

BAB V

PENUTUP

5.1 Kesimpulan

1. Pertanggungjawaban Pidana Pelaku Pemerasan dengan Menggunakan Virus

Perkembangan teknologi dan informasi yang semakin berkembang dengan pesat telah memberikan manusia banyak manfaat selain manfaat tersebut juga terdapat beberapa orang yang memanfaatkan kemajuan tersebut untuk melakukan tindak kejahatan dengan menggunakan teknologi maupun menjadikan teknologi terutama jaringan komputer sebagai sasaran dalam melakukan tindak kejahatannya. Tindak kejahatan dengan menggunakan *ransomware* di Indonesia saat ini tidak dapat disepelekan meski dalam kehidupan sehari – hari masih sedikit orang yang mengetahui mengenai tindak kejahatan *ransomware* itu sendiri bukan berarti tindak kejahatan tersebut tidak terjadi di Indonesia menurut data yang Diskominfo pada tahun 2023 lalu, sudah terjadi lebih dari 29 juta serangan siber di Indonesia dari semua serangan tersebut menurut kaspersky terdapat 97.226 serangan *ransomware* yang terjadi di Indonesia, berdasarkan hasil ini hal tersebut bukan merupakan angka yang kecil, sehingga perlu kita waspadai ke depannya. Hal ini dapat menimbulkan kerugian yang sangat besar jika kita mengacuhkan kejahatan *ransomware*, sebagai pengguna jaringan internet dan jaringan komputer harus dapat menjadi seorang pengguna yang cerdas dan berhati – hati agar dapat terhindar dari serangan *ransomware*.

UU ITE saat ini meski tidak memiliki peraturan yang secara khusus mengatur mengenai tindak kejahatan *ransomware* dan kemungkinan atas perkembangan dari kejahatan tersebut, masih terdapat pasal – pasal dalam UU ITE yang dapat dijadikan hukum untuk menjerat para pelaku tindak kejahatan *ransomware* yaitu, pasal 27 B, jo. pasal 32 ayat (1), jo. pasal 45 ayat (4), jo. Pasal 48 ayat (1) dan Pasal 33 jo. Pasal 49 Undang – Undang No. 1 Tahun 2024 tentang perubahan kedua atas Undang – Undang No. 11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik,

Meski memiliki aturan yang mengikat setiap orang yang melakukan kejahatan *ransomware* di wilayah Indonesia, tetapi Indonesia sendiri masih memiliki kendala atau halangan untuk meminta pertanggungjawaban kepada orang yang berada di luar wilayah Negara Indonesia atau orang yang merupakan warga negara asing yang berada

di luar wilayah Negara Indonesia karena kurangnya aturan yang dimiliki oleh Negara Indonesia.

2. Upaya Perlindungan Korban Serangan *Ransomware*

Melakukan sosialisasi baik kepada masyarakat maupun perusahaan atau kepada instansi pemerintahan agar dapat lebih mewaspadaai kejahatan *ransomware*, jangan sampai terjadi serangan ulang kepada instansi pemerintah maupun kepada lembaga lainnya, untuk itu untuk meminimalisir kemungkinan para pengguna jaringan komputer dan internet terkena serangan *ransomware*, para pengguna jaringan komputer harus selalu memperhatikan :

- a) Pastikan komputer mendapat patch terbaru dan pembaruan terbaru melalui aktivasi fitur “Windows Update”, dan usahakan untuk melakukan back-up atau pencadangan terhadap data penting sebelum melakukan pembaruan sistem untuk mencegah kerusakan, error, atau kehilangan data pada saat melakukan instalasi pembaruan sistem;
- b) Lakukan scanning komputer menggunakan Anti-Virus terbaru secara berkala untuk membantu sistem komputer mengetahui keberadaan aplikasi tidak dikenal atau mempunyai signature *malware*;
- c) Waspada pada setiap link yang diterima, terutama yang berasal dari e-mail spam atau e-mail phishing;
- d) Selalu aktifkan Windows Firewall yang berguna untuk membuat sebuah aturan/rules di dalam Windows Firewall sehingga program dapat melakukan pembaruan secara otomatis;
- e) Aktifkan fitur “safe browsing” pada aplikasi (browser) yang digunakan, contohnya fitur safe browsing yang disediakan oleh Google untuk mendeteksi situs-situs yang tidak aman dan memiliki kemungkinan disusupi oleh *malware*. Apabila suatu situs diindikasikan tidak aman, maka Google akan memberikan peringatan apabila situs yang hendak dikunjungi adalah situs berbahaya;
- f) Lakukan back-up data penting secara berkala menggunakan penyimpanan eksternal atau media penyimpanan *online* seperti Google Drive dan iCloud.

Selain dengan melakukan tindakan – tindakan pencegahan dengan cara atau teknik yang dapat dilakukan sendiri atau dengan mengandalkan sistem itu sendiri, para korban kejahatan *ransomware* dapat melakukan tindakan pelaporan atas tindak kejahatan pemerasan dengan menggunakan virus *ransomware* kepada aparat penegak hukum agar dapat segera ditindak lanjuti dan diselidiki oleh aparat penegak hukum, selain itu memberikan izin kepada aparat penegak hukum dalam melakukan pembukaan data pribadi demi tujuan melakukan penyelidikan atas kejahatan *ransomawre* yang telah terjadi, selain itu korban dapat melakukan pengumpulan bukti secara mandiri sebelum melakukan tindakan pelaporan agar mempermudah dan mempercepat proses penyelidikan yang akan dilakukan oleh aparat penegak hukum.

5.2 Saran

Dari kesimpulan di atas, saran yang diberikan oleh penulis adalah :

1. Memperbanyak perjanjian internasional dan meratifikasi perjanjian internasional agar dapat melakukan ekstradiksi atau dapat melakukan penangkapan atas pelaku kejahatan pemerasan dengan *ransomware* yang berada di luar wilayah Negara Indonesia atau orang asing yang berada di luar wilayah Negara Indonesia.
2. Melakukan penyuluhan secara menyeluruh kepada masyarakat dan semua instansi pemerintah agar selalu memperhatikan waktu untuk melakukan pengecekan sistem komputer agar dapat meminimalisir serangan *ransomware* yang mungkin terjadi di kemudian hari, serta melakukan kerjasama dengan para ahli di bidang teknologi informasi dan komunikasi untuk mempermudah proses penyelidikan atas kejahatan *ransomware*.

DAFTAR PUSTAKA

BUKU

- Abdul Wahid dan Labib Mohammad, 2005, *Kejahatan Mayantara (CYBER CRIME)*, Bandung, PT Refika Aditama.
- Aris Hardianto, 2019, *AKSES ILEGAL DALAM PERSPEKTIF HUKUM PIDANA*, Malang, Setara Press (cetakan ke-1).
- Barda Nawawi Arief, 2014, *Bunga Rampai Kebijakan Hukum Pidana (Perkembangan Penyusunan Konsep KUHP Baru)*, Semarang, Kencana Prenada Media Group.
- Barda Nawawi Arief, 2006, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, Jakarta, Kencana Prenada Media Group.
- Barda Nawawi Arief, 2006. *Tindak Pidana Mayantara: Perkembangan Kajian Cybercrime di Indonesia*. Jakarta, PT. Grafindo Persada.
- Didik M. Arief Mansur dan Alisatris Gultom dalam Sutarman, 2007, *Cyber Crime Modus Operandi dan Penanggulangannya Cetakan I*, Yogyakarta, Laksbang Pressindo.
- Maskun. 2013. *Kejahatan Cyber Crime Suatu Pengantar*. Jakarta, Kencana.
- Muljatno, 2012, *Kitab Undang-Undang Hukum Pidana*, Jakarta, PT Bumi Aksara.
- Nudirman Munir, 2017, *Pengantar Hukum Siber Indonesia*, Depok, Rajawali pers.
- P.A.F Lamintang, 2018, *Dasar-Dasar Hukum Pidana Indonesia*, Jakarta, Sinar Grafika. (cetakan ke-3)
- Suharsimi Arikunto, 2002, *Prosedur Penelitian Suatu Pendekatan Praktek*, Jakarta, Rineka Cipta.
- Soerjono Soekanto dan Sri Mamudji, 2006, *Penelitian Hukum Normatif Suatu Tinjauan Singkat*, Jakarta, PT Raja Grafindo Persada.
- Soesilo R, 1988, *Kitab Undang-Undang Hukum Pidana (KUHP) Serta Komentarnya Lengkap Pasal Demi Pasal*, Bogor, Politeia.

Jurnal

- Akbanoy, M, 2019, *WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms*, Journal of Telecommunications and Information Technology, Vol.1.
- Alcianno G. Gani, 2018, *CYBERCRIME (KEJAHATAN BERBASIS KOMPUTER)*, JSI (Jurnal Sistem Informasi) Universitas Suryadarma, Jurnal. Vol5, No 1.
- Desyanti Suka Asih, 2021, *PERLINDUNGAN HUKUM BAGI KORBAN SERANGAN RANSOMWARE, VYAVAHARA DUTA*, jurnal, Vol 16.
- Everett, C. 2016. *Ransomware: To pay or not to pay?* Copm. Fraud & Secure, Vol.4.
- Nazura Abdul Manap, 2014, *PROCEEDING, International Conference on-Electronic-Commerce Law “E-Commerce Law in Asia Opportunities and Challenges”* , CV. Indo Legal Service.
- Lita Sari Marita, 2015, *CYBER CRIME DAN PENERAPAN CYBER LAW DALAM PEMBERANTASAN CYBER LAW DI INDONESIA*, BSI, Jurnal, Vol 15.

Artikel

- Alcianno G. Gani, *PENGENALAN TEKNOLOGI INTERNET SERTA DAMPAKNYA*, Jakarta, 2015.
- Sally Timothy Talahatu, “*Cybercrime Sebagai Tindak Pidana Teknologi Informasi*”, Fakultas Hukum Universitas Dirgantara Marsekal Suryadarma, 2019.

Peraturan

- Kitab Undang - Undang Hukum Pidana.
- Undang - Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.
- Undang - Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang - Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Undang – Undang No. 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang – Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

WEBSITE

Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/DTC/DTC_rolling_text_01.09.2023_PM.pdf

Admin, Pengertian dan Ruang Lingkup Kebijakan Hukum Pidana, <http://mh.uma.ac.id/2020/09/pengertian-dan-ruang-lingkup-kebijakanhukum-pidana/> .

Aditya Wicaksono Irawan, Aan Yusufianto, Dwi Agustina, Reagan Dean, LAPORAN SURVEI INTERNET APJII 2019 – 2020 (Q2), Asosiasi Penyelenggara Jasa Internet Indonesia, <https://apjii.or.id/survei2019x> .

Akbar Evandio, Ini 5 Besar *Ransomware* yang Menyerang Indonesia pada Kuartal I/2020, <https://teknologi.bisnis.com/read/20200905/282/1287692/ini-5besar-ransomware-yang-menyerang-indonesia-pada-kuartal-i2020> .

Bernadetha Aurelia Oktavira, S.H., Waspada ! Kenali Macam – macam Kejahatan di Internet, <https://www.hukumonline.com/klinik/a/waspada-kenali-macam-macam-kejahatan-di-internet-cl294/> .

Diskominfo Kota Bogor, Kejahatan *Cyber*, <https://kominfo.kotabogor.go.id/index.php/post/single/847> .

Edavos, 7 Kasus *Ransomware* yang Menimbulkan Kerugian Besar, <https://edavos.com/kasus-ransomware/> .

Keminfo, Kominfo Dorong Kewaspadaan Antisipasi *Ransomware* Petya, https://www.kominfo.go.id/content/detail/10035/kominfo-dorongkewaspadaan-antisipasi-ransomware-petya/0/berita_satker .

Lesthia Kertopati, Dua Rumah Sakit di Jakarta Kena Serangan *Ransomware* WannaCry, <https://www.cnnindonesia.com/teknologi/20170513191519->

[192214642/dua-rumah-sakit-di-jakarta-kena-serangan-ransomware-wannacry](https://ejournal.bsi.ac.id/ejurnal/index.php/cakrawala/article/view/4901/284)

Lita Sari Marita, *CYBER CRIME DAN PENERAPAN CYBER LAW DALAM*

PEMBERANTASAN CYBER LAW DI INDONESIA,

<https://ejournal.bsi.ac.id/ejurnal/index.php/cakrawala/article/view/4901/284>

Mys, Bahasa Hukum: Tindak Pidana ‘Pemerasan’,

<https://www.hukumonline.com/berita/a/bahasa-hukum--tindak-pidanapemerasan-lt5056a2c308a48/> .

Novina Putri Bestari, Ngeri! Virus *Ransomware* Makan Korban, Rampok Rp 8,3 Triliun,

<https://www.cnbcindonesia.com/tech/20211027062322-37286775/ngeri-virus-ransomware-makan-korban-rampok-rp-83-triliun> .

Nur Rohmi Aida, Sari Hardiyanto, Pemuda Sleman Berhasil Retas Perusahaan Amerika dengan Ransomware, Apa Itu?

<https://www.kompas.com/tren/read/2019/10/27/191300865/pemudasleman-retas-perusahaan-amerika-dengan-ransomware-apa-itu-?page=all> .

Pratiwi Agustini, Warganet Meningkat, Indonesia Perlu Tingkatkan Nilai Budaya di

Internet, <https://aptika.kominfo.go.id/2021/09/warganet-meningkatindonesia-perlu-tingkatkan-nilai-budaya-di-internet/> .