Res Nullius
Law Journal
Fakultas Hukum Universitas Komputer Indonesia
p-ISSN 2656-7261
e-ISSN 2721-4206
Vol. 5 No. 1 Januari 2023

# TINDAKAN HUKUM TERHADAP PELAKU PENYEBARAN VIRUS KOMPUTER MELALUI *E-MAIL* (*CYBER SPAMMING)* BERDASARKAN KETENTUAN TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

***Legal Action Against The Persons Of Computer Virus Spread Through E-Mail (Cyber Spamming) Based On Provisions Regarding Information And Electronic Transactions***

**Hetty Hassanah**
**Fakultas Hukum Universitas Komputer Indonesia**
***hetty.hassanah@email.unikom.ac.id***
Naskah dikirim : 28 Oktober 2022
Naskah diterima untuk diterbitkan : 02 Januari 2023
DOI : 10.34010/rnlj.v%vi%i.8317

***ABSTRACT***

*The purpose of this study is to find out and analyze the legal actions that can be taken against perpetrators of spreading komputer viruses via email (cyber spamming) based on applicable law. The research is descriptive analytical, using a normative juridical approach, through laws and regulations related to information technology, then the data obtained are analyzed in a qualitative juridical manner. The results of the study show that the act of spreading komputer viruses via email (cyber spamming) can be applied to the provisions of Article 30 paragraph (2) in conjunction with Article 46 paragraph (2) of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions, provided that it must be proven that the actions taken by the perpetrators fulfill the subjective and objective elements of the article. The conclusion obtained from this research is that the act of spreading komputer viruses via email (cyber spamming) is a violation of the law as regulated in the Electronic Information and Transaction Law and the perpetrators must be given legal sanctions according to applicable regulations. The impact of this research is that the government must always supervise the development of information technology and violations that occur so that they are always accommodated by existing regulations, besides that the public must always be careful in using internet-based information media.*

*Key Words : Spread of Komputer Viruse; Email; Information Law and Electronic Transactions*

**Abstrak**

Tujuan penelitian ini adalah untuk mengetahui dan menganalisis tentang tindakan hukum yang dapat dilakukan terhadap pelaku penyebaran virus komputer melalui email (*cyber spamming)* berdasarkan hukum yang berlaku. Penelitian yang dilakukan bersifat deskriptif analitis, dengan metode pendekatan yurisis normatif, melalui peraturan perundang-undangan terkait teknologi informasi, selanjutnya data yang diperoleh dianalisis secara yuridis kualitatif. Hasil penelitian menunjukan bahwa terhadap perbuatan penyebaran virus komputer melalui email (*cyber spamming)* dapat diterapkan ketentuan Pasal 30 ayat (2) juncto Pasal 46 ayat (2) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, dengan syarat harus dapat dibuktikan bahwa perbuatan yang dilakukan pelaku memenuhi unsur subjektif dan unsur objektif dari pasal tersebut. Simpulan yang diperoleh dari penelitian ini bahwa perbuatan pelaku penyebaran virus komputer melalui email (*cyber spamming)* ini merupakan salah satu pelanggaran hukum sebagaimana diatur dalam Undang-Undang Informasi dan Transaksi Elektronik dan pelakunya harus diberi sanksi hukum sesuai peraturan yang berlaku. Dampak dari penelitian ini antara lain pemerintah harus selalu melakukan pengawasan terkait perkembangan teknologi informasi dan pelanggaran yang terjadi agar senantiasa terakomodir oleh peraturan yang ada, selain itu masyarakat pun harus selalu berhati-hati dalam menggunakan media informasi yang berbasis internet.

Kata Kunci : Penyebaran Virus Komputer; Email; Undang-Undang Informasi Dan Transaksi Elektronik

Res Nullius
Law Journal
Fakultas Hukum Universitas Komputer Indonesia
p-ISSN 2656-7261
e-ISSN 2721-4206
Vol. 5 No. 1 Januari 2023

## PENDAHULUAN

Perkembangan dunia teknologi informasi dewasa ini telah membawa manusia kepada era globalisasi yang memberikan kebebasan kepada setiap orang di dunia untuk saling bersosialisasi dengan siapapun dan dimanapun mereka berada. Internet merupakan media utama yang dapat digunakan, karena melalui media internet seseorang dapat terhubung dengan teman atau bahkan dengan orang asing yang sama sekali tidak dikenal dan berdomisili di luar negeri. Kemajuan teknologi informasi dan komunikasi telah melahirkan berbagai dampak, baik dampak positif maupun dampak negatif, karena di satu sisi memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, namun di sisi lain menjadi sarana efektif perbuatan melanggar hukum. Teknologi informasi dan komunikasi juga telah mengubah perilaku dan pola hidup masyarakat secara global, dan menyebabkan dunia menjadi tanpa batas (*borderless)*, serta menimbulkan perubahan di berbagai bidang kehidupan. Perkembangan teknologi informasi telah melahirkan beragam jasa di bidang teknologi informasi dan komunikasi dengan berbagai fasilitasnya, dalam hal ini internet merupakan bagian dari kemajuan teknologi informasi tersebut, yang memberi kemudahan dalam berinteraksi tanpa harus berhadapan secara langsung satu sama lain. Perkembangan teknologi informasi berdampak pada revolusi bentuk kejahatan yang konvensional menjadi lebih modern. Jenis kegiatannya mungkin sama, namun dengan media yang berbeda yaitu dalam hal ini internet, suatu kejahatan akan lebih sulit diusut, diproses, dan diadili.

Kejahatan yang seringkali berhubungan dengan internet antara lain penyebaran virus komputer melalui pengiriman *e*-mail (*cyber spamming*) sebagai kejahatan yang dapat dilakukan melalui kecanggihan teknologi informasi dan komunikasi dalam hal ini melalui penyalahgunaan media internet. Kitab Undang-Undang Hukum Pidana (selanjutnya ditulis KUHP) tidak mengatur pelanggaran di atas, sehingga harus diterapkan ketentuan hukum yang mengatur teknologi informasi yaitu Undang-Undang Nomor 19 tahun 2016 tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (selanjutnya ditulis UU ITE). Pada beberapa pemeriksaan kasus yang berbasis teknologi informasi, hakim harus melakukan penemuan hukum sendiri sebagaimana diamanatkan dalam Undang-Undang Nomor 4 Tahun 2004 Tentang Pokok-Pokok Kekuasaan Kehakiman, terkadang hakim pun mengusahakan pemecahannya melalui yurisprudensi, yang merupakan suatu keharusan[1]. Tujuan penelitian ini adalah untuk mengetahui dan menganalisis tentang ketentuan hukum dan tindakan hukum yang dapat dilakukan terhadap pelaku penyebaran virus komputer melalui email (*cyber spamming)* berdasarkan hukum yang berlaku, antara lain UU ITE dan peraturan lain yang terkait.

Penentuan suatu perbuatan sebagai tindak pidana merupakan kebijakan kriminal, yakni adanya usaha yang rasional dari masyarakat untuk menanggulangi kejahatan[2]. Penggunaan hukum pidana untuk penanggulangan kejahatan perlu memperhatikan fungsi hukum pidana yang subsider, yaitu hukum pidana baru digunakan apabila upaya-upaya lainnya diperkirakan kurang memberi hasil yang memuaskan atau kurang sesuai. Akan tetapi kalau hukum pidana akan tetap dilibatkan, maka hendaknya dilihat dalam hubungan keseluruhan politik kriminal

[1] Jan Smith, *Komputer : Suatu Tantangan Baru di Bidang Hukum*, Airlangga University Press, Surabaya, 2012, hlm.58.
[2] Sudarto, *Pembaharuan Hukum Pidana di Indonesia*. Simposium Hukum Pidana Nasional Semarang BPHN dan UNDIP. 2011, Hlm. 14.

Res Nullius
Law Journal
Fakultas Hukum Universitas Komputer Indonesia
p-ISSN 2656-7261
e-ISSN 2721-4206
Vol. 5 No. 1 Januari 2023

atau istilah yang lazim digunakan dalam kongres PBB IV 1970 adalah *planning for social defence* yang harus merupakan bagian yang integral dari rencana pembangunan nasional[3]. Tindak pidana teknologi informasi atau tindak pidana *cyber* berdasarkan ikatan dengan instrumen hukum internasional terkait, bersifat *hard law*, seperti perjanjian-perjanjian internasional, maupun soft law yang tersebar dalam berbagai dokumen seperti *Guidelines, Code of Conduct, Model Law, Principles* dan lain-lain[4].

Kemajuan teknologi informasi menjadi awal dari keberadaan *cyber crime*, secara yuridis dapat membawa dampak pada hukum yang mengatur tentang hal tersebut. Perhatian terhadap *cyber crime* tersebut disebabkan dampak *cyber crime* yang bersifat negatif dan dapat merusak seluruh bidang kehidupan modern saat ini, oleh karena kemajuan teknologi komputer menjadi salah satu pendukung kehidupan masyarakat. *Cyber Crime* adalah suatu upaya memasuki/ menggunakan fasilitas Komputer/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 alam maya) atau kejahatan dibidang komputer dengan secara illegal, dan terdapat difinisi yang lain yaitu sebagai kejahatan komputer yang ditujukan kepada sistem atau jaringan komputer, yang mencakup segala bentuk baru kejahatan yang menggunakan bantuan sarana media elektronik internet. Dengan demikian *Cyber Crime* merupakan suatu tindak kejahatan didunia alam maya, yang dianggap betentangan atau melawan undang-undang yang berlaku, oleh karenanya 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 komputer melalui *e mail (cyber spamming).* Virus komputer adalah 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[5]. Efek dari virus komputer ini 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 sangan beragam dengan nama tersendiri dan daya pengrusak tersendiri pula. Penyebaran virus komputer ini dapat terjadi dengan berbagai cara termasuk penyebaran virus komputer melalui pengiriman *e-mail (cyber spamming*). Tindakan untuk menyebarkan virus komputer melalui pengiriman *e-mail (cyber spamming*) ini dapat dianggap sebagai suatu perbuatan yang layak dipidana, karena sepintas terlihat bahwa pelaku penyebaran virus komputer melalui pengiriman *e-mail (cyber spamming*) ini memiliki niat untuk merusak dokumen bahkan komputernya, sehingga dapat merugikan pihak lain, dengan demikian terdapat unsur pertanggungjawaban pidana di dalamnya. Perbuatan menyebarkan virus komputer melalui pengiriman *e-mail (cyber spamming*) ini tidak diatur dalam Kitang Undang-Undang Hukum Pidana.

[3] Sudarto, *Hukum dan Hukum Pidana,* Alumni, Bandung, 2018, hlm.104.
[4] Supanto, Perkembangan Kejahatan Teknologi Informasi (Cyber Crime) Dan Antisipasinya Dengan Penal Policy, *Jurnal Yustisia,* Vol.5 No.1 Januari - April 2016, Hlm. 59.
[5] www.wikipedia.org, diakses 14 Agustus 2022, pukul 19.00 WIB.

Res Nullius
Law Journal
Fakultas Hukum Universitas Komputer Indonesia
p-ISSN 2656-7261
e-ISSN 2721-4206
Vol. 5 No. 1 Januari 2023

Saat ini, walaupun di Indonesia telah ada UU ITE, tetapi tindakan penyebaran virus komputer melalui pengiriman *e-mail* tidak diatur secara khusus. Namun demikian Pasal 30 ayat (2) UU ITE yang menegaskan beberapa perbuatan yang dilarang dan diancam sanksi pidana, termasuk larangan mengakses komputer dan atau sistem elektronik pihak lain secara melawan hukum, sehingga perbuatan menyebarkan virus komputer melalui pengiriman *e-mail (cyber spamming*) dapat dianggap sebagai sebuah tindak pidana. Pasal 30 ayat (2) UU ITE mengandung unsur-unsur, baik unsur subjektif maupun objektif, yaitu :

Unsur subjektif :
1. dengan sengaja
2. secara melawan hukum

Unsur Objektif :
1. mengakses komputer dan/atau sistem elektronik dengan cara apa pun
2. untuk tujuan memperoleh informasi elektronik dan/atau dokumen elektronik

Struktur desentralisasi internet menawarkan komunikasi yang cepat dengan jangkauan global, tetapi juga memberikan anonimitas, karakteristik sangat berharga untuk pelaksanaan kegiatan ilegal. Kejahatan dunia maya telah berkembang pesat seiring dengan penyebaran internet dan e-niaga. email yang tidak diminta, atau spam, hal ini menjadi dasar dari banyaknya bentuk kejahatan dunia maya. Salah satu penjahat online paling sering terjadi adalah antara pembuat malware dan email spammer, yang merekayasa email secara sosial untuk menyebarkan malware ke komputer dan perangkat digital lainnya; email tetap menjadi salah satu dari vektor utama penyebaran malware. Tidak seperti kejahatan dunia maya yang menargetkan korban bervolume rendah dan bernilai tinggi seperti bank dan membutuhkan kemampuan peretasan tingkat lanjut, spam memungkinkan malware untuk mencapai volume tinggi, target bernilai rendah, yang cenderung memiliki antivirus yang efektif atau tindakan pencegahan lainnya. Contoh tipikalnya adalah email berbahaya yang berisi konten yang membujuk penerima untuk mengeklik tautan URL ke tautan jahat situs web, atau untuk mengunduh lampiran berbahaya[6]. Email berbahaya merupakan tantangan global karena merupakan petunjuk utama penyebaran malware yang dapat memiliki dampak sosial dan dampak ekonomi. Malware umumnya didistribusikan melalui dua jenis spam: email dengan lampiran yang berisi virus atau Trojan, yang menginstal sendiri di komputer korban saat lampiran diunduh; dan email yang berisi hyperlink ke halaman web yang disusupi, tempat malware diunduh ke komputer korban. Peluang seperti itu menyebabkan kejahatan internet memiliki risiko rendah, biaya rendah, dan menguntungkan pelaku kejahatan tersebut seperti spamming yang menyebarkan malware ke dalam spam[7].

Berdasarkan ketentuan hukum yang berlaku di Indonesia khususnya UU ITE, setiap pelaku penyebaran virus komputer melalui email, sebagaimana diatur dalam Pasal 30 ayat (2) UU ITE, dapat dipidana dengan Pasal yakni dipidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak sebesar Rp. 700.000.000,00 (Tujuh ratus juta rupiah), sebagaimana diatur dalam Pasal 46 ayat (2) UU ITE.

## METODE PENELITIAN

[6] Mamoun Alazab and Roderic Broadhurst, Spam And Criminal Activity, *Trends & Issues In Crime And Criminal Justice Journal*, Australian Institute of Criminology, No. 526, December 2016, P. 1.
[7] Anderson R et al., Measuring the Cost of Cybercrime. In Böhme r (ed.), *The Economics of Information Security and Privacy Journal, No.* IV, 2013, P. 265–300

Res Nullius
Law Journal
Fakultas Hukum Universitas Komputer Indonesia
p-ISSN 2656-7261
e-ISSN 2721-4206
Vol. 5 No. 1 Januari 2023

Penelitian yang dilakukan bersifat deskriptif analitis[8], menggambarkan secara sistematis fakta-fakta dan permasalahan hukum yang diteliti sekaligus menganalisis peraturan perundang-undangan yang berlaku, dihubungkan dengan teori hukum dan praktis pelaksanaannya, berupa data sekunder bahan hukum primer antara lain Undang-Undang Nomor 19 tahun 2016 tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 8 Tahun 1981 Tentang Hukum Acara Pidana, kemudian data sekunder bahan hukum sekunder yaitu pendapat para ahli yang berkaitan dengan tindak pidana penyebaran virus komputer melalui pengiriman *e*-mail serta data sekunder bahan hukum tertier seperti kamus hukum. Sementara itu metode pendekatan yang digunakan adalah yurisis normatif, melalui peraturan perundang-undangan terkait teknologi informasi, selanjutnya data yang diperoleh dianalisis secara yuridis kualitatif, untuk mencapai kepastian hukum.

## HASIL DAN PEMBAHASAN

Tindakan penyebaran virus komputer melalui pengiriman *e-mail* tidak diatur secara khusus. Namun demikian Pasal 30 ayat (2) UU ITE yang menegaskan beberapa perbuatan yang dilarang dan diancam sanksi pidana, termasuk larangan mengakses komputer dan atau sistem elektronik pihak lain secara melawan hukum, sehingga perbuatan menyebarkan virus komputer melalui pengiriman *e-mail (cyber spamming*) dapat dianggap sebagai sebuah tindak pidana. Pada kasus penyebaran virus komputer melalui pengiriman *e-mail (cyber spamming*) ini sulit untuk membuktikannya, karena 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 dari ketentuan alat bukti sebagaimana telah diatur dalam pasal 184 Kitab Undang-Undang Hukum Acara Pidana (selanjutnya ditulis KUHAP), yaitu bahwa alat bukti yang sah adalah :

1. keterangan saksi;
2. keterangan ahli;
3. surat;
4. petunjuk;
5. keterangan terdakwa.

[8] Ayu Wulandari Wirawan, Wahyudi,. 2022. "PERLINDUNGAN HUKUM MASYARAKAT TERHADAP KEWAJIBAN VAKSINASI COVID 19 DALAM RANGKA PENANGGULANGAN PANDEMI CORONA VIRUS DISEASE 19". *Res Nullius Law Journal* 4 (1), 57-76. https://doi.org/10.34010/rnlj.v4i1.7243.

Res Nullius
Law Journal
Fakultas Hukum Universitas Komputer Indonesia
p-ISSN 2656-7261
e-ISSN 2721-4206
Vol. 5 No. 1 Januari 2023

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

1. *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 dalam persidangan.
2. *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.
3. 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 ditetapkan oleh undang-undang disertai keyakinan hakim dalam menentukan salah tidaknya terdakwa.
4. Teori Pembuktian menurut Undang-Undang Secara Negatif (*Negatief Wettelijke stelsel*), merupakan sistem pembuktian yang menggunakan teori perpaduan antara sistem pembuktian menurut 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.

Sementara itu, sistem pembuktian yang dianut oleh KUHAP adalah sistem pembuktian menurut undang-undang secara negative, 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 (2) KUHAP yang membatasi kewenangan hakim dalam memperoleh alat bukti petunjuk, yang secara limitatif hanya dapat diperoleh dari:

1. keterangan saksi;
2. surat;
3. keterangan terdakwa.

Berdasarkan hal di atas, 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 lain, namun hakim tidak terikat atas kebenaran persesuaian yang diwujudkan oleh petunjuk, sehingga hakim bebas untuk menilai

Res Nullius
Law Journal
Fakultas Hukum Universitas Komputer Indonesia
p-ISSN 2656-7261
e-ISSN 2721-4206
Vol. 5 No. 1 Januari 2023

dan mempergunakannya dalam upaya pembuktian. 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 dapat dianggap sebagai petunjuk, yang merupakan perluasan dari alat bukti surat sebagai bahan untuk dijadikan petunjuk bagi hakim dalam membuktikan suatu perkara termasuk kasus penyebaran virus komputer melalui pengiriman *e*-mail yang telah diuraikan pada bagian sebelumnya. Tindak pidana penyebaran virus komputer melalui pengiriman *e*-mail *(cyber spamming)* dimungkinkan melibatkan lebih dari satu sistem hukum 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.

Format email spam yang berbahaya dan dapat merugikan memiliki ciri yang khas, antara lain kalimat awal email berisi instruksi pengiriman untuk server email, dan badan email mungkin memiliki banyak bagian untuk teks dan lampiran. Subjek dan isi teks dari spam berbahaya dapat mengungkapkan metode rekayasa sosial dari berbagai tingkat kecanggihan untuk memanipulasi penerima pertama. Dalam hal ini, premisnya adalah paket yang tidak terkirim (pada kenyataannya, tidak ada); penerima diminta untuk mengunduh file yang terkompresi (isinya disamarkan, tetapi termasuk beberapa ekstensi file) untuk memfasilitasi pengiriman paket. File terkompresi menyembunyikan malware yang dapat dieksekusi dari pemindai virus yang diterapkan oleh server email, internet calon korban penyedia layanan (ISP) atau administrator sistem lokal. Malware umumnya didistribusikan melalui dua jenis spam: email dengan lampiran yang berisi virus atau Trojan, yang menginstal sendiri di komputer korban saat lampiran diunduh; dan email yang berisi hyperlink ke halaman web yang disusupi, tempat malware diunduh ke komputer korban. Email berbahaya merupakan tantangan global karena merupakan petunjuk utama penyebaran malware yang dapat memiliki dampak sosial dan dampak ekonomi

## Simpulan

Berdasarkan pembahasan di atas, dapat ditarik beberapa simpulan yaitu :

1. Saat ini perbuatan penyebaran virus komputer melalui *e-mail* (*Cyber Spamming)* belum diatur secara khusus dalam peraturan perundang-undangan di Indonesia, walaupun di Indonesia telah ada UU ITE, namun beblum diatur secara tegas. Jika dilihat dari unsur-unsur perbuatan pidananya, terhadap perbuatan penyebaran virus komputer melalui email (*cyber spamming)* dapat diterapkan Pasal 30 ayat (2) UU ITE.
2. Tindakan hukum yang dapat dilakukan terhadap pelaku penyebaran virus komputer melalui email (*cyber spamming*) berdasarkan hukum yang berlaku di Indonesia diatur dalam Pasal 46 ayat (2) UU ITE yakni dipidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak sebesar Rp. 700.000.000,00 (Tujuh ratus juta rupiah).

## Ucapan Terimakasih

Penulis mengucapkan terimakasih kepada yang terhormat Prof. Dr. Ir. H. Eddy Soeryanto Soegoto, M.T. sebagai Rektor Universitas Komputer Indonesia yang senantiasa mendukung Penulis dalam melaksanakan penelitian dan penulisan artikel ini.

**DAFTAR PUSTAKA**

Anderson R et al., Measuring the Cost of Cybercrime. In Böhme r (ed.), *The Economics of Information Security and Privacy Journal, No.* IV, 2013, P. 265–300

Ayu Wulandari Wirawan, Wahyudi,. 2022. "PERLINDUNGAN HUKUM MASYARAKAT TERHADAP KEWAJIBAN VAKSINASI COVID 19 DALAM RANGKA PENANGGULANGAN PANDEMI CORONA VIRUS DISEASE 19". *Res Nullius Law Journal* 4 (1), 57-76. https://doi.org/10.34010/rnlj.v4i1.7243.

Jan Smith, *Komputer : Suatu Tantangan Baru di Bidang Hukum*, Airlangga University Press, Surabaya, 2012, hlm.58.

Sudarto, *Pembaharuan Hukum Pidana di Indonesia*. Simposium Hukum Pidana Nasional Semarang BPHN dan UNDIP. 2011, Hlm. 14.

Sudarto, *Hukum dan Hukum Pidana,* Alumni, Bandung, 2018, hlm.104.

Supanto, Perkembangan Kejahatan Teknologi Informasi (Cyber Crime) Dan Antisipasinya Dengan Penal Policy, *Jurnal Yustisia*, Vol.5 No.1 Januari - April 2016, Hlm. 59.

www.wikipedia.org, diakses 14 Agustus 2022, pukul 19.00 WIB.

Mamoun Alazab and Roderic Broadhurst, Spam And Criminal Activity, *Trends & Issues In Crime And Criminal Justice Journal*, Australian Institute of Criminology, No. 526, December 2016, P. 1.