Rio Law Jurnal
Volume. 4 Nomor. 2, Desember 2023 ISSN 2722-9602
http://dx.doi.org/10.36355/.v1i2
Open Access at: https://ojs.umb-bungo.ac.id/index.php/RIO/index

PERLINDUNGAN HUKUM TERHADAP KORBAN PADA KASUS *CYBER SABOTAGE AND EXTORTATION* MENURUT HUKUM POSITIF DI INDONESIA

Dilla Ayuna Letri[1], Yunimar[2], Trie Rahmi Gettari[3]
Fakultas Hukum Universitas Ekasakti, Padang
Jl. Veteran No.26B, Purus, Kec. Padang Bar., Kota Padang, Sumatera Barat 25115
dillaayuna@gmail.com, yunimarchaniago@gmail.com gettaritari@gmail.com

ABSTRACT

The term cyber crime has emerged a lot along with the development of technology. Cyber crime is more often referred to as crimes related to cyberspace or crimes using computers. Cyber crime and cyber law where this crime violates criminal law. With the cases that occur in cyberspace, many victims have fallen. The conventional perspective on cyber crime will cause difficulties and inequality in the investigative process. However, we still have to take a positive attitude towards Law Number 11 of 2008 concerning the Internet and Electronic Transactions as a legal umbrella in the world of Cyber Crime. There are many kinds of cyber crimes in Indonesia, one of which is cyber sabotage and extortion. This crime is the most tragic crime. The way this is done is by disrupting, damaging or destroying a power, computer program or computer network system connected to the internet. Usually this crime is committed by inserting a logic bomb, computer virus or certain program, so that the data, computer program or computer network system cannot be used, does not work as it should.

Keywords: Protection, Crime, Cyber Sabotage and Extortion

ABSTRAK

Istilah *cyber crime* banyak bermunculan seiring dengan berkembangnya teknologi. *Cyber crime* lebih sering disebut dengan tindak kejahatan yang berhubungan dengan dunia maya (*cyber space*) atau tindak kejahatan menggunakan komputer.. *Cyber crime* dan *cyber law* dimana kejahatan ini sudah melanggar hukum pidana. Dengan adanya kasus yang terjadi di dunia maya tersebut, telah banyak menjatuhkan korban, Cara pandang konvensional terhadap tindak pidana *cyber crime* akan menimbulkan kesulitan dan ketimpangan dalam proses penyelidikan, penyidikan. Namun sikap positif tetap harus kita ambil terhadap Undang-Undang Nomor 11 Tahun 2008 tentang Internet dan Transaksi Elektronik sebagai payung hukum dalam dunia *Cyber Crime*. Kejahatan *cyber crime* di Indonesia begitu banyak macamnya, salah satunya adalah *cyber sabotage* dan *extortion*. Kejahatan ini merupakan kejahatan yang paling menggenaskan. Cara yang dilakukannya adalah dengan membuat gangguan, perusakan atau penghancuran terhadap suatu daya, program computer atau sistem jaringan computer yang terhubung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu *logic bomb,* virus computer ataupun suatu program tertentu, sehingga data, program computer atau sistem jaringan computer tidak dapat digunakan, tidak berjalan sebagaimana mestinya.

Kata Kunci : Perlindungan, Tindak Pidana, *Cyber Sabotage and Extortation*

[1] Fakultas Hukum Universitas Ekasakti, Padang
[2] Fakultas Hukum Universitas Ekasakti, Padang
[3] Fakultas Hukum Universitas Ekasakti, Padang

PENDAHULUAN

Berbicara tentang kejahatan sebenarnya tidak lepas dari dunia nyata dalam kehidupan masyarakat itu berada. Kejahatan merupakan cap atau sebutan yang digunakan oleh masyarakat dalam menilai suatu perbuatan seseorang. Dalam mendefinisikan kejahatan, ada beberapa pandangan mengenai perbuatan apakah yang dapat dikatakan sebagai kejahatan.

Dalam KBBI kejahatan mempunyai pengertian perilaku yang bertentangan dengan nilai dan norma yang berlaku yang telah disahkan oleh hukum tertulis. Sedangkan secara empiris, definisi kejahatan dalam pengertian yuridis tidak sama dengan pengertian kejahatan dalam kriminologi yang dipandang secara sosiologis.

Secara yuridis, kejahatan dapat didefinisikan sebagai suatu tindakan yang melanggar undang-undang atau ketentuan yang berlaku dan diakui secara legal. Secara kriminologi yang berbasis sosiologis kejahatan merupakan suatu pola tingkah laku yang merugikan masyarakat (dengan kata lain terdapat korban) dan suatu pola tingkah laku yang mendapatkan reaksi sosial dari masyarakat.[4]

Sedangkan Bonger menyatakan bahwa kejahatan adalah merupakan perbuatan anti sosial yang secara sadar mendapat reaksi dari negara berupa pemberian derita dan kemudian sebagai reaksi terhadap rumusan-rumusan hukum (*legal definitions*) mengenai kejahatan.[5]

J.E. Sahetapy dan B. Marjono Reksodiputro dalam bukunya "Paradoks Dalam Kriminologi" yang dikutip oleh Syahrudin Husein menyatakan bahwa, kejahatan mengandung konotasi tertentu, merupakan suatu pengertian dan penamaan yang relatif, mengandung variabilitas dan dinamik serta bertalian dengan perbuatan atau tingkah laku (baik aktif maupun pasif), yang dinilai oleh sebagian mayoritas atau minoritas masyarakat sebagai suatu perbuatan anti sosial, suatu perkosaan terhadap skala nilai sosial dan atau perasaan hukum yang hidup dalam masyarakat sesuai dengan ruang dan waktu.[6]

Istilah *cyber crime* banyak bermunculan seiring dengan berkembangnya teknologi. *Cyber crime* lebih sering disebut dengan tindak kejahatan yang berhubungan dengan dunia maya (*cyber space*) atau tindak kejahatan menggunakan komputer. Ada beberapa pendapat yang menyamakan antara tindak pidana kejahatan komputer dengan *cyber crime*, dan ada pendapat yang membedakan antara keduannya. Meskipun belum ada kesepahaman mengenai definisi kejahatan teknologi informasi, namun ada kesamaan pengertian mengenai kejahatan komputer.

Cyber Crime merupakan perkembangan dari computer crime. *Cyber crime* dan *cyber law*

[4] Abdul Wahid dan Muhammad Labib, *Kejahatan Mayantara (Cyber Crime)*, PT. Refika Aditama, Bandung, 2005, hlm 37

[5] Nasrulloh, *Pengertian Kejahatan*, https://nasrullaheksplorer.blogspot.com/2008/10/pengertian-kejahatan.html diakses pada tanggal 30 Oktober 2023 pukul 19.00 WIB

[6] *Ibid*

dimana kejahatan ini sudah melanggar hukum pidana. Dengan adanya kasus yang terjadi di dunia maya tersebut, telah banyak menjatuhkan korban, bukan hanya pada kalangan remaja namun disemua usia. Hal tersebut mengharuskan satuan kepolisian untuk segera bertindak dalam menangani kasus *cyber crime* (kejahatan dunia maya) yang cakupan kejahatannya sangat luas bahkan tidak terbatas.

Semakin banyaknya kasus *cybercrime* (khususnya di Indonesia) telah menarik perhatian pemerintah untuk segera memberlakukan undang-undang yang dapat digunakan untuk menjebak pelaku kejahatan di dunia maya. Pemerintah Indonesia sendiri telah memasukkan UU Cybercrime (UU Siber) ke dalam UU ITE Nomor 11 Tahun 2008, dan berharap dengan adanya UU ITE Nomor 11 Tahun 2008 dapat mengatasi, mengurangi, dan menghentikan pelaku kejahatan di dunia maya.[7]

Kejahatan *cyber crime* di Indonesia begitu banyak macamnya, salah satunya adalah *cyber sabotage* dan *extortion*. Kejahatan ini merupakan kejahatan yang paling menggenaskan. Cara yang dilakukannya adalah dengan membuat gangguan, perusakan atau penghancuran terhadap suatu daya, program computer atau sistem jaringan computer yang terhubung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu *logic bomb,* virus computer ataupun suatu program tertentu, sehingga data, program computer atau sistem jaringan computer tidak dapat digunakan, tidak berjalan sebagaimana mestinya.[8]

METODE PENELITIAN

Spesifikasi penelitian yang digunakan dalam penelitian ini adalah bersifat *deskriptif analitis* yaitu suatu usaha untuk menggambarkan tentang perlindungan hukum terhadap korban tindak pidana *cyber sabotage and extortation* menurut hukum positif di Indonesia. Metode pendekatan yang digunakan adalah pendekatan *Yuridis Normatif* yaitu penelitian hukum yang dilakukan berdasarkan norma dan kaedah dalam peraturan perundang-undangan. Sumber Data yang digunakan adalah Data Sekunder, yang terdiri dari :

a. Bahan Hukum Primer, yang terdiri dari :
   1) Undang-undang Dasar Negara Republik Indonesia Tahun 1945;
   2) Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
b. Bahan Hukum Sekunder, yaitu semua bahan yang memberikan penjelasan terhadap bahan hukum primer. Meliputi jurnal, buku-buku referensi, hasil karya ilmiah para sarjana, hasil-hasil penelitian ilmiah.
c. Bahan Hukum Tersier, yaitu bahan-bahan yang memberikan informasi atau petunjuk serta penjelasan terhadap bahan-bahan hukum primer dan sekunder, seperti Kamus Umum Bahasa Indonesia (KUBI) dan Kamus Inggris-

[7] Miftakhur Rokhman Habibi, Isnatul Liviani, *Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia*, Jurnal Al-Qanun : Jurnal pemikiran dan Pembaharuan Hukum Islam, Vol 23, No. 2, Desember 2020, hlm 401

[8] M. Syukri Akub, *Pengaturan Tindak Pidana Mayantara (Cyber Crime) Dalam Sistem Hukum Indonesia*, Jurnal Fakultas Hukum Universitas Hasanuddin, Vol. 20 No. 2 November 2018, hlm 86

Indonesia serta Kamus Hukum dan Ensiklopedia.

Teknik pengumpulan data dilakukan dengan cara studi dkomen, dan data akan dianalisa dengan metode kualitatif.

PEMBAHASAN DAN ANALISIS

A. Pengertian *Cyber Crime* dan *Cyber Sabotase* dan *Extortion*

Perkembangan teknologi komputer saat ini menghasilkan berbagai bentuk kejahatan komputer di lingkungan *cyberspace* yang kemudian melahirkan istilah baru yang dikenal dengan *Cybercrime*, *Internet Fraud*, dan lain-lain. Sebagian besar dari perbuatan *Cybercrime* dilakukan oleh seseorang yang sering disebut dengan *cracker*.

Menurut Gregory *Cybercrime* adalah suatu bentuk kejahatan virtual dengan memanfaatkan media komputer yang terhubung ke internet, dan mengekploitasi komputer lain yang terhubung dengan internet juga. Adanya lubang-lubang keamanan pada sistem operasi menyebabkan kelemahan dan terbukanya lubang yang dapat digunakan para *hacker, cracker* dan *script* kiddies untuk menyusup ke dalam komputer tersebut.[9]

Beberapa julukan/sebutan lainnya yang cukup keren diberikan kepada kejahatan baru ini dalam berbagai tulisan, antara lain sebagai "kejahatan dunia maya". "*cyber crime*". Sehubung dengan kekhawatiran akan ancaman/bahaya *cyber crime* ini, karena berkaitan erat dengan "*economi crime*" dan "*organized crime*" (terutama untuk tujuan "*money laundering*). Jadi *cyber crime* dapat didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan internet yang berbasis pada kecanggihan teknologi computer dan telekomunikasi.

IPTEK "telah mengalami evolusi, yang semula digunakan untuk kepentingan militer dan ilmiah menjadi sasaran dan sarana kejahatan. Para pengguna internet tidak saja hanya para ilmuwan, pengguna umum melainkan dipakai oleh mata-mata dan teroris. Seiring berjalannya waktu, muncul suatu kejahatan siber yang dikenal dengan istilah cyber terorism.[10]

Cyber Sabotage adalah kejahatan yang dilakukan dengan membuat gangguan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu virus komputer atau program tertentu, sehingga data yang ada pada program komputer atau sistem jaringan komputer tersebut tidak dapat digunakan, tidak berjalan sebagai mana mestinya atau berjalan sebagaimana yang dikehendaki.

Kejahatan ini sering juga disebut dengan *cyber terrorism*. Setelah hal tersebut terjadi maka tidak lama para pelaku menawarkan diri kepada korban untuk memperbaiki data, program komputer atau sistem jaringan yang disabotase oleh para pelaku. Dan tentunya dengan bayaran tertentu sesuai permintaan yang diinginkan oleh pelaku.

Sedangkan *Extortion* atau pemerasan adalah tindak pidana dimana seseorang individu memperoleh uang, barang dan jasa atau perilaku yang diinginkan dari yang lain dengan lalim mengancam atau menimbulkan kerugian bagi

[9] Dista Amalia Arifah, *Kasus Cybercrime di Indonesia*, Jurnal Bisnis dan Ekonomi (JBE), Vol. 18, No. 2, 2011, hlm 186

[10] Dwila Annisa Rizki Amalia, Mujiono Hafidh Prasetyo, Kebijakan Hukum Pidana Dalam Upaya Penanggulangan *Cyber Crime*, Jurnal pembangunan Hukum Indonesia, Vol. 3, No. 2, 2021, hlm 229

dirinya, properti atau reputasi. Pemerasan adalah tindak pidana yang berbeda dari perampokan, dimana pelaku mencuri properti melalui kekuatan.

B. Analisa Kasus *Cyber Sabotage dan Extortion*

Cyber crime memiliki sifat efisien dan cepat serta sangat menyulitkan bagi pihak penyidik dalam melakukan penangkapan terhadap pelakunya. Hal ini disebabkan antara lain oleh kurangnya pemahaman dan pengetahuan masyarakat terhadap jenis kejahatan cyber crime, pemahaman dan pengetahuan ini menyebabkan upaya penanggulangan cyber crime mengalami kendala, dalam hal ini kendala yang berkenaan dengan penataan hukum dan proses pengawasan masyarakat terhadap setiap aktivitas yang diduga berkaitan dengan kejahatan cyber crime tersebut.[11]

Salah satu kasus kejahatan *cyber sabotage dan extortion* yang pernah terjadi adalah serangan virus *Ransomware WannaCry*. Serangan ini terjadi pada tahun 2017 yang diperkirakan menginfeksi 300.000 sistem komputer di 150 negara. Virus ini adalah sejenis *Ransomware* yang bernama *WannaCry* dimana virus ini menyandera file milik korbannya yang ada di dalam komputer dengan metode enkripsi yang sulit ditembus. Bila korban ingin mendapatkan kunci enkripsi sehingga file yang disandera bisa diakses lagi, maka mereka harus membayar uang tebusan sejumlah $300 dalam bentuk bitcoin melalui tautan yang tertera di layar komputer korban ketika virus ini menginfeksi.[12]

Virus *Ransomware WannaCry* ini awalnya adalah senjata siber milik National Security Agency (NSA) Amerika Serikat yang bernama EternalBlue. EternalBlue merupakan program anti teroris yang digunakan untuk mengambil data dari komputer sasaran NSA yang dianggap mengancam negara Amerika Serikat. Namun, pada tanggal 14 April 2017 program ini dicuri oleh kelompok hacker bernama Shadow Broker dan menghilang hingga akhirnya serangan Ransomware WannaCry ini terjadi.[13]

Di Indonesia virus ini terdeteksi pada bulan Mei 2017 yang tidak hanya menyerang komputer pribadi tetapi juga korporasi, bahkan virus ini menyerang sistem komputer rumah sakit di Jakarta yakni Rumah Sakit Harapan Kita dan Rumah Sakit Dharmais Jakarta yang mana menyebabkan sistem computer mengalami kelumpuhan dalam melayani pasien. 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. R*ansomware* itu mengunci semua data dan mengganggu sistem teknologi informasi yang

[11] A. Aco Agus, *Penanganan Kasus Cyber Crime Di Kota Makassar (Studi Pada Kantor Kepolsiian Resort Kota Besar Makassar)*, Jurnal Supremasi, Vol. XI, Nomor 1, April 2016, hlm 21

[12] Oik Yusuf, *Kronologi Serangan Ransomware WannaCry yang Bikin Heboh Dunia*, https://tekno.kompas.com/read/2017/05/15/09095437/kronologi.serangan.ransomware.wannacry.yang.bikin.heboh.internet?page=all diakses pada tanggal 30 Oktober 2023 pukul 19.00 WIB

[13] *Ibid*

menyimpan seluruh data kesehatan pasien juga catatan pembayaran rumah sakit.[14]

Tujuan dari serangan virus Ransomware WannaCry rata-rata sama, yaitu menargetkan uang tebusan dari korbannya. Dengan skema yang cukup mudah, yaitu melancarkan serangan secara acak dan menunggu tebusan dari korbannya untuk mendapatkan kembali datanya. Mirip dengan kasus-kasus hacking lainnya, dimana penyerang harus masuk ke komputer target, mencuri data yang diinginkan, mencari pembeli untuk data itu, menegosiasikan kesepakatan, dan memproses pembayaran.

Menurut pedoman Pasal 27 ayat (4) jo Pasal 45 ayat (1) UU ITE, maka Ransomware dikualifikasikan sebagai pemerasan dan/atau pengancaman, yang berbunyi :

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 pemerasandan/atau pengancaman".

Pasal 45 ayat (1) :

> "Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3), atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah)".

Sedangkan Menurut Pasal 368 ayat 1 Kitab Undang-undang Hukum Pidana (KUHP) menyatakan bahwai :

> "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."

Jadi, dapat disimpulkan bahwa 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. Didalam pengaturan hukum di Indonesia hal ini telah melanggar Pasal 27 ayat (4) jo Pasal 45 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik jo Pasal 368 ayat (1) KUHP.

C. Kajian Teori Perlindungan Hukum Bagi Korban Tindak Pidana *Cyber Sabotage and Extortaion*

Wabah *Ransomware WannaCry* adalah salah satu kasus tindak pidana *cyber sabotage and extortation* yang 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

[14] Gilang Ramadhan, *Perlindungan Hukum Bagi Korban Ransomwhere Wannacry Tindak Pidana Ransomwhere*, Jurnal Das Sollen : Kajian Kontemprorer Hukum dan Masyarakat, Vol. 1 No. 2, 2023, hlm 4

lunak mereka dengan patch keamanan yang dirilis oleh penyedia, terutama untuk melindungi dari kerentanan yang dimanfaatkan oleh WannaCry.

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.[15]

Perlindungan hukum adalah suatu perlindungan yang diberikan kepada subyek hukum yakni orang atau badan hukum yang bersifat preventif maupun represif, serta baik yang berbentuk lisan maupun tulisan. Perlindungan hukum tersebut akan diberikan kepada masyarakat yang merasa dirugikan atas hak asasi manusia yang mereka miliki. Perlindungan tersebut diberikan kepada masyarakat agar mereka dapat menikmati hak-hak yang telah diberikan oleh aparat penegak hukum.

Perlindungan hukum bagi setiap warga Negara Indonesia tanpa terkecuali, dapat ditemukan dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.Oleh karena itu setiap produk undang-undang yang dihasilkan oleh lembaga legislatif harus senantiasa mampu memeberikan jaminan perlindungan hukum bagi semua orang, bahkan harus mampu menampung aspirasi hukum yang berkembang ditengah-tengah masyarakat.

Menurut Philipus M. Hadjon, yang menyatakan bahwa :

> "Perlindungan hukum bagi rakyat sebagai tindakan pemerintah yang bersifat preventif dan represif".[16]

Perlindungan hukum yang preventif bertujuan untuk mencegah terjadinya sengketa, yang mengarahkan tindakan pemerintah bersikap hati-hati dalam pengambilan keputusan berdasarkan diskresi, dan perlindungan yang represif bertujuan untuk menyelesaikan terjadinya sengketa, termasuk penanganannya di lembaga peradilan.Perlindungan hukum harus melihat tahapan yakni perlindungan hukum lahir dari suatu ketentuan yang pada dasarnya merupakan kesepakatan masyarakat tersebut untuk mengatur hubungan perilaku antara anggota-anggota masyarakat dan antara perseorangan dengan pemerintah yang dianggap mewakili kepentingan masyarakat.

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

[15] *Ibid*

[16] Philipus M. Hardjon, *Perlindungan Hukum Bagi Rakyat Indonesia*, Penerbit PT. Bina Ilmu, Surabaya,1987, hlm 2

internasional yang telah diratifikasi oleh Indonesia.[17]

Mengatasi tindak pidana internet dapat dilakukan dengan berbagai inisiatif, termasuk tindakan preemtif, preventif, dan hukuman. Langkah-langkah tersebut terdiri dari :

1. Langkah Preemptif, yaitu bentuk pencegahan dengan meratifikasi konvensi kejahatan siber internasional ke dalam sistem hukum Indonesia.
2. Langkah preventif, yaitu 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.
3. Langkah represif, dapat 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.

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.

KESIMPULAN

Cyber Sabotage and Extortation merupakan kejahatan yang paling mengenaskan. Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet. Dalam beberapa kasus setelah hal tersebut terjadi, maka pelaku kejahatan tersebut menawarkan diri kepada korban untuk memperbaiki data, program komputer atau sistem jaringan komputer yang telah disabotase tersebut, tentunya dengan bayaran tertentu yang dapat dilakukannya dengan cara memeras bahkan sampai mengancam korban.

Ransomware adalah jenis kejahatan siber yang berupa *cyber sabotage and extortation* 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. 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

[17] Gilang Ramadhan, *Op.cit*, hlm 12

memberikan keadilan bagi korban Ransomware. Bentuk perlindungan lainnya adalah membangun pertahanan di dunia maya. Serta aktif memperbarui UU ITE untuk memberikan perlindungan hukum yang lebih baik bagi korban *Ransomware.*

SARAN

Berdasarkan kesimpulan diatas, maka saran yang dapat diberikan adalah Pemerintah harus lebih serius lagi dalam memberikan perlindungan hukum bagi korban tindak pidan cyber crime sabotage and extortation tersebut dengan cara melakukan pengawasan yang lebih ketat lagi terhadap kejahatan di dunia maya ini dan juga dengan memberikan sanksi yang lebih tegas bagi pelaku yang melakukan tindak pidana tersebut.

DAFTAR PUSTAKA

Abdul Wahid dan Muhammad Labib, *Kejahatan Mayantara (Cyber Crime),* PT. Refika Aditama, Bandung, 2005.

Kamus Besar Bahasa Indonesia (KBBI), Edisi Kedua, Cet. 1, Balai Pustaka, Jakarta

Philipus M. Hardjon, *Perlindungan Hukum Bagi Rakyat Indonesia*, Penerbit PT. Bina Ilmu, Surabaya,1987

A. Aco Agus, *Penanganan Kasus Cyber Crime Di Kota Makassar (Studi Pada Kantor Kepolsiian Resort Kota Besar Makassar),* Jurnal Supremasi, Vol. XI, Nomor 1, April 2016

Dista Amalia Arifah, *Kasus Cybercrime di Indonesia*, Jurnal Bisnis dan Ekonomi (JBE), Vol. 18, No. 2, 2011

Dwila Annisa Rizki Amalia, Mujiono Hafidh Prasetyo, Kebijakan Hukum Pidana Dalam Upaya Penanggulangan *Cyber Crime*, Jurnal pembangunan Hukum Indonesia, Vol. 3, No. 2, 2021

Gilang Ramadhan, *Perlindungan Hukum Bagi Korban Ransomwhere Wannacry Tindak Pidana Ransomwhere*, Jurnal Das Sollen : Kajian Kontemprorer Hukum dan Masyarakat, Vol. 1 No. 2, 2023

Miftakhur Rokhman Habibi, Isnatul Liviani, *Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia*, Jurnal Al-Qanun : Jurnal pemikiran dan Pembaharuan Hukum Islam, Vol 23, No. 2, Desember 2020

Nasrulloh, *Pengertian Kejahatan*, https://nasrullaheksplorer.blogspot.com/2008/10/pengertian-kejahatan.html

Oik Yusuf, *Kronologi Serangan Ransomware WannaCry yang Bikin Heboh Dunia,* https://tekno.kompas.com/read/2017/05/15/09095437/kronologi.serangan.ransomware.wannacry.yang.bikin.heboh.internet?page=all