkan pengamana siber dengan membangun pertahanan siber bagi data-data pribadi saat menggunakan internet. Kesadaran serta pengetahuan tentang penggunaan ruang siber juga harus ditingkatkan, sehingga pengguna akan paham keuntungan serta bahaya ketika mempergunakan internet. Negara dapat memfasilitasi dengan menyediakan akses internet yang lebih amat bagi pengguna. Karena dalam upaya membangun pertahanan di ruang siber, dibutuhkan biaya yang besar serta SDM yang professional.

Bentuk perlindungan lain yang dapat dilakukan Negara adalah meratifikasi konvensi-konvensi *cybercrime. Convention on Cyber Crime* 2001 yang digagas oleh Uni Eropa adalah konvensi yang sedang mendapat perhatian. Konvensi ini pada awalnya digagas oleh Uni Eropa yang kemudian dapat diratifikasi oleh diakses oleh negara manapun di dunia yang memiliki komitmen dalam upaya mengatasi kejahatan *cyber*. Keaktifan negara dalam meratifikasi konvensi-konvensi *cybercrime* adalah salah satu upaya untuk selalu *update* dalam menghadapi bentuk-bentuk baru kejahatan *cyber*. Hal ini juga menjadi salah satu upaya untuk bersama-sama dengan negara di dunia memerangi kejahatan siber dan membangun pertahanan global.

PENUTUP

Ransomware adalah salah satu bentuk kejahatan siber yang di kualitifkasikan sebagai tindak pidana pemerasan. Hal ini karena *Ransomware* adalah tindakan dimana merupakan jenis malware dan digunakan oleh penyerang (*attacker*) untuk menginfeksi sistem pengguna (*user*) dengan tujuan akhir meminta tebusan dari pengguna. Kualifikasi meminta tebusan membuat tindakan *Ransomware* termasuk kedalam tindak pidana pemerasan dengan ancaman. Dimana bentuk ancamanya adalah pengguna akan kehilangan akses terhadap data-data yang dimilikinya di ruang siber. Pemerintah telah berupaya memberikan perlindungan hukum kepada korban *Ransomware*, yaitu dengan mengatur dalam UU ITE yang menjadi aturan khusus dari KUHP dalam tindak pidana pemerasan di ruang siber. Bentuk-bentuk perlindungan yang diberikan antara lain berupa pengenaan sanksi kepada pelaku. Pengenaan sanksi ini adalah upaya memberikan keadilan kepada korban *Ransomware*. Walaupun dalam

UU ITE pengenaan sanski untuk semua tindak pidana siber yang diatur dalam Pasal 27 sama. Dimana pada kenyataan penerapan sanksi yang sama bagi setiap pelanggaran terhadap ketentuan Pasal 27 tidak bijaksana karena tingkat kerugian serta tingkat kejahatan yang dilakukan akan berbeda-beda. Bentuk perlindungan lain adalah dengan membangun pertahanan di ruang siber. Serta secara aktif melakukan revisi terhadap UU ITE sehingga dapat memberikan perlidunga hukum yang lebih baik bagi korban *Ransomware.*

DAFTAR PUSTAKA

Akbanoy, M. (2019). WannaCry Ransomware: Analysis of Infection, Persistance, Recovery Prevention and Propagation Mechanisms. *Journal of Telecommunications and Information Technology, Vol.1*, 15.

Arief, B. N. (2006). *Tindak PIdana Mayantara: Perkembangan Kajian Cybercrime di Indonesia.* Jakarta: PT. Grafindo Persada.

Everett, C. (2016). Ransomware: To pay or not to pay? *Copm. Fraud & Secure, Vol.4*, 8-12.

Kusumawardani, Q. D. (2019, Maret). Perlindungan Hukum Bagi Pengguna Internet Terhadap Konten Web Umpan Klik Di media Online. *Jurnal Penelitian Hukum DE JURE, Vol.19*(No.1), 18.

Ramopolii, C. B. (2014, Mei-Juli). Wewenang Khusus Penyidik Untuk Melakukan Penyidikan Tindak Pidana Teknologi Informasi. *Lex Crimen, Vo.III*(No.3), 6.

Soesilo, R. (1988). *Kitab Undang-Undang Hukum Pidana (KUHP) Serta Komentar-Komentarnya Lengkap Pasal Demi Pasal.* Bogor: Politeia.

Suhariyanto, B. (2013). *Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi Pengaturan dan Celah Hukumnya.* Jakarta: PT. Raja Grafindo Persada.

Talinusa, S. C. (2015, Agustus). Tindak Pidana Pemerasan Dan/Atau Pengancaman Melalui Sarana Internet Menurut Undang-Undang Nomor 11 Tahun 2008. *Lex Crimen, Vol.IV*(No.6), 162.

Tanthawi, e. a. (2014). Perlindungan Korban Tindak Pidana CyberCrime Dalam Sistem Hukum Pidana Indonesia. *Jurnal Ilmu Hukum Pascasarjana Universitas Syiah Kuala, Vol.2*(No.1), 38.

Kitab Undang-Undang Hukum Pidana

Undang-Undang Republik Indonesia Nomor 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843).

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016

Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952).

Alamsyah, E. S. (2018, Juni Jumat). *Republika*. Retrieved Desember Jumat, 2019, from republika.co.id: https://www.republika.co.id/berita/trendtek/internet/18/06/08/p9zfaw349-kejahatan-Ransomware-kian-meningkat-apa-penyebabnya

Makarim, E. (2003). *Kompilasi Hukum Telematika.* Jakarta: PT. Raja Grafindo.

Maskun. (2013). *Kejahatan CYber Crime Suatu Pengantar.* Jakarta: Kencana.

Putra, N. N. (2017, Mei Senin). *Hukum Online*. Retrieved Desember Jumat, 2019, from hukumonline.com: https://www.hukumonline.com/berita/baca/lt59199334233e5/ransomware--momentum-lawyer-pekerjakan-pakar-it-di-firma-hukum

Roy. (2019, Agustus Senin). *CNBC Indonesia*. Retrieved Desember Jumat, 2019, from CNBD Indonesia: https://www.cnbcindonesia.com/tech/20190826192258-37-94875/awas-5-jenis-kejahatan-siber-ini-sedang-mengintaimu.

Ulun, M. (2019, Oktober Jumat). *kabar24*. Retrieved Desember Jumat, 2019, from kabar24.bisnis.com: https://kabar24.bisnis.com/read/20191025/16/1163365/penyebar-ransomware-dan-pemeras-korbannya-ditangkap-di-sleman

Wibowo, S. (2019, Desember Rabu). *CNN Indonesia*. Retrieved Desember Jumat, 2019, from cnnindonesia.com: https://www.cnnindonesia.com/teknologi/20191203160104-186-453782/ransomware-merajalela-lagi