PAMPAS: *Journal of Criminal Law*
Volume 6 Nomor 2, Tahun 2025
(ISSN 2721-8325)

Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Ransomware dalam Perspektif Peraturan Perundang-Undangan

Suci Wahyuning Robbi[1], Hafrida[2], Yulia Monita[3]
Fakuktas Hukum Universitas Jambi[1]
Fakuktas Hukum Universitas Jambi[2]
Fakuktas Hukum Universitas Jambi[3]
Author's Email Correspondence: suciwahyuningrobbi@icloud.com

ABSTRAK
Pertanggungjawaban pidana terhadap pelaku tindak pidana ransomware adalah untuk menentukan apakah seseorang yang melakukan perbuatan pidana tersebut dapat diminta pertanggungjawaban atau tidak atas tindakannya. Pelaku tindak pidana ransomware harus memenuhi unsur-unsur pertanggungjawaban pidana. Pengaturan tentang pertanggungjawaban pidana bagi pelaku tindak pidana ramsomware dapat berpedoman pada Pasal 27B ayat (1) UU ITE, Pasal 30 ayat (2) UU ITE, Pasal 32 ayat (1) UU ITE, Pasal 368 ayat (1) KUHP, dan Pasal 67 ayat (1) UU perlindungan data pribadi dengan menjatuhkan sanksi pidana sebagai bentuk pertanggungjawaban pidana atas tindak pidana ransomware, tetapi pada pengaturan pasal tersebut masih mengalami kekaburan norma , yang dimana terdapat unsur-unsur ransomware yang belum terpenuhi dalam pasal tersebut sehingga belum ada pasal yang mengatur secara jelas mengenai tindak pidana ransomware. Maka pelaku tindak pidana ransomware sulit untuk diminta pertanggungjawaban pidana, serta tidak ada penegasan dakam aturan tersebut sehingga kasus ini sulit di buktikan. Oleh karena itu, bentuk pertanggungjawaban pidana terhadap pelaku tindak pidana dalam perspektif peraturan perundang- undangan belum terwujud. Sehingga dalam menjatuhkan sanksi pidana terhadap pelaku tindak pidana ransomware belum ada pasal yang digunakan secara jelas, sehingga pelaku sulit untuk dikenakan pasal tersebut dalam pertanggungjawaban pidana.

Kata Kunci:
Pertanggungjawaban pidana; Pelaku; Tindak Pidana Ransomware.

ARTICLE HISTORY
Submission: 2025-05-15
Accepted: 2025-07-08
Publish: 2025-07-08

KEYWORDS: *Criminal Liability; Perpetrator; Ransomware crime.*

ABSTRACT
Criminal liability for perpetrators of ransomware crimes is to determine whether or not a person who commits the crime can be held accountable for his actions. Perpetrators of ransomware crimes must fulfill the elements of criminal liability. Regulations on criminal liability for perpetrators of ransomware crimes can be guided by Article 27B paragraph (1) of the ITE Law, Article 30 paragraph (2) of the ITE Law, Article 32 paragraph (1) of the ITE Law, Article 368 paragraph (1) of the Criminal Code, and Article 67 paragraph (1) of the Personal Data Protection Law by imposing criminal sanctions as a form of criminal liability for ransomware crimes, but in the regulation of these articles there is still a lack of norms, where there are elements of ransomware that have not been fulfilled in these articles so that there are no articles that clearly regulate ransomware crimes. So it is difficult for perpetrators of ransomware crimes to be held criminally accountable, and there is no affirmation in these regulations so that this case is difficult to prove. Therefore, the form of criminal liability for perpetrators of criminal acts from the perspective of statutory regulations has not been realized. So that in imposing criminal sanctions on perpetrators of ransomware crimes, there is no article that is used clearly, making it difficult for perpetrators to be subject to this article in criminal responsibility.

A. PENDAHULUAN

Pertanggungjawaban pidana berarti bahwa setiap orang yang melakukan tindak pidana atau melanggar hukum sebagaimana telah diatur dalam undang-undang, harus bertanggungjawab atas tindakannya sesuai dengan kesalahannya.[1] Dalam tindak pidana cyber crime unsur kesalahan yang dapat dipertanggungjawabkan oleh pelaku terdapat pada unsur mengakses atau menggunakan sistem elektronik milik orang lain tanpa izin dengan merusak sistem keamanan. Pada umumnya pelaku kejahatan cyber crime dilakukan oleh mereka yang memiliki kekuasaan atas sistem komputer dan jaringan internet.[2] Internet memberikan pilihan bagi khalayak tidak hanya dalam mencari dan mengonsumsi informasi semata, tetapi khalayak bisa mengakses informasi itu. Internet semakin gampang untuk digunakan tidak lagi menggunakan komputer yang besar, dari kemajuan teknologi internet sudah dapat digunakan pada telepon gengam atau lebih tepatnya smartphone.[3]

[1] Nisa Nindia Putri, Sahuri Lasmadi, and Erwin Erwin, "Pertanggungjawaban Pidana Perusahaan Pers Terhadap Pemberitaan Yang Mencemarkan Nama Baik Orang Lain Melalui Media Cetak Online," *PAMPAS: Journal of Criminal Law* 2, no. 2 (2021): 123–39, https://doi.org/10.22437/pampas.v2i2.14761.

[2] Rafi Septia Budianto Pansariadi and Noenik Soekorini, "Tindak Pidana Cyber Crime Dan Penegakan Hukumnya," *Binamulia Hukum* 12, no. 2 (2023): 287–98, https://doi.org/10.37893/jbh.v12i2.605.

[3] Agung, A., Hafrida, H., & Erwin, E. (2022). Pencegahan Kejahatan Terhadap Cybercrime. PAMPAS: Journal of Criminal Law, 3(2), 212–222. Https://Doi.Org/10.22437/Pampas.V3i2.23367, n.d.

Salah satu jenis kejahatan cyber crime adalah tindak pidana ransomware. Ransomware merupakan serangan siber yang sering terjadi, dimana penyerang mematikan perangkat lunak untuk mematikan sistem bisnis atau membuat bisnis menjadi offline maka tebusan harus dibayar sebelum ransomware dihapus atau di nonaktifkan, jika tidak dibayarkan penyerang mengancam akan membuat data terenkripsi sehingga tidak dapat digunakan. [4] Menurut Everrt, ransomware merupakan jenis malware yang menyerang pengguna dalam mengakses atau membatasi akses mereka kedalam sistem maupun file data, dengan mengunci atau mengenkripsi file sampai dengan tuntutannya terpenuhi maupun terbayarkan. [5] Dalam hal ini pelaku kejahatan ransomware yang telah berhasil mengunci data milik korban akan melakukan pemerasan dengan meminta sejumlah tebusan yang harus dibayarkan oleh pemilik data tersebut. Tindak pidana ransomware juga merupakan suatu tindak pidana pemerasan dengan ancaman yang menggunakan suatu virus malware dengan menerobos sistem keamanan pada komputer tanpa izin.

Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE) merupakan Hukum Siber Pertama Indonesia dan pembentukannya bertujuan untuk memberikan kepastian hukum bagi masyarakat yang melakukan transaksi secara elektronik, mendorong pertumbuhan ekonomi, mencegah terjadinya kejahatan berbasis teknologi informasi dan komunikasi serta melindungi masyarakat pengguna jasa yang memanfaatkan teknologi informasi dan komunikasi.[6]

Tindak pidana cyber crime bukan hanya merusak data pribadi dan mencuri informasi pribadi, tetapi cyber crime dapat menimbulkan dampak negatif yang lebih besar terhadap ekonomi dan bisnis, serta dapat mengancam keamanan dalam stabilitas nasional suatu negara. Tahun 2017 kejahatan ransomware menyerang sistem komputer dirumah sakit Harapan kita dan rumah sakit Dharmais dijakarta. Pada tahun 2022 Indonesia mengalami peningkatan serangan siber dari tahun sebelumnya dan data statistik dari Badan Siber dan Sandi Negara mencatat bahwa telah terjadi 370,02 juta, sedangkan tahun sebelumnya terjadi 266,74 juta serangan siber.[7] Bank Syariah Indonesia (BSI) juga mengalami serangan siber ransomware, yang dimana data nasabah mengalami kebocoran data akibat dari tebusan sejumlah uang yang diminta oleh pelaku tidak terpenuhi. Pada tahun 2024, Badan Siber dan Sandi Negara menyatakan bahwa server Pusat Data Nasional Kementerian Komukasi Dan informatika (Kominfo) mengalami serangan ransomware yang mengakibatkan server down serta 282 layanan publik terganggu, akibat dari serangan ransomware ini menyebabkan data-data terenkripsi.[8] Kejahatan siber yang selanjutnya disebut cybercrime merupakan kejahatan yang termasuk baru dibandingkan dengan

[4] Desyanti Suka Asih K.Tus, "Perlindungan Hukum Bagi Korban Serangan Ransomware," *Vyavahara Duta* 16, no. 2 (2021): 126, https://doi.org/10.25078/vd.v16i2.2909.

[5] G Ramadhan, "Perlindungan Hukum Bagi Korban Ransomware Wannacry Tindak Pidana Ransomware," Jurnal Kajian Kontemporer Hukum Dan Masyarakat Vol 1 no 2 2023, hlm. 10, https://doi.org/10.11111/dassollen.xxxxxxx.

[6] Sahat Maruli T. Situmeang. *Cyber Law*. Bandung: Penerbit Cakra, 2020. hlm.18

[7] nasional, "BPPTIK Kementerian Komunikasi Dan Informatika RI," 2022.

[8] Badan Siber dan Sandi Negara (BSSN), "BSSN Identifikasi Pusat Data Nasional Sementara Diserang Ransomware," *Jun 24, 2024*, 2024.

kejahatan pembunuhan ataupun pencurian, akan tetapi kejahatan siber sama merugikannya bagi manusia. Kejahatan siber memang tidak dapat dirasakan secara fisik namun sama merugikannya seperti pembunuhan, perampokan atau pencurian.[9]

Dalam tindak pidana ransomware dapat berpedoman dengan Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, Kitab Undang-Undang Hukum Pidana, Dan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. Dalam hukum pidana seseorang yang melakukan perbuatan melanggar hukum yang karena kesalahannya dapat dipertanggungjawabkan apabila telah terpenuhinya unsur-unsur dalam pertanggungjawaban pidana. Dalam pasal 27B ayat (1) Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas UndangUndang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, menyatakan bahwa:

Setiap orang dengan sengaja atau tanpa hak mendistribusikan dan/atau mentranmisikan informasi elektronik dan/atau dokumen elektronik, dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, memaksa orang dengan ancaman kekerasan untuk:

A. Memberikan suatu barang, yang sebagian atau seluruhnya milik orang tersebut atau milik orang lain; atau
B. Memberi utang, membuat pengakuan utang, atau menghapuskan piutang.

Pasal ini menitikberatkan pada pelaku yang melakukan ancaman kekerasan dengan menyebarkan dokumen elektronik. Tetapi dalam hal ini yang dimaksud dengan pemerasan yang dilakukan oleh pelaku dengan ancaman pidana pada pasal 45 ayat (8) dipidana penjara paling lama enam tahun dan/atau pidana denda paling banyak satu miliar rupiah, dengan mengacu pada ketentuan Pasal 45 ayat (9) menyatakan bahwa "Dalam hal perbuatan sebagaimana dimaksud pada ayat (8) dilakukan dalam lingkungan keluarga, penuntutan pidana hanya dapat dilakukan atas aduan. Selain itu pasal yang dikaitkan dengan tindak pidana ransomware adalah pasal 30 ayat (2) UU ITE,Pasal 32 ayat (1) UU ITE, Pasal 368 ayat (1) KUHP, dan pasal 67 UU Perlindungan Data pribadi. Namun, pasal-pasal yang dikaitkan dengan tindak pidana ransomware belum ada unsur-unsur ransomware yang terpenuhi dalam pasal tersebut, sehingga pelaku tindak pidana ransoware sulit untuk diminta pertanggungawaban pidana, yang dimana hasil analisis belum ada pasal yang mengatur secara spesifik sehingga menimbulkan kekaburan norma dalam pertanggungjawaban pidana terhadap pelaku tindak pidana ransomware dalam perspektif peraturan perundang-undangan. Dalam kasus ransomware ini sampai saat ini belum ada putusan pengadilan yang menjatuhkan pidana pada perkara tersebut, yang dimana pada kasus ini telah sampai pada tahap penyidikan namun ada beberapa kendala seperti sulitnya alat bukti yang digunakan untuk dideteksi. Pada umumnya, alat bukti yang digunakan merupakan alat bukti elektronik yang sangat sulit untuk diungkap dikarenakan pelaku dalam kejahatan ini merupakan orang-orang yang memiliki keahlian dibidang komputer.

[9] Agung, A., Hafrida, H., & Erwin, E. (2022). Pencegahan Kejahatan Terhadap Cybercrime. PAMPAS: Journal of Criminal Law, 3(2), 212–222. Https://Doi.Org/10.22437/Pampas.V3i2.23367.

Maka Rumusan masalah dan Tujuan penelitian ini adalah untuk mengetahui dan menganalisis pertauran tentang pertanggungjawaban pidana terhadap pelaku tindak pidana ransomware dan bentuk pertanggungjawaban pidana bagi pelaku tindak pidana ransomware dalam perspektif peraturan perundang-undangan.

B. METODE PENELITIAN

Metode penelitian yang digunakan adalah metode penelitian yuridis normatif. Pendekatan penelitian yang digunakan adalah pendekatan perundang-undangan *(statute Approach)*, pendekatan konseptual, dan pendekatan kasus (*Case Approach)*. "Menurut Peter mahmud Marzuki: "Penelitian hukum adalah suatu proses untuk menemukan suatu aturan hukum, prinsip-prinsip hukum, serta doktrin-doktrin hukum yang digunakan untuk menjawab isu-sisu hukum yang sedang dihadapi."[10] Bahan hukum yang digunakan dalam penelitian ini ada 3 yaitu bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier.

C. PEMBAHASAN

1. Pengaturan Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Ransomware

Ransomware merupakan serangan siber dengan menginfeksi sistem komputer, mengenkripsi data sehingga tidak dapat diakses oleh pengguna data dan pelaku kejahatan ini meminta tebusan untuk mengembalikan akses yang terkunci pada data tersebut.[11] Salah satu bentuk kejahatan atau tindak pidana yang memanfaatkan kecanggihan teknologi atau sistem jaringan internet adalah tindak pidana ransomware, yakni pemerasan dengan merusak sistem komputer kemudian mengenkripsi data-data pada sistem komputer. Kejahatan ransomware sedang marak terjadi sekarang baik di Indonesia maupun di luar negeri. Tindak pidana ransomware ini merupakan kejahatan transnasional yang dimana kejahatan ini terjadi malelui lintas negara, bahkan merupakan tindak pidana yang jaringannya sangat luas serta dapat mengancam keamanan data pada suatu negara.[12] Hal ini mempersulit upaya untuk mendeteksi, melaporkan, dan menangani kejahatan siber dengan efektif. Pendidikan dan kesadaran publik tentang cybercrime perlu ditingkatkan agar masyarakat dapat berperan aktif dalam melindungi diri dan melaporkan kegiatan yang mencurigakan terkait sistem informasi dan komunikasi.[13]

Pengaturan tentang pertanggungjawaban pidana terhadap pelaku tindak pidana ransomware dalam Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua

---

[10] Peter Mahmud Marzuki, *Penelitian Hukum*, Edisi Revi (Jakarta: Penerbit Kencana Prenada Media Grup, 2005).

[11] Nur Syamsi Tajriyani, "Pertanggungjawaban Pidana Tindak Pidana Pemerasan Dengan Modus Operandi Penyebaran Ransomware Cryptolocker," *Jurist-Diction* 4, no. 2 (2021): 706–7, https://doi.org/10.20473/jd.v4i2.25785.

[12] Cok Rai Kusuma Putra, I Nyoman Gede Sugiartha, and I Made Minggu Widyantara. "Analisis Yuridis Atas Keabsahan Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Pembobolan Sistem Data Keamanan Komputer (Cracking)". *Jurnal Prefensi Hukum Vol. 5*, Nomor 1, (2024). Hlm. 4. https://doi.org/10.22225/jph.5.1.8636.1-7.

[13] "Maharani, P., Hafrida, H., & Rapik, M. (2024). Pertanggungjawaban Pidana Hacktivist Dalam Perspektif Hukum Pidana Di Indonesia. PAMPAS: Journal of Criminal Law, 5(2), 242–252. Https://Doi.Org/10.22437/Pampas.V5i2.33291," n.d.

Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transasksi Elektronik. Maka, Pertanggungjawaban pidana pelaku tindak pidana ransomware dapat dikenakan dengan UndangUndang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, yang dimana pelaku dapat dipertanggungjawabkan karena melanggar Pasal 27B ayat (1) Jo. Pasal 45 ayat (8), Pasal 30 ayat (2) Jo. Pasal 46 ayat (2), Pasal 32 ayat (1) Jo. Pasal 48 ayat (1).

Pasal 27B ayat (1) UU ITE merupakan pasal yang mengatur mengenai tindak pidana pemerasan yang melalui informasi elektronik atau dokumen elektronik. Meskipun demikian, tindak pidana ransomware dapat dikaitkan dengan pasal 27B ayat (1) karena terdapat unsur pemerasan dalam tindak pidana ini. Pasal 27B ayat (1) berbunyi bahwa:

1. Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau menstransmisikan Informasi Elektronik dan/atau Dokumen Elektronik, dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, memaksa orang dengan ancaman kekerasan untuk:
    a. Memberikan suatu barang, yang sebagian atau seluruhnya milik orang tersebut atau milik orang lain; atau
    b. Memberi utang, membuat pengakuan utang, atau menghapuskan piutang.

Hal ini dikarenakan tindak pidana ransomware termasuk dalam tindak pidana pemerasan dengan mengakses sistem komputer milik orang lain untuk mengenkripsi data pada komputer. Pasal 27B ayat (1) ini meskipun tidak secara spesifik menjelaskan mengenai unsur-unsur tindak pidana ransomware, tetapi ada beberapa unsur yang sama bahkan berkaitan dengan tindak pidana pemerasan. Kemudian, dalam pasal tersebut hanya menjelaskan dengan cara mendistribusikan dan/atau mentransmisikan informasi elektronik dan/atau dokumen elektronik. Mendistribusikan artinya melakukan penyebaran secara luas informasi elektronik dan/atau dokumen elektronik, sedangkan mentransmisikan adalah mengirimkan suatu informasi elektronik. Pada unsur "ancaman kekerasan" sebagaimana dimaksud dalam penjelasan pasal 27B ayat (1) UU ITE, ialah yang ditujukan untuk menimbulkan rasa takut, cemas, atau khawatir akan dilakukannya kekerasan.

Terkait dengan unsur memberikan sesuatu barang, pemerasan dianggap telah terjadi apabila serangan ransomware telah menginfeksi pada sistem komputer, kemudian korban telah memberikan sejumlah uang tebusan sebagaimana yang telah diminta oleh pelaku. Dalam pasal 27B ayat (1) ini ketentuan pidana diatur dalam pasal 48 ayat (8) Jo. Pasal 45 ayat (9) UU ITE yang menyatakan bahwa dipidana penjara paling lama enam bulan dan/atau denda paling banyak Rp. 1.000.000.000,00 (satu miliar rupiah).

Pada pasal 45 ayat (9) UU ITE yang menyatakan bahwa "Dalam hal perbuatan sebagaimana dimaksud pada ayat (8), dilakukan dalam lingkungan keluarga, penuntutan pidana hanya dapat dilakukan atas aduan". Artinya pada pasal 27B ayat (1) ini merupakan tindak pidana pemerasan yang hanya terjadi di dalam lingkungan keluarga serta penuntutan pidananya pun hanya bisa dilakukan berdasarkan delik aduan. Maka terdapat beberapa unsur objektif yang belum terpenuhi dalam tindak pidana ransomware pada pasal 27B ayat (1). pada dasarnya, unsur-unsur yang

terkandung dalam pasal 27B ayat (1) identik dan memiliki beberapa kesamaan dengan tindak pidana pemerasan konvensional yang diatur dalam Pasal 368 ayat (1) KUHP. Pasal 368 ayat (1) KUHP berbunyi bahwa:

"Barang siapa 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 atau menghapuskan piutang, diancam karena pemerasan dengan pidana penjara paling lama Sembilan bulan".

Akan tetapi, tindak pidana pemerasan yang diatur dalam pasal 368 ayat (1) KUHP ini pelaku yang melakukan kejahatan tidak menggunakan sistem elektronik, tentunya pada alat bukti yang digunakan sudah berbeda. Terdapat perbedaan dua pasal antara KUHP dan UU ITE yaitu pada rumusan pasal 368 ayat (1) KUHP tidak mensyaratkan adanya unsur "tanpa hak mendistribusikan dan/atau mentransmisikan informasi elektronik dan/atau dokumen elektronik" sebagaimana diatur dalam pasal 27B ayat (1) UU ITE tentang pemerasan.

Kemudian berkaitan dengan tindak pidana ransomware juga dapat dikaitkan dengan Pasal 30 ayat (2) UU ITE yang berbunyi "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik". Dalam pasal ini, unsur mengakses komputer dan sistem elektronik terpenuhi untuk membuktikan pelaku tindak pidana ransomware, yang dimana pelaku tindak pidana ransomware ini mengakses sistem komputer untuk mengenkripsi data. Tetapi, terdapat unsur pemerasan yang belum terpenuhi pada pasal 30 ayat (2) UU ITE, dikarenakan pada pasal 30 ayat (2) ini tujuan dari pelaku tindak pidana mengakses sistem komputer untuk memperoleh informasi elektronik atau dokumen elektronik yang tidak dijelaskan secara spesifik terkait dengan tujuan memperoleh informasi elektronik.

Ancaman pidana yang dijatuhkan kepada pelaku yang melanggar pasal 30 ayat (2) ini terdapat 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 tujuh tahun dan/atau denda paling banyak Rp. 700.000.000,00 (tujuh ratus juta rupiah). Pasal 30 ayat (2) Jo. Pasal 46 ayat (2) ini dapat dikenakan terhadap pelaku tindak pidana ransomware apabila perbuatan pelaku ini menimbulkan akibat dengan diperolehnya informasi elektronik dan/atau dokumen elektronik dari komputer korban yang diakses dengan cara apapun. Pengaturan tentang tindak pidana ransomware juga dapat dikaitkan dengan Pasal 32 ayat (1) Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, yang menyatakan bahwa "setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu informasi elektronik dan/atau dokumen elektronik milik orang lain atau milik publik". Dalam pasal 32 ayat (1) ini memiliki unsur-unsur sebagai berikut:

a. Setiap orang;
b. Dengan sengaja;

c. Tanpa hak atau Melawan hukum;
d. Mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, dan menyembunyikan;
e. Informasi elektronik dan/atau dokumen elektronik

Dalam pasal 32 ayat (1) UU ITE ini dapat dipertanggungjawabkan kepada pelaku tindak pidana ransomware, yang dimana terdapat unsur-unsur yang terpenuhi dalam pasal ini. meskipun ada unsur yang tidak mejelaskan secaraspesifik mengenai penafsiran tindak pidana ransomware. Berdasarkan dengan modus operandi serangan ransomware, pelaku menggunakan enkripsi kode binari yang ditambahkan pada dokumen elektronik melalui sistem komputer milik korban yang mengakibatkan data milik korban terkunci. Oleh sebab itu, unsur tanpa hak atau melawan hukum mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan dan menyembunyikan informasi elektronik dan/atau dokumen elektronik telah terpenuhi. Kemudian pengaturan pertanggungawaban tindak pidana ransomware dapat berpedoman pada Pasal 67 ayat (1) UndangUndang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi yang menyatakan bahwa:

> Setiap orang yang dengan sengaja atau melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi sebagaimana dimaksud pada pasal 65 ayat (1) dipidana dengan pidana penjara paling lama lima tahun dan/atau denda paling banyak Rp. 5.000.000.000,00 (lima miliar rupiah).

Dalam Pasal 67 ayat (1) UU Perlindungan Data Pribadi memiliki unsur-unsur dalam tindak pidana yaitu dengan sengaja atau melawan hukum memperoleh atau mengumpulkan data pribadi, tetapi dalam memperoleh atau mengumpulkan data pribadi ini tidak secara spesifik dijelaskan cara memperoleh data tersebut dengan mengakses sistem komputer dengan mengenkripsi file, tetapi unsur pemerasan dengan menguntungkan diri sendiri atau orang lain dalam pasal ini terpenuhi. Penanggulangan kejahatan melalui pendekatan penal akan memiliki fungsi sebagai upaya pencegahan apabila pengaturan pidana tersebut dapat mencegah sejauh mungkin terjadinya tindak pidana tersebut dalam hal ini adalah tindak pidana siber.[14]

Pada kasus tindak pidana ransomware yang terjadi pada rumah sakit dijakarta dan pada tahun 2024 Pusat Data Nasional milik Kementerian Komunikasi dan informatika mengalami serangan ransomware, yang dimana menimbulkan banyak kerugian serta dalam kasus ini sulitnya dilakukan upaya penyidikan dikarenakan sulitnya menemukan alat bukti elektronik yang diguanakan dalam kejahatan ransomware ini. Kejahatan ransomware termasuk dalam kejahatan yang sangat berbahaya dan merugikan berbagai pihak. Oleh karena itu, perlu mengambil Langkah preventif untuk mencegah sistem komputer terkena serangan ransomware, maka terdapat beberapa langkah yang dapat digunakan sebagai berikut:

[14] "Maharani, P., Hafrida, H., & Rapik, M. (2024). Pertanggungjawaban Pidana Hacktivist Dalam Perspektif Hukum Pidana Di Indonesia. PAMPAS: Journal of Criminal Law, 5(2), 242–252. Https://Doi.Org/10.22437/Pampas.V5i2.33291."

a. Memastikan komputer mendapat patch terbaru dan pembaruan terbaru melalui aktivasi fitur "Windows Update", serta 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. Selalu mengaktifkan Windows Firewall yang berguna untuk membuat sebuah aturan pada Windows Firewall sehingga program atau sistem komputer dapat melakukan pembaruan secara otomatis;
d. Berhati-hati pada setiap link yang diterima, terutama berasal dari email spam;
e. mengaktifkan 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 diindikasi tidak aman, maka Google akan memberikan peringatan apabila situs yang hendak dibuka adalah situs berbahaya;
f. melakukan pencadangan data-data penting secara teratur menggunakan media penyimpanan online seperti google drive atau icloud, bahkan bisa juga menggunakan penyimpanan eksternal.[15]

Dari uraian tersebut maka pengaturan petanggungawaban pidana terhadap pelaku tindak pidana ransomware masih kurang jelas. Sehingga, tindak pidana ransomware yang berpedoman pada Pasal 368 ayat (1) KUHP , Pasal 27B ayat (1), Pasal 30 ayat (2), Pasal 32 ayat (1) UU ITE, dan pasal 67 ayat (1) UU Perlindungan Data Pribadi tidak menjelaskan secara spesifik mengenai proporsi "ransomware", terutama pada pemerasan yang mengakses sistem komputer tanpa izin kemudian mengenkripsi data milik korban yang selanjutnya pelaku tindak pidana ransomware meminta tebusan sejumlah uang agar dapat membuka kunci enkripsi pada data tersebut, dan lemahnya keamanan pada sistem komputer yang menyebakan dapat terjadinya serangan ransomware, sehingga kasus serangan ransomware belum diatur secara jelas dalam pasal tersebut, maka dalam pemidanaan pelaku sulit dijatuhi hukuman pidana dan mengingat kejahatan ransomware sangat sulit untuk dibuktikan karena semua peralatan yang digunakan sebagai alat bukti adaah elektronik. Oleh sebab itu, sangat sulit bagi pelaku untuk mempertanggungawabkan tindak pidana ransomware karena unsur-unsurnya belum terpenuhi.

Seharusnya dalam UU ITE ini tindak pidana ransomware memang harus diatur secara langsung serta tidak merujuk pada perbuatannya lainnya. Pada pasal 27B ayat (1) UU ITE mengenai ransomware atau pemerasan, tetapi pemerasan yang dilakukan pada lingkungan keluarga, maka penuntutan pidananya pun hanya dapat dilakukan oleh pihak yang merasa dirugikan *(delik aduan).* Tindak pidana ransomware tidak dapat diselesaiakan dengan pasal 368 ayat (1) KUHP lama dikarenakan ada beberapa unsur yang tidak terpenuhi dalam KUHP yaitu sebagai berikut:

a. Tidak terpenuhinya unsur media utama yang digunakan untuk melakukan tindak pidana ransomware yang belum dikenal didalam KUHP;

[15] Tajriyani, "Op.Cit," n.d., 706–7.

b. Modus operandi pemerasan ransomware berbeda dengan kejahatan konvensional;
c. Dalam KUHP ada keterbatasan yaitu tidak dapat membebankan pertanggungjawaban pidana pada subyek hukum korporasi atau badan hukum yang melakukan tindak pidana ransomware.

Namun, penting untuk dicatat bahwa interpretasi dan penerapan pasal-pasal di atas dapat bervariasi dan memerlukan analisis lebih lanjut Dalam hal ini, ransomware yang tidak diatur secara khusus dalam peraturan di atas menjadikan penafsiran dalam undang-undang masih bersifat terbatas.[16]

2. Bentuk Pertanggungjawaban Pidana Bagi Pelaku Tindak Pidana Ransomware Dalam Perspektif Peraturan Perundang-undangan

Kasus pemerasan dengan ransomware semakin marak terjadi, dengan salah satu contoh menggunakan modus operandi email phising untuk mengenkripsi data yang kemudian pelaku meminta sejumlah uang tebusan agar data tersebut dapat diakses kembali. Salah satu contoh kasus serangan ransomware yaitu terjadi pada Bank Syariah Indonesia (BSI), yang dimana salah satu nasabah BSI asal solo bernama Rochmat Purwanti yang menjadi korban serangan ransomware dengan kerugian Rp. 278.251.749 kerugian ini terjadi setelah korban menerima email dari BSI Net Banking.[17] Kasus ransomware berikutnya adalah serangan ransomware pada pusat data nasional milik Kementerian Komunikasi dan Informasi RI (Kominfo) dengan bentuk serangan ransomware Brain Chiper pengembangan terbaru lockbit yangmengakibatkan beberapa sistem pusat data nasional mengalami gangguan, yang dimana pelaku serangan ransomware ini meminta sejumlah uang tebusan dalam bentuk bitcoin sebanyak US$8 juta (131 miliar).[18]

Akan tetapi, dari kedua kasus diatas belum ada putusan pengadian yang menjatuhkan pidana dalam perkara ini, dikarenakan keterbatasan alat bukti elektronik yang digunakan sebagai barang bukti untuk menjatuhkan sanksi pidana terhadap pelaku sangat sulit untuk diketahui dan peraturan perundang-undangan yang belum secara spesifik mengatur tindak pidana ini.

Selanjutnya penulis berpendapat bahwa pasal-pasal yang dikaitkan dengan tindak pidana ransomware belum secara spesifik mengatur mengenai tindak pidana tersebut, maka dalam menjatuhkan sanksi pidana sebagai bentuk pertanggungawaban pidana bagi pelaku tindak pidana ransomware yang sebagaimana diatur dalam Kitab Undang-Undang Hukum Pidana dan UndangUndang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, dan Undang-Undang Nomor 27 tahun 2022 Tentang Perlindungan Data Pribadi belum terwujud.

---

[16] "Maharani, P., Hafrida, H., & Rapik, M. (2024). Pertanggungjawaban Pidana Hacktivist Dalam Perspektif Hukum Pidana Di Indonesia. PAMPAS: Journal of Criminal Law, 5(2), 242–252. Https://Doi.Org/10.22437/Pampas.V5i2.33291."

[17] Andri wijaya Aksana, "Pemidanaan Cyber Crime Dalam Perspektif Huum Pidana Positif," *Journal of Physics A: Mathematical and Theoretical* 35, no. 1 (2019): 1–14, https://doi.org/10.1088/1751-8113/44/8/085201.

[18]CNNIndonesia,DiaksesPada20Januari2025padapukul11.40WIB.https://www.cnnindonesia.com/teknologi/20240624140714-185-1113434/pusat-data-nasional-diserang-pelaku-minta-tebusan-rp131-miliar/amp,

Bentuk pertanggungjawaban pidana terhadap pelaku tindak pidana ransomware yang diatur dalam Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas UndangUndang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, selain itu diatur juga dalam pasal 67 ayat (1) UndangUndang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. rumusan UU ITE yang dikaitkan dengan tindak pidana ransomware yaitu Pasal 27B ayat (1) Jo. Pasal 45 ayat (8), Pasal 30 ayat (2) Jo. Pasal 46 ayat (2), dan Pasal 32 ayat (1) Jo. Pasal 48 ayat (1) UU ITE. Berdasarkan rumusan pasal tersebut yang dikaitkan dengan tindak pidana ransomware dalam UU ITE. Subyek hukum dalam tindak pidana cyber crime sebagaimana dimaksud dalam Pasal 1 angka 21 UU ITE yang berbunyi bahwa "Orang adalah orang perseorangan, baik warga negara Indonesia, warga negara asing, maupun badan hukum". Maka pelaku tindak pidana ransomware atau yang biasa disebut dengan subjek hukum dapat diminta pertanggungawaban pidana atas perbuatan pidana yang dilakukan pelaku, dimana orang yang memiliki arti bahwa pelaku tindak pidana, serta badan hukum yaitu korporasi sebagai subyek hukum tindak pidana cyber crime. Terdapat syarat-syarat pertanggungjawaban pidana korporasi sebagai subyek hukum yaitu mengenai kondisi suatu korporasi yang dikatakan telah melakukan tindak pidana, yang dimana terkait dengan pihak-pihak yang pada dasarnya dimintai pertanggungjawaban dalam hal korporasi itu sendiri yang melakukan tindak pidana apakah pelaku tindak pidana itu pengurusnya, atau pengurus dan korporasi, ataukah justru korporasi itu sendiri yang dapat dimintai pertanggungjawaban. Selain itu pula perlu diatur tentang bentuk pedoman pemidanaan terhadap korporasi agar tidak terjadi disparitas pemidanaan.[19]

Maka dapat dikatakan bahwa Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik menganut ajaran identifikasi *(Doctrine of Identification),* dapat dibuktikan dengan diterimanya pertanggungjawaban pidana korporasi *(corporate criminal liability)* yang dimana pelaku tindak pidananya adalah korporasi itu sendiri *(corporate crime)*.[20] Dengan adanya adagium hukum yang telah lama sekali dianut dalam peraturan perundang-undangan pidana yaitu '*Actus non facit reum, nisi mens sit rea'*, yang dimana dinyatakan bahwa tiada pidana tanpa kesalahan (geen straf zonder schuld) yang merupakan perlindungan bagi setiap orang, terutama bagi pelaku tindak pidana agar tidak terjadi kesewenangan dari aparat yang berwenang.[21] Konsep pertanggungjawaban pidana dalam KUHP menganut ajaran pertanggungjawaban yang ketat *(Doctrine of strict liability)*, selain itu dalam KUHP juga menggunakan konsep pertanggungjawaban pidana dengan menganut ajaran pengganti *(Doctrine of*

[19] Imam Makhali, "Bentuk Pertanggung Jawaban Pidana Bagi Pelaku Tindak Pidana Mayantara," *Jurnal Transparansi Hukum* 6, no. 1 (2023): 31–43, https://doi.org/10.30737/transparansi.v6i1.4226.

[20] Laila Mulasari, "Ajaran Pertanggungjawaban Pidana Korporasi Dalam Kebijakan Hukum Pidana Di Bidang Mayantara," *Jurnal Hukum Dan Dinamika Masyarakat* 9, no. 2 (2019): 113–20. https://jurnal.untagsmg.ac.id/index.php/hdm/article/view/301

[21] Sahuri Lasmadi, "Pertanggungjawaban Korporasi Dalam Perspektif Kebijakan Hukum Pidana Indonesia," *Disertasi Universitas Airlangga*, 2003, 1–239. https://repository.unair.ac.id/28616/

vicarious liability) yang secara khsusu mengatur mengenai pertanggungjawaban pidana terhadap korporasi sebagai pelaku.[22]

Bentuk pertanggungjawaban pidana terhadap pelaku ransomware dikenakan sanksi berdasarkan pada perbuatannya, seperti pertanggungjawaban pidana yang pelakunya adalah orang sebagai pelaku utama dalam kejahatan ransomware dikenakan pidana dengan berpedoman pada beberapa peraturan perundang-undangan yaitu KUHP, UU ITE, dan UU Perlindungan Data pribadi yang telah dijelaskan diatas, setelah itu jika pertanggungawaban pidana yang dilakukan oleh organisasi atau perusahaan sebagai pelaku maka diterapkan pertanggungawaban pidana korporasi. Dalam kasus ransomware, bukti yang diperlukan untuk mempertanggungajawabkan perbuatan pelaku sulit untuk ditemukan.

D. SIMPULAN

Pengaturan pertanggungjawaban pidana terhadap pelaku tindak pidana ransmware dapat berpedoman pada Pasal 27B ayat (1) UU ITE, Pasal 30 ayat (2) UU ITE, Pasal 32 ayat (1) UU ITE, Pasal 368 KUHP, dan pasal 67 ayat (1) UU Perlindungan Data Pribadi dengan cara menjatuhkan sanksi pidana terhadap pelaku sebagai bentuk pertanggungawaban pelaku tindak pidana ransomware. Akan tetapi, pengaturan tentang pertanggungjawaban pidana terhadap pelaku tindak pidana ransomware dalam peraturan perundang-undangan tersebut masih mengalami kekaburan norma, dimana unsur-unsur pasal yang digunakan untuk menjerat pelaku agar mempertanggungawabkan perbuatannya belum terpenuhi, serta tidak adanya penegasan aturan mengenai tindak pidana ransomware sehingga menyebabkan kasus ini sulit untuk dibuktikan. Bentuk pertanggungawaban pidana terhadap pelaku tindak pidana ransomware dalam perspektif peraturan perundang-undangan, selain berpedoman dalam Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan kedua Atas UndangUndang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, dapat berpedoman juga pada KUHP dan UndangUndang Nomor 27 Tahun 2022 Tentang Perindungan Data Pribadi. Menjatuhkan sanksi pidana bagi pelaku tindak pidana ransomware sebagai bentuk pertanggungawaban pidana sampai saat ini belum terwujud, hal ini dikarenakan belum ada pasal yang mengatur secara jelas sehingga tidak dapat dipertanggungawabkan.

[22] *Mulasari, Op.Cit. Hlm. 118*

DAFTAR PUSTAKA

(BSSN), Badan Siber dan Sandi Negara. "BSSN Identifikasi Pusat Data Nasional Sementara Diserang Ransomware." Jun 24, 2024, (2024).

Agung, Hafrida, Erwin. Pencegahan Kejahatan Terhadap Cybercrime. PAMPAS: Journal of Criminal Law, Vol.3 No.2, (2022).

Aksana, Andri wijaya. "Pemidanaan Cyber Crime Dalam Perspektif Hukum Pidana Positif." Journal of Physics A: Mathematical and Theoretical Vol. 35 No.1 (2019). DOI: https://doi.org/10.1088/1751-8113/44/8/085201.

K. Tus, Desyanti Suka Asih. "Perlindungan Hukum Bagi Korban Serangan Ransomware." Vyavahara Duta Vol.16, No. 2 (2021). DOI: https://doi.org/10.25078/vd.v16i2.2909.

Lasmadi, Sahuri. "Pertanggungjawaban Korporasi Dalam Perspektif Kebijakan Hukum Pidana Indonesia." Disertasi Universitas Airlangga, 2003.

Maharani, P., Hafrida, H., & Rapik, M. (2024). Pertanggungjawaban Pidana Hacktivist Dalam Perspektif Hukum Pidana Di Indonesia. PAMPAS: Journal of Criminal Law, Vol.5 No.2 (2024), DOI: Https://Doi.Org/10.22437/Pampas.V5i2.33291.

Makhali, Imam. "Bentuk Pertanggung Jawaban Pidana Bagi Pelaku Tindak Pidana Mayantara." Jurnal Transparansi Hukum 6, no. 1 (2023): 31–43. DOI: https://doi.org/10.30737/transparansi.v6i1.4226.

Marzuki, Peter Mahmud. Penelitian Hukum. Edisi Revi. Jakarta: Penerbit Kencana Prenada Media Grup, 2005.

Mulasari, Laila. "Ajaran Pertanggungjawaban Pidana Korporasi Dalam Kebijakan Hukum Pidana Di Bidang Mayantara." Jurnal Hukum Dan Dinamika Masyarakat Vol.9 No. 2 (2019).

Nasional. "BPPTIK Kementerian Komunikasi Dan Informatika RI," 2022.

Pansariadi, Rafi Septia Budianto, and Noenik Soekorini. "Tindak Pidana Cyber Crime Dan Penegakan Hukumnya." Binamulia Hukum Vol.12 No. 2 (2023). DOI: https://doi.org/10.37893/jbh.v12i2.605.

Putri, Nisa Nindia, Sahuri Lasmadi, and Erwin Erwin. "Pertanggungjawaban Pidana Perusahaan Pers Terhadap Pemberitaan Yang Mencemarkan Nama Baik Orang Lain Melalui Media Cetak Online." PAMPAS: Journal of Criminal Law Vol.2 No. 2 (2021). DOI: https://doi.org/10.22437/pampas.v2i2.14761.

Republik Indonesia, Undang-Undang Nomor 1 Tahun 1946 Tentang Peraturan hukum pidana (Kitab Undang-Undang Hukum Pidana).

Republik Indonesia, Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan transaksi elektronik, LNRI Tahun 2024 Nomor 1, TLNRI Nomor 6905.

Republik Indonesia, Undang-undang Nomor 27 Tahun 2022 Tentang Perlindungan Data

Pribadi, LNRI Tahun 2022 Nomor 196, TLNRI Nomor 6820.

Tajriyani, Nur Syamsi. "Pertanggungjawaban Pidana Tindak Pidana Pemerasan Dengan Modus Operandi Penyebaran Ransomware Cryptolocker." Jurist-Diction Vol.4 No. 2 (2021). DOI: https://doi.org/10.20473/jd.v4i2.25785.