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.[1] 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.[2] 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

---

[1]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.

[2]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.[3] 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).

[3]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.[4]

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

[4]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.[5]

[5]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.[6]

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

[6]*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).[7] 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

[7]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.[8]

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).*[9] 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

[8]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.

[9]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.[10]

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.[11]

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.[12] 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

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

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

[12]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.