Proceeding of Conference on Law and Social Studies
http://prosiding.unipma.ac.id/index.php/COLaS
Held in Madiun on August 6th 2021
e-ISSN: 2798-0103

Pertanggungjawaban Pidana *Cybercrime* dalam Penyebaran Virus dan Trojan Horse berdasarkan Undang-Undang Informasi dan Transaksi Elektronik

Ghalib Akbar [1], Krista yitawati[2]
FH Universitas Merdeka Madiun, ghalibakbar81@gmail.com
FH Universitas Merdeka Madiun, krista@unmer-madiun.ac.id

Abstrak

Kejahatan dunia maya atau kejahatan di dunia maya memiliki banyak bentuk,peretasan adalah kejahatan pertama, juga dilihat dari aspek teknis, peretasan memiliki kelebihan, pertama orang yang melakukan peretasan harus bisa melakukan bentuk lain *cybercrime* dengan kemampuan masuk ke sistem komputer dan kemudian merusak sistem itu. Kedua, secara teknis kualitas hasil peretasan dari peretasan itu lebih serius jika dibandingkan dengan bentuk-bentuk cybercrime lainnya, seperti Virus dan Trojan Horse. Tujuan dilakukannya penelitian ini yaitu untuk mengetahui bagaimana pengaturan tindak pidana virus dan trojan horse dan bagaimana tanggung jawab pidana terhadap pelaku penyebaran virus dan trojan horse berdasarkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pendekatan penelitian menggunakan yuridis normatif, data yang dikumpulkan baik data primer maupun sekunder ditelaah oleh kajian yuridis dengan tidak menghilangkan unsur non yuridis lainnya. Pendekatan ini mengarah pada hukum dan perilaku pelaku yang salah menggunakan teknologi dan informasi sebagai dukungan kongkrit untuk memperkuat analisis yuridis tersebut. Hasil penelitian menunjukkan bahwa peran penegak hukum dalam menangani kejahatan Virus dan Trojan Horse yang dilakukan selama ini masih sangat minim. Hal ini menyebabkan banyak hambatan yang ditemukan oleh penegak hukum, hambatan hukum yang ada, kendala penyelidikan, dan perlawanan masyarakat itu sendiri. Yang paling penting adalah verifikasi sistem untuk mengatasi kejahatan Virus dan Trojan Horse melalui perbaikan atau revisi baru hukum yang ada, apakah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Peraturan lain yang terkait dengan Kejahatan Virus dan Trojan Horse.

Kata kunci: Tindakan kriminal, Cyberspace, Virus, dan Trojan Horse

Abstract

Cybercrime or cybercrime has many forms, hacking is the first crime, also seen from the technical aspect, hacking has advantages, first the person who does the hacking must be able to carry out other forms of cybercrime with the ability to enter a computer system and then damage the system. Second, technically the quality of the hacking results from the hack is more serious when compared to other forms of cybercrime, such as Viruses and Trojan Horses. The purpose of this research is to find out how to regulate the crime of viruses and Trojan horses and how the criminal responsibility for the perpetrators of spreading viruses and Trojan horses is based on Law Number 11 of 2008 concerning Information and Electronic Transactions. The research approach uses normative juridical, data collected both primary and secondary data are reviewed by juridical studies without eliminating other non-juridical elements. This approach leads to the law and behavior of wrongdoers using technology and information as concrete support to strengthen the juridical analysis. The results show that the role of law enforcement in dealing with Virus and Trojan Horse crimes that have been carried out so far is still very minimal. This causes many obstacles found by law enforcement, existing legal barriers, investigation obstacles, and community resistance itself. The most important thing is the verification of the system to overcome the crime of Viruses and Trojan Horses through improvements or new revisions to existing laws, whether Law Number 11 of 2008 concerning Information and Electronic Transactions and other Regulations related to Virus and Trojan Horse Crimes.

Keywords*: Criminal Act, Cyberspace, Viruses, and The Trojan Horse*

I. Pendahuluan

Teknologi Informasi (selanjutnya disebut TI) berkembang dengan pesat menyebabkan banyak perubahan pada segi kehidupan sosial masyarakat baik ekonomi bisnis, sosial politik, sistem komunikasi dan interaksi, pendidikan, termasuk juga hukum. *Currently, the industrial era 4.0 still goes on in the various aspects of life, including the business sector. The business actors respond quickly by competing in making changes of business concepts from that which is conventional (offline) to that which is digital (online) to face the ever-tightening business competition.* (Dimas Pramodya Dwipayana, 2020) TI internet pada awalnya dikembangkan semata-mata untuk memudahkan manusia dalam menjalankan rutinitas kehidupannya. *Au ce moment, dans toutes les lignes de la vie moderne, la machine intelligente ou l'intelligence artificielle a un grand rôle qui risque à changer les rôles des humains dans beaucoup de secteurs d'occupation.* (Sofyan Wimbo Agung Pradnyawan, 2020) Internet, sesungguhnya merupakan suatu jaringan besar yang

terdiri dari jumlah besar jaringan komputer dari seluruh dunia saling terhubung antara satu dengan yang lainnya. Masyarakat penggunanya kemudian dikenal dengan istilah *global community* dan mereka seakan-akan mendapati satu dunia baru yang dinamakan dunia maya (*cyber space*) (Nara Amelia, 2013).

Cyber Crime merupakan tindak kriminal yang dilakukan dengan menggunakan teknologi komputer sebagai alat kejahatan utama. *Cybercrime* yaitu kejahatan yang memanfaatkan perkembangan teknologi komputer khususnya internet. *Cybercrime* didefinisikan sebagai perbuatan melanggar hukum yang memanfaatkan teknologi komputer yang berbasis pada kecanggihan perkembangan teknologi internet (Sofwan Jannah, 2012). Selanjutnya dalam catatan ini saya memakai *cyber crime* sebagai tindak pidana TI dalam kaitannya dengan tindak pidana yang tidak diatur secara khusus dalam Kitab Undang-Undang Hukum Pidana (selanjutnya disebut KUHP). Kejahatan yang seringkali berhubungan dengan internet antara lain penyebaran Virus dan Trojan Horse sebagai kejahatan yang dapat dilakukan melalui kecanggihan TI dan komunikasi dalam hal ini melalui penyalahgunaan media internet. The Trojan Horse, diartikan sebagai suatu prosedur untuk menambah, mengurangi atau mengubah instruksi pada sebuah program, sehingga program tersebut selain menjalankan tugas yang sebenarnya juga akan melaksanakan tugas lain yang tidak sah (Muhammad Yustisia, 2010). Tindakan ini dapat dikategorikan sebagai tindak pidana penggelapan (Pasal 372 dan 374 KUHP). Ketika berhadapan dengan tindak pidana penyebaran Virus dan Trojan Horse menimbulkan masalah baru yang akan muncul, karena dalam hukum acara pidana yang berlaku tidak diatur mengenai alat bukti elektronik. Namun demikian, saat ini telah berlaku Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (selanjutnya disebut UU ITE) yang didalamnya mengatur berbagai aktifitas yang dilakukan dan terjadi di dunia maya, termasuk pelanggaran hukum yang terjadi. Salah satu pelanggaran hukum tersebut adalah penyebaran Virus dan Trojan Horse. UU ITE telah mengatur tentang pembuktian yang menyangkut TI termasuk internet, tetapi masih banyak kendala-kendala dalam kenyataannya sehingga seringkali pelaku penyebaran Virus dan Trojan Horse melalui internet lolos dari jeratan hukum (Agus Tedyyana, 2018). UU ITE ini mempunyai 13 (tiga belas) Bab dan 54 (lima puluh empat) Pasal di dalamnya yang mengatur berbagai kegiatan di dunia siber serta menerapkan azas-azas Ekstra Teritorial. Azas Kepastian Hukum, Azas Manfaat, Azas Kehati-hatian, Azas Itikad Baik dan Azas Netral Teknologi (Raida L. Tobing, 2010).

Pemanfaatan Internet tidak hanya membawa dampak positif, tapi juga dampak negatif. Salah satu dampak negatif dari pemanfaatan internet adalah penyebaran Virus dan Trojan Horse yang menjadi perhatian serius Pemerintah di berbagai Negara termasuk Indonesia.

Kejahatan ini merupakan salah satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negatif sangat luas bagi seluruh bidang kehidupan modern saat ini. Kekhawatiran demikian terungkap pula dalam makalah "*cyber crime*" yang disampaikan oleh Information *Technology Association of Canada* (ITAC) pada "*International Information Industry Congress* (IIC) 2000 *Mellenium Congress*" di quebec pada tanggal 19 September 2000, yang menyatakan bahwa "*cyber crime is a real and growing threat to economic and social development around af human life and so can electronically enabled crime*" (Arief Muliawan, 2010). Pada dasarnya masyarakat Indonesia harus mendapat perlindungan hukum dari dampak yang diakibatkan oleh berbagai kejahatan yang terjadi baik secara nyata maupun di dunia maya, termasuk tindak pidana penyebaran Virus dan Trojan Horse melalui internet.

Perlindungan terhadap masyarakat tersebut terkandung dalam Pembukaan Undang-Undang Dasar 1945 alinea keempat yang menyebutkan bahwa:

> "Kemudian daripada itu untuk membentuk suatu Pemerintah Negara Indonesia yang melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia dan untuk memajukan kesejahteraan umum".

Amanat dalam alinea keempat Pembukaan Undang-Undang Dasar 1945 tersebut merupakan konsekuensi hukum yang mengharuskan pemerintah tidak hanya melaksanakan tugas pemerintahan saja, melainkan juga kesejahteraan sosial melalui pembangunan nasional. Selain itu juga merupakan landasan perlindungan hukum kepada masyarakat, karena kata "melindungi" mengandung asas perlindungan hukum bagi segenap bangsa Indonesia untuk mencapai keadilan. Pada dasarnya, Indonesia telah berusaha mengantisipasi adanya dampak dari tindak pidana dunia maya terhadap masyarakat, melalui beberapa tindakan baik secara preventif, antisipatif maupun secara represif.

Proses penegakan hukum di Indonesia sampai saat ini masih terus dilakukan. Kerjasama antara sesama penegak hukum (Polisi, Jaksa, Hakim dan Advokat) terus dijalin dalam mengatasi semua permasalahan hukum baik di bidang perdata, pidana, tata usaha negara dan lingkup peradilan lainnya. Sampai saat ini, tingkat kejahatan di Indonesia terus melaju cepat seiring dengan perkembangan TI dan telekomunikasi yang semakin canggih (Neri Widya Ramailis, 2020). Pesatnya TI dan telekomunikasi ini selain memberikan manfaat bagi masyarakat di satu sisi, sering pula disalahgunakan sehingga menimbulkan perbuatan melawan hukum, tidak terkecuali pada tindak pidana penyebaran Virus dan Trojan Horse melalui internet (Sofwan Jannah, 2012).

Berdasarkan larat belakang masalah diatas maka penulis merumuskan beberapa rumusan masalah sebagai berikut *pertama,* Bagaimana pengaturan tindak pidana virus dan trojan horse dalam Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi

Elektronik? dan *kedua,* Bagaimana tanggung jawab pidana terhadap pelaku penyebaran virus dan trojan horse berdasarkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik?

II. Metode Penelitian

Bentuk penelitian ini adalah yuridis normatif, yaitu dengan menelaah norma hukum tertulis disandingkan dengan pokok permasalahan yang menjadi pembahasan dalam penelitian ini (Zulfi Diane Zaini, 2011). Data yang digunakan dalam penelitian ini, yaitu data sekunder melalui bahan-bahan kepustakaan, teori-teori yang diambil dari berbagai literatur hukum, Undang-Undang Dasar Negara Republik Indonesia 1945 serta Peraturan Perundang-undangan lainnya. (Nizam Zakka Arrizal, 2020)

Peneliti menggunakan alat pengumpulan data berupa studi dokumen dan teori serta peraturan-peraturan yang ada.

Metode analisis data yang digunakan dalam mengolah data yang berkaitan dengan penelitian ini adalah metode kualitatif karena pengolahan data tidak dilakukan dengan mengukur data sekunder terkait, tetapi menganalisis secara deskriptif data tersebut. Pada pendekatan kualitatif, tata cara penelitian menghasilkan data deskriptif analitis (Jonathan. R. Raco, 2010).

III. Pembahasan

1. Pengaturan Tindak Pidana Virus dan Trojan Horse dalam Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik

Berdasarkan Pasal 1 ayat (1) UU ITE, yang dimaksud dengan informasi elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data interchange (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy, atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya. Selain itu, yang dimaksud dengan sistem elektronik menurut Pasal 1 ayat (5) adalah serangkaian perangkat atau prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan dan/atau menyebarkan informasi elektronik.

Penafsiran dengan metode yang sama terhadap KUHP sebelum ada UU ITE perlu dilakukan tentang pengertian dalam UU ITE sehingga terdapat batasan dan kejelasan makna agar tidak menimbulkan celah hukum (*loopholes*), yaitu: “Melakukan tindakan apapun yang berakibat terganggunya sistem elektronik”. Pasal 33 UU ITE menyebutkan bahwa:

> “Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apapun yang berakibat terganggunya Sistem

Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya".

Sehubungan dengan hal itu, setiap orang yang melakukan tindakan apapun yang berakibat terganggunya sistem elektronik karena banyak kegiatan-kegiatan di dunia nyata yang secara nyata tidak ada hubungannya dengan *cybercrime* sehingga kalimat dari pasal ini kegiatan penyebaran Virus dapat dikategorikan sebagi suatu tindak kejahatan (Dheny Wahyudi, 2013). Pada kasus penyebaran Virus dan Trojan Horse ini untuk membuktikannya, dapat dipakai semua alat bukti berbentuk informasi dan/atau dokumen elektronik, namun hal tersebut dapat dijadikan alat bukti sebagaimana ditentukan dalam Pasal 5 ayat (1) UU ITE yang berbunyi :

"Informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah".

Dan Pasal 5 ayat (2) UU ITE juga menegaskan bahwa:

"Informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat 1 merupakan perluasan dari alat bukti yang sah sesuai dengan hukum acara yang berlaku di Indonesia".

Dengan demikian, alat bukti yang digunakan hakim untuk menjatuhkan putusan pada perkara pidana, dapat diperluas menjadi 6 (enam) dari 5 (lima) ketentuan alat bukti sebagaimana telah diatur dalam Pasal 184 KUHAP, yaitu bahwa alat bukti yang sah adalah :

a. Keterangan saksi;
b. Keterangan ahli;
c. Surat;
d. Petunjuk;
e. Keterangan terdakwa;
f. Alat bukti menurut Pasal 5 ayat (1) dan ayat (2) UU ITE.

Ketentuan mengenai alat bukti di atas merupakan ketentuan hukum acara pidana yang bersifat memaksa (*dwingen recht*), artinya semua jenis alat bukti yang telah di atur dalam pasal tersebut tidak dapat ditambah atau dikurangi (Debby Natalia Ang, 2015). Secara umum terdapat beberapa teori mengenai sistem pembuktian yakni:

a. *Conviction in time Theory*, yaitu sistem pembuktian yang menyatakan bahwa salah tidaknya seorang terdakwa semata-mata ditentukan oleh penilaian keyakinan hakim. Keyakinan hakim ini dapat diperoleh melalui alat-alat bukti yang diajukan Keterangan Ahli dalam persidangan;
b. *Conviction Raisonee Theory*, merupakan sistem pembuktian berdasarkan keyakinan hakim untuk menentukan salah tidaknya terdakwa, namun dalam sistem ini keyakinan hakim dibatasi dan harus didasari dengan alasan-alasan yang jelas dan dapat diterima yang wajib diuraikan dalam putusannya, sesuai yang diuraikan juga oleh Keterangan Ahli dalam persidangan;

c. Teori Pembuktian Menurut Undang-Undang secara Positif, merupakan pembuktian yang berlatar belakang sistem pembuktian berdasarkan keyakinan atau *Conviction in time Theory*. Pembuktian pada sistem ini didasari dengan alat-alat bukti yang sah yang telah di tetapkan oleh undang-undang disertai keyakinan hakim dalam menentukan salah tidaknya terdakwa;
d. Teori Pembuktian menurut Undang-Undang Secara Negatif (*Negatief Wettelijkestelsel*), merupakan sistem pembuktian yang menggunakan teori perpaduan antara sistem pembuktian undang-undang secara positif dengan sistem pembuktian menurut keyakinan atau *Conviction in time Theory*. Rumusan teori ini adalah bahwa salah tidaknya seorang terdakwa ditentukan oleh keyakinan hakim yang didasarkan pada cara dan dengan alat-alat bukti yang sah menurut undang-undang (Hendri Jayadi Pandiangan, 2017).

Sementara itu, sistem pembuktian yang dianut oleh KUHAP adalah sistem pembuktian menurut undang-undang secara negatif, karena merupakan perpaduan antara sistem pembuktian menurut undang-undang secara positif dengan sistem pembuktian menurut keyakinan atau *Conviction in time Theory*. Hal ini terlihat dari ketentuan Pasal 183 KUHAP yang menegaskan bahwa:

> "Hakim tidak boleh menjatuhkan pidana kepada seseorang kecuali apabila dengan sekurang-kurangnya dua alat bukti yang sah ia memperoleh keyakinan bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukannya."

Berbicara mengenai alat bukti petunjuk, tidak terlepas dari ketentuan Pasal 188 ayat (2) KUHAP yang membatasi kewenangan hakim dalam memperoleh alat bukti petunjuk, yang secara limitatif hanya dapat diperoleh dari :

a. Keterangan saksi;
b. Surat;
c. Keterangan Terdakwa.

Berdasarkan hal tersebut diatas, alat bukti petunjuk hanya dapat diambil dari ketiga alat bukti di atas. Pada umumnya, alat bukti petunjuk baru diperlukan apabila alat bukti lainnya belum mencukupi batas minimum pembuktian yang diatur dalam Pasal 183 KUHAP di atas. Dengan demikian, alat bukti petunjuk merupakan alat bukti yang bergantung pada alat bukti lainnya yakni alat bukti saksi, surat dan keterangan terdakwa. Alat bukti petunjuk memiliki kekuatan pembuktian yang sama dengan alat bukti yang lain, namun hakim tidak terikat atas kebenaran persesuaian yang diwujudkan oleh petunjuk, sehingga hakim bebas untuk menilai dan mempergunakannya dalam upaya pembuktian (Hendri Jayadi Pandiangan, 2017). Selain itu, petunjuk sebagai alat bukti tidak dapat berdiri sendiri membuktikan kesalahan terdakwa, karena hakim tetap terikat pada batas minimum pembuktian sesuai ketentuan Pasal 183 KUHAP.

Informasi elektronik atau dokumen elektronik sebagai alat bukti, yang merupakan perluasan dari alat bukti surat sebagai bahan untuk dijadikan petunjuk bagi hakim dalam membuktikan suatu perkara termasuk kasus penyebaran Virus dan Trojan Horse yang telah diuraikan pada bagian sebelumnya. *Cyber Crime* yang merupakan suatu upaya memasuki atau menggunakan fasilitas komputer atau jaringan komputer tanpa ijin dan melawan hukum atau tanpa menyebabkan perubahan atau kerusakan pada fasilitas komputer yang dimasuki atau digunakan tersebut atau kejahatan yang dengan menggunakan sarana media elektronik internet (merupakan kejahatan dunia maya) atau kejahatan dibidang komputer dengan secara illegal (Suharyo, 2010). Terdapat definisi yang lain yaitu sebagai kejahatan komputer ditujukan kepada sistem atau jaringan komputer, yang mencakup segala bentuk baru kejahatan yang menggunakan bantuan sarana media elektronik internet (Sofwan Jannah, *OpCit*). Dengan demikian *Cyber Crime* merupakan suatu tindak kejahatan didunia alam maya, yang dianggap bertentangan atau melawan undang-undang yang berlaku, oleh karena untuk menegakkan hukum serta menjamin kepastian hukum di Indonesia perlu adanya *Cyber Law* yaitu hukum yang mengatasi kejahatan siber (kejahatan dunia maya melalui jaringan internet).

Teknologi informasi menyentuh setiap aspek kehidupan modern dan tidak menutup kemungkinan dapat menimbulkan kejahatan dalam dunia maya. Salah satu kejahatan di dunia maya (*cyber crime*) ini adalah penyebaran Virus dan Trojan Horse. Virus yang merupakan suatu program komputer yang menduplikasi atau menggandakan diri dengan menyisipkan salinannya ke dalam media penyimpanan dokumen serta ke dalam jaringan komputer secara diam-diam tanpa sepengetahuan pengguna komputer tersebut, mempunyai efek sangat beragam mulai dari munculnya pesan-pesan aneh, sampai pada tahap merusak dokumen atau file dan bahkan dapat merusak jaringan komputer itu sendiri.

Virus komputer ini berasal dari penciptaan pengguna komputer yang dengan sengaja menyebarkan virus tersebut ke seluruh dunia. Virus komputer yang dimaksud sangat beragam dengan nama tersendiri dan daya rusak tersendiri pula. Trojan Horse atau Kuda Troya atau yang lebih dikenal sebagai Trojan dalam keamanan komputer merujuk kepada sebuah bentuk perangkat lunak yang mencurigakan (*maliciousso*ftware/ *malware*) yang dapat merusak sebuah sistem atau. Tujuan dari Trojan Horse adalah memperoleh informasi dari target (password, kebiasaan user yang tercatat dalam sistem log, dan data), serta mengendalikan target (memperoleh hak akses pada target). Trojan Horse berbeda dengan perangkat lunak mencurigakan lainnya seperti virus komputer atau worm karena Trojan Horse bersifat "*stealth*" (siluman dan tidak terlihat) dalam operasinya dan seringkali berbentuk seolah-olah program tersebut merupakan program baik-baik, sementara virus komputer atau

worm bertindak lebih agresif dengan merusak sistem atau membuat sistem menjadi crash dan Trojan Horse dikendalikan dari komputer lain (*computer attacker*) (Lisda Juliana Pangaribuan, 2013).

Penggunaan istilah Trojan Horse dimaksudkan untuk menyusupkan kode-kode mencurigakan dan merusak di dalam sebuah program baik-baik dan berguna; seperti halnya dalam Perang Troya, para prajurit Sparta bersembunyi di dalam Kuda Troya yang ditujukan sebagai pengabdian kepada Raja Poseidon. Kuda Troya tersebut menurut para petinggi Troya dianggap tidak berbahaya, dan diijinkan masuk ke dalam benteng Troya yang tidak dapat ditembus oleh para prajurit Yunani selama kurang lebih 10 perang Troya bergejolak). Kebanyakan Trojan Horse saat ini berupa sebuah berkas yang dapat dieksekusi (*.EXE atau *.COM dalam sistem operasi Windows dan DOS atau program dengan nama yang sering dieksekusi dalam sistem operasi UNIX, seperti ls, cat, dan lain-lain) yang dimasukkan ke dalam sistem yang ditembus oleh seorang cracker untuk mencuri data yang penting bagi pengguna (password, data kartu kredit, dan lain-lain (Lisda Juliana Pangaribuan, 2013).

Trojan Horse juga dapat menginfeksi sistem ketika pengguna mengunduh aplikasi (seringnya berupa game komputer) dari sumber yang tidak dapat dipercayai dalam jaringan internet. Aplikasi-aplikasi tersebut dapat memiliki kode Trojan Horse yang diintegrasikan di dalam dirinya dan mengijinkan seorang cracker untuk mengacak-acak sistem yang bersangkutan.

2. Tanggung Jawab Pidana terhadap Pelaku Penyebaran Virus dan Trojan Horse Berdasarkan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.

Ada beberapa hal yang dapat dilakukan terhadap pelaku penyebaran virus dan Trojan Horse ini, yakni: pendekatan teknologi, pendekatan budaya-etika dan pendekatan hukum (Renny N.S. Koloay, 2016). Untuk mengatasi gangguan keamanan, pendekatan teknologi mutlak untuk dilakukan, karena tanpa suatu pengamanan melalui teknologi tertentu, maka jaringan akan mudah disusupi, diintersepsi atau diakses secara illegal dan tanpa hak. Pada ruang *cyber* pelaku pelanggaran seringkali menjadi sulit untuk dijerat hukum, karena tidak terpenuhinya unsur-unsur suatu ketentuan hukum, dalam hal ini berhubungan dengan masalah pembuktian. Selain itu, seringkali pengadilan di Indonesia tidak memiliki yurisdiksi terhadap pelaku dan perbuatan hukum yang terjadi, mengingat pelanggaran hukum ini bersifat transnasional yang akibat hukumnya memiliki implikasi hukum di Indonesia.

Berdasarkan hukum internasional, terdapat tiga macam yurisdiksi yakni: yurisdiksi untuk menetapkan undang-undang (*The Jurisdiction to prescribe*), yurisdiksi untuk penegakan hukum (*The Jurisdiction to*

enforce), dan yurisdiksi untuk menuntut (*The Jurisdiction to adjudicate*) (Dian Khoreanita Pratiwi, 2017). Berbicara mengenai *cyber spamming* sebagai kejahatan transnasional erat kaitannya dengan beberapa yurisdiksi yaitu yurisdiksi untuk menetapkan undang-undang (*The Jurisdiction to Prescribe*), yurisdiksi untuk menghukum (*The Juridicate to Enforce*) dan yurisdiksi untuk menuntut (*The Jurisdiction Adjudicate*). Pada *The Jurisdiction to Adjudicate* terdapat beberapa asas yang dikenal dalam menentukan hukum yang berlaku yaitu:

a. Asas *Subjective Territorial* yaitu berlaku hukum yang menekankan berdasarkan bahwa keberlakuan hukum ditentukan berdasarkan tempat pembuatan dan penyelesaian tindak pidana di lakukan di Negara lain;
b. Asas *Objective Territorial* yang menyatakan bahwa hukum yang berlaku adalah hukum dimana akibat utama perbuatan itu terjadi dan memberikan dampak yang sangat merugikan bagi Negara yang bersangkutan;
c. Asas *Active Nationality* yang menentukan bahwa Negara memiliki yurisdiksi untuk menentukan hukum berdasarkan kewarganegaraan pelaku;
d. Asas *Passive Nationality* adalah hukum berlaku berdasarkan kewarganegaraan korban;
e. Asas *Protective Principle* adalah berlakunya berdasarkan atas keinginan Negara untuk melindungi kepentingan Negara dari kejahatan yang dilakukan di luar wilayahya, dalam hal ini digunakan apabila korban adalah Negara atau pemerintahan;
f. Asas *Protective Principle* adalah berlakunya berdasarkan atas keinginan Negara untuk melindungi kepentingan Negara dari kejahatan yang dilakukan di luar wilayahnya, dalam hal ini digunakan apabila korban adalah Negara atau pemerintahan;
g. Asas *Universality* yang pada mulanya menentukan bahwa setiap Negara berhak untuk menangkap dan menghukum para pelaku (*cybercrime*) kemudian diperluas sampai pada kejahatan terhadap kemanusiaan, dan berlaku untuk lintas Negara terhadap kejahatan yang diangggap sangat serius seperti pembajakan dan terorisme (*crime against humanity*) (Yuliana Surya Galih, 2019).

Tindak pidana penyebaran Virus dan Trojan Horse dimungkinkan melibatkan lebih dari satu sistem atau menyangkut sistem hukum beberapa negara, sehingga dapat dikategorikan sebagai kejahatan transnasional. Pada praktiknya terdapat banyak faktor yang menyebabkan adanya kepentingan lebih dari satu negara dalam suatu kejahatan, baik pelakunya, korbannya, tempat terjadinya kejahatan atau perpaduan unsur-unsur tersebut. Tindak pidana penyebaran Virus dan Trojan Horse dapat melibatkan orang-orang dari berbagai negara, menjadikan sebagai kejahatan transnasional, sehingga dalam proses

penegakan hukumnya, harus pula memperhatikan jalinan kerjasama antara kepolisian Indonesia dengan negara-negara lain.

Berbicara mengenai *cyber spamming* sebagai kejahatan transnasional erat kaitannya dengan beberapa yurisdiksi yaitu, yurisdiksi untuk menetapkan undang-undang (*The Juridiction to Prescribe*), yurisdiksi untuk menghukum (*The Juridicate to Enforce*) dan yurisdiksi untuk menuntut (*The Jurisdiction to Adjudicate*). Dengan demikian, tindakan hukum yang dapat dilakukan terhadap pelaku penyebaran Virus dan Trojan Horse harus dilakukan sesuai yurisdiksinya dengan memperhatikan hokum yang berlaku. Apabila telah terbukti bahwa penyebaran Virus melalui pengiriman email termasuk perbuatan yang dilarang sebagaimana diatur dalam Pasal 33 UU ITE, maka pelaku dapat dijerat dengan ketentuan ancaman pidana pada Pasal 49 UU ITE yang berbunyi:

> "Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 33, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp. 10.000.000.000,00 (sepuluh miliar rupiah)."

Apabila telah terbukti bahwa penyebaran Trojan Horse melalui pengiriman email termasuk perbuatan yang dilarang sebagaimana diatur dalam Pasal 30 ayat (2) UU ITE, maka pelaku dapat dijerat dengan ketentuan ancaman pidana pada Pasal 46 ayat (2) UU ITE yang berbunyi:

> "Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp.700.000.000,00 (tujuh ratus juta rupiah)."

Ketentuan tersebut sudah sesuai dengan tindak pidana penyebaran Virus dan Trojan Horse, mengingat cakupan wilayah penyebarannya yang transnasional serta dampak kerugian yang ditimbulkan Virus secara umum yakni dapat menyebabkan antara lain: loading start sistem operasi Windows (98, XP, Vista, Seven, dll) menjadi lambat, terdapat file yang tidak dapat dibuka (muncul pesan error), bahkan ada file yang hilang meski telah disimpan di Hard disk dan media penyimpanan lain seperti Disket, Flashdisk, Hard Disk External, dll. Sedangkan dampak kerugian yang ditimbulkan Trojan Horse secara umum yakni dapat menyebabkan antara lain: penyusupan pada data log history user computer dan pengintaian terhadap data/dokumen dengan extension*.doc, *.xlx, *.txt; dimana pada umumnya user menyimpan data user name maupun password untuk akses e-banking, dan akses sebagai member dari sebuah toko online atau website jual beli (www.jual beli.com, www.berniaga.com, www.kaskus.co.id, dll), komputer beroperasi dengan lambat, terkadang ada file yang tidak dapat dibuka bahkan hilang dari komputer dan media penyimpanan data lainnya (Petrus Dwi Ananto, 2018). Di Indonesia sendiri diperkirakan setidaknya

ada 1 (satu) dari 3 (tiga) komputer/laptop pasti telah terinfeksi virus / Trojan Horse (terutama komputer/laptop yang program anti virusnya tidak rutin update virus definition secara otomatis dan periodik), sehingga ancaman pidana tersebut diatas cukup berat bagi pelakunya. Sehingga tidak perlu ada hukuman minimal dari ancaman pidana penjara dan/atau denda pada Pasal 49 dan Pasal 46 ayat (2) UU ITE, karena dapat dinilai bahwa ancaman pidana tersebut diatas cukup setimpal bagi pelakunya.

IV. Simpulan dan Saran

Pertanggungjawaban Perbuatan penyebaran Virus dan Trojan Horse melalui email merupakan salah satu perbuatan yang dilarang sebagaimana diatur dalam UU ITE, karena dalam hal ini email dianggap sebagai informasi dan/atau dokumen elektronik yang dapat dijadikan salah satu alat bukti sebagaimana diatur dalam pasal 5 ayat (1) dan (2) UU ITE. Selain itu, email dapat pula dianggap sebagai alat bukti surat yang selanjutnya dijadikan alat bukti petunjuk sesuai ketentuan Pasal 184 KUHAP. Dengan demikian, tindakan penyebaran Virus dapat dijerat dengan Pasal 33 juncto Pasal 49 UU ITE, sedangkan tindakan penyebaran Trojan Horse dijerat dengan Pasal 30 ayat (2) juncto Pasal 46 ayat (2) UU ITE.

Tindakan hukum yang dapat dilakukan terhadap pelaku penyebaran Virus dan Trojan Horse antara lain dengan tuntutan secara hukum dengan memperhatikan yurisdiksi dan hukum yang berlaku, karena hal ini dimungkinkan pelaku berada di negara yang berbeda dengan negara tempat korban kejahatan ini berada, selain itu, sulit pula menentukan tempat kejadian (locus delicti) karena kejahatan ini terjadi di dunia maya. Namun demikian yurisdiksi dan hukum yang berlaku dapat ditentukan berdasarkan beberapa asas yang berlaku antara lain Asas Subjective Territorial yaitu berlaku hukum berdasarkan tempat pembuatan dan penyelesaian tindak pidana dilakukan di Negara lain, Asas Objective Territorial yaitu hukum yang berlaku adalah akibat utama perbuatan itu terjadi dan memberikan dampak kerugian bagi negara yang bersangkutan. Asas Active Nationality adalah hukum berlaku berdasarkan kewarganegaraan pelaku, Asas Passive Nationality adalah hukum berlaku berdasarkan kewarganegaraan korban, Asas Protective Principle adalah berlakunya berdasarkan atas keinginan negara untuk melindungi kepentingan negara dari kejahatan yang dilakukan di luar wilayahnya dan Asas Universality adalah yang berlaku untuk lintas negara terhadap kejahatan yang dianggap sangat serius seperti pembajakan dan terorisme (crime against humanity). Apabila hukum pidana Indonesia yang berlaku, maka terhadap pelaku penyebaran Virus dan Trojan Horse tersebut dapat dikenakan Pasal 33 dan Pasal 30 ayat (2) UU ITE.

Untuk mengurangi munculnya kejahatan dunia cyber khususnya virus dan trojan horse dapat menegakkan sanksi yang tegas mengenai kejahatan cyber crime di Indonesia, yang harus secara jelas dan tegas menindak pelaku praktik cyber crime. Hendaknya aparat penegak hukum khususnya polisi lebih jeli dan professional dalam proses penyidikan untuk menentukan pelaku dalam jaringan kejahatan dunia digital untuk mendapatkan kepastian hukum dan keadilan bagi masyarakat bagi korban kejahatan dunia cyber

V. Ucapan Terima Kasih

Ucapan terima kasih yang sebesar-besarnya kami sampaikan kepada semua pihak yang terlibat dalam penelitian ini. Terima kasih kepada Fakultas Hukum UNIPMA telah melaksanakan kegiatan COLaS yang kedua, sehingga bias memberikan wadah bagi karya kami.

Daftar Pustaka

Ang, D. N. (2015). Tinjauan Yuridis Terhadap Perluasan Alat Bukti Penyadapan Dalam Tindak Pidana Korupsi. *Lex Crimen*, *4*(1).

Dimas Pramodya Dwipayana. (2020). *Legal Protection For Debtors Of Online Loans*. Legal Standing Jurnal Ilmu Hukum Vol.4 No.1, Maret 2020

Galih, Y. S. (2019). Yurisdiksi Hukum Pidana Dalam Dunia Maya. *Jurnal Ilmiah Galuh Justisi*, *7*(1), 59-74.

Kitab Undang-Undang Hukum Acara Pidana

Kitab Undang-Undang Hukum Pidana

Koloay, R. N. (2016). Perkembangan Hukum Indonesia Berkenaan dengan Teknologi Informasi dan Komunikasi oleh: Renny Ns Koloay. *Jurnal Hukum Unsrat*, *22*(5).

Muliawan, Arief, *Penegakan Hukum Tindak Pidana Informasi dan Transaksi Elektronika (cybercrime)*, disampaikan dalam *seminar sehari dalam rangka sosialisasi Undang-Undang Nomor 11 Tahun 2008 di Medan pada 7 Mei 2010*, Fakultas Hukum, Universitas Medan Area.

Nara, A. (2013). *Pengaturan Ganti Rugi Akibat Penghinaan Di Situs Jejaring Sosial Menurut Hukum Perdata* (Doctoral dissertation, Universitas Pelita Harapan).

Naufal, M. M., & Jannah, H. S. (2012). Penegakan Hukum Cyber Crime Ditinjau dari Hukum Positif dan Hukum Islam. *Al-Mawarid Journal of Islamic Law*, *12*(1), 42565.

Nizam Zakka Arrizal. (2020). *Perlindungan Hukum Sebagai Instrumen Penjaga Muruah Bangsa Indonesia.* Prosiding Seminar Nasional Unhamzah 2020. Artikel Ke 8, Universitas Amir Hamzah: Medan.

Pamungkas, P. D. A. (2018). Analisis Cara Kerja Sistem Infeksi Virus Komputer. *Bina Insani ICT Journal*, *1*(1), 15-40.

Pandiangan, H. J. (2017). Perbedaan Hukum Pembuktian Dalam Perspektif Hukum Acara Pidana Dan Perdata. *to-ra*, *3*(2), 565-582.

Pangaribuan, L. J. (2013). Ancaman Trojan Horse pada Keamanan Komputer. *Jurnal Ilmiah MBP*, *1*(2), 63-76.

Pratiwi, D. K. Pelaksanaan Prinsip Yurisdiksi Universal Mengenai Pemberantasan Kejahatan Perompakan Laut Di Wilayah Indonesia. *Jurnal Selat*, *5*(1), 36-51.

Raco, J. R. (2010). Metode Penelitian Kualitatif Jenis Karakteristik, dan keunggulannya, Jakarta: PT. Raja Grafindo.

Ramailis, N. W. (2020). Cyber Crime Dan Potensi Munculnya Viktimisasi Perempuan Di Era Teknologi Industri 4.0. *Sisi Lain Realita*, *5*(01), 1-20.

Sofyan Wimbo Agung Pradnyawan. (2020). *L'application Des Lois À L'ère De La Société 5.0*. Legal Standing Jurnal Ilmu Hukum Vol.4 No.1, Maret 2020

Suharyo, 2010, *Laporan Penelitian Penerapan Bantuan Timbal Balik Dalam Masalah Pidana Terhadap Kasus-Kasus Cybercrime*, Badan Pembinaan Hukum Nasional Departemen Hukum dan HAM.

Tedyyana, A., & Supria, S. (2018). Perancangan Sistem Pendeteksi Dan Pencegahan Penyebaran Malware Melalui SMS Gateway. *INOVTEK Polbeng-Seri Informatika*, *3*(1), 34-40.

Tobing, Raida L., 2010, *Laporan Akhir Penelitian Hukum tentang Efektifitas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*, Badan Pembinaan Hukum Nasional Kementrian Hukum dan HAM Republik Indonesia.

Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Undang-Undang Dasar Negara Republik Indonesia tahun 1945

Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik

Wahyudi, D. (2013). Perlindungan Hukum Terhadap Korban Kejahatan Cyber Crime Di Indonesia. *Jurnal Ilmu Hukum Jambi*, *4*(1), 43295.

Yustisia, M. (2010). Pembuktian dalam Hukum Pidana Indonesia terhadap Cyber Crime. *Jurnal Hukum Universitas Bandar Lampung* (*UBL*), *2*(5).

Zaini, Z. D. (2011). Implementasi pendekatan yuridis normatif dan pendekatan normatif sosiologis dalam penelitian ilmu hukum. *Pranata Hukum*, *6*(2).