
**PENYEBARAN VIRUS RANSOMWARE WANNACRY BERDASARKAN
UNDANG-UNDANG NO. 11 TAHUN 2008**

Oleh

Irfan Arief Kurniawan¹⁾, Hadi Mahmud²⁾ & Nourma Dewi³⁾

^{1,2,3}Fakultas Hukum Universitas Islam Batik Surakarta

Email: irvanboyz7535@gmail.com

Abstract

This study aims to find and describe the legal provisions for perpetrators of the crime of spreading computer viruses. analyze how the law is enforced against the perpetrators of the spread of computer viruses regulated in Law Number 11 of 2008. This study uses a method of normative legal approach to law enforcement against the perpetrators of the spread of computer virus wannacry ransomware based on Law No. 11 of 2008 concerning Information and Electronic Transactions. Data was collected by reviewing legal materials which were then analyzed using qualitative analysis techniques and interpreted logically and systematically and then drawn conclusions. Law enforcement against the perpetrators of the spread of computer viruses Ransomware wannacry, among others by prosecuting law by observing jurisdiction and applicable law, because in this case it is possible for the perpetrator to be in a country different from the country where the victim of this crime is located, besides, it is difficult to determine the place events (*locus delicti*) because these crimes occur in cyberspace. The perpetrators of the spread of computer viruses through Ransomware wannacry viruses can be subject to Article 46 paragraph (2) in conjunction with Article 30 paragraph (2) of the ITE Law. Law No. 11 of 2018 concerning ITE regulates and explains various actions for violating the law in the misuse of Information Technology. The spread of computer viruses Wannacry Ransomware is one of the prohibited acts as regulated in Article 30 paragraph (2) of the ITE Law, because in this case the virus contained in the computer component is considered as electronic information and / or documents that can be used as one of the evidence as stipulated in article 5 paragraph (1) and (2) of the ITE Law. Thus, the act of spreading computer viruses can be charged under Article 46 paragraph (2) in conjunction with Article 30 paragraph (2) of the ITE Law.

Keywords: Law Enforcement, Computer Virus & Wannacry Ransomware.

PENDAHULUAN

Teknologi informasi telah mengubah pola kejahatan yang didalamnya adalah kejahatan dunia maya, , yang mana pertanggungjawaban pelaku kejahatan dilakukan secara pidana sesuai yurisdiksinya. Satu contoh kejahatan dunia maya adalah virus komputer. Tahun 2015 Indonesia mengalami kejahatan virus komputer yaitu virus *Ransomware Wannacry* yang menyerang komputer di RS Harapan Kita dan juga di RS Dharmais Jakarta. Keberadaan *Ransomware Ransomware Wannacry* akan mengenkripsi *file* pada komputer terinfeksi. *Ransomware Wannacry* mengunci komputer/mencegah pengguna untuk mengakses isi komputer sampai pembayaran

dilakukan kepada pembuatnya. Ada dua Rumah Sakit yang terkena *Ransomware Wannacry* yaitu RS Dharmais dan RS Harapan Kita.

Kejahatan virus komputer diatur sesuai Pasal 33 ayat 1 UU No. 11 Th. 2008 dimana dinyatakan bahwa seorang dengan sengaja dan atau tanpa hak atau tindakan melawan hukum dengan melakukan tindakan apapun yang dapat mengakibatkan sistem Elektronik terganggu dan/atau adanya akibat sistem elektronik menjadikan tidak dapat bekerja seperti mestinya. Terkait kondisi tersebut perlu adanya perlindungan hukum terhadap pengguna komputer di Indonesia khususnya komputer jaringan.

METODE PENELITIAN

Jenis penelitian adalah tinjauan pustaka, bersifat deskriptif-analisis. Penelitian memakai pendekatan rundang-undang dan menggunakan pendekatan konsep (*conceptual approach*). Bahan hukum digunakan yaitu bahan Hukum Primer, yang terdiri dari adanya tindakan pelanggaran hukum dalam UU No. 8/1981 mengenai Hukum Acara Pidana, dan UU No. 11/2008 mengenai Informasi dan Transaksi Elektronik. Untuk bahan hukum sekunder, digunakan berbagai buku, jurnal dan dokumen tentang penelitian ini. Sementara bahan untuk hukum tersier adalah bahan dari petunjuk seperti kamus hukum, dan sumber hukum tersier lainnya.

Penelitian kepustakaan mengenai UU No. 8/1981 dan UU No. 11/2008; sebagai data sekunder. Bahan hukum sekunder yaitu pendapat para ahli terkait penyebaran virus komputer serta bahan hukum tertier. Analisis data menggunakan analisis kualitatif melalui beberapa tahap yaitu mengumpulkan data, mengklasifikasikan dan menghubungkannya dengan berbagai teori dan masalah, kemudian ditarik kesimpulan untuk menentukan hasil. Adapun model analisis yang digunakan *Interactive Model of Analysis*.

HASIL DAN PEMBAHASAN

Tindak Pidana Penyebaran Virus Komputer *Ransomware Wannacry* Menurut UU No. 11/2008 mengenai ITE

Virus komputer baik oleh pembuat maupun yang menyebarkannya dan mengakibatkan kerugian ada unsur kesengajaan melakukan kejahatan, maka pelaku dijerat sesuai pasal 32 ayat 1 UU ITE, Pasal 33 UU ITE serta pasal 36. Pelanggaran terhadap pasal 33 tersebut dikaitkan ketentuan dalam Pasal 49 yang mana ketentuan terhadap hukum atas adanya pelanggaran yang telah dilakukan. Virus komputer jika dikaitkan dengan UU tentang ITE yang melanggar beberapa pasal 3, Pasal 4a, b, c, d, e. Dari sudut pandang orang yang membuat virus itu sendiri dikaitkan UU ITE yaitu Pasal 32 ayat 1 dan juga pada ketentuan Pasal 33 UU tentang ITE.

Pada kasus penyebaran virus *Ransomware Wannacry* tersangka dengan sengaja menyebarkan virus dengan memblokir data-data yang ada di komputer yang ditujunya dengan maksud untuk meminta tebusan. Perbuatan tersangka tersebut dapat dijerat dengan menggunakan Pasal 32 pada ayat (1) juncto Pasal 33 UU No. 11/2008 tentang ITE. Pada Pasal 32 ayat (1), dimana disebutkan yaitu: seseorang sengaja dan/tanpa hak atau perbuatan melawan ketentuan hukum dan dengan bagaimana telah mengubah, menambah atau mengurangi, serta melakukan kegiatan transmisi dengan merusak, memindahkan, menghilangkan, dan menyembunyikan sesuatu kegiatan terhadap informasi elektronik dan/atau terhadap dokumen berupa data elektronik yang menjadi milik publik atau orang lain.

Penyebaran virus *Ransomware Wannacry* pada hakekatnya memenuhi berbagai unsur subyektif dan juga unsur obyektif dalam Pasal 32 (1) maka didasarkan pada Pasal 48 UU No 11/2008 tentang ITE maka semua orang yang mana memenuhi telah unsur yang dimaksudkan pada Pasal 32 ayat (1) maka dipidana penjara dengan waktu paling lama yaitu delapan tahun dan/atau pemberian denda uang paling sebanyak dua miliar rupiah. Didasarkan pada Pasal 49 UU No. 11/2008 tentang ITE maka bagi setiap orang yang mana telah memenuhi unsur Pasal 33, dipidana kurungan atau penjara selama sepuluh tahun maksimal atau denda maksimal sepuluh miliar rupiah.

Penegakan Hukum Bagi Pelaku Penyebaran Virus *Ransomware Wannacry* berdasarkan UU No. 8/1981 Tentang Hukum Acara Pidana

Adanya pasal 30 ayat 2 UU No. 8/1981 Tentang Hukum Acara Pidana dapat diterapkan pada adanya kasus terhadap penyebaran virus *Ransomware wannacry*, hal ini disebabkan untuk orang penyebar virus *Ransomware wannacry*, dianggap telah mengakses komputer dan atau sistem elektronik yang lain secara sengaja dan melanggar hukum. Hal itu dilakukan dengan mengirim virus *Ransomware wannacry*, yang mempunyai fungsi untuk mengunci

berbagai data pengguna komputer yang telah terkena virus, dengan demikian tujuan guna memperoleh informasi, merusak dan juga dokumen elektronik yang dimiliki pihak lain secara melawan hukum.

Pada kasus penyebaran virus komputer *Ransomware Wannacry* sangat sulit dibuktikan, mengingat semua peralatan sebagai bukti tersebut mempunyai berbagai bentuk informasi atau dokumennya adalah elektronik, namun demikian penyebaran virus itu dapat juga dijadikan sebagai alat bukti sesuai ketentuan Pasal 5 (1) ketentuan UU No. 8/1981 mengenai Hukum Acara Pidana bahwa adanya akses terhadap informasi dan dokumen elektronik serta printoutnya dapat dijadikan sebagai alat bukti hukum yang sah. Pasal 5 ayat (2) UU No. 8/1981 Tentang Hukum Acara Pidana ditegaskan pula bahwa adanya perluasan terhadap adanya alatbukti sah sesuai dengan hukum acara di Indonesia. Ketentuan lain alat bukti juga menjadi ketentuan pidana bersifat memaksa, yang mana terhadap semua alatbukti tersebut tidak ditambah/dikurangi. Alat bukti ini diperluas pada Pasal 184 KUHAP, terkait adanya kasus penyebaran virus komputer adalah alatbukti petunjuk sah. Terhadap alatbukti petunjuk, tidak dapat dilepaskan dari Pasal 188 ayat (2) KUHAP yang mana disebutkan adanya kewenangan terhadap hakim untuk mencari alatbukti petunjuk dari berbagai keterangan dari saksi; terdakwa dan keterangan surat.

Komputer yang terkena virus *Ransomware Wannacry* dapat sebagai petunjuk, yang menjadikan perluasan terhadap alatbukti surat yaitu bahan yang menjadikan petunjuk hakim untuk membuktikan perkara masuk dalam kasus penyebaran virus *Ransomware Wannacry* sebagaimana sebelumnya. Adanya tindakan pidana terhadap penyebaran virus *Ransomware Wannacry* memungkinkan terlibatnya lebih dari satu sistem hukum dan dari berbagai negara, sehingga penyebaran *Ransomware Wannacry* masuk dalam kategori sebagai suatu kejahatan berbagai negara, mengingat banyak faktor penyebab seperti kepentingan dari beberapa negara terhadap suatu kejahatan, baik pelaku, korban, maupun lokasi

kejahatan atau perpaduan beberapa unsur tersebut terjadi.

Tindak pidana yang dilakukan dengan menyebarkan virus *Ransomware Wannacry* juga melibatkan beberapa orang dari beberapa negara, sehingga dalam proses penegakan, harus kerja sama dengan beberapa negara lain tersebut. Penyebaran virus *Ransomware Wannacry* sebagai suatu kejahatan transnasional juga erat kaitannya dari sisi yurisdiksi guna penetapan undang-undang, dan yurisdiksi bagaimana menghukum serta yurisdiksi guna menuntut pelaku penyebaran virus tersebut. Pelanggaran pidana terhadap penyebaran virus komputer *Ransomware Wannacry* sangat mungkin melibatkan lebih satu sistem hukum atau negara lainnya. Berbagai faktor penyebab yaitu kepentingan terhadap lebih satu negara, pelakunya, korbannya, atau perpaduan unsur-unsur kejahatan tersebut. Dengan demikian penegakan hukum, harus juga memperhatikan adanya kerjasama dari kepolisian antar berbagai negara.

Adanya perundang-undangan terhadap informasi dan transaksi elektronik di Indonesia, juga diatur mengenai berbagai aktivitas di dunia maya, namun demikian kejatahan terhadap penyebaran virus komputer *Ransomware Wannacry* tidak mengatur secara khusus, namun demikian ketentuan Pasal 30 ayat (2) dapat diterapkan.

Beberapa kendala yang muncul dalam penegakan terhadap pelaksanaan kebijakan penegakan hukum bagi pelaku penyebaran virus komputer *Ransomware Wannacry* berdasarkan ketentuan hukum yang terdapat dalam UU No 11 Tahun 2008 tentang ITE adalah sebagai berikut:

1. Kendala dalam penanganan pidana penyebaran virus komputer *Ransomware wannacry*
 - a. Aspek Penyidik
 - b. Aspek Alat Bukti
 - c. Aspek Fasilitas
 - d. Aspek yurisdiksi
2. Penanganan pidana penyebaran virus komputer *Ransomware wannacry*
 - a. Penanganan Tindakan Hukum

Perlu ada suatu tindakan yang efektif untuk mengantisipasi kegiatan-kegiatan pengembangan virus computer secara preventif agar tidak mengancam terus menerus dan mengganggu para pemakai computer. Bertambahnya jenis-jenis virus computer saat ini akan berdampak semakin meresahkan dan menjadi ancaman bagi pengguna computer. Ancaman virus computer saat ini belum terasa secara signifikan dibuktikan belum banyaknya complain dari mereka yang terinfeksi, karena masih dapat ditanggulangi dengan anti virus yang dijual dipasar. Tetapi tidak menutup kemungkinan pada titik waktu tertentu akan muncul virus yang dapat membahayakan pengguna computer. Perlu segera ditindaklanjuti agar tidak semakin tambah membahayakan, khususnya bagi seluruh profesi dibidang komputer harus bersatu untuk mengantisifasinya dengan didampingi pemerintah sebagai regulasi kebijakan yang telah ditentukan arah dan aturan yang jelas.

Kenyataan yang ada mengenai virus komputer jika di kaitkan dengan UU ITE maka virus komputer keberadaannya banyak melanggar beberapa pasal, yaitu ;

- 1) Memanfaatkan teknologi dalam bidang informasi pada dasarnya dilaksanakan sesuai dengan asas manfaat dan juga iktikad yang baik, tetapi kenyataannya virus komputer dibuat dan dikembangkan untuk mengganggu keamanan dan kenyamanan pengguna komputer yang artinya pembuat program virus tidak memiliki iktikad baik.
- 2) Memanfaatkan kemajuan teknologi informasi dengan melaksanakan tujuan mencerdaskan kehidupan berbagai bangsa tetapi keberadaan virus komputer malah menularkan mental negatif.
- 3) Meningkatkan efektifitas dan efisiensi pelayanan publik, munculnya virus pada komputer layanan public akan menghambat proses dari aktifitas layanan yaitu virus dapat membuat lambat akses komputer atau lebih ekstrimnya lagi dapat menghilangkan data.
- 4) Membuka seluas-luasnya terhadap kesempatan kepada setiap orang untuk memajukan serta pemanfaatan teknologi informasi dan bertanggung jawab. Program virus jelas tidak bertanggung jawab karena program yang dibuat untuk mengganggu orang lain.
- 5) Memberikan rasa aman bagi pengguna hal ini bertolak belakang dengan misi pembuat virus itu sendiri jika kita lihat dari cara pandang dari orang yang membuat virus jika dikaitkan dengan UU ITE yaitu :
 - a) Seseorang dengan cara sengaja dan tanpa hak atau melanggar ketentuan hukum dengan cara mengurangi, mengubah, merusak, menambah, atau memindahkan, dan juga menyembunyikan adanya suatu informasi elektronik dan atau dokumen elektronik yang menjadi milik public atau milik orang lain. Jika kita cermati pasal ini dimana sifat virus-virus tertentu dapat menambah file-file gak jelas, mengubah data, menghilangkan file tertentu, yang akhirnya bertujuan merusak informasi jelas ini masuk pasal 32.
 - b) Hampir semua virus mengganggu system elektronik hingga mengurangi akses kinerja ini artinya orang yang membuat program virus hampir mayoritas bertujuan mengganggu aktifitas system computer dan elektronik. Dan dengan UU ITE pada pasal 38 sampai dengan pasal 43 pemerintah memiliki kepedulian terhadap perlindungan masyarakat kaitan dengan penggunaan teknologi informasi. Yaitu mengatur mulai dari pengajuan gugatan dengan cara perwakilan kepada pihak penyelenggara sistem informasi dan memanfaatkan perkembangan teknologi informasi dengan akibat yang ditimbulkan yaitu kerugian dalam masyarakat, hal ini sesuai sesuai ketentuan undang-undang

sampai mengatur mengenai penerimaan laporan adanya tindak pidana kaitan dengan penggunaan teknologi informasi. Meskipun kaitan antara uu ITE dan keberadaan virus komputer belum secara tersurat mengatur tentang keberadaan virus komputer. Dan jika mengamati uu ITE pemerintah belum secara aktif untuk menyingkapi para pembuat virus apakah kategori tindak kriminal atau bukan

b. Penanganan Terhadap komputer

Terhadap penanganan terhadap komputer tersebut, maka pemerintah merumuskan berbagai langkah virus *Ransomware Wannacry* yaitu dengan cara

- 1) Mencabut LAN dan mematikan jaringan Wi-Fi pada komputer untuk mencegah infeksi pada komputer terhadap virus *Ransomware Wannacry*
- 2) *Meng-Up date* security Windows yaitu memasang komputer dengan *patch* MS17-010.
- 3) Fungsi SMB v1 tidak diaktifkan dan memblokir port 139 / 445 serta 3389.
- 4) Memperbarui *anti virus Ransomware Wannacry*
- 5) File yang penting di komputer dibackup di tempat lain yang tidak terhubung secara langsung dalam internet atau jaringan lainnya.

c. Penanganan Pribadi

Terhadap penanganan pribadi dapat dilakukan dengan cara :

- 1) Komputer tidak secara langsung dinyalakan dan menyambung komputer secara langsung ke internet atau LAN.
- 2) Mem-*backup* terlebih dahulu data penting dan *update Windows*, mengingat yang dieksploitasi oleh virus *Ransomware Wannacry* biasanya sudah ditutup *Microsoft*, namun demikian belum semua

komputer telah memasang *update software* tersebut.

PENUTUP

Kesimpulan

1. Penyebaran virus *ransomware wannacry* adalah suatu tindak pidana yang diatur UU ITE pada pasal 32, pasal 33 dan juga pasal 36. Perbuatan *Ransomware Wannacry* telah terpenuhi unsur subjektif dan juga unsur dipidana delapan tahun dan/atau denda dua miliar rupiah paling banyak. Berdasarkan Pasal 49 UU ITE orang melanggar Pasal 33, dapat selama 10 tahun dan/atau denda sepuluh milyar.
2. Kebijakan hukum penyebaran *Ransomware wannacry* dengan penuntutan secara hukum yang memperhatikan yurisdiksi serta hukum tiap negara, yang satu sama lain berbeda, dan adanya kesulitan lain karena terjadi di dunia maya. Pelaku penyebaran *Ransomwarewannacry* dikenakan Pasal 46 ayat (2) juncto Pasal 30 ayat (2) UU ITE yang mengatur dan menjelaskan tentang berbagai tindakan bagi pelanggaran hukum dalam penyalahgunaan Teknologi Informasi.

Saran

1. Pemerintah hendaknya terus mengkaji ketentuan dalam UU ITE perlu terus disesuaikan mengikuti perkembangan teknologi yang ada.
2. Perlunya segera dilakukan tindakan antisipasi jangan sampai berlarut-larut hingga terjadi hal yang tidak terduga seperti adanya penyebaran virus *Ransomware wannacry* yang dapat merugikan masyarakat. Maka perlu ada suatu inisiatif dari semua unsur yang terlibat secara profesional yang bekerja dengan media komputer sebagai alat dalam bekerja untuk membahas secara konsisten memecahkan masalah ini.

DAFTAR PUSTAKA

- [1] Abdul Kadir M, *Hukum dan Penelitian Hukum*. PT. Citra Aditya Bakti, Bandung, 2004.
- [2] Satria, BR. Cracking Dalam Perspektif UU No. 11/2008 tentang ITE dan Hukum Pidana, *Skripsi*, Fak. Syari'ah dan Hukum Univ. Islam Sunan Kalijaga, Yogyakarta, 2016
- [3] Sutopo, HB. *Metodologi Penelitian Kualitatif*. UNS Press, Surakarta, 2002
- [4] Widodo, *Aspek Hukum Pidana Kejahatan Mayantara*, Aswaja Pressindo, Yogyakarta
- [5] <https://filemoch.blogspot.com/2017/05/cara-menangkal-virus-ransomware.html>, diakses tanggal 15 Mei 2018 pukul 18.58 WIB