KEMENTERIAN PENDIDIKAN TINGGI,
SAINS, DAN TEKNOLOGI
UNIVERSITAS JAMBI
FAKULTAS HUKUM

PERTANGGUNGJAWABAN PIDANA TERHADAP PELAKU TINDAK PIDANA RANSOMWARE DALAM PERSPEKTIF PERATURAN PERUNDANG-UNDANGAN

SKRIPSI

Disusun sebagai salah satu syarat untuk memperoleh gelar
Sarjana Hukum (S.H)

SUCI WAHYUNING ROBBI
B1A121104

Pembimbing:

Prof. Dr. Hafrida, S.H., M.H.,

Tri Imam Munandar, S.H., M.H.,

JAMBI

2025

KEMENTERIAN PENDIDIKAN TINGGI,
SAINS, DAN TEKNOLOGI
UNIVERSITAS JAMBI
FAKULTAS HUKUM

PERSETUJUAN SKRIPSI

Skripsi ini diajukan oleh :

Nama	: **Suci Wahyuning Robbi**
Nomor Mahasiswa	: **B1A121104**
Program Kekhususan	: **Hukum Pidana**
Judul Skripsi	:**Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Ransomware Dalam Perspektif Peraturan Perundang-undangan.**

Telah disetujui oleh pembimbing pada tanggal seperti tertera di bawah ini untuk dipertahankan di hadapan Tim Penguji Fakultas Hukum Universitas Jambi

Jambi, Februari 2025

Pembimbing I	**Pembimbing II**
Prof. Dr. Hafrida, S.H., M.H.,	**Tri Imam Munandar, S.H., M.H.,**
NIP. 196505181990012001	**NIP. 199006072024211001**

i

KEMENTERIAN PENDIDIKAN TINGGI,
SAINS, DAN TEKNOLOGI
UNIVERSITAS JAMBI
FAKULTAS HUKUM

PENGESAHAN SKRIPSI

Skripsi ini diajukan oleh	:	
Nama	:	Suci Wahyuning Robbi
NIM	:	B1A121104
Program Kekhususan	:	Hukum Pidana
Judul Skripsi	:	Pertanggungjawaban Pidana Terhadap pelaku Tindak Pidana Ransomware Dalam Perspektif Peraturan Perundang-undangan.

Tugas Akhir ini telah dipertahankan di hadapan Tim Penguji Fakultas Hukum Universitas Jambi, pada tanggal Maret 2025

Dan dinyatakan LULUS

TIM PENGUJI

NAMA	JABATAN	TANDA TANGAN
1. Prof. Dr. Hafrida, S.H., M.H.,	Ketua Tim Penguji	.....
2. Dr. Elizabeth Siregar, S.H., M.H.,	Penguji Utama	.....
3. Tri Imam Munandar, S.H., M.H.,	Anggota	.....

Mengetahui
Dekan Fakultas Hukum
Universitas Jambi

Prof. Dr. Usman, S.H., M.H.,
NIP. 196405031990031004

PERNYATAAN ORISINALITAS

Dengan ini menyatakan bahwa:

1. Tugas akhir ini adalah asli dan belum pernah diajukan untuk mendapat gelar akademik sarjana, baik di Universitas Jambi maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini murni gagasa, rumusan dan penelitian saya tanpa bantuan pihak lain, kecuali arahan Pembimbing Tugas Akhir.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat yang ditulis atau dipublikasikan orang lain secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan dicantumkan dalam daftar Pustaka.
4. Pernyataan ini saya buat dengan sesungguhnya dan apabila kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya tulis ini, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Jambi, 29 Januari 2025

Yang membuat pernyataan

SUCI WAHYUNING ROBBI
B1A121104

KATA PENGANTAR

Puji Syukur penulis panjatkan kehadirat Allah SWT, karena atas berkat dan Rahmat-Nya penulis dapat menyelesaikan penulisan skripsi ini yang berjudul "Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Ransomware Dalam Perspektif Peraturan Perundang-undangan". Skripsi ini sebagai salah satu syarat untuk memperoleh gelar Sarjana Hukum (S.H) pada Fakultas Hukum Universitas Jambi.

Dalam penulisan skripsi ini penulis terkhusus mengucapkan terima kasih kepada kedua orang tua tercinta, Bapak Mawarno dan Ibu Sukarti yang telah berjuang serta berkorban tiada henti memberikan dukungan, semangat, doa, dan serta telah memberikan kasih dan sayang sehingga penulis dapat menyelesaikan skripsi ini dan menyandang gelar Sarjana Hukum. Penulis juga diberikan arahan, bimbingan serta saran yang membangun, motivasi, nasehat serta banyak dukungan dari Dosen Pembimbing, sehingga penulis mengucapkan terima kasih yang sebesar-besarnya kepada Dosen Pembimbing I Prof. Dr. Hafrida, S.H., M.H., dan Dosen Pembimbing II Tri Imam Munandar, S.H., M.H., Selain itu, Penulis juga mengucapkan terimakasih yang sebesar-besarnya kepada semua pihak yang telah memberikan dukungan dan semangat selama proses penyusunan skripsi ini.

1. Prof. Dr. Helmi, S.H., M.H., Rektor Universitas Jambi, yang telah memberikan kesempatan kepada penulis sebagai mahasiswa untuk melaksanakan studi di Fakultas Hukum Universitas Jambi.

2. Prof. Dr. Usman, S.H., M.H., Dekan Fakultas Hukum Universitas Jambi, yang telah memberikan fasilitas perkuliahan dalam melaksanakan studi di Fakultas Hukum Universitas Jambi.
3. Prof. Dr. Hj. Muskibah, S.H., M.Hum., Wakil Dekan Bidang Akademik, Kerja sama, dan Sistem Informasi pada Fakultas Hukum Universitas Jambi, yang telah memberikan persetujuan terhadap syarat siding skripsi.
4. Dr. Umar Hasan, S.H., M.H., Wakil Dekan Bidang Umum, Perencanaan, dan Keuangan Pada Fakultas Hukum Universitas Jambi yang telah memenuhi sarana dan prasarana perkuliahan sehingga penulis dapat mengenyam Pendidikan kuliah dengan layak.
5. Dr. Zarkasi, S.H., M.Hum., Wakil Dekan Bidang Kemahasiswaan dan Alumni pada Fakultas Hukum Universitas Jambi, yang telah memenuhi sarana dan prasarana perkuliahan sehingga penulis dapat mengenyam pendidikan kuliah dengan layak.
6. Dr. Akbar Kurnia Putra, S.H., M.H., Ketua Program Studi Ilmu Hukum Fakultas Hukum Universitas Jambi, yang telah menyetujui judul dalam penulisan skripsi ini dan memberikan kemudahan kepada penulis dalam menyelesaikan administrasi yang berkaitan dengan skripsi.
7. Dr. Taufik Yahya, S.H., M.H., Dosen Pembimbing Akademik Penulis, yang telah banyak membantu, memberikan arahan serta nasihat dari awal penulis menjadi mahasiswa di Fakultas Hukum Universitas Jambi.

8. Bapak dan Ibu Dosen Fakultas Hukum Universitas Jambi yang telah memberikan banyak ilmu dan pengetahuan yang sangat berguna kepada penulis selama masa perkuliahan.
9. Seluruh Staf dan Karyawan Kependidikan Tata Usaha Fakultas Hukum Universitas jambi yang telah banyak membantu penulis dalam hal keadministrasian.
10. Kepada adik tercinta penulis, Alesha Ayunindya Robbi yang senantiasa memberikan doa, memberikan semangat dan kasih sayang kepada penulis serta telah memberikan banyak dukungan kepada penulis sehingga penulis dapat menyelesaikan skripsi ini dengan baik dan akhirnya penulis menyandang gelar Sarjana Hukum.
11. Kepada Pratiwi Arnandes Putri, terimkasih telah menjadi saudara tak sedarah penulis, yang telah membersamai penulis selama masa perkuliahan dan memberikan semangat kepada penulis serta banyak membantu penulis dalam penulisan skripsi.
12. Kepada Nopi Novriyanti, S.H., Rehan Fahri Septiawan, S.H., Clara Kirani Masywandi, Hati Hayati, Sukri Pratama Putra, Rizki Adi Pratama, Bayu Rizky, Jeremi Kelvin Hutagalung, Andreas Prasojo, Kisan Rudianto Sianturi, selaku sahabat penulis selama masa perkuliahan yang telah memberikan banyak dukungan serta semangat kepada penulis.

Penulis menyadari bahwa dalam penulisan skripsi ini masih jauh dari kata sempurna, maka penulis memohon maaf jika dalam penulisan skripsi ini terdapat kekeliruan penulisan atas kesalahan yang tidak disengaja oleh penulis serta penulis

penulis menyadari bahwa masih terdapat banyak kekurangan pada penulis. Oleh karena itu, penulis mengharapkan kritik dan saran dari Dosen Pembimbing sangattlah membantu penulis guna untuk kesempurnaan dalam penulisan skripsi ini.

Semoga segala kebaikan yang telah mereka berikan kepada penulis balasan, diberikan Kesehatan lahir dan batinnya, serta dilancarkan segala rezeki dan urusannya oleh Allah SWT. Penulis juga memohon maaf kepada semua pihak apabila terdapat kesalahan dalam bertutur kata dan tindakan selama berinteraksi dan berproses selama masa perkuliahan di Fakultas Hukum Universitas Jambi. Semoga skripsi ini dapat bermanfaat dan menambah pengetahuan kepada seluruh orang yang membaca skripsi ini. Aaminn

Jambi, 30 Januari 2025

Penulis

SUCI WAHYUNING ROBBI
NIM B1A121104

ABSTRAK

Tujuan dari penelitian ini adalah untuk mengetahui dan menganalisis pengaturan pertanggungjawaban pidana terhadap pelaku tindak pidana ransomware, dan untuk mengetahui dan menganalisis bentuk pertanggungjawaban pidana bagi pelaku tindak pidana ransomware dalam perspektif peraturan perundang-undangan. Jenis penelitian adalah yuridis normative. Perumusan masalah ini adalah Bagaimana pengaturan pertanggungjawaban pidana terhadap pelaku tindak pidana ransomware, dan Bagaimana bentuk pertanggungjawaban pidana bagi pelaku tindak pidana ransomware dalam perspektif peraturan perundang-undangan. Adapun hasil dari penelitian ini menunjukkan bahwa pengaturan tentang pertanggungawaban pidana terhadap pelaku tindak pidana ransomware 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 cara menjatuhkan pidana sebagai bentuk pertanggungjawaban pidana pelaku atas tindak pidana ransomware. Akan tetapi, pengaturan tentang pertanggungjawaban pidana tehadap pelaku tindak pidana ransomware dalam peraturan perundang-undangan tersebut masih mengalami kekaburan norma, yang dimana terdapat unsur-unsur ransomware yang tidak terpenuhi sehingga belum ada pasal yang secara spesifik mengatur mengenai ransomware, maka pelaku tindak pidana ransomware sulit untuk diminta pertanggungjawaban pidana, serta tidak ada penegasan dalam aturan tersebut sehingga kasus ini sulit dibuktikan. Bentuk pertanggungjawaban pidana bagi pelaku tindak pidana ransomware dalam perspektif peraturan perundang-undangan sebagaimana telah berpedoman pada UU ITE, KUHP dan UU Perlindungan Data Pribadi belum terwujud, hal ini dikarenakan dalam menjatuhkan sanksi pidana kepada pelaku beum ada pasal yang digunakan secara jelas, sehingga tidak dapat diminta pertanggungjawaban pidana.

Kata kunci: pertanggungjawaban pidana, pelaku, dan tindak pidana ransomware

CRIMINAL LIABILITY FOR PERPETRATORS OF RANSOMWARE CRIMES FROM THE PERSPECTIVE OF STATUTORY REGULATIONS

ABSTRACT

The purpose of this study is to find out and analyze the regulation of criminal liability for perpetrators of ransomware crimes, and to find out and analyze the form of criminal liability for perpetrators of ransomware crimes from the perspective of laws and regulations. The type of research is normative juridical. The formulation of this problem is How is the regulation of criminal liability for perpetrators of ransomware crimes, and What is the form of criminal liability for perpetrators of ransomware crimes from the perspective of laws and regulations. The results of this study indicate that the regulation of 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 penalties as a form of criminal liability for perpetrators of ransomware crimes. However, the regulation on criminal liability for perpetrators of ransomware crimes in the legislation is still experiencing unclear norms, where there are elements of ransomware that are not fulfilled so that there are no articles that specifically regulate ransomware, so it is difficult to hold perpetrators of ransomware crimes criminally accountable, and there is no affirmation in the regulation so that this case is difficult to prove. The form of criminal liability for perpetrators of ransomware crimes in the perspective of legislation as guided by the ITE Law, the Criminal Code and the Personal Data Protection Law has not been realized, this is because in imposing criminal sanctions on the perpetrators there are no articles that are used clearly, so they cannot be held criminally accountable.

***Keywords**: criminal liability, perpetrators, and ransomware crime*

DAFTAR ISI

BAB I
PENDAHULUAN

A. Latar Belakang Masalah

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 hukum pidana Indonesia menganut sistem pertanggungjawaban berdasarkan dengan unsur kesalahan. Seseorang dapat dipidana atas perbuatannya yang melanggar hukum melalui proses pertanggungjawaban pidana. Menurut Roeslan Saleh, pertanggungjawaban ini terdiri dari dua komponen yaitu celaan objektif artinya tindakan yang dilarang dan celaan subjektif artinya tindakan yang dilakukan oleh pelaku, Adanya kesalahan, baik secara sengaja maupun tidak sengaja, merupakan elemen penting dalam pertanggungjawaban pidana.[2] Jika tidak ada kesalahan, seseorang tidak dapat dipertanggungjawabkan secara pidana berdasarkan asas legalitas dan tiada pidana.

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

[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* Vol 2, no. 2 (2021): hlm 131. https://doi.org/10.22437/pampas.v2i2.14761.

[2]Roeslan saleh, *Pikiran-Pikiran Tentang Pertanggung Jawaban Pidana*, Cetakan Pertama, Jakarta, Ghalia Indonesia, 1982. hlm 33.

yang memiliki kekuasaan atas sistem komputer dan jaringan internet.[3] Salah satu jenis kejahatan *cyber crime* yaitu kejahatan 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 Everret, Ransomware merupakan jenis malware yang menyerang pengguna *(user)* dalam mengakses atau membatasi akses mereka kedalam sistem maupun file, dengan mengunci atau mengenkripsi file sampai 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

---

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

[4]Desyanti Suka Asih K.Tus, "Perlindungan Hukum Bagi Korban Serangan Ransomware," *Jurnal Vyavahara Duta* Vol 16, no. 2 (2021): hlm. 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.

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] Hukum Siber *(Cyber Law)* adalah istilah hukum yang terkait dengan pemanfaatan teknologi informasi. Istilah lain yang juga digunakan adalah hukum Teknologi Informasi *(Law of Information Techonology)*, Hukum Dunia Maya *(Virtual World Law)* dan Hukum Mayantara.[7]

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.[8] Menurut data Kaspersky, pada tahun 2023 kejahatan *cyber crime* menggunakan *ransomware* kepada pengguna terdeteksi yang terjadi di Indonesia semakin meningkat.[9] Bank Syariah Indonesia (BSI) juga mengalami serangan siber

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

[7]Ibrahim Fikma Edrisy, *Pengantar Hukum Siber*, cetakan Pertama (Lampung: Sai Wawai Publishing, 2019),

[8]BPPTIK Kementerian Komunikasi Dan Informatika RI, 2022, di akses pada 26 Agustus 2024 pukul 12.00, *https://bpptik.kominfo.go.id/Publikasi/detail/logo-dan-identitas-visual#.*

[9]CNN Indonesia, "Serangan Siber Menggila, 411 Ribu Malware Baru Muncul Tiap Hari Di RI," n.d. diakses pada 26 agustus 2024 pukul 12.00, *https://www.cnnindonesia.com/teknologi/20240522130109-185-1100872/serangan-siber-menggila-411-ribu-malware-baru-muncul-tiap-hari-di-ri/amp.*

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.[10]

Dalam kasus ini terdapat alat-alat bukti elektronik yang digunakan untuk penyidikan lebih lanjut untuk mengungkap serangan ransomware yang menggunakan virus malware pengembangan terbaru dari ransomware yaitu *lockbit 3.0.* Hal ini diketahui setelah melakukan penyelidikan sejak terjadinya gangguan pada pusat data nasional. Serangan kejahatan siber juga dapat dideteksi melalui analisis data, maka dengan menganalisis data yang dikumpulkan dari berbagai sumber, seperti log jaringan, sensor keamanan, atau riwayat aktivitas pengguna, organisasi dapat menemukan pola atau kejanggalan tertentu yang mengindikasikan adanya serangan kejahatan siber.[11] Motif yang digunakan pelaku dalam kasus ini adalah motif ekonomi yang dimana pelaku meminta sejumlah uang sebagai tebusan dari data korban yang terkunci. Ada 3 (tiga) hal yang menjadi panduan dalam menggunakan alat bukti elektronik dalam suatu perkara Informasi dan transaksi elektronik yaitu:

a. Adanya motif *(alasan dalam melakukan perbuatan pidana).*

[10]Badan Siber dan Sandi Negara (BSSN), "BSSN Identifikasi Pusat Data Nasional Sementara Diserang Ransomware," Jun 24, 2024, Di akses pada 11 september 2024 pukul 14.00, *https://www.bssn.go.id/bssn-identifikasi-pusat-data-nasional-sementara-diserang-ransomware/.*

[11]Tri Ginanjar Laksana and Sri Mulyani, "Pengetahuan Dasar Identifikasi Dini Deteksi Serangan Kejahatan Siber Untuk Mencegah Pembobolan Data Perusahaan," *Jurnal Ilmiah Multidisiplin* 3, no. 01 (2024): 109–22, https://doi.org/10.56127/jukim.v3i01.1143.

b. Adanya pola *(modus operandi)* yang relatif sama dengan melakukan tindak pidana menggunakan sistem komputer.

c. Adanya persamaan dengan peristiwa yang lain. [12]

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 Undang-Undang 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".

[12]Sahuri Lasmadi, "Pengaturan Alat Bukti Dalam Tindak Pidana Dunia Maya," *Jurnal Ilmu Hukum*, no. 2 (2014): 1–23. https://media.neliti.com/media/publications/43274-ID-pengaturan-alat-bukti-dalam-tindak-pidana-dunia-maya.pdf.

Pemerasan yang dilakukan dalam lingkungan keluarga pelaku yang dimana termasuk dalam kategori delik aduan artinya hanya dapat dilaporkan oleh pihak yang merasa dirugikan akibat dari tindak pidana pemerasan tersebut. Terdapat beberapa Unsur-sunsur kejahatan ransomware tidak terpenuhi dalam pasal tersebut. Sehingga pelaku tindak pidana ransomware tidak dapat dipertanggungjawabkan dengan pasal 27B ayat (1). Tetapi, tindak pidana ransomware dapat dikaitkan dengan ketentuan pasal 30 ayat (2) Undang-Undang ITE yang menyatakan bahwa "Setiap orang dengan sengaja atau tanpa hak melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik". Pasal ini mengatur mengenai pelaku yang mengakses komputer untuk mencuri dokumen elektronik atau informasi elektronik yang biasa disebut dengan hacker *(peretas)*, terdapat unsur pemerasan yang tidak terpenuhi dalam pasal ini.

Pertanggungjawaban pidana terhadap kejahatan ransomware juga dapat dikaitkan dengan pasal 32 ayat (1) Undang-Undang ITE menyatakan bahwa: "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan tranmisi, merusak, menghilangkan, memindahkan, menyembunyikan sesuatu informasi elektronik dan/atau dokumen elektronik milik orang lain atau milik publik". Menurut pasal 368 ayat (1) Kitab Undang-Undang Hukum Pidana (KUHP):

> 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 mengahapuskam piutang, diancam karena pemerasan dengan pidana penjara paling lama Sembilan bulan.

Pasal 368 ayat (1) KUHP ini menjelaskan bahwa seseorang yang melakukan pemerasan tetapi tidak menggunakan kecanggihan teknologi dalam menguntungkan diri sendiri. Tindak pidana pemerasan merupakan suatu kejahatan konvensional, tetapi dengan adanya kejahatan pemerasan jenis baru yang menggunakan sistem komputer atau sistem elektronik maka unsur-unsur tindak pidananya pun berbeda karena menggunakan teknologi serta alat bukti digital. Undang-undang ITE pada dasarnya mengatur berbagai tindak pidana yang dilakukan melalui dunia maya atau sistem komputer. Namun, kejahatan ransomware yang menyebarkan virus malware pada komputer belum ada pasal yang secara jelas mendeskripsikam unsur-unsur tindak pidana ransomware dalam undang-undang ITE. Oleh karena itu, tindak pidana ransomware menimbulkan kekaburan norma, yang dimana dalam Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik belum ada pasal yang mengatur secara jelas tentang tindak pidana ransomware.

Beberapa kendala yang muncul dalam penegakan terhadap pelaksanaan kebijakan penegakan hukum bagi pelaku penyebaran virus komputer *Ransomware Wannacry* berdasarkan ketentuan hukum yang terdapat dalam Undang-Undang Informasi Dan Transaksi Elektronik adalah sebagai berikut:[13]

a. Kendala dalam penanganan pidana penyebaran virus komputer *Ransomware wannacry.*

[13]Nourma dewi irfan arief kurniawan, hadi mahmud, "Penyebaran Virus Ransomware Wannacry Berdasarkan Undang-Undang Nomor 11 Tahun 2008," *Jurnal Inovasi Penelitian* 1, no. 2 (2021): 48–55.

b. Penanganan pidana penyebaran virus komputer *Ransomware wannacry.*

Memperbaiki aturan hukum pidana merupakan tujuan kebijakan dalam memerangi kejahatan. Dengan demikian, kebijakan hukum pidana merupakan bagian dari kebijakan penanggulangan kejahatan *(politik kriminal)*.[14] Pertanggungjawaban pidana adalah bagian penting dari hukum pidana dan tidak ada artinya pidana diancamkan pada pelaku tindak pidana jika pelakunya tidak diminta untuk mempertanggung jawabkan tindak pidana tersebut. Proses penegakan hukum acara pidana sangat penting untuk menentukan apakah seseorang dapat atau tidak dapat diminta mempertanggung jawabkan tindak pidana yang diduga dilakukan.[15] Pertanggungjawaban pidana adalah keadaan yang dimana dapat menyebabkan pelaku tindak pidana *(strafuitsluitingsgronden),* yang Sebagian adalah untuk penghapus kesalahan.[16] Dipidananya seorang pelaku kejahatan ransomware tidak cukup jika hanya melakukan perbuatan yang bersifat melawan hukum, tetapi harus memenuhi unsur bahwa pelaku yang melakukan tindak pidana mempunyai kesalahan.

Berdasarkan hal-hal yang telah diuraikan diatas, maka penulis tertarik untuk Menyusun skripsi yang berjudul **"Pertanggungjawaban Pidana Terhadap**

---

[14]Pansariadi and Soekorini, "Tindak Pidana Cyber Crime Dan Penegakan Hukumnya". *Jurnal Binamulia Hukum* Vol 12 No. 2, 2023, hlm. 293, https://doi.org/10.37893/jbh.v12i2.605.

[15]Putu Andhika Kusuma Yadnya I Dewa Gede Budiarta and I Dewa Nyoman Gde Nurcana, "Kajian Yuridis Terhahap Pertanggungjawaban Tindak Pidana Informasi Dan Transaksi Elektronik (ITE)," *Jurnal Unhi Vidya Wertta,* Vol 6 No 1, 2023, hlm 3. https://books.google.com/books?hl=en&lr=&id=lRKfEAAAQBAJ&oi=fnd&pg=PP1&dq=yuridis+or+hukum+and+rekam+medis+elektronik+and+implementasi+or+penerapan&ots=_NNtz_FJrY&sig=LRrqJ7LADqfGIjr7gVTvYStmtn*c.*

[16]Hukum Online,*https://www.hukumonline.com/berita/a/memahami-pertanggungjawaban-pidana-dalam-kuhp-baru-lt65da29d97d621/%23*. Diakses pada tanggal 9 september 2024 pukul 13.00 WIB.

Pelaku Tindak Pidana Ransomware Dalam Perspektif Peraturan Perundang-Undangan."

B. Rumusan Masalah

Berdasarkan uraian yang telah dipaparkan diatas, maka penulis menarik suatu rumusan masalah, yaitu sebagai berikut:

1. Bagaimana pengaturan pertanggungjawaban pidana terhadap pelaku tindak pidana ransomware?
2. Bagaimana bentuk pertanggungjawaban pidana bagi pelaku tindak pidana ransomware dalam perspektif peraturan perundang-undangan?

C. Tujuan Penelitian

Berdasarkan pada rumusan masalah diatas, penelitian ini bertujuan sebagai berikut:

a. Untuk mengetahui dan menganalisis peraturan tentang pertanggungjawaban pidana terhadap pelaku tindak pidana ransomware.
b. Untuk mengetahui dan menganalisis bentuk pertanggungjawaban pidana bagi pelaku tindak pidana ransomware dalam perspektif peraturan perundang-undangan.

D. Manfaat Penelitian

Berdasarkan permasalahan, penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

a. Manfaat Teoretis

Secara teoretis hasil penelitian ini diharapkan dapat menjadi dasar untuk penelitian tambahan dalam berbagai karya ilmiah, yang kemudian dapat

bermanfaat untuk kemajuan ilmu hukum pidana. Khususnya terkait pertanggungjawaban pidana terhadap pelaku tindak pidana ransomware dalam perspektif peraturan perundang-undangan.

b. Manfaat Praktis

Secara praktis manfaat penelitian ini dapat dijadikan masukan dan pengetahuan bagi masyarakat dan pedoman penegakan hukum agar tidak melanggar asas-asas hukum positif. Diharapkan penelitian ini dapat menjadi rujukan atau referensi bagi penelitian-penelitian diwaktu yang akan datang.

E. Kerangka Konseptual

Sebelum melangkah pada uraian selanjutnya, penulis terlebih dahulu akan menjelaskan maksud dari judul penelitian ini agar mempermudah dalam menjabarkan permasalahan serta untuk menghindari penafsiran yang berbeda, maka penulis memberikan Batasan sebagai berikut:

1. Pertanggungjawaban Pidana

Pertanggungjawaban pidana *(Criminal Responsibility)* adalah suatu pemidanaan yang dimana pelaku tindak pidana telah terbukti melakukan suatu perbuatan pidana dan memenuhi unsur-unsur yang terdapat dalam peraturan perundang-undangan yang berlaku.[17] Pertanggungjawaban pidana didasarkan pada asas kesalahan yang artinya seseorang dapat dipidana jika telah terbukti melakukan tindak pidana.

[17]Lukman Hakim, *Asas-Asas Hukum Pidana.* Penerbit Deepublish; Sleman, 2020. Hlm. 35

2. Pelaku

Pelaku *(pleger)* adalah seseorang yang melakukan suatu perbuatan yang dilarang oleh undang-undang dan melakukan suatu tindak pidana yang dapat menimbulkan sanksi pidana. Menurut pasal 55 ayat (1) Kitab Undang-undang Hukum Pidana, pelaku tindak pidana adalah:

1) Dipidana sebagai pelaku tindak pidana:
   1. Mereka yang melakukan, yang menyuruh melakukan, dan yang turut serta melakukan perbuatan;
   2. Mereka yang dengan memberi atau menjanjikan sesuatu dengan menyalahgunakan kekuasaan atau martabat dengan kekerasan, ancaman, atau penyesatan, atau dengan memberi kesempatan, sarana atau keterangan, sengaja menganjurkan orang lain supaya melakukan suatu perbuatan.

3. Tindak Pidana

Simons menyatakan bahwa *Strafbaar feit* sebagai perbuatan pidana. Tindak pidana *(Starfbaar feit)* adalah suatu perbuatan melanggar hukum yang dengan sengaja telah dilakukan oleh seseorang yang atas tindakannya dapat dipertanggungjawabkan, dinyatakan dapat dihukum.[18] Menurut Pompe; "*Strafbaar feit* secara teoretis dapat diartikan sebagai pelanggaran norma yang dengan sengaja maupun tidak sengaja dilakukan oleh seorang pelaku tindak pidana, maka penjatuhan sanksi pidana terhadap pelaku itu sangat perlu demi kepentingan hukum".[19]

[18]Nur Azisa Andi Sofyan, *Buku Ajar Hukum Pidana*, *Makassar; Pustaka Pena Press*, 2020, hlm. 97.

[19]Tofik Yanuar Chandra, *Hukum Pidana*, Cetakan Pertama; Penerbit Sangir Multi Usaha, Jakarta, 2022. hlm.40

4. Ransomware

Ransomware adalah suatu bentuk perangkat lunak atau malware yang digunakan untuk mengenkripsi data korban agar tidak dapat masuk ke sistem, kemudian pelaku dari kejahatan ini meminta tebusan kepada korban mengembalikan data tersebut.[20] Ramsomware adalah salah satu bentuk kejahatan modern berupa virus komputer yang bersembunyi di dalam *software,* salah satu kerjanya bila komputer diaktifasi maka virus ini akan bekerja dengan otomatis, mengambil data untuk kemudian hacker diluar sana akan memberi kabar bahwa data akan kembali jika ada uang tebusan, bila tidak data akan dijual di pasar internsional.[21]

F. Landasan Teoretis

1. Teori Pertanggungjawaban Pidana

Dalam Bahasa asing pertanggungjawaban pidana dikenal dengan istilah *"Teorekenbaarheid", "criminal Responsibility", dan "criminal liability"*. Dikemukakan bahwa pertanggungjawaban pidana adalah untuk menentukan apakah seseorang tersangka dapat dipertanggungjawabkan atas suatu tindak pidana yang terjadi, dengan kata lain bahwa tersangka akan dipidana atau dibebaskan.[22] Unsur-unsur pertanggungjawaban pidana ada dua yaitu unsur subjektif terdiri atas kesalahan, kesengajaan, kealpaan, sifat melawan hukum dan unsur objektif terdiri atas perbuatan dan sifat melawan hukum.

[20]G Ramadhan, *Op.Cit.* hlm 6.

[21]A Praptono and H Yusuf, "Tinjauan Kriminologi Terhadap Pelaku Kejahatan Pemerasan Dengan Menggunakan Virus, Ransomware Wannacry Sebagai Suatu Kejahatan Modern," *Jurnal Intelek Dan Cendikiawan Nusantara*, 2024, 1530–39.

[22]E.Y. Kanter dan R. Sianturi, *Asas-Asas Hukum Pidana Di Indonesia Dan Penerapannya*, cetakan ke (Jakarta, Storia Grafika, 2002).), hlm. 250.

Pertanggungjawaban pidana *(Criminal responsibility)* merupakan suatu perbuatan yang bertujuan untuk menentukan pemidanaan kepada pelaku dapat diminta pertanggungjawaban dan mampu bertanggungjawab atas suatu tindak pidana yang dilakukan, jika terdapat kesalahan maka perbuatan tersebut melawan hukum, maka pelaku dapat dikenakan sanksi pidana. Menurut G.A Van Hamel, syarat-syarat orang dapat dipertanggungjawabkan sebagai berikut:[23]

a. Orang harus dapat menentukan kehendaknya terhadap perbuatannya;
b. Jiwa orang harus sedemikian rupa seningga dia mengerti dan menginsyafi nilai dari perbuatannya;
c. Orang harus menginsyafi bahwa perbuatannya menurut tata cara kemasyarakatan adalah dilarang.

Menurut Roeslan Saleh, pertanggungjawaban pidana adalah tanggungjawab pidana diartikan sebagai referensi obyek yang berkelanjutan kepada mereka yang dihukum karena melakukan perbuatan pidana dengan dasar adanya kejahatan adalah asas legalitas.[24] Hukum pidana di Indonesia juga menganut asas kesalahan, yang dimana sebagai asas fundamental yang menganut sistem hukum *civil law* termasuk KUHP dan ketentuan peraturan perundang-undangan lainnya. Dalam hukum pidana ada dua hal yang harus diperhatikan dalam menjatuhkan sanksi pidana, yaitu dilakukannya suatu delik

[23]Amir Ilyas, *Asas-Asas Hukum Pidana: Memahami Tindak Pidana Dan Pertanggungjawaban Pidana Sebagai Syarat Pemidanaan*, *Rangkang Education Yogyakarta & PuKAP-Indonesia*, 2012. Hlm. 112.

[24]Moh. Mujibur Rohman Ady Purwoto Mia Amalia et al., *Asas-Asas Hukum Pidana,* Padang; Global Eksekutif Teknologi, 2023, hlm. 37.

yang berkaitan dengan objek atau pelaku delik *(actus reus)* dan dalam bahasa latin doktrin ini dikenal dengan *mensrea* terkait dengan pertanggungjawaban pidana.[25]

Bentuk-bentuk kesalahan itu ada 2 yaitu kesengajaan *(Opzet/Dolus)* dan kealpaan *(Culpa).* Kesengajaan merupakan seseorang yang melakukan suatu perbuatan pidana dengan sengaja, maka pelaku atau petindak yang dengan sengaja melakukan suatu tindak pidana dapat dikenakan sanksi pidana berdasarkan peraturan perundang-undangan yang berlaku. Kemudian, kesengajaan dibagi menjadi 3 bagian yaitu sebagai berikut:[26]

a. Sengaja sebagai niat *(Oogmerk)*
b. Sengaja sadar akan kepastian atau keharusan
c. Sengaja sadar akan kemungkingan

Kealpaan atau kelalaian adalah suatu perbuatan yang terjadi karena kurangnya pengetahuan dan kurang kehati-hatian dari pelaku yang menimbulkan suatu tindak pidana. Kelalaian *(culpa)* dibagi menjadi 2 yaitu *culpa lata* dan *culpa levis.*[27]

2. Teori Pemidanaan

Menurut Sudarto, bahwa pemidanaan itu sama dengan penghukuman. Penghukuman berasal dari kata dasar hukum, yang artinya menetapkan hukum atau memutuskan tentang hukumnya. Penghukuman dalam perkara pidana ialah pemidanaan atau pemberian atau penjatuhan pidana oleh hakim.[28] Tujuan

[25]*Ibid, hlm. 35*
[26]Amir Ilyas, *Op.Cit*. hlm.78
[27]*Ibid, hlm. 85.*
[28]Andi Sofyan, *Buku Ajar Hukum Pidana*.*Op.Cit*, hlm.84

menjatuhkan hukuman dalam hukum pidana yaitu untuk memelihara dan melindungi ketertiban hukum guna mempertahankan ketertiban Masyarakat.[29] Teori Pemidanaan adalah suatu konsep dalam hukum pidana yang dimana untuk mengetahui alasan dan tujuan dalam penjatuhan pidana terhadap pelaku tindak pidana. Menurut Adami, ada beberapa teori tentang tujuan pemidanaan yaitu sebagai berikut:[30]

a. Teori Pembalasan *(Teori Absolut/vergeldings theorien)*

Aliran teori ini menganggap bahwa dasar dari hukum pidana adalah suatu pembalasan. Menurut Kant, pembalasan atau suatu perbuatan melawan hukum adalah syarat mutlak menurut hukum dan keadilan, yang dimana hukuman mati terhadap pelaku tindak pidana pembunuhan berencana harus dijatuhkan pidananya.[31]

b. Teori Tujuan *(Teori relative/doel theorien)*

Teori tujuan menganggap bahwa dasar dari suatu pemidanaan itu adalah tujuan dari pidana itu sendiri karena pada dasarnya pidana itu mempunyai tujuan tertentu. Dalam mencapai tujuan itu ada beberapa bagian yang terdapat dalam aliran-aliran teori tujuan yaitu prevensi khusus dan prevensi umum.[32] Prevensi khusus adalah bahwa pencegahan kejahatan melalui pemidanaan dengan maksud mempengaruhi tingkah laku terpidana untuk tidak melakukan tindak pidana lagi. Pengaruhnya ada pada diri

[29]John Kenedi, *Kebijakan Hukum Pidana (Penal Policy)*, Cetakan Pertama, Yogyakarta: Pustaka Pelajar, 2017. hlm.130

[30]Amir Ilyas, *Op.Cit,* hlm. 97

[31]*Ibid, hlm. 98*

[32]*Ibid, hlm. 99*

terpidana itu sendiri dengan harapan agar si terpidana dapat berubah menjadi orang yang lebih baik dan berguna bagi masyarakat. Sedangkan prevensi umum bahwa pengaruh pidana adalah untuk mempengaruhi tingkah laku anggota masyarakat untuk tidak melakukan tindak pidana.[33]

c. Teori gabungan

Teori gabungan menyatakan bahwa pemidanaan berdasarkan atas pembalasan dan tujuan pemidanaan itu sendiri. Karena pada dasarnya dalam teori gabungan ini harus ada keseimbangan antara pembalasan dengan tujuan pemberian pemidanaan terhadap seseorang yang melakukan kejahatan, agar dapat tercapai keadilan.

Teori ini tidak boleh lebih berat dari yang ditimbulkan dan gunanya juga tidak boleh lebih besar dari yang sebenarnya. Pidana hanya bersifat pembalasan karena pidana hanya dijatuhkan terhadap delik-delik yaitu suatu perbuatan yang dianggap melawan hukum. Menurut Vos, "pidana berfungsi sebagai prevensi umum, bukan yang khusus kepada terpidana, karena jika ia sudah pernah masuk penjara ia tidak terlalu takut lagi, karena sudah berpengalaman".[34]

G. Orisinalitas Penelitian

Berdasarkan penelusuran yang penulis lakukan mengenai penelitian dalam skripsi ini, terdapat beberapa penelitian terdahulu yang melakukan penelitian dengan perbedaan dan persamaan topik yang diteliti, sebagai berikut:

[33]Amalia et al., *Op.Cit,* hlm. 120.
[34]Amir Ilyas, *Op.Cit,* hlm. 103

No	Nama, Tahun	Judul	Metode	Perbedaan
1	Andi Rian Jubhari, 2021	Tinjauan Hukum Pidana Internasional Terhadap Serangan Siber Menggunakan Ransomware Wannacry Di Indonesia	Penelitian Hukum Normatif	Penelitian terdahulu mengevaluasi pada tinjauan hukum pidana internasional yang mencakup sistem hukum pidana diseluruh negara dan kasus-kasus serangan siber ransomware yang ada di 150 negara. Sementara itu, penelitian yang dilakukan penulis mengenai pertanggungjawaban pidana dengan menggunakan hukum pidana positif di Indonesia dan kasus-kasus yang terjadi di Indonesia dan hanya menggunakan aturan hukum pidana Indonesia, termasuk KUHP dan UU ITE.
2	Qasyid Zhafran, 2024	Analisis Perlindungan Hak Konsumen Terhadap Serangan Ransomware Pada Nasabah BSI	Penelitian Hukum Normatif	Penelitian terdahulu fokus pada pemenuhan hak-hak nasabah yang dilakukan oleh Bank Syariah Indonesia terhadap serangan ransomware dan pemenuhan hak-hak nasabah tersebut harus sesuai dengan Undang-Undang Perlindungan Konsumen. Sementara itu, penelitian yang dilakukan oleh

				penulis fokus pada pertanggungjawaban pidana pada pelaku serangan ransomware dan bagaimana pengaturan terkait ransomware tersebut didalam Undang-Undang Informasi dan Transaksi Elektronik.

H. Metode Penelitian

1. Tipe Penelitian

Jenis penelitian yang digunakan adalah penelitian yuridis normatif yang merupakan ciri khas dari ilmu hukum. Dalam penulisan ini penulis akan melakukan penelitian terhadap peraturan perundang-undangan, teori, dan asas yang berkaitan dengan hukum pidana. Menurut Abdulkadir Muhammad: "Penelitian hukum Normatif *(Normatif law research)* adalah suatu penelitian hukum yang mengkaji hukum yang dimana dikonsepkan sebagai norma atau kaidah yang berlaku dimasyarakat serta menjadi acauan prilaku bagi semua orang".[35] 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 ".[36]

2. Pendekatan Penelitian

[35]Muhaimin, *Metode Penelitian Hukum*, mataram; penerbit mataram university fers, 2020, hlm. 29.

[36]Peter Mahmud marzuki, *Penelitian Hukum*, edisi revisi; Penerbit Kencana Prenada Media Grup, Jakarta, 2005. hlm. 82

Pendekatan penelitian yang digunakan dalam penelitian ini adalah:

a. Pendekatan Perundang-undangan *(Statute Approach)*

Dalam skripsi ini penulis menggunakan pendekatan perundang-undangan *(Statute Approach)*. Pendekatan perundang-undangan adalah suatu pendekatan yang dilakukan dengan menelaah semua peraturan perundang-undangan dan regulasi yag berikatan dengan isu hukum yang diteliti.[37] Pendekatan perundang-undangan adalah suatu pendekatan yang dilakukan dengan menganlisa serta menelaah setiap peraturan perundangan yang berkaitan dengan masalah yang sedang dibahas.[38]

b. Pendekatan Konseptual

Pendekatan konseptual ialah suatu pendekatan dalam penelitian hukum yang dimana memberikan sudut pandang dalam analisis penyelesaiaan masalah yang dilihat dari aspek konsep-konsep yang melatar belakanginya, maupun dapat dilihat dari nilai-nilai yeng terkandung didalam norma sebuah peraturan yang terkait dengan sebuah konsep yang digunakan.[39]

3. Pengumpulan Bahan Hukum

Bahan hukum yang penulis gunakan dalam penulisan proposal skripsi ini adalah:

a. Bahan hukum primer merupakan suatu bahan hukum yang memiliki sifat autoritatif, yang artinya mempunyai otoritas. Bahan-bahan hukum primer

[37]Muhaimin, *Op.Cit.* hlm. 56

[38]Irwansyah, *Penelitian Hukum Pilihan Metode & Praktik Penulisan artikel, Edisi Revisi*, Mira Buana Media, Yogyakarta, 2021, hlm.133.

[39]*Ibid, hlm. 57*

terdiri atas perundang-undangan, catatan-catatan resmi atau risalah dalam pembuatan perundang-undangan dan putusan-putusan hakim.[40]

b. Bahan hukum sekunder yaitu berupa semua publikasi tentang hukum yang bukan merupakan dokumen-dokumen resmi. Publikasi tentang hukum meliputi buku-buku teks, jurnal-jurnal hukum, kamus hukum, dan komentar-komentar atas putusan pengadilan.[41]

c. Bahan hukum tersier yang diteliti adalah berkitan dengan ensiklopedia, dan berbagai kamus hukum yang relevan dalam penelitian ini.

4. Analisis Bahan Hukum

Analisis bahan hukum yang dilakukan setelah bahan hukum terkumpul kemudian dianalisis dengan yuridis normatif. Dalam melakukan analisis diterapkan teknik-teknik sebagai berikut:

a. Teknik inventarisir berupa pengumpulan bahan-bahan hukum, nrma hukum dengan cara melihat isi dari berbagai peraturan perundang-undangan terkait dengan "Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Ransomware."

b. Teknik sistematsasi yang merupakan upaya mencari hubungan suatu norma hukum aturan perundang-undangan yang sederaat maupun tidak sederajat.

c. Teknik interpretasi diterapkan terhadap norma-norma hukum yang masih kabur, sehingga selanjutnya ditafsirkan untuk dapat dimengerti.

[40]Peter Mahmud Marzuki, *Op.Cit*, hlm. 181
[41]*Ibid*, *hlm. 182*

I. Sistematika Penelitian

Untuk mengetahui Gambaran secara umum dalam penulisan proposal skripsi ini, maka penulis akan menggambarkannya dalam suatu rangkaian yang disusun sistematis sebagai berikut:

BAB I **Pendahuluan**, ini menjelaskan mengenai Latar Belakang Masalah, Rumusan Masalah, Tujuan Penelitian, Manfaat Penelitian, Kerangka Konseptual (Pengertian Pertanggungjawaban Pidana, Pelaku, Tindak Pidana, Ransomware); Landasan Teori (Teori Pertanggungawaban Pidana, dan Teori Pemidanaan); Orisinalitas Penelitian, Metode Penelitian dan Sistematika Penelitian.

BAB II **Tinjauan Pustaka** Tentang Pertanggungjawaban Pidana, Pelaku, Tindak pidana Ransomware, dan Tindak Pidana Informasi Dan Transaksi Elektronik.

BAB III **Pembahasan**. Pada bab ini merupakan pembahasan dari rumusan masalah mengenai pengaturan pertanggungawaban pidana terhadap pelaku tindak pidana ransomware dan bentuk pertanggungjawaban pidana bagi pelaku tindak pidana ransomware dalam perspektif peraturan perundang-undangan.

BAB IV **Penutup**. yang berisikan bagian akhir dari penulisan ini yang terdiri dari kesimpulan dan saran. Kesimpulan yang dibuat merupakan jawaban singkat terhadap permasalahan yang telah dirumuskanpada Bab.I, sedangkan saran merupakan sumbangan pemikiran terhadap permasalahan yang dibahas pada Bab. III.

BAB II
TINJAUAN PUSTAKA

A. Pertanggungjawaban Pidana

1. Pengertian Pertanggungjawaban Pidana

Dalam bahasa Belanda istilah pertanggungjawaban pidana dikenal dengan *"Teorekenbaarheid",* sedangkan dalam Bahasa inggris dikenal dengan istilah *"Criminal Responsibility"* atau *"Criminal Liability".* Pertanggungjawaban pidana ini ialah untuk menentukan apakah seseorang pelaku tindak pidana dapat dipertanggungjawabkan atau tidak terhadap suatu perbuatan yang dilakukan. Seseorang dapat dipidana jika orang tersebut telah melakukan suatu perbuatan pidana yang melawan hukum, serta memenuhi unsur kesalahan dan mampu bertanggungjawab. Simons berpendapat bahwa:

> Kemampuan bertanggungjawab diartikan sebagai suatu keadaan psikis yang dimana pada penerapan suatu upaya pemidanaan yang ditinjau baik secara umum maupun dari sudut orangnya yang dapat dibenarkan, kemudian seseorang pelaku tindak pidana mampu bertanggung jawab apabila:
> a. Mampu mengetahui/menyadari bahwa perbuatannya tersebut bertentangan dengan hukum;
> b. Mampu menentukan kehendaknya sesuai dengan kesadaran.[42]

Barda Nawawi Arief, mengemukakan bahwa pertanggungjawaban pidana memiliki arti:

> Pencelaan pembuat (subyek hukum) atas tindak pidana yang telah dilakukannya. Oleh karena itu, pertanggungjawaban pidana mengandung di dalamnya pencelaan obyektif dan pencelaan subyektif. Artinya secara obyektif si pembuat telah melakukan tindak pidana (perbuatan terlarang/melawan hukum dan diancam pidana menurut hukum yang berlaku) dan secara subyektif si pembuat patut dicela atau dipersalahkan/

[42]Teguh Prasetyo. *Hukum Pidana*. Cetakan Ke-10; Penerbit Rajawali Pers. Depok, 2019. Hlm.85.

dipertanggungjawabkan atas tindak pidana yang dilakukannya itu sehingga ia patut dipidana.[43]

Pertanggungjwaban pidana tanpa adanya kesalahan dari pihak yang melanggar tidak dapat dipertanggungjawabkan, maka orang yang tidak mungkin dipertanggungjawabkan dan dijatuhi pidananya kalau tidak melakukan perbuatan pidana, meskipun dia melakukan perbuatan pidana tidak selalu dia dapat dipidana.[44]

2. Unsur-Unsur Pertanggungawaban Pidana

Menurut hukum pidana, pertanggungjawaban pidana merupakan suatu konsep yang sentral dimana dikenal sebagai unsur kesalahan. Menurut Amir Ilyas dalam bukunya Asas-Asas Hukum Pidana, unsur pertanggungjawaban Pidana itu ada 4 yaitu perbuatan melawan hukum, mampu bertanggungjawab, unsur kesalahan, dan tidak ada alasan pemaaf.[45]

a. Perbuatan melawan hukum

b. Mampu bertanggungjawab

Kemampuan bertanggungjawab merupakan syarat wajib yang sangat diperlukan dalam pertanggungjawaban pidana, maka pelaku tindak pidana yang melakukan suatu perbuatan yang melanggar hukum harus mampu mempertanggungjawabkan atas tindakannya tersebut. Moeljatno

[43]Krismiyarsi. *Pertanggungjawaban Pidana Individual*. Cetakan Pertama; Penerbit Pustaka Magister, Semarang. 2018. Hlm.7.

[44]Aryo Fadlian, "Pertanggungjawaban Pidana Dalam Suatu Kerangka Teoritis," *Jurnal Hukum Positum* Vol. 5, no. 2 (2020): hlm. 14, https://journal.unsika.ac.id/index.php/positum/article/view/5556

[45]Amir Ilyas*, Op.Cit. hlm.75*

mengemukakan pendapat bahwa untuk adanya kemampuan bertanggungjawab harus memiliki:

a. Kemampuan untuk membeda-bedakan antara perbuatan yang baik dan buruk, yang sesuai dengan hukum dan yang melawan hukum;
b. Kemampuan untuk menentukan kehendaknya menurut keinsyafan tentang baik dan buruknya perbuatannya. pertama merupakan faktor akal *(intelektual factor)* yaitu dapat memperbeda-bedakan antara perbuatan yang diperbolehkan dan yang tidak. Yang kedua adalah faktor perasaan atau kehendak *(volitional factor)* yaitu dapat menyesuaikan tingkah lakunya. dengan keinsyafan atas nama yang diperbolehkan dan mana yang tidak. Sebagai konsekuensinya, maka orang yang tidak mampu menentukan kehendaknya menurut keinsyafan tentang baik dan buruknya perbuatan tadi, dia tidak mempunyai kesalahan dan kalau melakukan perbuatan pidana, orang yang demikian itu tidak dapat dipertanggungjawabkan.[46]

Dalam Kitab Undang-Undang Hukum Pidana, tidak ada ketentuan pasal yang mendefinisikan mengenai arti kemampuan bertanggung jawab, tetapi ada menjelaskan tentang ketidakmampuan bertanggung jawab, seperti yang dijelaskan dalam pasal 44 ayat (1) KUHP yang menyatakan bahwa; "Barang siapa yang melakukan perbuatan yang tidak dipertanggungkan kepadanya karena jiwanya cacat dalam pertumbuhan atau terganggu karena penyakit tidak dipidana".

c. Unsur kesalahan

Suatu kesalahan dianggap ada apabila seseorang dengan sengaja atau karena kealpaannya melakukan suatu perbuatan yang menimbulkan akibat yang dilarang oleh hukum pidana dan pada dasarnya seseorang tersebut mampu mempertanggungjawabkan perbuatan yang telah dilakukan. Unsur

[46]Krismiyarsi. *Op.Cit*, hlm.27.

kesalahan yang disebut sebagai *"mens rea"* dapat berbentuk seperti kesengajaan *(Dolus)* dan kelalaian *(Culpa).*[47]

1) Kesengajaan *(dolus/opzet)*

MvT menjelaskan bahwa yang dimaksud dengan kesengajaan adalah *"willens en watens"* artinya mengkehendaki dan menginsyafi atau mengetahui, dijelaskan bahwa seseorang yang melakukan suatu Tindakan dengan sengaja harus mengkehendaki Tindakan tersebut dan harus mengetahui akibat yang akan terjadi karena tindakannya.[48] Adapun bentuk kesengajaan *(dolus)* yaitu sebagai berikut:

a) Kesengajaan sebagai maksud *(opzet als oogmerk)*

Kesengajaan sebagai maksud merupakan suatu kehendak yang jelas untuk menimbulkan suatu akibat tertentu yang berasal dari tindakan yang dilakukan oleh pelaku, artinya pelaku menginginkan hasil dari suatu perbuatan yang dilakukan serta memahami konsekuensinya.[49] Kesengajaan sebagai maksud menimbulkan dua teori yaitu teori kehendak dan teori bayangan. Teori kehendak merupakan suatu teori yang menganggap bahwa suatu kesengajaan ini ada apabila tindakan serta akibat suatu delik dikehendaki oleh pelaku. Kemudian, pada teori bayangan menyatakan bahwa pada saat pelaku melakukan perbuatan ada bayangan yang jelas bahwa akibat dari perbuatan tersebut akan

[47]Ishaq. *Hukum Pidana*. Cetakan ke-2; Penerbit Raja Grafindo Persada, Depok, 2022. Hlm.94

[48]Teguh Prasetyo. *Op.Cit*,hlm.96.

[49]*https://konspirasikeadilan.id/artikel/unsur-kesengajaan-dalam-hukum-pidana0463*, Diakses pada tanggal 26 November 2024 pukul 16.00 WIB.

tercapai.[50] Perbuatan si pelaku bertujuan untuk menimbulkan akibat yang dilarang.

b) Kesengajaan dengan sadar kepastian *(opzet met zekerheidsbewustzijn atau noodzakelikheidbewustzijn).*

Kesengajaan dengan sadar kepastian adalah suatu keadaan yang dimana pelaku melakukan suatu perbuatan yang tidak memiliki tujuan untuk mencapai suatu akibat tertentu, tetapi pelaku tersebut menyadari bahwa akibat tersebut akan terjadi sebagai konsekuensi dari perbuatan tersebut. Dalam hal ini, pelaku mengerti bahwa meskipun ia tidak ingin akibat tersebut terjadi tetapi ia harus menerima bahwa akibat tersebut akan terjadi untuk mencapai suatu tujuan yang diinginkan.

c) Kesengajaan dengan sadar kemungkinan *(dolus eventualis/voorwaardelijk opzet)*

Amir Ilyas berpendapat bahwa "kesengajaan dengan sadar kemungkinan adalah terwujudnya delik bukan tujuan dari pelaku, melainkan merupakan syarat yang mungkin timbul sebelum atau pada saat maupun sesudah tujuan pelaku tercapai, ada tindak pidana yang mungkin terjadi sebelum atau pada saat maupun sesudah tujuan pelaku kemungkinan tercapai".[51]

[50]Hukum Online, *https://www.hukumonline.com/klinik/a/perbedaan-sengaja-dan-tidak-sengaja-dalam-hukum-pidana-lt5ee8aa6f2a1d3*/, Diakses pada tanggal 27 November 2024 pada pukul 17.00 WIB.

[51]Amir Ilyas. *Op.Cit.hlm.83*

2) Kelalaian/Kealpaan*(culpa)*

Kelalaian (Culpa) adalah suatu bentuk kesalahan yang dimana terjadi akibat kurang kehati-hatian dari pelaku sehingga menimbulkan suatu peristiwa yang tidak diinginkan. Menurut Simons, "kelalaian atau kealpaan terjadi karena tidak ada kehati-hatian dan kurangnya perhatian terhadap akibat yang mungkin saja terjadi."[52] Kelalaian/kealpaan dibedakan menjadi 2 jenis yaitu sebagai berikut:

a) Kealpaan berat *(Culpa lata)*

Culpa lata merupakan suatu bentuk kealpaan berat dalam hukum pidana yang terjadi Ketika pelaku tindak pidana tidak berhati-hati, sehingga dapat menimbulkan kerugian. Dalam hal ini, akibat yang ditimbulkan oleh pelaku tindak pidana ini juga termasuk kematian, yang karena kurang kehati-hatiannya menyebabkan kematian terhadap seseorang.[53] *Culpa lata* dibedakan menjadi 2 jenis yaitu *culpa lata* disadari adalah pelaku tindak pidana menyadari bahwa kemungkinan akibat dari tindakan yang dilakukannya dapat menimbulkan akibat lain yang tidak sesuai dengan yang di inginkan pelaku tetapi tetap melakukan tindakan tersebut, dan *culpa lata* yang tidak disadari adalah seseorang

[52]Tofik Yanuar Chandra. *Op.Cit.hlm.77*

[53]Seva Maya Sari and Toguan Rambe, "Delik Culpa Dalam Kajian Fiqh Jinayah (Analisis Terhadap Pasal 359 KUHP Tentang Kealpaan Yang Mengakibatkan Matinya Orang)," *Jurnal Penelitian Ilmu-Ilmu Sosial Dan Keislaman* 6, no. 2 (2020): 254, https://doi.org/10.24952/tazkir.v6i2.3031.

pelaku tindak pidana yang tidak memperkirakan akibat yang timbul dari perbuatannya serta tetap melakukan perbuatan pidana.[54]

b) Kealpaan ringan *(Culpa levis)*

Culpa levis merupakan pelanggaran ringan yang dimana tindakan yang dilakukan karena kecerobohan karena pelaku tidak menyadari akibat dari tindakannya yang disebabkan oleh ketidaktahuan atau keadaan tertentu yang dapat menghalangi pemahaman.[55]

d. Tidak ada alasan pemaaf

Tidak ada alasan pemaaf ialah tidak adanya kondisi yang menghapuskan kesalahan pelaku dalam melakukan suatu tindak pidana, kemudian dalam hukum pidana alasan pemaaf mengacu pada kedaan psikologis atau subjektif pelaku yang membuatnya tidak dapat diminta pertanggungawaban pidana seperti ketidakmampuan bertanggungjawab atau daya paksa *(overmacht)*.

B. Makna Pelaku

Pasal 55 ayat (1) Kitab Undang-Undang Hukum Pidana, merumuskan mengenai pelaku yakni:

1) Dipidana sebagai pelaku tindak pidana
   1. Mereka yang melakukan, yang menyuruh melakukan, dan yang turut serta melakukan perbuatan.
   2. Mereka yang memberi atau menjanjikan sesuatu dengan menyalahgunakan kekuasaan atau martabat dengan kekerasan, ancaman atau penyesatan, atau dengan memberi kesempatan, sarana

[54]Aprianto J Muhaling, "Kelalaian Yang Mengakibatkan Matinya Orang Menurut Perundang –Undangan Yang Berlaku," *Lex Crimen* 8, no. 3 (2019): 35. https://ejournal.unsrat.ac.id/index.php/lexcrimen/article/view/25628

[55]*Ibid.hlm.29.*

atau keterangan, sengaja menganjurkan orang lain supaya melakukan perbuatan.

Pasal 55 KUHP merumuskan ada empat gologan pembuat *(dader)* yang dapat dipidana sebagai berikut:

1. Pelaku *(Pleger)*

   Simons berpendapat bahwa pelaku *(pleger)* adalah mereka yang melakukan sendiri suatu perbuatan pidana maka apabila seseorang melakukan sendiri suatu perbuatan pidana artinya melakukan tanpa bantuan orang lain.[56]

2. Orang yang menyuruh lakukan *(Doenpleger)*

   Orang yang menyuruh lakukan *(doenpleger)* adalah seseorang yang melakukan suatu tindak pidana dengan menggunakan orang lain sebagai perantara, maka perantara hanya digunakan sebagai alat yang dikendalikan oleh penyuruh.[57] Orang yang disuruh disebut sebagai pelaku langsung *(manus manistra)* dan orang yang menuruh disebut sebagai pelaku tidak langsung *(manus domina),* oleh karena itu terdapat Unsur-unsur *doenpleger* sebagai berikut:

   a. Alat yang dipakai berbuat;
   b. Alat yang dipakai adalah manusia;
   c. Alat yang dipakai tidak dapat dipertanggungjawabkan.[58]

3. Orang yang turut serta *(Medepleger)*

[56]Lukman Hakim*, Op.Cit,* hlm.79.
[57]Ishaq. *Op.Cit*, hlm.134.
[58]*Ibid, hlm.135.*

Orang yang turut serta *(Medepleger)* adalah setiap orang yang dengan sengaja turut melakukan suatu perbuatan dalam suatu tindak pidana. Menurut Satochid Kartanegara, ada 2 syarat tentang adanya *medepleger* sebagai berikut:

a. Harus ada kerja sama secara fisik;

b. Harus ada kesadaran kerja sama.[59]

4. Penganjur *(Uitlokker)*

Penganjur adalah orang yang dengan sengaja menggerakkan orang lain untuk melakukan suatu perbuatan pidana dengan menggunakan sarana yang telah ditentukan dalam peraturan perundang-undangan seperti yang dijelaskan dalam pasal 55 ayat (1) angka 2 Kitab Undang-Undang Hukum Pidana.[60]

C. Tindak Pidana Ransomware

1. Tindak Pidana

a. Pengertian Tindak Pidana

Dalam Bahasa Belanda, istilah yang digunakan dalam tindak pidana adalah *Strafbaarfeit,* yang mencakup beberapa isitilah yang sering digunakan seperti perbuatan pidana, peristiwa pidana, dan delik yang dalam bahasa latin disebut dengan *delictum.* Tindak pidana merupakan suatu istilah resmi yang digunakan dalam peraturan perundang-undangan di Indonesia.[61] Tindak pidana dalam Bahasa Belanda digunakan istilah *Strafbaar feit* yang terdiri dari tiga kata yaitu *Straf* artinya pidana dan hukum; *baar* artinya dapat; dan *feit* arinya tindak, peristiwa, dan perbuatan, maka *Strafbaar feit*

[59]*Ibid,hlm.136.*
[60]Teguh Prasetyo. *Op.Cit.* hlm. 208.
[61]Tofik Yanuar Chandra. *Op.Cit*, hlm.37.

adalah suatu pebuatan yang dapat dipidana, sedangkan delik yang dalam Bahasa inggris disebut *delict* adalah suatu tindakan yang atas perbuatannya tersebut pelakunya dapat dikenakan hukuman.[62]

Tindak pidana adalah suatu perbuatan atau tindakan yang dilarang oleh hukum dan dikenakan sanksi pidana bagi pelaku yang melakukan perbuatan pidana. Moeljatno berpendapat bahwa perbuatan pidana adalah "Perbuatan pidana adalah suatu perbuatan yang dilarang oleh aturan hukum, larangan yang disertai dengan ancaman (sanksi) yang berupa pidana tertentu bagi orang yang melanggar larangan tersebut."[63]

b. Unsur-Unsur Tindak Pidana

Simons membedakan Unsur-unsur tindak pidana terdiri menjadi 2 macam yaitu unsur subjektif dan unsur objektif;

a. Unsur subjektif tindak pidana meliputi:
   1) Perbuatan orang;
   2) Akibat yang terlihat dari perbuatan itu;
   3) Mungkin ada suatu keadaan tertentu yang menyertai dalam suatu perbuatan itu, seperti di muka umum *(openbaar)* seperti pada pasal 181 KUHP.
b. Unsur objektif tindak pidana mencakup beberapa unsur sebagai berikut:
   1) Orang yang mampu bertanggung jawab;
   2) Adanya kesalahan *(Kesengajaan atau Kealpaan)*.[64]

Menurut Hazewinkel Suringa, unsur-unsur tindak pidana yaitu sebagai berikut:

a. Unsur tingkah laku atau perbuatan seseorang;

[62]Amir Ilyas. Op.Cit, hlm.19.

[63]Aksi Sinurat. *Azas-Azas Hukum Pidana Materil Di Indonesia*. Cetakan Pertama; Penerbit LP2M Universitas Nusa Cendana, Kupang, 2023. Hlm.114.

[64]Tofik Yanuar Chandra. *Op.Cit*, hlm.43.

b. Unsur akibat ialah unsur pada tindak pidana yang dirumuskan secara materil;
c. Unsur psikis *(dolus atau culpa)*;
d. Unsur objektif yang menyertai keadaan tindak pidana, seperti tindak pidana yang dilakukan dimuka umum;
e. Unsur syarat tambahan untuk dapat dipidananya seseorang yang karena perbuatannya (pada pasal 164 dan pasal 165 KUHP) disyaratkan apabila tindak pidana terjadi;
f. Unsur melawan hukum.[65]

Kemudian mengenai unsur-unsur tindak pidana terdapat perbedaan pandangan yang dibagi menjadi dua yaitu pandangan monistis dan pandangan dualistis.[66] Pandangan monistis merupakan suatu pandangan yang dengan syarat dapat ditentukannya suatu pidana harus terdapat dua hal yaitu sifat dan perbuatan. D.Simons mengemukakan pendapat bahwa tindak pidana merupakan suatu tidakan melanggar hukum yang dilakukan dengan sengaja maupun tidak sengaja oleh seseorang yang dapat dipertanggungjawabkan atas tindakannya serta undang-undang menyatakan bahwa tindakan tersebut dapat dihukum.[67] Menurut Muladi, pandangan dualistis yaitu dapat memudahkan dalam melakukan suatu sistematika

[65]*Ibid. hlm.44.*
[66]Krismiyarsi. *Op.Cit*.hlm.8
[67]Fitri Wahyuni. *Dasar-Dasar Hukum Pidana Di Indonesia*. Cetakan Ke-1; Penerbit Nusantara Persada Utama, Tanggerang. 2017. Hlm. 42.

unsur-unsur yang dimana suatu tindakan yang masuk kedalam perbuatan dan yang masuk ke dalam pertanggungjawaban pidana.[68]

c. Jenis-Jenis Tindak Pidana

Berdasarkan Kitab Undang-Undang Hukum Pidana, jenis tindak pidana dibagi menjadi dua (2) macam yaitu kejahatan *(misdrijven)* yang diatur dalam buku II KUHP dan pelanggaran *(overtredingen)* diatur dalam buku III KUHP. Tindak pidana juga dibedakan menjadi dua macam yaitu tindak pidana formil dan tindak pidana materil. Tindak pidana formil adalah suatu tindak pidana yang dianggap telah selesai yang karena perbuatannya dilarang oleh undang-undang tanpa menyebutkan akibat dari perbuatan tersebut.[69] Sedangkan, tindak pidana materil adalah suatu tindak pidana selesai dengan menimbulkan suatu akibat yang dilarang serta diancam dengan pidana oleh undang-undang yang berlaku.[70] Jadi tindak pidana materil dapat dikatakan telah selesai jika akibat dari perbuatan tersebut telah terjadi.

Tindak pidana juga dapat dibedakan menjadi tindak pidana aktif *(Delicta commissionis)* dan tindak pidana pasif *(Delicta ommisionis)*. *Delicta commissionis* adalah suatu tindak pidana yang perbuatannya ialah perbuatan aktif, yang dimaksud dengan perbuatan aktif adalah suatu perbuatan yang dimana untuk mewujudkannya disyaratkan dengan adanya

[68]Krismiyarsi. *Op.Cit*. hlm. 13
[69]Ishaq. *Op.Cit*, hlm.85.
[70]Hukum Online, https://www.hukumonline.com/klinik/a/apa-perbedaan-delik-formil-dan-delik-materil-lt569f12361488b/, Di akses pada tanggal 8 Januari 2025 pada pukul 09.35 WIB.

Gerakan anggota tubuh yang melakukan perbuatan.[71] Tindak pidana yang sebagaian besar dirumuskan dalam Kitab Undang-Undang Hukum Pidana yang merupakan tindak pidana aktif. Tindak pidana pasif *(Delicta ommisionis)* adalah adalah suatu tindak pidana yang dapat terjadi karena seseorang tidak berbuat sesuatu atau melalaikan suruhan, yang dimana biasanya ialah delik formil, seperti yang terdapat didalam beberapa pasal yang ada didalam KUHP.[72]

Tindak pidana pasif dibedakan menjadi 2 macam yaitu tindak pidana pasif murni dan tindak pidana pasif tidak murni. Tindak pidana pasif murni merupakan suatu tindak pidana yang dimana dirumuskan secara formil atau tindak pidana yang berdasarkan atas unsur perbuatannya ialah suatu perbuatan pasif. Sedangkan, tindak pidana pasif yang tidak murni merupakan suatu tindak pidana yang pada dasarnya ialah tindak pidana positif, tetapi dapat dilakukan dengan cara tidak berbuat aktif atau tindak pidana yang mengandung suatu akibat terlarang.[73]

2. Ransomware

a. Sejarah Ransomware

Ransomware pertama kali diciptakan pada tahun 1989 oleh seorang ahli biologi evolusi lulusan *Harvard* bernama Joseph Popp, dimana ia membuat membuat sebuah *software* jahat yang disebut dengan *"Trojan AIDS"* yang kemudian dikirimkan ke 90 negara didunia dengan cara

[71]Fitri Wahyuni. *Op.Cit*. Hlm.57.
[72]Ishaq. *Op.Cit*.hlm. 86.
[73]Fitri Wahyuni. *Op.Cit*.hlm.58.

memasukkannya di dalam 20.000 disket melalui pos.[74] Ransomware pertama ini mengunci sistem komputer dengan cara mengenkripsi file dan meminta tebusan yang harus dikirim dalam kotak surat tertentu dalam bentuk cek, akan tetapi ransomware modern yang muncul pada tahun 2005 yang menggunakan *kriptocurrency* sebagai metode pembayaran dengan varian ransomware *GpCode*.[75]

Ransomware *GpCode* ini mengenkripsi data milik korban dengan mengakses sistem komputer kemudian meminta tebusan kepada korban agar mendapatkan kunci deskripsinya, tetapi ransomware jenis ini masih bias di deteksi oleh anti virus,berbeda dengan jenis baru yang sekarang ini sulit undtuk dideteksi. Sejak saat itu ransomware berkembang secara pesat seiring dengan kemajuan teknologi yang semakin canggih. ransomware yang kini menjadi ancaman dalam keamanan siber diseluruh dunia termasuk indonesia. Sebagian besar ransomware awal dikembangkan dirusia oleh penjahat terorganisir.

Pada tahun 2007 muncul ransomware jenis baru yaitu ransomware locker, yang dimana pertama kali menyerang rusia dengan menampilkan gambar porngrafi pada mesin tersebut dan meminta pembayaran untukmenghapusnya, baik melalui pesan teks SMS maupun telepon tarif premium, kemudian muncul ransomware baru yang sangat terkenal pada

[74]Allan Liska dan Timothy Gallo, *Ransomware: Defending Againts Digital Extortion, Sebastopol,* Penerbit O‟Reilly Media, Amerika Serikat, 2017. Hlm. 1.

[75]Kanwil DJKN Jawa Barat. https://www.djkn.kemenkeu.go.id/kanwil-jabar/baca-artikel/16188/Ransomware-Ancaman-dan-Langkah-Langkah-untuk Menghindarinya. Diakses pada tanggal 5 Februari 2025 pada pukul 17.00 WIB.

tahun 2013 yaitu ransomware cryptolocker yang dibuat oleh hacker bernama Slavik[76]

b. Pengertian Ransomware

Ransomware berasal dari kata *'ransom'* artinya tebusan paksa dan malware yang diartikan sebagai pembayaran atas data yang dicuri atau akses terbatas melalui enkripsi, jadi ransomware merupakan serangan malware yang mengakses sistem komputer dengan mengenkripsi data-data milik korban yang kemudian meminta uang sebagai tebusan agar enkripsi itu terbuka, yang dimana uag tebusan yang diminta oleh pelaku menggunakan mata uang kripto dalam melakukan transaksi keuangan yang memiliki sifat anonym sehingga sangat sulit untuk dilacak keberadaannya.[77]

Ransomware adalah serangan siber dengan mengunci file-file dan data pengguna dengan menahan akses ke data-data tersebut kemudian meminta sejumlah tebusan yang harus dibayarkan.[78] Terdapat dua jenis ransomware yang sering digunakan oleh pelaku kripto yaitu:

a. *Ransomware Locker,* yaitu jenis ransomware yang mengunci akses komputer korban pada saat layar telah terkunci, pelaku meminta

[76]Ronny Richardson and Max M North, "Ransomware : Evolution , Mitigation and Prevention," *Authorized Administrator of DigitalCommons@Kennesaw State University* Vol. 13, no. 1 (2017): hlm. 11-12, https://digitalcommons.kennesaw.edu/facpubs Recommended.

[77]Winnie Stevani and Hari Sutra Disemadi, "Urgency of Cryptocurrency Regulation in Indonesia: The Preventive Action for Ransomware Crime," *Hang Tuah Law Journal* Vol 5, no. 1 (2021):hlm.54, https://doi.org/10.30649/htlj.v5i1.32.

[78]Sindy Ariyaningsih et al., "Korelasi Kejahatan Siber Dengan Percepatan Digitalisasi Di Indonesia," *Justisia: Jurnal Ilmu Hukum* Vol 1, no. 1 (2023): hlm. 6, https://doi.org/10.56457/jjih.v1i1.38.

sejumlah uang agar dapat mengembalikan akses kesistem komputer tersebut.

b. *Ransomware Cryptolocker,* yaitu jenis serangan ransomware yang mengenkripsi data digital dari sistem komputer milik korban dan pada akhirnya pelaku meminta sejumlah uang tebusan agar mendapatkan kunci enkripsi pada data tesebut.[79]

Ransomware dalam melakukan tindakannya akan melibatkan seorang peretas untuk mengenkripsi data yang dimana cara kerja ransomware dengan menyalurkan virus pada software melalui rekayasa dan antar pengguna saling berinteraksi.[80] Pada kenyataannya, pelaku tindak pidana ransomware tidak akan mengirimkan kunci kode enkripsi setelah uang tebusan dibayarkan, modus pelaku ransomware mendeskripsikan beberapa file sebelum tebusan dibayaran.[81]

D. Tindak Pidana Informasi Dan Transasksi Elektronik

1. Definisi Tindak Pidana Informasi Dan Transasksi Elektronik

Menurut istilah informasi elektronik terbentuk dari dua kata yaitu kata informasi dan kata elektronik. Dalam Bahasa inggris istilah informasi yaitu *Information.* Gordon B. Davis mengemukakan bahwa informasi sebagai *"Information is data that has been processed into a form that is meaningful to*

[79]Winnie Stevani and Hari Sutra Disemadi. *Op.Cit*. hlm.59.

[80]Diana Afifah, "Perlindungan Konsumen Di Sektor Jasa Keuangan Pada Kasus Serangan Siber Ransomware Yang Menimpa Perbankan," *JIIP - Jurnal Ilmiah Ilmu Pendidikan* Vol 6, no. 11 (2023): hlm. 9318, https://doi.org/10.54371/jiip.v6i11.3176.

[81]Ronny Richardson and Max M North. *Op.Cit*.hlm.14

the recipient and is used of real or proceived value in current or prospective action or decision".[82]

Menurut pasal 1 angka 1 Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, pengertian informasi elektronik adalah:

> 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, symbol, atau perforasi yang telah di olah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) disebut juga dengan istilah *Cyber Law* atau Hukum Siber Indonesia. Cyber Law secara internasional digunakan untuk istilah hukum yang berkaitan dengan penggunaan teknologi informasi dan komunikasi, kemudian ada beberapa istilah yang digunakan adalah Hukum Dunia Maya *(virtual world law)*, Hukum Teknologi Informasi *(law of information technology)*, dan Hukum Mayantara.[83] Undang-Undang ITE merupakan suatu peraturan perundang-undangan yang mengatur tentang bagaimana batasan seseorang ketika menggunakan hal-hal yang berkaitan dengan dunia maya atau internet dalam memanfaatkan sistem elektronik untuk media sosial, berdagang barang dan jasa.[84] Selain itu, Undang-Undang ITE juga mengatur perbuatan yang dilarang

[82]Abdul Halim Barkatullah. *Hukum Transaksi Elektronik.* Cetakan Ke-1, Penerbit Nusa Media; Bandung, 2017. Hlm.24-25

[83]*Ibid. Hlm.29.*

[84]Andi Najemi, Tri Imam Munandar, and Aga Hanum Prayudi, "Bahaya Penyampaian Berita Bohong Melalui Media Soaial," *Jurnal Karya Abdi* vol 5, no. 3 (2021): hlm. 578.

dengan menggunakan sistem elektronik atau jaringan elektronik sebagaimana yang telah diatur dalam pasal-pasal Undang-Undang Informasi dan Transaksi Elektronik, maka pelaku tindak pidana yang melakukan perbuatan sebagaimana diatur dalan UU ITE akan dikenakan sanksi pidana.

Tindak pidana informasi dan transaksi elektronik pada dasarnya merujuk pada berbagai kejahatan yang muncul akibat dari kemajuan teknologi, tindak pidana ini dilakukan dengan menggunakan kecanggihan teknologi terutama pada komputer dan jaringan internet. Tindak Pidana Informasi dan Transaksi Elektronik adalah suatu aktivitas kriminal yang dilakukan dengan menggunakan kecanggihan teknologi, tindak pidana ini sering dikenal dengan istilah *cyber crime*. Tindak pidana *cyber crime* adalah suatu tindakan kriminal yang menggunakan kecanggihan teknologi komputer dan jaringan internet sebagai alat, sasaran atau tempat terjadinya suatu kejahatan.[85] Kejahatan ini meliputi berbagai bentuk aktivitas illegal seperti penipuan online, peretasan, pencurian data, penyebaran virus dan sebagainya.

Berdasarkan dua dokumen Kongres PBB mengenai *The Prevention Of Crime and The Treatment of Offenders* di Havana, Cuba pada tahun 1990 dan di Wina, Austria pada tahun 2000, terdapat dua istilah yang dikenal sebagai berikut:

[85]Miftakhur Rokhman Habibi and Isnatul Liviani, "Kejahatan Teknologi Informasi (Cyber Crime) Dan Penanggulangannya Dalam Sistem Hukum Indonesia," *Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam,* Vol. 23, no. 2 (2020): 400–426, https://doi.org/10.15642/alqanun.2020.23.2.400-426.

a. *Cyber crime* dalam arti sempit disebut *computer crime*, yaitu prilaku illegal atau melanggar secara langsung menyerang system keamanan suatu komputer atau data yang diproses oleh komputer

b. *Cyber crime* dalam arti luas disebut *computer related crime*, yaitu prilaku ilegal atau melanggar yang berkaitan dengan sistem komputer atau jaringan.[86]

2. Jenis-Jenis Tindak Pidana Informasi Dan Transaksi Elektronik

Berdasarkan literature dan praktiknya, tindak pidana *cyber crime* dibedakan menjadi beberapa jenis sebagai berikut:

a. *Unauthorized Acces to computer system and service*

Unauthorized Acces to computer system and service adalah suatu kejahatan yang terjadi Ketika seseorang mengakses dalam sistem jaringan komputer tanpa izin atau tanpa sepengatahuan dari pemilik sistem jaringan komputer yang di aksesnya.[87]

b. *Illegal Contents*

Illegal contents adalah kejahatan yang dilakukan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang di anggap tidak benar dan melanggar peraturan perundang-undangan yang berlaku, termasuk dengan pencemaran nama baik, penyebaran berita bohong *(Hoax)* dan tindakan yang berkaitan dengan kesusilaan. Ujaran kebencian *(hate speech)* termasuk kedalam kategori *illegal lcontents,*

[86]Eliasta Ketaren, "Cybercrime, Cyber Space, Dan Cyber Law," *Jurnal TIMES* 5, no. 2 (2016): 35–42, https://doi.org/10.51351/jtm.5.2.2016556.

[87]Sahat Maruli T. Situmeang. *Op.Cit*. Hlm.25

Perbuatan ujaran kebencian dapat menimbulkan beragam macam bentuk dalamtindakannya, misalnya menghina, hasutan, memprovokasi, menista, mencemarkan nama baik, menyebarkan berita yang tidak benar dan lain-lain.[88]

c. *Carding*

Carding adalah suatu kejahatan siber yang dilakukan dengan cara pencurian informasi dalam kartu kredit atau data perbankan lainnya untuk melakukan transaksi perdagangan secara illegal melalui jaringan internet.[89] Dampak dari kejahatan ini dapat menimbulkan kerugian finansial yang sangat besar bagi individu maupun bisnis. Pelaku carding dalam memperoleh kartu kredit tanpa izin kemudian menggunakan kartu kredit tersebut untuk melakukan transaksi seperti membeli barang secara online, diluar sepengetahuan pemilik kartu kredit.

d. *Data forgery*

Pemalsuan data *(data forgery)* adalah suatu perbuatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan pada *scriptless document* melalui internet. Pada umumnya, kejahatan ini banyak tejadi pada dokumen-dokumen *e-comerce* yang seakan-akan terjadi salah ketik yang akhirnya tindakan tersebut menguntungkan bagi pelaku.[90]

e. Penyebaran virus malware

[88]Andi Najemi et al., "Meningkatkan Pemahaman Masyarakat Terhadap Tindak Pidana Ujaran Kebencian Melalui Media Sosial," *Joong-Ki : Jurnal Pengabdian Masyarakat* Vol. 1, no. 3 (2022): hlm.401, https://doi.org/10.56799/joongki.v1i3.804.

[89]Thea farina, Rizki S. Sangalang. *Hukum Pidana Cyber*. Cetakan Ke-1, Media Penerbit Indonesia; Medan. 2023. Hlm. 89.

[90]Ibrahim Fikma Edrisy. *Op.Cit*. Hlm.6.

Penyebaran virus malware dengan sengaja merupakan suatu tindakan yang dapat menimbulkan dampak yang sangat luas. Penyebaran ini seringkali dilakukan oleh pihak-pihak yang memiliki tujuan untuk merusak sistem pada komputer, mencuri informasi-informasi dan dokumen penting, sehingga akibat dari perbuatan tersebut menimbulkan gangguan umum. Salah satu penyebaran virus yang saat ini marak terjadi di dunia maya yaitu ransomware. Ransomware adalah suatu malware yang menyandera data korban serta meminta sejumlah uang tebusan untuk memulihkan data tersebut.

f. *Hacking* dan *Cracker*

Secara umum, hacker adalah orang yang memiliki pengetahuan mendalam terhadap sistem komputer dan jaringan, serta memiliki kemampuan untuk memanipulai atau mengeksplorasi data pada sistem tersebut, hacker melakukan peretasan terhadap data pribadi tanpa izin. Cracker adalah suatu kelompok atau individu yang mencuri data pada jaringan komputer dengan merusak sistem keamanan pada komputer serta melakukan perusakan data.[91]

3. Karakteristik Tindak Pidana Informasi Dan Transaksi Elektronik

Tindak pidana *cyber crime* memiliki beberapa karakteristik yaitu sebagai berikut:

a. Ruang lingkup kejahatan;
b. Sifat kejahatan;
c. Pelaku kejahatan;
d. Modus kejahatan;

[91]Thea farina, Rizki S. Sangalang. *Op.Cit*.hlm.92.

e. Jenis kerugian yang ditimbulkan.[92]

a. Ruang lingkup kejahatan

Ruang lingkup dalam kejahatan dunia maya itu sangat luas, banyak kejahatan-kejahatan *cyber crime* yang terjadi secara transnasional yang melintasi antar negara. Oleh karena itu, tidak dapat di pastikan yuridiksi hukum negara mana yang akan di kenakan terhadap pelaku tindak pidana.

b. Sifat kejahatan

Cyber crime memiliki sifat kejahatan yang tidak menimbulkan kekacauan yang mudah terlihat.

c. Pelaku kejahatan

Kejahatan cyber crime merupakan suatu kejahataan yang dilakukan oleh orang-orang yang menguasai sistem komputer atau jaringan internet. Pelaku kejahatan ini pada umumnya sangat sulit untuk di identifikasi, maka dalam melakukan penyidikan terhadap kasus-kasus *cyber crime* juga harus menggunakan alat-alat bukti eleketronik yang valid.[93]

d. Modus kejahatan

Modus yang digunakan dalam kejahatan cyber crime adalah modus operandi, yang dimana hanya bisa dimengerti oleh orang-orang yang memiliki pengetahuan atau ahli dalam sistem komputer maupun jaringan internet, seperti tentang pemograman sistem perangkat lunak dalam komputer.[94]

[92]Sahat Maruli T. Situmeang. *Op.Cit.* Hlm. 24.
[93]Ibrahim Fikma Edrisy. *Op.Cit*. Hlm.7.
[94]Sahat Maruli T. Situmeang. *Loc.Cit*. Hlm. 25.

e. Jenis kerugian yang ditimbulkan

Cyber crime berpotensi menimbulkan kerugian pada banyak bidang seperti politik, ekonomi, sosial budaya yang lebih besar dampaknya dibandingkan dengan kejahatan berintensitas tinggi lainnya.[95]

[95]*Ibid.hlm.26*

BAB III
PEMBAHASAN

A. 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.[96] Ransomware termasuk tindak pidana *cyber crime* yang sedang marak terjadi sekarang. Tindak pidana *cyber crime* juga merupakan kejahatan transnasional yang dimana kejahatan ini terjadi melalui lintas negara, bahkan merupakan tindak pidana yang jaringan sangat luas serta bisa mengancam keamanan data pada suatu negara.[97] 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.

Dampak yang ditimbulkan oleh tindak pidana ransomware ini sangat besar. Oleh karena itu, perlu dilakukan penegakan hukum terhadap tindak pidana ransomware ini. Di negara Indonesia sudah memiliki peraturan perundang-undangan yang mengatur mengenai kejahatan-kejahatan yang dilakukan melalui sistem komputer dan jaringan internet. Peraturan perundang-undangan tersebut

[96]Nur Syamsi Tajriyani, "Pertanggungjawaban Pidana Tindak Pidana Pemerasan Dengan Modus Operandi Penyebaran Ransomware Cryptolocker," *Jurnal Jurist-Diction,* Vol 4, no. 2 (2021): hlm.688, https://doi.org/10.20473/jd.v4i2.25785.

[97]Cok Rai Kesuma 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 Preferensi Hukum* 5, no. 1 (2024): 4, https://doi.org/10.22225/jph.5.1.8636.1-7.

adalah Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua atas Undang-Undang Nomor 11 tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Dalam hukum pidana, manusia merupakan subjek hukum yang memiliki peran sangat penting karena pada dasarnya subjek hukum pidana adalah individu yang melakukan perbuatan melawan hukum dan dapat diminta pertanggungjawaban atas perbuatannya, hal ini sebagaimana tercermin dalam KUHP yang mengatur berbagai bentuk tindak pidana dan sanksinya.[98] Berdasarkan pasal 55 KUHP tentang penyertaan dalam melakukan tindak pidana, yang dapat mempertanggungjawabkan perbuatannya adalah pelaku yang menyuruh lakukan dan turut serta melakukan tindak pidana. Kemudian, terdapat produk-produk hukum yang mengakui bahwa korporasi adalah subjek hukum yaitu UU ITE. Pada Pasal 1 angka 21 menyatakan bahwa "Orang adalah orang perseorangan, baik warga negara Indonesia, warga negara asing, maupun badan hukum.

Pengaturan tentang pertanggungjawaban pidana terhadap pelaku tindak pidana ransomware dalam Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transasksi Elektronik. Maka, Pertanggungjawaban pidana pelaku tindak pidana ransomware dapat dikenakan dengan Undang-Undang 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).

[98]Thea farina, Rizki S. Sangalang. *Op.Cit*. Hlm.62.

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 45 ayat (8) Jo. Pasal 45 ayat (9) UU ITE yang menyatakan bahwa dipidana penjara paling lama enam tahun 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, memkasa 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) 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 secara spesifik 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.

Sehingga pasal 32 ayat (1) ini dapat dikenakan terhadap pelaku tindak pidana ransomware jika perbuatan pelaku itu sudah sampai pada enkripsi kode binary kedalam sistem komputer milik korban. Tetapi pada unsur pemerasan yang dilakukan pelaku tindak pidana ransomware belum terpenuhi pada pasal 32 ayat (1). Ancaman pidana pada pasal 32 ayat (1) UU ITE diatur dalam Pasal 48 ayat (1) yang berbunyi "Setiap orang yang memenuhi unsur sebagaimana dimaksud pada Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp. 2.000.000.000,00 (dua miliar rupiah)".

Kemudian pengaturan pertanggungawaban tindak pidana ransomware dapat berpedoman pada Pasal 67 ayat (1) Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi yang menyatakan bahwa:

> 1) 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.

Kemudian pada Pasal 332 Undang-Undang Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana, yang menyatakan bahwa:

1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun, dipidana dengan pidana penjara paling lama enam tahun atau pidana denda paling banyak kategori V.
2) 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, dipidana dengan pidana penjara paling lama tujuh tahun atau pidana denda paling banyak kategori V.
3) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan, dipidana dengan pidana penjara paling lama delapan tahun atau pidana denda paling banyak kategori VI.

Pada pasal 332 KUHP baru yang mengatur mengenai tindak pidana *cyber crime* yang menggunakan sistem komputer sebagai alat kejahatan, tetapi dalam pasal ini unsur-unsur dari tindak pidana ransomware yang melakukan pemerasan belum terpenuhi dengan pasal ini. Maka pasal ini kurang relevan jika dikaitkan dengan tindak pidana ransomware. Oleh karena itu, dalam KUHP baru belum juga mengatur secara spesifik terkait dengan pertanggungjawaban pidana terhadap pelaku tindak pidana ransomware.

Berdasarkan seluruh aturan dalam UU ITE, KUHP lama maupun dalam UU Perlindungan Data Pribadi dan Undang-Undang Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana, maka penulis berpendapat bahwa pengaturan terkait dengan tindak pidana ransomware masih mengalami kekaburan, yang dimana belum ada pasal yang menjelaskan secara spesifik terkait dengan tindak pidana jenis baru ini. Hal ini dikarenakan dalam UU ITE tidak memberikan batasan secara khusus yang mengatur mengenai “serangan ransomware”,

melainkan tindak pidana ransomware masih dikategorikan sebagai bentuk tindak pidana yang lain, seperti tindak pidana peretasan. Maka, menyebabkan tindak pidana ransomware sampai saat ini marak terjadi, bahkan modus operandinya terus berkembang dengan memanfaatkan teknologi, terutama melalui sistem komputer. Sehingga serangan ransomware ini semakin canggih dan kasusnya pun sulit untuk diungkap, bahkan sampai saat ini belum ada putusan pengadilan yang mengadili kasus tersebut.

Seharusnya didalam UU ITE ini tindak pidana ransomware memang diatur secara langsung serta tidak merujuk sebagai perbuatan yang lainnya. Pada pasal 27B ayat (1) UU ITE menjelaskan mengenai ransomware atau pemerasan, tetapi dalam pasal ini pemerasan yang dimaksudkan dilakukan dalam lingkungan keluarga, maka penuntutan pidananya pun hanya dilakukan oleh pihak yang merasa dirugikan (delik aduan). Tindak pidana ransomware cukup sulit untuk diselesaikan dengan menggunakan pasal 368 ayat (1) KUHP. Hal ini disebabkan karena ada beberapa unsur tindak pidana ransomware 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.
b) Modus operandi pemerasan ransomware berbeda dengan kejahatan konvensional.
c) Dalam KUHP ada keterbatasan yaitu tidak dapat membebankan pertanggungjawaban pidana pada subyek huum Korporasi atau badan hukum yang melakukan tindak pidana ransomware.

Selanjutnya penulis berasumsi bahwa dalam pengaturan UU ITE mengenai penggunaan Pasal 30 ayat (2) dan Pasal 32 ayat (1) UU ITE juga belum cocok dalam mengatur mengenai tindak pidana ransomware. Hal ini dikarenakan bahwa dalam Pasal 27B ayat (1), Pasal 30 ayat (2), Pasal 32 ayat (1) UU ITE dan Pasal 368 ayat (1) KUHP, dan pasal 67 ayat (1) UU Perlindungan Data Pribadi tidak menegaskan mengenai proporsi "ransomware" secara spesifik, terutama pada pemerasan yang dilakukan dengan mengakses sistem komputer, sehingga dalam kasus tindak pidana ransomware belum diatur secara spesifik dalam pasal-pasal tersebut. Hal ini menunjukkan bahwa telah terjadi kekaburan norma dalam pengaturan pertanggungjawaban pidana terhadap pelaku tindak pidana ransomware, sehingga menyebabkan pelaku tindak pidana ransomware sulit untuk diminta pertanggungawaban pidana atas perbuatannya.

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:

1. 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;
2. Lakukan scanning komputer menggunakan Anti-Virus terbaru secara berkala untuk membantu sistem komputer mengetahui keberadaan aplikasi tidak dikenal atau mempunyai *signature malware*;
3. Selalu mengaktifkan *Windows Firewall* yang berguna untuk membuat sebuah aturan pada *Windows Firewall* sehingga program atau sistem komputer dapat melakukan pembaruan secara otomatis;
4. Berhati-hati pada setiap link yang diterima, terutama berasal dari email spam;
5. 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;
6. melakukan pencadangan data-data penting secara teratur menggunakan media penyimpanan online seperti *google drive* atau *icloud,* bahkan bisa juga menggunakan penyimpanan eksternal.[99]

Tindak pidana ransomware merupakan kejahatan yang dilakukan dengan memanfaatkan kecanggihan teknologi, pelakunya pun berasal dari orang-orang

[99]Nur Syamsi Tajriyani. *Op.Cit*. Hlm. 706-707.

maupun kelompok yang sudah terorganisir memiliki keahlian dalam dunia siber. Berdasarkan hal ini, penulis mengutip cara kerja ransomware dari jurnal Perlindungan Hukum Bagi Korban Serangan Ransomware, diantaranya adalah sebagai berikut:

a. Pengguna menerima sebuah email masuk yang seolah-olah berasal dari Alamat email yang meyakinkan;
b. Link membuka suatu window browser serta mengarahkan pengguna kesuatu *website* yang aman tanpa ada pemberitahuan apapun;
c. Pada saat membuka halaman, web server yang menyimpan file tertentu yang berbahaya serta mulai berkomunikasi dengan sistem komputer milik korban, setelah itu menyimpan link yang mengarahkan pada ransomware;
d. Pada saat versi kerentanan sudah terkonfirmasi, *exploit kit* memanfaatkan kerentanan tersebut;
e. Setelah tahap ini, kode-kode binary tersebut melakukan kembangbiak, termasuk kedalamnya *vssadmin.exe* atau Salinan bayangan, agar mengahapus bayangan yang sudah ada dimesin korban serta membuat yang baru untuk dapat disembunyikan;
f. Kemudian mengenkripsi file korban serta *malware* mengirimkan kunci enkripsi;
g. Terakhir, server mengirimkan pesan ke korban untuk meminta sejumlah uang tebusan agar dapat mendapatkan kunci enkripsi file tersebut.[100]

[100]Desyanti Suka Asih K.Tus, *Op.Cit*. Hlm.130-131.

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.

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

Pada sub bab sebelumnya telah dijelaskan bahwa pengaturan petanggungawaban pidana terhadap pelaku tindak pidana ransomware masih mengalami ketidakjelasan yang menyebabkan unsur-unsur yang harus dipetanggungawabkan pelaku belum terpenuhi secara optimal. Sebagaimana yang sudah dijelaskan bahwa pengaturan tentang pertanggungawaban dapat berpedoman

pada Pasal 27B ayat (1), Pasal 30 ayat (2), Pasal 32 ayat (1) UU ITE, Pasal 368 Ayat (1) KUHP dan Pasal 67 ayat (1) UU Perlindungan Data Pribadi. Namun dari beberapa peraturan dan pasal-pasal yang dikaitkan dengan tindak pidana ransomware justru tidak ada satu pasal pun yang mengatur secara spesifik yang mengatur mengenai pertanggungawaban pidana terhadap pelaku tindak pidana ransomware, sehingga pelaku tidak dapat diminta pertanggungjawaban sebagaimana mestinya.

Hal ini dikarenakan pengaturan tentang tindak pidana ransomware masih mengalami kekaburan norma, maka tindak pidana ini masih marak terjadi dan sudah banyak pihak yang dirugikan baik secara materiil maupun imateril, yang dimana pihak yang dirugikan ini disebut sebagai korban. Selain itu, 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.[101]

Kejahatan ransomware yang terjadi pada Bank BSI dapat dikatakan menjadi suatu bentuk kelalaian dalam mengelola data dan/atau informasi nasabah Bank BSI

[101]*https://www.tempo.co/ekonomi/bsi-kena-serangan-ransomware-nasabah-mengaku-rugi-ratusan-juta-188320*, Diakses pada 20 Januari 2025 pada Pukul 11.00 WIB.

oleh Pelaku Usaha Jasa Keuangan (PUJK), yang dimana seharusnya PUJK melakukan pengecekan terkait dengan kelayakan teknologi informasi tersebut secara berkala guna menjaga keamanan data nasabah pada Bank BSI. Bentuk kelalaian yang dilakukan oleh PUJK ini dapat dikenakan sanksi administratif mengacu pada Pasal 19 Peraturan Otoritas Jasa keuangan RI Nomor 22 Tahun 2023 Tentang Perlindungan Konsumen dan Masyarakat Di Sektor Jasa Keuangan, dengan denda paling banyak Rp. 15.000.000.000,00 (lima belas miliar rupiah)

Kasus ransomware berikutnya adalah serangan ransomware pada pusat data nasional milik Kementerian Komunikasi dan Informasi RI *(Kominfo)* dengan bentuk serangan ransomware *Brain Chipe*r pengembangan terbaru *lockbit* yang mengakibatkan 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).[102] 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

[102]CNN Indonesia, *https://www.cnnindonesia.com/teknologi/20240624140714-185-1113434/pusat-data-nasional-diserang-pelaku-minta-tebusan-rp131-miliar/amp*, Diakses Pada 20 Januari 2025 pada pukul 11.40 WIB.

pertanggungawaban pidana bagi pelaku tindak pidana ransomware yang sebagaimana diatur dalam Kitab Undang-Undang Hukum Pidana dan Undang-Undang 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.

Bentuk pertanggungjawaban pidana terhadap pelaku tindak pidana ransomware yang diatur dalam Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, selain itu diatur juga dalam pasal 67 Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. Dalam 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*.

Dengan demikian dapat dipastikan apabila korporasi melakukan tindak pidana ransomware maka dapat diminta pertanggungjawaban pidana kepada

korporasi tersebut sebagai subjek 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.[103]

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).*[104] 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

[103]Imam Makhali, "Bentuk Pertanggung Jawaban Pidana Bagi Pelaku Tindak Pidana Mayantara," *Jurnal Transparansi Hukum,* Vol. 6, no. 1 (2023): hlm. 37, https://doi.org/10.30737/transparansi.v6i1.4226.

[104]Laila Mulasari, "Ajaran Pertanggungjawaban Pidana Korporasi Dalam Kebijakan Hukum Pidana Di Bidang Mayantara," *Jurnal Hukum Dan Dinamika Masyarakat* Vol 9, no. 2 (2019): hlm. 116. http://jurnal.untagsmg.ac.id/index.php/hdm/article/view/301.

bagi setiap orang, terutama bagi pelaku tindak pidana agar tidak terjadi kesewenangan dari aparat yang berwenang.[105]

Doctrine Of Identification merupakan suatu ajaran yang dianut oleh peraturan perundang-undangan khususnya yang terkait dengan hukum pidana, dalam *Doctrine Of Identification* telah mengajarkan bahwa suatu korporasi dapat diberikan beban pertanggungawaban pidana. Terkait dengan bentuk pembebanan yang ditujukan kepada pelaku tindak pidana ransomware harus bertanggungjawab secara hukum, maka jika korporasi yang melakukan tindak pidana tersebut yang dapat menentukan beban pertanggungjawaban pidana adalah Jaksa Penuntut Umum.[106]

Kemudian bentuk pertanggungjawaban pidana terhadap pelaku tindak pidana ransomware dalam KUHP lama yang dikaitkan dengan Pasal 368 ayat (1) KUHP. Dalam konsep KUHP, bentuk pertanggungjawaban pidana dalam tindak pidana *cyber crime* menganut ajaran pertanggungawaban yang ketat *(doctrine of strict liability)*, selain itu) KUHP juga menggunakan ajaran pertanggungjawaban pengganti *(doctrine of vicarious liability)* yang secara khusus mengatur mengenai pertanggungawaban pidana terhadap korporasi sebagai pelaku.[107] Menurut penulis ajaran pertanggungawaban ketat ini hanya diterapkan dalam konteks tertentu yang dimana difokuskan pada kejahatan yang tidak memerlukan pembuktian adanya kesalahan atau bahan niat jahat dari pelaku tindak pidana, maka dalam ajaran ini

[105]Sahuri Lasmadi, "Pertanggungjawaban Korporasi Dalam Perspektif Kebijakan Hukum Pidana Indonesia," *Disertasi Universitas Airlangga*. 2003. hlm.116. https://repository.unair.ac.id/28616/

[106]Imam Makhali. *Op.Cit*. hlm. 39.

[107]Mulasari,Op.Cit.hlm.118

hanya memungkinkan seseorang dikenakan sanksi pidana hanya berdasarkan pada fakta bahwa telah melakukan suatu perbuatan yang dilarang tanpa mempertimbangkan kesalahan *(mens rea)*. Dalam KUHP menggunakan prinsip bentuk pertanggungjawaban pidana berdasaran kesalahan yang sebagaimana telah ditegaskan dalam konsep pertanggungawaban pidana.

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.

BAB IV
PENUTUP

A. Kesimpulan

1. Pengaturan tentang pertanggungawaban pidana terhadap pelaku tindak pidana ransomware 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.
2. 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 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, dapat berpedoman juga pada KUHP dan Undang-Undang Nomor 27 Tahun 2022 Tentang Perindungan Data Pribadi. Dalam kasus ransomware yang terjadi pada Bank BSI dapat dikenakan sanksi administratif juga karena telah terjadi kelalaian pelaku usaha jasa keuangan dalam keamanan data pribadi nasabah yang dikenakan Pasal 19 Peraturan Otoritas Jasa Keuangan. 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.

B. Saran

1. Perlu adanya pengaturan yang secara spesifik mengatur mengenai pertanggungawaban pidana terhadap pelaku tindak pidana ransomware, sehingga tindak pidana ransomware atau tindak pidana pemerasan secara online dapat ditindak secara tegas dan pelaku dapat diminta pertanggungjawaban pidana atas tindakanya.
2. Perlu adanya penegakan hukum yang tegas terhadap pelaku tindak pidana ransomware untuk memberikan efek jera kepada pelaku dan dapat dikenakan sanksi pidana bagi pelaku tindak pidana ransomware sebagai bentuk pertanggungjawaban pidana, dan perlu ditingkatkannya kesadaran akan pentingnya keamanan siber untuk mencegah dan melindungi dari serangan ransomware yang dapat mengakibatkan kerugian.

DAFTAR PUSTAKA

A. BUKU :

Abdul Halim Barkatullah. *Hukum Transaksi Elektronik*. Cetakan Ke-1, Penerbit Nusa Media; Bandung, 2017.

Aksi Sinurat. *Azas-Azas Hukum Pidana Materil Di Indonesia.* Cetakan Pertama; Penerbit LP2M Universitas Nusa Cendana, Kupang, 2023.

Allan Liska dan Timothy Gallo. *Ransomware: Defending Againts Digital Extortion, Sebastopol*. Penerbit O‟Reilly Media, Amerika Serikat, 2017.

Amalia, Moh. Mujibur Rohman Ady Purwoto Mia, dkk. *Asas-Asas HukumPidana.* Cetakan Pertama. Penerbit Global Eksekutif Teknologi, Padang, 2023.

Amir Ilyas. *Asas-Asas Hukum Pidana: Memahami Tindak Pidana Dan Pertanggungjawaban Pidana Sebagai Syarat Pemidanaan*. Cetakan Pertama; Penerbit Rangkang Education Yogyakarta & PuKAP-Indonesia, Yogyakarta, 2012.

Andi Sofyan, Nur Azisa. *Buku Ajar Hukum Pidana*. Cetakan Ke-1; Penerbit *Pustaka Pena Press*, Makassar, 2020.

Angkasa, Nitaria, Yulia Kusuma Wardani, dkk. *Metode Penelitian Hukum: Sebagai Suatu Pengantar*.Cetakan Pertama; Penerbit Laduny Alifatama, Lampung, 2019.

Chandra, Tofik Yanuar. *Hukum Pidana*. Cetakan Pertama. Penerbit Sangir Multi Usaha, Jakarta, 2022.

Edrisy, Ibrahim Fikma. *Pengantar Hukum Siber*. Cetakan Pertama. Penerbit Sai Wawai Publishing, Lampung, 2019.

Fitri Wahyuni. *Dasar-Dasar Hukum Pidana Di Indonesia*. Cetakan Ke-1; Penerbit Nusantara Persada Utama, Tanggerang. 2017.

Irwansyah. *Penelitian Hukum Pilihan Metode & Praktik Penulisan artikel*. Edisi Revisi, Penerbit Mira Buana Media, Yogyakarta, 2021.

Ishaq. *Hukum Pidana.* Cetakan ke-2; Penerbit Raja Grafindo Persada, Depok, 2022.

Kenedi, John. *Kebijakan Hukum Pidana (Penal Policy)*. Cetakan Pertama. Penerbit Pustaka Pelajar, Yogyakarta, 2017.

Krismiyarsi. *Pertanggungjawaban Pidana Individual*. Cetakan Pertama; Penerbit

Pustaka Magister, Semarang. 2018.

Muhaimin. *Metode Penelitian Hukum*. Cetaan Pertama; Penerbit mataram university fers, Mataram, 2020.

Peter Mahmud marzuki. *Penelitian Hukum*. edisi revisi; Penerbit Kencana Prenada Media Grup, Jakarta, 2005.

Roeslan saleh. *Pikiran-Pikiran Tentang Pertanggung Jawaban Pidana*. Cetakan Pertama, Penerbit Ghalia Indonesia, Jakarta,1982.

Sahat Maruli T. Situmeang. *Cyber Law*. Cetakan Pertama; Penerbit Cakra, Bandung, 2020.

Sianturi, E.Y. Kanter dan R. *Asas-Asas Hukum Pidana Di Indonesia Dan Penerapannya*. Cetakan ke-3, Penerbit Storia Grafika, Jakarta, 2002.

Teguh Prasetyo. *Hukum Pidana.* Cetakan Ke-10; Penerbit Rajawali Pers. Depok, 2019.

Thea farina, Rizki S. Sangalang. *Hukum Pidana Cyber*. Cetakan Ke-1, Media Penerbit Indonesia; Medan. 2023.

B. JURNAL DAN KARYA ILMIAH :

Afifah, Diana. "Perlindungan Konsumen Di Sektor Jasa Keuangan Pada Kasus Serangan Siber Ransomware Yang Menimpa Perbankan." *JIIP - Jurnal Ilmiah Ilmu Pendidikan* Vol. 6, no. 11 (2023): 9318–23. https://doi.org/10.54371/jiip.v6i11.3176.

Andi Najemi, Hafrida Hafrida, Tri Imam Munandar, and Aga Hanum Praydhi. "Meningkatkan Pemahaman Masyarakat Terhadap Tindak Pidana Ujaran Kebencian Melalui Media Sosial." *Joong-Ki : Jurnal Pengabdian Masyarakat* Vol. 1, no. 3 (2022): 400–407. https://doi.org/10.56799/joongki.v1i3.804.

Ariyaningsih, Sindy, A. Ari Andrianto, Adri Surya Kusuma, and Rina Arum Prastyanti. "Korelasi Kejahatan Siber Dengan Percepatan Digitalisasi Di Indonesia." *Justisia: Jurnal Ilmu Hukum* Vol. 1, no. 1 (2023): 1–11. https://doi.org/10.56457/jjih.v1i1.38.

Budiarta, Putu Andhika Kusuma Yadnya I Dewa Gede, and I Dewa Nyoman Gde Nurcana. "Kajian Yuridis Terhahap Pertanggungjawaban Tindak Pidana Informasi Dan Transaksi Elektronik (ITE)." *Jurnal Unhi Vidya Wertta* Vol 6, No. 1 (2022): 50–59. https://books.google.com/books?hl=en&lr=&id=lRKfEAAAQBAJ&oi=f

nd&pg=PP1&dq=yuridis+or+hukum+and+rekam+medis+elektronik+and+implementasi+or+penerapan&ots=_NNtz_FJrY&sig=LRrqJ7LADqfGIjr7gVTvYStmtnc

Cok Rai Kesuma 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 Preferensi Hukum* 5, no. 1 (2024): 4. https://doi.org/10.22225/jph.5.1.8636.1-7.

Fadlian, Aryo. "Pertanggungjawaban Pidana Dalam Suatu Kerangka Teoritis." *Jurnal Hukum Positum* Vol. 5, no. 2 (2020): hlm. 10–19. https://journal.unsika.ac.id/index.php/positum/article/view/5556

Habibi, Miftakhur Rokhman, and Isnatul Liviani. "Kejahatan Teknologi Informasi (Cyber Crime) Dan Penanggulangannya Dalam Sistem Hukum Indonesia." *Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam* Vol. 23, no. 2 (2020): 400–426. https://doi.org/10.15642/alqanun.2020.23.2.400-426.

Irfan arief kurniawan, hadi mahmud, Nourma dewi. "Penyebaran Virus Ransomware Wannacry Berdasarkan Undang-Undang Nomor 11 Tahun 2008." *Jurnal Inovasi Penelitian* Vol. 1, no. 2 (2021): 48–55. https://cloudmatika.co.id/blog-detail/keamanan-sistem-informasi

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

Ketaren, Eliasta. "Cybercrime, Cyber Space, Dan Cyber Law." *Jurnal TIMES Vol.* 5, no. 2 (2016): 35–42. https://doi.org/10.51351/jtm.5.2.2016556.

Laksana, Tri Ginanjar, and Sri Mulyani. "Pengetahuan Dasar Identifikasi Dini Deteksi Serangan Kejahatan Siber Untuk Mencegah Pembobolan Data Perusahaan." *Jurnal Ilmiah Multidisiplin* Vol. 3, no. 01 (2024): 109–22. https://doi.org/10.56127/jukim.v3i01.1143.

Lasmadi, Sahuri. "Pengaturan Alat Bukti Dalam Tindak Pidana Dunia Maya." *Jurnal Ilmu Hukum*, Vol. 1, no. 2 (2014): 1–23. https://media.neliti.com/media/publications/43274-ID-pengaturan-alat-bukti-dalam-tindak-pidana-dunia-maya.pdf

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

Makhali, Imam. "Bentuk Pertanggung Jawaban Pidana Bagi Pelaku Tindak Pidana

Mayantara." *Jurnal Transparansi Hukum* Vol. 6, no. 1 (2023): 31–43. https://doi.org/10.30737/transparansi.v6i1.4226.

Muhaling, Aprianto J. "Kelalaian Yang Mengakibatkan Matinya Orang Menurut Perundang –Undangan Yang Berlaku." *Lex Crimen* vol. 8, no. 3 (2019): 35. https://ejournal.unsrat.ac.id/index.php/lexcrimen/article/view/25628

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

Najemi, Andi, Tri Imam Munandar, and Aga Hanum Prayudi. "Bahaya Penyampaian Berita Bohong Melalui Media Soaial." *Jurnal Karya Abdi* Vol. 5, no. 3 (2021): 578. https://online-journal.unja.ac.id/JKAM/article/view/16646

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

Praptono, A, and H Yusuf. "Tinjauan Kriminologi Terhadap Pelaku Kejahatan Pemerasan Dengan Menggunakan Virus, Ransomware Wannacry Sebagai Suatu Kejahatan Modern." *Jurnal Intelek Dan Cendikiawan Nusantara*, Vol. 1, No 2, (2024), hlm. 1530–39. https://jicnusantara.com/index.php/jicn/article/view/192%0Ahttps://jicnusantara.com/index.php/jicn/article/download/192/244

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): 123–39. https://doi.org/10.22437/pampas.v2i2.14761.

Ramadhan, G. "Perlindungan Hukum Bagi Korban Ransomware Wannacry Tindak Pidana Ransomware." *Jurnal Kajian Kontemporer Hukum Dan Masyarakat*, Vol. 1, no. 2 2023, 1–15. https://doi.org/10.11111/dassollen.xxxxxxx.

Richardson, Ronny, and Max M North. "Ransomware : Evolution , Mitigation and Prevention." *Authorized Administrator of DigitalCommons@Kennesaw State University* 13, no. 1 (2017): 10–21. https://digitalcommons.kennesaw.edu/facpubs Recommended.

Sari, Seva Maya, and Toguan Rambe. "Delik Culpa Dalam Kajian Fiqh Jinayah (Analisis Terhadap Pasal 359 KUHP Tentang Kealpaan Yang

Mengakibatkan Matinya Orang)." *Jurnal Penelitian Ilmu-Ilmu Sosial Dan Keislaman* Vol. 6, no. 2 (2020): 254. https://doi.org/10.24952/tazkir.v6i2.3031.

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

Winnie Stevani, and Hari Sutra Disemadi. "Urgency of Cryptocurrency Regulation in Indonesia: The Preventive Action for Ransomware Crime." *Hang Tuah Law Journal* Vol. 5, no. 1 (2021): 52–66. https://doi.org/10.30649/htlj.v5i1.32.

C. PERATURAN PERUNDANG-UNDANGAN :

Republik Indonesia. Undang-Undang Tentang Peraturan Tentang Hukum Pidana. UU Nomor 1 Tahun 1946.

Republik Indonesia. Undang-Undang Tentang Perlindungan Data Pribadi.UU Nomor 27 tahun 2022. Lembaran Negara RI Tahun 2022 Nomor 196. Tambahan Lembaran Negara RI Nomor 6820.

Republik Indonesia. Undang-Undang Tentang Kitab Undang-Undang Hukum Pidana. UU Nomor 1 Tahun 2023. Lembaran Negara RI Tahun 2023 Nomor 1. Tambahan Lembaran Negara RI Nomor 6842.

Republik Indonesia. Undang-Undang Tentang Perubahan Kedua Tentang Informasi Dan Transaksi Elektronik. UU Nomor 1 Tahun 2024. Lembaran Negara RI Tahun 2024 Nomor 1. Tambahan Lembaran Negara RI Nomor 6905.

Republik Indonesia. Peraturan Otoritas Jasa Keuangan Tentang Perlidungan Konsumen Dan Masyarakat Di Sektor Keuangan. Peraturan Nomor 22 Tahun 2023. Lembaran Negara RI Tahun 2023 Nomor 40. Tambahan Lembaran Negara RI Nomor 62.

D. INTERNET :

Hukum Online *https://www.hukumonline.com/berita/a/memahami-pertanggungjawaban-pidana-dalam-kuhp-baru-lt65da29d97d621/%23.* Diakses pada tanggal 9 september 2024 pukul 13.00 WIB.

Hukum Online, https://www.hukumonline.com/klinik/a/perbedaan-sengaja-dan-tidak-sengaja-dalam-hukum-pidana-lt5ee8aa6f2a1d3/, Diakses pada tanggal 27 November 2024 pada pukul 17.00 WIB.

Hukum Online, https://www.hukumonline.com/klinik/a/apa-perbedaan-delik-formil-dan-delik-materil-lt569f12361488b/, Di akses pada tanggal 8 Januari 2025 pada pukul 09.35 WIB.

https://www.tempo.co/ekonomi/bsi-kena-serangan-ransomware-nasabah-mengaku-rugi-ratusan-juta-188320, Diakses pada 20 Januari 2025 pada Pukul 11.00 WIB.

CNN Indonesia, https://www.cnnindonesia.com/teknologi/20240624140714-185-1113434/pusat-data-nasional-diserang-pelaku-minta-tebusan-rp131-miliar/amp, Diakses Pada 20 Januari 2025 pada pukul 11.40 WIB

Konspirasi keadian. https://konspirasikeadilan.id/artikel/unsur-kesengajaan-dalam-hukum-pidana0463, Diakses pada tanggal 26 November 2024 pukul 16.00 WIB.

CNN Indonesia. https://www.cnnindonesia.com/teknologi/20240522130109-185-1100872/serangan-siber-menggila-411-ribu-malware-baru-muncul-tiap-hari-di-ri/amp, diakses pada 9 September 2024 pukul 14.00 WIB.

BPPTIK Kementerian Komunikasi Dan Informatika RI https://bpptik.kominfo.go.id/Publikasi/detail/logo-dan-identitas-visual# diakses pada tanggal 12 september 2024 pukul 11.00 WIB.

Badan Siber dan Sandi Negara. “BSSN Identifikasi Pusat Data Nasional Sementara Diserang Ransomware.” Juni 24 2024. https://www.bssn.go.id/bssn-identifikasi-pusat-data-nasional-sementara-diserang-ransomware/. Diakses pada 10 September 2024 pukul 19.00 WIB.

Kanwil DJKN Jawa Barat. https://www.djkn.kemenkeu.go.id/kanwil-jabar/baca-artikel/16188/Ransomware-Ancaman-dan-Langkah-Langkah-untuk Menghindarinya. Diakses pada tanggal 5 Februari 2025 pada pukul 17.00 WIB.