Das Sollen: Jurnal Kajian Kontemporer Hukum dan Masyarakat (2023) 1:2, 1-25
ISSN 1111-1111 | DOI: 10.11111/dassollen.xxxxxxx
Diterbitkan oleh FORIKAMI (Forum Riset Ilmiah Kajian Masyarakat Indonesia)
Tersedia online Pada Bulan Mei 2023.

Perlidungan Hukum Bagi Korban Ransomware Wannacry Tindak Pidana Ransomware

Gilang Ramadhan

Fakultas Hukum, Universitas Pasundan, gilangfoust677@gmail.com

ABSTRACT: In this age of globalisation, technological advancement is the main factor that has an impact on cases in the cyber world, one example is data. Data is an important part in the era of Information Technology which has a high level of sensitivity for anyone. Data for now or personal data or group data requires a good level of data security needed to ensure the confidentiality of data including from the attack of several types of malware and Ransomware viruses. Malware and Ransomware are types of viruses that work with the concept of damaging, stealing and locking data for profit. The data locked by Ransomware is data that is encrypted and targeted so that the data cannot be accessed again, users affected by a Ransomware attack are required to contact the contact of the Ransomware creator by paying a certain amount of money to decrypt the locked data. Ransomware attacks have fulfilled the requirements of the criminal offence of extortion as stipulated in Article 368 paragraph (1) of the Criminal Code. As a perpetrator who has committed extortion which is also regulated in Article 27 paragraph 4 of the ITE Law, coupled with the threat of closing access to the victim's data itself. With the efforts of the government, it has made a legal protection for Ransomware victims, among others, through the regulation in Article 27 Paragraph (4) of the ITE Law. As well as the application of confinement sanctions and fines for perpetrators of Ransomware crime attacks. With the legal protection of cyberspace users, it can be done by individuals (private) by building defences in cyber attacks. In an effort to provide legal protection for Ransomware victims, a form of cooperation between the government in making laws with Ransomware victims is needed to deal with cybercrime in the future. Therefore, all forms of cybercrime cannot be touched by conventional laws.

KEYWORDS: : Legal Protection, Victims, Ransomware

ABSTRAK: Di zaman globalisasi sekarang ini Kemajuan Teknologi menjadi faktor utama yang memiliki dampak dari kasus kasus di dunia siber, salah satu contohnya Data. Data merupakan bagian penting di era Teknologi Informasi yang memiliki tingkat sesnsitifitas yang cukup tinggi bagi siapapun. Data untuk saat ini maupun itu data pribadi atau data kelompok memerlukan tingkat pengamanan data yang baik diperlukan dalam menjamin kerahasiaan suatu data termasuk dari serangan beberapa jenis virus malware maupun Ransomware. Malware maupun Ransomware adalah jenis virus yang bekerja dengan konsep merusak, mencuri hingga mengunci data yang bertujuan untuk mencari keuntungan. Data-data yang dikunci oleh Ransomware adalah data yang dienksripsi dan diincar sehingga data tersebut tidak dapat diakses kembali, pengguna yang terkena serangan Ransomware diharuskan menghubungi kontak dari pembuat Ransomware tersebut dengan membayar pada

sejumlah uang dalam melakukan decrypt dari data yang terkunci tersebut. Serangan Ransomware telah memenuhi untur Tindak Pidana pemerasan yang diatur dalam ketentuan Pasal 368 ayat (1) KUHP. Sebagai pelaku yang telah melakukan pemeraran yang diatur juga dalam Pasal 27 ayat 4 UU ITE dibarengi dengan adanya pengancaman dengan menutup akses data korban itu sendiri. Dengan adanya upaya dari pemerintah telah melakukan sebuah perlindungan hukum bagi korban Ransomware antara lain melalui pengaturan dalam Pasal 27 Ayat (4) UU ITE. Serta adanya penerapan sanksi kurungan dan denda bagi pelaku serangan kejahatan Ransomware. Dengan adanya perlindungan hukum terhadap pengguna ruang siber dapat dilakukan oleh perorangan (pribadi) dengan cara membangun pertahanan dalam serangan siber. Dalam upaya memberikan perlindungan hukum bagi korban Ransomware diperlukannya bentuk kerjasama antara pemerintah dalam pembuatan UU dengan korban Ransomware untuk menagani tindak kejahatan siber kedepannya. Oleh karena itu segala bentuk kejahatan siber tidak dapat disentuh oleh aturan hukum konvensional.

KATA KUNCI: Perlindungan Hukum, Korban, Ransomware

I. PENDAHULUAN

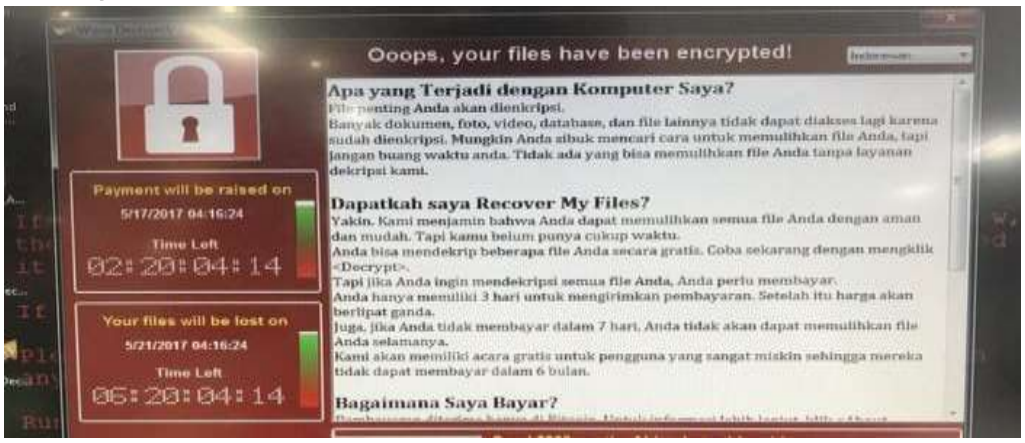
Ransomware telah menjadi salah satu ancaman siber yang paling signifikan dalam beberapa tahun terakhir. Artikel ini memberikan gambaran latar belakang tentang Ransomware, termasuk asal usulnya, perkembangan, dan dampaknya pada korban serangan. Kami menjelaskan bagaimana Ransomware menyebar, teknik yang digunakan oleh pelaku, dan motif di balik serangan ini. Selain itu, kami membahas perlindungan hukum yang tersedia bagi korban serangan Ransomware dan tantangan yang dihadapi dalam menangani ancaman ini. Data adalah kebutuhan paling penting di era Teknologi Informasi saat ini. Data yang semakin berkembang saat ini, baik secara luring maupun daring, membutuhkan tingkat keamanan tertentu saat diakses. Sebagian besar populasi di Indonesia memiliki setidaknya memiliki satu akun media sosial, media sosial memainkan peran penting dalam masyarakat saat ini. Selebriti, bisnis, dan bahkan politisi menggunakan media sosial untuk berinteraksi dengan masyarakat umum untuk berbagi proyek atau produk yang akan datang.

Dengan data yang diambil dari Sumber DataIndonesia.id yang diakses pada tanggal 11 Juni 2023 jumlah besar sebanyak 167 juta orang pada Januari 2023 yang menggunakan media sosial, potensi bagi pengguna untuk mengalami serangan siber adalah tidak dapat dihindari. Teknik pengamanan data yang baik sangat dibutuhkan dalam menjamin kerahasiaan sebuah data, yang bekerja dengan konsep merusak, mencuri, dan mengunci data dengan berbagai macam tujuan, salah satunya untuk mendapatkan keuntungan. Ransomware adalah serangan virus Malware terhadap perangkat masing-masing. Salah satu contoh kasus di Indonesia yaitu Ransomware Wannacry menurut detiknet.com. Teknologi informasi telah mengubah cara kejahatan dilakukan, khususnya kejahatan dunia maya, di mana pelaku kejahatan dapat dituntut secara pidana sesuai dengan hukum setempat. Penggunaan virus komputer adalah salah satu jenis kejahatan siber. Dengan data yang diambil dari sumber CNN Indonesia, "Pada tahun 2017, terjadi insiden virus komputer di Indonesia, khususnya Malware Ransomware

Wannacry yang menginfeksi sistem di Rumah Sakit Harapan Kita dan Rumah Sakit Dharmais di Jakarta."

Data-data di komputer yang terinfeksi akan terenkripsi karena adanya Ransomware Wannacry. Hingga pengembang Wannacry dibayar, Ransomware ini akan mengunci mesin dan melarang pengguna untuk mengakses datanya. Rumah Sakit Dharmais dan Rumah Sakit Harapan Kita merupakan dua rumah sakit yang terkena dampak dari Ransomware Wannacry.akibat lumpuhnya sistem antrian Rumah Sakit Harapan Kita dan Rumah Sakit Dharmais, Ransomware Wannacry ini nyaris semua komputer di rumah sakit terpengaruh. Ransomware itu mengunci semua data dan mengganggu sistem teknologi informasi yang menyimpan seluruh data kesehatan pasien juga catatan pembayaran rumah sakit.

Mengingat kejadian tersebut terdapat barang bukti dari korban Ransomware Wannacry pada tahun 2017 yang fotonya telah diambil oleh @ilhamnegara. Sumber tersebut telah diambil dari Detikinet oleh Muhammad Alif Goenawan yang diakses pada hari Minggu 29 Mei 2023. Serangan tersebut telah memblokir lebih dari 176 juta serangan WannaCry di 217 negara sejak serangan awal tahun lalu. Bahkan serangan ini nyatanya masih terus berlanjut di tahun 2018. Menurut CTO Avast, Ondrej Vlcek Avast menurut keterangan melalui email yang bersumber dari detik.com "bahwa pihaknya telah mendeteksi dan memblok lebih dari 176 juta serangan WannaCry di 217 negara sejak serangan awal tahun lalu. Bahkan serangan ini nyatanya masih terus berlanjut di tahun 2018."



Gambar 1. Bentuk Ransomware Wannacry di Indonesia (Sumber detik.com)

Mengingat kejadian tersebut agar tidak terulang kembali dan untuk menjaga diri kita sendiri dengan adanya peningkatan kesadaran dalam merespons langsung terhadap serangan WannaCry, pemerintah Indonesia juga meningkatkan upaya kesadaran dan pendidikan tentang keamanan siber secara umum. Kampanye dan pelatihan keamanan siber diadakan untuk mengajarkan masyarakat tentang ancaman Ransomware dan langkah-langkah pencegahan yang dapat diambil. Dalam menghadapi serangan Ransomware WannaCry, Indonesia menerapkan pendekatan yang melibatkan berbagai pihak, termasuk pemerintah, CERT-CC, dan aparat penegak hukum. Upaya ini bertujuan untuk melindungi masyarakat dan organisasi dari serangan Ransomware serta meningkatkan kesadaran akan keamanan siber. Maka dari itu diperlukannya perlindungan hukum bagi korban dari serangan Ransomware Wannacry tersebut.

II. METODE

Penelitian ini menggunakan pendekatan penelitian yuridis normatif. Jenis data yang digunakan dalam penelitian hukum normatif adalah data sekunder, yang sering dikenal sebagai bahan hukum. Ada dua jenis bahan hukum: bahan hukum primer dan bahan hukum sekunder. Metode studi kepustakaan digunakan untuk memperoleh data dalam penelitian ini. Teknik pengolahan data adalah kegiatan merapikan data yang dihasilkan dari pengumpulan data sehingga siap untuk dikaji secara kualitatif. Setelah dilakukan pengolahan secara selektif, data tersebut dikarakteristikkan secara deskriptif deskriptif, yaitu diuraikan dalam bentuk uraian-uraian yang selanjutnya dapat digunakan untuk menjawab permasalahan yang dibahas.

III. HASIL PENELITIAN & PEMBAHASAN

A. Ransomware Wannacry

Institusi dengan basis pengguna internet yang besar hampir pasti memiliki beberapa masalah manajemen jaringan. Serangan oleh individu dengan niat jahat adalah salah satunya. Mereka yang terlibat dalam perilaku seperti itu untuk keuntungan pribadi dapat mengunci data privasi target atau memanipulasi data atau file. Menurut Everett "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 (Asih, 2021)." Biasanya, pelaku memasukkan program yang dibuat untuk kepentingan mereka sendiri ke dalam jaringan, meskipun dapat juga terjadi melalui aplikasi dan file program. Aplikasi ini disebut sebagai perangkat lunak berbahaya (malware). Malware adalah perangkat lunak yang bertujuan untuk mengumpulkan informasi pribadi; contohnya adalah Ransomware. Tindakan malware memblokir proses sistem dan menyembunyikan data dengan menggunakan teknik enkripsi yang membahayakan data. Penyelidikan lebih lanjut tentang malware diperlukan karena evolusi dan penyebaran infeksi yang bervariasi.

Ransomware adalah Suatu bentuk malware atau perangkat lunak berbahaya yang disebut Ransomware mengenkripsi data atau mencegah akses ke sistem korban, kemudian meminta tebusan dari korban untuk membuka kunci sistem atau mengembalikan data. Ransomware menyusup ke dalam sistem atau jaringan komputer melalui berbagai teknik, termasuk email phishing, situs web berbahaya, dan eksploitasi kelemahan sistem. Ransomware memerlukan kunci enkripsi yang cukup sulit untuk memecahkan kode enkripsi tersebut karena tersimpan secara remote di server yang sudah diatur. Setelah diaktifkan, Ransomware akan mengenkripsi data-data penting milik korban dengan kunci enkripsi rahasia yang hanya diketahui oleh penyerang. Korban kemudian akan diberikan instruksi tentang cara mendapatkan kunci dekripsi dan memulihkan akses ke data mereka dengan membayar sejumlah uang

dalam bentuk mata uang digital, seperti Bitcoin, dalam jangka waktu yang telah ditentukan. Penyerang dapat menyimpan data yang dienkripsi atau menghapusnya jika uang tebusan tidak dibayarkan. Dalam beberapa tahun terakhir, Ransomware telah menjadi salah satu ancaman siber yang paling berbahaya dan meluas, mempengaruhi orang, bisnis, dan organisasi di seluruh dunia.

Sedangkan Ransomware Wannacry atau Wanna Decryptor adalah program ransomware spesifik yang mengunci semua data pada sistem komputer dan membiarkan korban hanya memiliki dua file instruksi tentang apa yang harus dilakukan selanjutnya dan program Wanna Decryptor itu sendiri. Ransomware WannaCry juga dapat diartikan virus yang menyerang komputer dengan cara melakukan enkripsi pada data komputer sasarannya, dimana virus ini mampu mencuri data pengguna, menghapus informasi, merusak sistem, dan sebagainya. Karena Ransomware disimpan dari jarak jauh di server yang terkontrol, Ransomware membutuhkan kunci enkripsi yang sangat sulit untuk dipecahkan. Menurut pedoman Pasal 27 ayat (4) UU ITE, Ransomware dikualifikasikan sebagai pemerasan dan/atau pengancaman. Menurut KUHP Pasal 368 ayat 1, "Barangsiapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, memaksa seseorang 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.". Menurut Soesilo "Unsur-unsur yang ada dalam pasal ini adalah sebagai berikut:

1. Memaksa orang lain;
2. Untuk memberikan barang yang sama sekali atau sebagian termasuk kepunyaan orang itu sendiri atau kepunyaan orang lain, atau membuat utang atau menghapuskan piutang;
3. Dengan maksud hendak menguntungkan diri sendiri atau orang lain dengan melawan hak;

4. Memaksanya dengan memakai kekerasan atau ancaman kekerasan (Asih, 2021).”

Virus Ransomware WannaCry harus mendapatkan akses ke file atau sistem yang akan diserangnya. Sama halnya dengan virus biologis sebuah virus komputer membutuh akses untuk menyerang sasarannya. Akses tersebut didapatkan melalui 3 metode, yaitu:

1. Email

   Lampiran email adalah cara yang umum digunakan untuk menyebarkan infeksi Ransomware. Sebuah email disamarkan sebagai pemberitahuan penting, seperti yang dikirim oleh bank kepada nasabahnya, dan mengarahkan korban ke sebuah lampiran atau tautan yang, ketika dibuka, kosong tetapi berisi virus Ransomware WannaCry, yang memungkinkan virus memasuki sistem tanpa disadari.

2. Message

   Penyerang virus Ransomware juga dapat mengirimkan komunikasi kepada korbannya melalui media sosial. Untuk mengirim pesan dengan lampiran file, akun palsu yang menyamar sebagai "teman" korban dibuat. Virus Ransomware WannaCry bisa mendapatkan akses ke sistem dan mengunci jaringan yang terhubung ke perangkat yang terinfeksi setelah dibuka.

3. Pop-Ups

   Metode penyerangan virus Ransomware lain yang umum namun lebih tua adalah iklan "pop-ups". Sebuah iklan dibuat untuk muncul di layar komputer korban ketika mengakses situs-situs tertentu dengan maksud memancing korban untuk meng-klik tautan yang dilampirkan di iklan tersebut sehingga korban akan mengikuti petunjuk-petunjuk yang tersedia yang ternyata dirancang untuk mendistribusikan virus Ransomware WannaCry ke sistem komputer korbannya

Rata-rata serangan virus Ransomware WannaCry memiliki tujuan yang sama, yaitu mendapatkan uang tebusan dari para korbannya. Dengan rencana yang cukup sederhana, mereka memulai serangan secara acak dan menunggu uang tebusan dari korbannya untuk memulihkan data mereka. Mirip dengan skenario peretasan sebelumnya, penyerang harus mendapatkan akses ke komputer target, mencuri data yang dibutuhkan, menemukan pembeli untuk data tersebut, mengatur kontrak, dan memproses pembayaran.

B. Perlindungan Hukum Bagi Korban Serangan Ransomware Wannacry

Wabah Ransomware WannaCry telah diperingatkan oleh pihak berwenang di Indonesia, termasuk Kementerian Komunikasi dan Informatika. Pemerintah memberikan informasi tentang ancaman dan tindakan pencegahan yang diperlukan melalui berbagai saluran komunikasi, termasuk situs web resmi dan media sosial. Pemerintah Indonesianya diperlukan untuk mendorong pengguna komputer dan jaringan di Indonesia untuk segera memperbarui sistem operasi dan perangkat lunak mereka dengan patch keamanan yang dirilis oleh penyedia, terutama untuk melindungi dari kerentanan yang dimanfaatkan oleh WannaCry. Informasi dan panduan teknis juga diberikan kepada organisasi dan individu untuk memastikan langkah-langkah pembaruan yang tepat diambil. Peningkatan keamanan siber belum menjadi jaminan bahwa masyarakat umum, pemerintah, dan korporasi akan aman ketika mengakses dunia maya. Menurut Kusumawardani "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 (Asih, 2021)." Keamanan pengguna internet harus tetap menjadi prioritas utama. Pemerintah telah menerapkan hukum dan peraturan untuk melindungi pengguna internet,

namun sulit untuk menyelesaikan masalah di dunia maya karena kejahatan online dilakukan melalui komunikasi. Dengan kemajuan teknologi, salah satu cara untuk memberikan rasa aman kepada pengguna internet adalah dengan memahami bagaimana memberikan perlindungan hukum yang memadai bagi pengguna internet, sehingga pengguna internet dapat menikmati manfaat menjelajah di dunia maya atau melakukan transaksi online di dunia maya.

Mengingat pengetahuan kini telah menjadi komoditas, maka diperlukan upaya untuk melindungi aset-aset tersebut. Salah satu metode perlindungannya adalah melalui hukum pidana, baik pidana maupun non-pidana. Pasal 27 UU ITE mengatur tentang perbuatan melawan hukum di internet, berbunyi :

1. Setiap Orang dengan sengaja dan tanpa hak mendistribusikan, mentransmisikan, 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, mentransmisikan, atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian.

3. Setiap Orang dengan sengaja dan tanpa hak mendistribusikan, mentransmisikan, 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, mentransmisikan, atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan pemerasan dan/atau pengancaman.

Ketentuan Pasal 27 ayat (4) mengatur tindak pidana Ransomware:

"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 diklasifikasikan sebagai kejahatan pemerasan. Kualifikasi perbuatan yang dikategorikan sebagai pemerasan dan/atau pengancaman dalam KUHP Pasal 368 ayat (1), dan ketentuannya dalam Pasal 27 ayat (4) menggabungkan tindak pidana pemerasan dan/atau pengancaman dalam satu ketentuan, sedangkan dalam KUHP tindak pidana pemerasan diatur dalam Pasal 368 dan pengancaman diatur dalam Pasal 369.

Karena internet tidak secara otomatis diklasifikasikan hanya sebagai media komunikasi khusus antar pihak, tetapi juga sebagai media komunikasi global yang dapat diakses oleh semua pihak, informasi yang disiarkan atau disebarkan secara tidak sah di internet tidak menyiratkan bahwa hal tersebut merupakan hak asasi manusia untuk berkomunikasi. Oleh karena itu, meskipun internet bukanlah media yang bebas hukum, internet tidak dapat dilepaskan dari penerapan hukum terhadap penemu, pengguna, dan pihak-pihak yang menyelenggarakannya sebagai infrastruktur publik untuk berkomunikasi dan memberikan informasi dalam skala nasional dan global. Terkait dengan rumusan perbuatan dalam Pasal 27 ayat (1), ayat (2), ayat (3), dan ayat (4) dalam Pasal 45 ayat (1), perbuatan-perbuatan tersebut diancam dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 1.000.000.000,- (satu milyar rupiah). Rancangan sanksi pidana tersebut tidak tepat dan tidak proporsional karena menyamaratakan sanksi pidana terhadap perbuatan yang memiliki kualifikasi dan tingkat keparahan tindak pidana yang berbeda-beda. Pasal 27 mengatur beberapa tindak pidana yang berbeda, baik dari segi berat ringannya ancaman pidana maupun jenis tindak pidana itu sendiri. Ancaman pidana disamakan dalam Pasal 45 ayat (1) untuk tindak pidana permufakatan jahat. Akibat pidana untuk suatu tindak pidana tidak boleh lebih berat dari tindak pidana itu sendiri. Adanya ancaman pidana yang diatur dalam UU ITE tidak menjamin bahwa pelanggaran tebusan

tidak akan terulang kembali. Selain itu, penerapan pidana denda ini tidak menjamin adanya perlindungan hukum yang lebih jelas bagi pengguna dunia maya. Hukuman dan penjara yang dijatuhkan kepada pelaku kejahatan tidak seberapa jika dibandingkan dengan kerugian yang diderita korban Ransomware.

Penegakan hukum terhadap pelaku kejahatan mayantara merupakan upaya untuk melindungi pengguna internet dari para peretas yang memanfaatkan media internet untuk melakukan kejahatannya. Meskipun belum ada hukum siber khusus di Indonesia yang berorientasi pada kepentingan korban, namun diperlukan upaya hukum untuk melindungi kepentingan penghuni dunia maya (netizen) dan privasinya melalui penggunaan hukum yang telah ada sebelumnya seperti peraturan perundang-undangan, yurisprudensi, dan konvensi internasional yang telah diratifikasi oleh Indonesia. Mengatasi tindak pidana internet dapat dilakukan dengan berbagai inisiatif, termasuk tindakan preemtif, preventif, dan hukuman. Langkah-langkah pencegahan termasuk meratifikasi konvensi kejahatan siber internasional ke dalam sistem hukum Indonesia. Upaya penanggulangan kejahatan siber yang bersifat preventif dapat dilakukan melalui penguatan keamanan, kelayakan perangkat komputasi, kompetensi, dan kedisiplinan dalam menggunakan gawai saat berselancar di dunia maya. Kegiatan tersebut dapat berbentuk aksi yang dapat dilakukan dalam skala personal, nasional, maupun global. Adapaun menurut Tanthawi, "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 (Asih, 2021)."

Berdasarkan alasan-alasan yang dikemukakan di atas, keberadaan UU ITE dalam ketentuan Pasal 27 ayat (4) telah secara tegas mengatur perbuatan-perbuatan yang dilarang di dunia maya, di mana Ransomware Wannacry termasuk di dalamnya. Ransomware yang dikualifikasikan sebagai tindakan pemerasan yang dilakukan di dunia maya, telah memenuhi syarat KUHP Pasal 368 ayat (1) yang diancam

dengan pidana pemerasan. Pencantuman UU ITE dan KUHP merupakan salah satu inisiatif negara untuk melindungi pengguna internet. Ketentuan-ketentuan dalam UU ITE dan KUHP memberikan perlindungan hukum yang bersifat memaksa kepada negara. Sebagai fasilitator, pemerintah berusaha memberikan keadilan bagi korban Ransomware dengan menjatuhkan hukuman pidana kepada para pelaku kejahatan. Meskipun demikian, ketentuan-ketentuan dalam UU ITE dan KUHP masih perlu diubah dan diperbaharui untuk memberikan perlindungan hukum yang lebih optimal. Hal ini dikarenakan kejahatan siber, khususnya Ransomware, terus meningkat. Tidak hanya berhenti pada kasus WannaCry, sebenarnya masih ada kasus Ransomware lainnya seperti Locky, Petya, dan Not Petya. Kejahatan Ransomware biasanya dilakukan secara berkelompok dan terorganisir dengan baik, membuat para penyerang bergerak lebih cepat daripada kemampuan negara untuk memberlakukan peraturan dan regulasi untuk melindungi pengguna internet. Karena dunia maya tidak memiliki batasan ruang dan waktu, hukum tradisional tidak dapat diterapkan pada kejahatan dunia maya. Oleh karena itu, diperlukan terobosan yang lebih baik dalam menangani dan memberikan perlindungan hukum bagi para korban.

Bentuk-bentuk perlindungan yang dapat digunakan sebagai tindakan pencegahan dapat diimplementasikan. Individu dapat menyediakan jenis perlindungan ini sendiri atau melalui kolaborasi nasional dan global. Pengguna dunia maya dapat meningkatkan keamanan siber dengan membangun pertahanan siber untuk data pribadi saat mengakses internet. Selain itu, perlu juga untuk meningkatkan kesadaran dan pemahaman tentang penggunaan dunia maya sehingga pengguna memahami keuntungan dan kerugian dari penggunaan internet. Pemerintah dapat membantu dengan meningkatkan akses internet bagi pengguna. Karena dibutuhkan biaya yang tidak sedikit dan sumber daya manusia yang ahli untuk membangun pertahanan siber. Meratifikasi konvensi kejahatan siber adalah jenis perlindungan lain yang dapat diberikan oleh negara. Perjanjian Uni Eropa tentang Kejahatan Dunia Maya 2001 adalah perjanjian yang mulai populer. Konvensi ini

diprakarsai oleh Uni Eropa dan dapat diratifikasi oleh pemerintah manapun di dunia yang berkomitmen untuk memerangi kejahatan dunia maya. Kesediaan negara-negara untuk mengadopsi perjanjian kejahatan siber merupakan salah satu inisiatif untuk tetap mengikuti perkembangan dalam menghadapi jenis-jenis kejahatan siber yang muncul. Ini juga merupakan inisiatif untuk berkolaborasi dengan pemerintah lain di seluruh dunia untuk memerangi kejahatan dunia maya dan mengembangkan pertahanan global.

IV. KESIMPULAN

Ransomware adalah jenis kejahatan siber yang diklasifikasikan sebagai pelanggaran pemerasan. Hal ini karena Ransomware adalah sejenis perangkat lunak yang digunakan penyerang untuk menginfeksi mesin pengguna dengan tujuan akhir untuk meminta tebusan dari korban. Ransomware Wannacry atau Wanna Decryptor adalah program Ransomware spesifik yang mengunci semua data pada sistem komputer dan membiarkan korban hanya memiliki dua file instruksi tentang apa yang harus dilakukan selanjutnya dan program Wanna Decryptor itu sendiri. Kualifikasi meminta tebusan ini memasukkan Ransomware ke dalam tindak pidana pemerasan dengan ancaman. Ancamannya adalah pengguna akan kehilangan akses ke data mereka di dunia maya. Pemerintah telah berupaya untuk memberikan perlindungan hukum kepada korban Ransomware, yaitu dengan mengatur UU ITE, yang merupakan aturan yang unik dalam tindak pidana pemerasan di dunia maya. Sanksi terhadap pelaku merupakan salah satu bentuk perlindungan yang diberikan. Pemberlakuan sanksi tersebut merupakan upaya untuk memberikan keadilan bagi korban Ransomware. Meskipun penjatuhan sanksi untuk semua tindak pidana siber yang diatur dalam Pasal 27 UU ITE adalah sama. Namun pada kenyataannya, menggunakan hukuman yang sama untuk setiap pelanggaran ketentuan Pasal 27 tidaklah bijaksana karena tingkat kerugian dan kejahatan yang dilakukan akan berbeda. Jenis pertahanan lainnya adalah membangun pertahanan di dunia maya. Serta aktif memperbarui UU ITE untuk

memberikan perlindungan hukum yang lebih baik bagi korban Ransomware.

DAFTAR REFERENSI

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

Undang-Undang (Uu) Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

Undang-Undang (Uu) Tentang Kitab Undang-Undang Hukum Pidana

Jubhari, Andi Rian, (2022), Tinjauan Hukum Pidana Internasional Terhadap Serangan Siber Menggunakan Virus Ransomware Wannacry Indonesia, Skripsi, Thesis, Universitas Hassanudi Makassar

Kholiviya, Hasna (2021) Perlindungan Hukum Terhadap Korban Pencurian Data Pribadi Dalam Kasus Tindak Pidana Mayantara (Cyber Crime). Undergraduate Thesis, Universitas Islam Sultan Agung Semarang.

(Kurniawan, Irfan Arief, Mahmud Hadi, Dewi, Nourma, 2021). Penyebaran Virus Ransomware Wannacry Berdasarkan Undang-Undang No. 11 Tahun 2008, Dalam Jurnal Jurnal Inovasi Penelitian, (Vol 2, Nomor 2). 01-16

Asih, Desyanti Suka, Perlindungan Hukum Bagi Korban Serangan Ransomware, Dalam Jurnal Vyavahara Duta, Vol 16 No 2, 1-11.

M, Akbanov, V, Vassikalis, Logothesis M, (2019). Wannacry Ransomware:

Analysis Of Infection, Persistence, Recovery. Journal Baztech, Prevention And Propagation Mechanisms, Vol 1, Hal 113-12

Akraman,R, Candiwan, Priyadi, Yudi. (2018). Pengukuran Kesadaran Keamanan Informasi Dan Privasi Pada Pengguna Smartphone Android Di Indonesia. Dalam Jurnal Sistem Informasi Bisnis, Vol 2

(Wahidin,W., Syaifuddin., Zamah, Sari. (2022). Analisis Ransomware Wannacry Menggunakan Aplikasi Cuckoo Sandbox. Dalam Jurnal Repositor, Vol 4,. No 1.

(Widi, Shilvina,. (2023, Februari 3),. Pengguna Media Sosial Di Indonesia Sebanyak 167 Juta Pada 2023. Indonesia.Id

(Yusuf, Oik, (2017, Mei 15),. Kronologi Serangan Ransomware Wannacry Yang Bikin Heboh, Kompas.Com

(Kertopati, L, (2017,)Mei 13),. Dua Rumah Sakit Di Jakarta Kena Serangan Ransomware Wannacry, Cnnindonesia.Com