PERTANGGUNGJAWABAN PIDANA ATAS SERANGAN *RANSOMWARE* TERHADAP DATA ASET INFORMASI NEGARA [1]

Oleh :
Monica Mutmainah Sabillah [2]
Caecilia J. J. Waha [3]
Youla O. Aguw [4]

ABSTRAK

Penelitian ini bertujuan untuk mengetahui pengaturan hukum terkait perlindungan data aset informasi negara dan untuk mengetahui bentuk pelaksanaan pertanggungjawaban pidana atas serangan *ransomware* terhadap data aset informasi negara. Dengan menggunakan metode penelitian normatif, dapat ditarik kesimpulan yaitu : 1. Di Indonesia, dasar hukum mengenai perlindungan aset informasi milik negara sebenarnya sudah tersedia, namun masih tersebar di berbagai regulasi yang berbeda-beda. Beberapa peraturan penting yang mengatur hal ini antara lain: Undang-Undang tentang Informasi dan Transaksi Elektronik (UU ITE), yang mengatur mengenai penggunaan serta keamanan sistem informasi elektronik, Undang-Undang Perlindungan Data Pribadi (UU PDP), yang mengatur perlindungan terhadap data pribadi, termasuk data milik aparatur pemerintah, Peraturan Presiden mengenai Sistem Pemerintahan Berbasis Elektronik (SPBE), yang mengatur pengelolaan sistem elektronik dalam layanan pemerintahan, Peraturan dan kebijakan dari Badan Siber dan Sandi Negara (BSSN), yang memiliki tugas utama menjaga keamanan siber, termasuk perlindungan terhadap data strategis negara. 2. Pelaksanaan pertanggungjawaban pidana atas serangan ransomware dapat diterapkan melalui ketentuan dalam UU ITE, khususnya Pasal 30, 32, 46, dan Pasal 27B. Pelaku yang terbukti melakukan akses tanpa hak, perusakan data, dan pemerasan secara elektronik dapat dijatuhi pidana sesuai asas kesalahan dalam hukum pidana Indonesia. Tindak pidana *ransomware* memenuhi unsur-unsur seperti akses tanpa hak, perusakan data, serta pemerasan melalui sistem elektronik. Pertanggungjawaban pidana didasarkan pada asas kesalahan dan mensyaratkan adanya unsur perbuatan melawan hukum serta niat jahat (mens rea) dari pelaku.

Kata Kunci : *ransomware, data aset informasi negara*

PENDAHULUAN

A. Latar Belakang

Konsep negara hukum sangat berkembang dalam lintas sejarah ditambah dengan perkembangan teknologi yang semakin maju membuat kejahatan semakin meningkat. Dengan perkembangan zaman yang semakin maju ditandai dengan meningkatnya penggunaan teknologi elektronik dan era digital. Teknologi dan era digital ini telah memengaruhi berbagai aspek kehidupan , seperti cara kita bekerja, berkomunikasi, hingga mengakses layanan sehari-hari. Kemajuan teknologi sangat mempermudah kita dalam melakukan aktivitas, tetapi juga menuntut kita untuk lebih bertanggungjawab atas hal tersebut. Salah satu tantangan diera digital ini adalah keamanan siber yang beragam.

Untuk mengatasi hal ini Pemerintah Indonesia telah mendirikan lembaga Kementerian Komunikasi dan Informatika (Kominfo) yang telah berganti nama menjadi Kementerian Komunikasi dan Digital (Komdigi) dan Badan Siber dan Sandi Negara (BSSN). Fungsi dari lembaga Komdigi sebagai perumusan kebijakan dibidang komunikasi dan digitalisasi, pelaksanaan bimbingan teknis dan supervisi, pengelolaan barang milik/kekayaan negara, pengawasan atas pelaksanaan tugas di lingkungan kementerian dan digital, yang diatur dalam Peraturan Presiden Nomor 174 Tahun 2024 Tentang Kementerian Komunikasi dan Digital.[5] Selain itu fungsi dari BSSN adalah perumusan kebijakan keamanan siber, pemantauan dan tanggapan insiden siber, edukasi dan kesadaran keamanan siber yang diatur dalam Peraturan Presiden Nomor 28 Tahun 2021.[6]

Untuk mengatasi hal ini, pemerintah Indonesia juga telah menerapkan berbagai regulasi guna menanggulangi kejahatan di dunia maya. Seperti Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE), yang direvisi melalui Undang-Undang Nomor 19 Tahun 2016 dan pembaruan kedua pada Undang-Undang Nomor 1 Tahun 2024, yang mengatur berbagai tindak pidana siber, seperti akses ilegal ke sistem elektronik, penyebaran

---

[1] Artikel Skripsi
[2] Mahasiswa Fakultas Hukum Unsrat, NIM 210711010321
[3] Fakultas Hukum Unsrat, Doktor Ilmu Hukum
[4] Fakultas Hukum Unsrat, Doktor Ilmu Hukum

[5] Lihat dalam Peraturan Presiden Nomor 174 Tahun 2024 tentang Kementerian Komunikasi dan Digital.
[6] Lihat dalam Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara.

informasi palsu serta pencurian data pribadi.[7] Selain itu, untuk meningkatkan perlindungan data masyarakat, pemerintah mengesahkan Undang-Undang Perlindungan Data Pribadi (UUPDP) Nomor 27 Tahun 2022, yang mewajibkan penyelenggaraan sistem elektronik untuk menjaga keamanan data pengguna. Pelanggaran terhadap regulasi ini dapat berujung pada sanksi administratif hingga pidana.

Dengan adanya perkembangan yang sangat pesat dalam era digital, kini teknologi informasi memainkan peran yang sangat penting dalam kehidupan masyarakat, baik secara individu maupun dalam konteks pemerintahan dan sektor publik. Oleh karena itu, kita perlu memahami bahwa data adalah salah satu aset paling berharga di era digital saat ini.

Data memiliki nilai tinggi dalam bidang ekonomi, politik, dan sosial, sehingga sering menjadi sasaran pihak yang tidak bertanggungjawab. Oleh karena itu, perlindungan data dan informasi, terutama yang berkaitan dengan kepentingan negara, menjadi sangat penting. Selain itu meskipun banyak orang menyadari pentingnya data tersebut dan diakui secara luas, namun ancaman terhadap keamanannya juga terus meningkat. Salah satu bentuk ancaman yang sangat mengkhawatirkan adalah serangan siber yang dikenal dengan istilah *"ransomware". Ransomware* merupakan jenis *malware* (perangkat lunak berbahaya) yang dapat mengenkripsi data dan meminta tebusan untuk mengembalikan akses terhadap data yang terkunci.[8] Serangan semacam ini telah mengakibatkan kerugian besar, tidak hanya individu atau perusahaan tetapi juga bagi Lembaga Pemerintahan dan Instansi Publik yang menyimpan data sensitif dan penting.

Ransomware adalah sejenis *malware* (Perangkat lunak berbahaya) yang menyerang perangkat korban dan menghalangi akses ke data mereka.[9] *Ransomware* Pertama kali muncul pada tahun 1989 dengan nama *AIDS Trojan* atau *PC Cyborg Trojan* (PCT), yang dibuat oleh Dr. Joseph Popp, seorang ahli biologi lulusan Universitas Harvard.[10] Pada saat itu, *PCT* menyerang data yang tersimpan di *disket* (floppy disk). *Ransomware* berkembang pada tahun 2000an dan lebih meningkat dengan jenis dan varian baru yang lebih canggih.[11] Beberapa varian *ransomware* ini menyebar melalui email spam, *phishing* dan *exploit kit*. Ada beberapa kasus *ransomware* yang pernah terjadi seperti *WannaCry, Petya/NotPetya, Locky*. Salah satu *ransomware* yang pernah menyerang Indonesia adalah *LockBit 3.0 Brain Cipher*.[12]

Pada tahun 2024, Indonesia menjadi sorotan besar. Salah satu kasus yang menonjol adalah serangan *ransomware* terhadap Pusat Data Nasional (PDN) 2 pada Juni 2024. Serangan ini menyebabkan data penting hilang atau terkunci, termasuk Aset Informasi Negara yang seharusnya dijaga dan dikelola dengan baik. Insiden ini mulai terjadi pada 17 Juni 2024 pukul 23.15 WIB, pada saat itu ditemukan upaya penonaktifkan fitur keamanan *Windos Defender*, serangan ini diketahui pada 20 Juni 2024 dari hasil investigasi. Setelah *Windos Defender* dinonaktifkan terdapat aktivitas *malicious* (berbahaya) yang mulai terjadi pada server PDNS.[13] Serangan ini mencakup berbagai aktivitas berbahaya, file yang berhubungan dengan penyimpanan, seperti instalasi file berbahaya, menghapus file penting, dan menonaktifkan layanan yang sedang berjalan. Selain itu, file yang berhubungan dengan penyimpanan, seperti *VSS, Hyper-V Volume, VirtualDisk,* dan *Veaam vPower NFS,* juga mulai dinonaktifkan dan gangguan.[14]

Dampak dari serangan *ransomware* ke Pusat Data Nasional Sementara teridentifikasi pertama kali pada saat layanan keimigrasian di seluruh bandara di Indonesia hingga pelabuhan Batam Center dan Nongsa lumpuh. Pada 25 Juni 2024 layanan instansi pemerintah yang terganggu akibat serangan *ransomware* ini sekitar 282 layanan. Pada 1 Juli 2024, kelompok peretas *Brain Cipher* mengumumkan melalui dark web bahwa mereka akan memberikan kunci untuk *mendekripsi* data PDNS yang telah *terenkripsi*. Mereka berjanji akan memberikan kunci tersebut

[7] Microsoft, *"Apa itu Ransomware?",* https://www.microsoft.com/id-id/security/business/security-101/what-is-*ransomware*?utm_source=chatgpt.com, diakses 5 Februari 2025.
[8] *Ibid.*
[9] Budi Hartono, *"Ransomware: Memahami Ancaman Keamanan Digital",* Bincang Sains dan Teknologi, Vol.2 No.2, Agustus 2024, Hal 56.
[10] *"Sejarah Ransomware: Lengkap Dari Awal Sampai Sekarang",* ASDF.ID, https://www. asdf.id/sejarah-*ransomware*/, diakses 5 Februari 2025.
[11] *Ibid.*
[12] Zulfikar Hardiansyah, *"Kronologi Serangan Ransomware ke PDN dan Penanganannya yang Tak Kunjung Usai",* https://tekno.kompas.com/read/2024/07/10/12350077/kronologi-serangan-*ransomware*-ke-pdn-dan-penanganannya-yang-tak-kunjung-usai, diakses 5 Februari 2025.
[13] *Ibid.*
[14] *Ibid.*

secara gratis pada 3 Juli 2024. sebelumnya, *Brain Cipher* sempat meminta tebusan sebesar 8 Juta dolar AS (sekitar Rp 131 miliar) kepada pemerintah untuk membuka data PDNS yang terkunci, namun permintaan tersebut ditolak. Pada 4 Juli 2024, Kominfo mengonfirmasi bahwa kunci yang diberikan oleh Brain Cipher dapat digunakan untuk membuka data PDNS, dan pada hari yang sama Direktur Jendral Aplikasi Informatika Kominfo, Semuel Pangerapan, mengumumkan pengunduran dirinya.[15]

Dalam kasus ini terdapat alat bukti elektronik yang digunakan untuk penyidikan lebih lanjut untuk mengungkap serangan *ransomware* pada Pusat Data Nasional ini. Kejahatan cyber dapat diketahui dengan menganalisis data. Caranya dengan mengumpulkan data dari berbagai sumber, seperti log aktivitas jaringan (catatan lalu lintas data di internet), sensor keamanan (alat yang mendeteksi ancaman), dan riwayat aktivitas pengguna (apa saja yang dilakukan pengguna di sistem).[16] Dalam kasus ini, pelaku melakukan kejahatan karena alasan ekonomi, yaitu ingin mendapat uang dengan cara meminta tebusan dari korban agar datanya yang terkunci bisa dibuka kembali. Dalam menangani kasus yang berkaitan dengan sistem informasi dan transaksi elektronik, ada 3 hal penting yang menjadi pedoman dalam penggunaan alat bukti elektronik yaitu, adanya motif, adanya pola, dan adanya persamaan dengan pristiwa yang lain.[17]

B. Rumusan Masalah

1. Bagaimana pengaturan hukum terkait perlindungan data aset informasi negara?
2. Bagaimana bentuk pelaksanaan pertanggungjawaban pidana atas serangan *ransomware* terhadap data aset informasi negara?

C. Metode Penulisan

Metode yang digunakan oleh penulis adalah Hukum Yuridis Normatif.

PEMBAHASAN

A. Pengaturan Hukum Terkait Perlindungan Data Aset Informasi Negara

Aset negara menurut Peraturan Pemerintah Nomor 38 Tahun 2008 Tentang Pengelolaan Barang Milik Negara/Daerah yang menggunakan istilah barang negara adalah semua barang yang dibeli atau diperoleh atas beban APBN atau berasal dari perolehan lainnya yang sah.[18]

Menurut Pasal 2 Peraturan Pemerintah Nomor 6 Tahun 2006, aset negara terdiri atas dua jenis, yaitu barang yang dibeli atau diperoleh atas beban APBN/APBD dan barang yang berasal dari perolehan lainnya yang sah yang meliputi:

a. barang yang diperoleh dari hibah/sumbangan atau yang sejenis;
b. barang yang diperoleh sebagai pelaksanaan dari perjanjian/ kontrak;
c. barang yang diperoleh berdasarkan ketentuan undang-undang, atau;
d. barang yang diperoleh berdasarkan putusan pengadilan yang telah memperoleh kekuatan hukum tetap.

Sedangkan pengertian aset dalam bentuk digital secara umum adalah segala sesuatu yang disimpan secara digital dan memberikan nilai bagi individu atau perusahaan.[19] Digital aset merupakan salah satu bentuk perkembangan dari konsep aset yang mulanya hanya sebatas terdapat dalam dunia riil namun berkembang kedalam dunia siber. Digital aset merupakan aset atau benda yang kepemilikannya tercatat secara digital yang dikendalikan langsung oleh pemiliknya.[20]

Menurut Peraturan BSSN No. 8 Tahun 2020 tentang Perlindungan Infrastruktur Informasi Vital "Aset informasi merupakan sumber daya informasi yang memiliki nilai bagi organisasi, termasuk data, perangkat lunak, dokumentasi sistem, dan perangkat keras pendukung yang digunakan dalam penyelenggaran sistem elektronik." (Pasal 1 angka 7).[21] Peraturan Presiden No. 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) menjelaskan "Data dan informasi pemerintah merupakan aset strategis yang wajib dikelola dan

[15] *Ibid*.
[16] 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.
[17] Sahuri Lasmadi, *"Pengaturan Alat Bukti Dalam Tindaak 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.
[18] Lihat dalam Peraturan Pemerintah Nomor 38 tahun 2008 Tentang Pengelolaan Barang Milik negara/Daerah.
[19] "Aset Digital, *"Contoh dan Untung Rugi Memperjual belikannya",* discus.com diakses dari https://www.qiscus.com/id/blog/aset-digital/ pada tanggal 25 Mei 2025 pukul 8:57.
[20] Firda Nur Amalina Wijaya, *"Bitcoin Sebagai Digital Aset Pada Transaksi Elektronik Di Indonesia (Studi Pada PT. Indodax Nasional Indonesia)"*, Jurnal Hukum Bisnis Bonum Commune Vol. 2 No. 2, (2019) Hal. 128.
[21] Badan Siber dan Sandi Negara (BSSN), *Peraturan BSSN Nomor 8 Tahun 2020 tentang Perlindungan Infrastruktur Informasi Vital*, Pasal 1 angka 7.

dilindungi untuk menjamin keberlangsungan pemerintahan dan pelayanan public." (Pasal 25 ayat (2)).[22]

Dengan demikian, aset informasi negara bukan hanya mencakup data administratif internal, melainkan juga informasi publik, data rahasia negara, dan data pribadi warga negara yang dikelola oleh pemerintah. Perlindungan terhadap aset ini merupakan bentuk nyata dari kedaulatan negara di ruang siber, dan menjadi landasan utama dalam membentuk sistem pertanggungjawaban hukum apabila terjadi pelanggaran, seperti dalam kasus serangan *ransomware*.

Menurut Peraturan Presiden Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital, informasi strategis termasuk dalam kategori Infrastruktur Informasi Vital (VII) yang mencakup sektor-sektor penting seperti energi, kesehatan, transportasi, keuangan, dan pemerintahan digital, beberapa contoh diantaranya:[23]

a. Data kepegawaian internal instansi
b. Rencana anggaran internal sebelum disahkan
c. Dokumen notulensi rapat strategis instansi
d. Informasi teknis sistem aplikasi pemerintahan

Berdasarkan Pasal 1 ayat (1) Perpres Nomor 95 Tahun 2018 tentang SPBE yang berbunyi "Sistem Pemerintah Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE".[24] Pengguna SPBE adalah semua pengguna yang memanfaatkan layanan SPBE termasuk pemerintah. Untuk mendukung pernyataan tentang pentingnya SPBE (Sistem Pemerintahan Berbasis Elektronik) dalam kaitannya dengan hukum pidana, terutama dalam konteks perlindungan terhadap sistem informasi pemerintah dari tindak pidana siber, kita bisa menggunakan kombinasi referensi dari:

1. Perpres No. 95 Tahun 2018 tentang SPBE; sebagai dasar tujuan transparansi dan pelayanan publik berbasis TIK.
2. UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE); sebagai dasar hukum pidana terhadap kejahatan siber yang menyerang sistem informasi pemerintah.

Keamanan Infrastruktur Informasi Kritis Nasional merupakan prasyarat mutlak yang harus diimplementasikan di Indonesia agar dapat menjamin efektivitas keandalan, ketersediaan, dan integritas jaringan informasi, baik secara nasional maupun global. Namun demikian, dampak besar dan potensi gangguan serta ancaman terhadap keamanan infrastruktur kritis nasional masih belum disadari sepenuhnya oleh masyarakat yang kini mengintai kita semua. Hal ini tampak dari belum tersedianya kebijakan Proteksi Infarastruktur Informasi Kritis Nasional dan belum dipetakan / diklasifikasikannya Infrastruktur Kritis Nasional, khususnya infrastruktur jaringan informasi. Ancaman terhadap Keamanan Infrastruktur Informasi Kritis Nasional dapat menimbulkan suatu kerugian yang tidak dapat ternilai terhadap stabilitas, perekonomian bahkan kedaulatan Negara. Pemerintah perlu mengambil langkah-langkah dan upaya preventif untuk menjamin agar setiap upaya yang dapat mengancam stabilitas negara tersebut dapat dicegah dan bagi pelakunya dapat disidik secara hukum dan dikenai ancaman pidana yang berat.[25]

Lebih lanjut disampaikan bahwa, pemerintah hendaknya juga dapat menerapkan Sebelas Prinsip Dasar tentang *Critical Information Infrastructure Protection* yang diusulkan oleh beberapa negara yang tergabung di dalam negara-negara G8 pada bulan Mei 2003, memuat strategi-strategi dalam menekan resiko terhadap potensi ancaman dan gangguan terhadap infrastruktur informasi kritis Nasional yang antara lain:[26]

a. Prinsip pertama; menekankan, pemerintah hendaknya memiliki jaringan peringatan dini (*emergency early warning networks*) untuk memantau kelemahan, ancaman dan kejadian terhadap infrastruktur informasi kritis Nasional.
b. Prinsip kedua; pemerintah berkewajiban meningkatkan kepekaan dalam memfasilitasi pemahaman para stakeholder mengenai sifat dan keadaan infrastruktur informasi kritis

[22] Presiden Republik Indonesia, *Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik*, Pasal 25 ayat (2).
[23] Presiden Republik Indonesia, *Peraturan Presiden Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital*, Pasal 1 dan Pasal 2
[24] Presiden Republik Indonesia, *Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik*, Pasal 1 ayat (1)
[25] Pusat Informasi dan Komunikasi Nasional (Pusinfokomnas), *Kajian Strategi Pengamanan Infrastruktur Sumber Daya Informasi Kritis*, (Jakarta: Laporan Penelitian, 2015), hal. 2–3, diakses dari https://media.neliti.com/media/publications/41201-ID-kajian-strategi-pengamanan-infrastruktur-sumber-daya-informasi-kritis-study-of-c.pdf. pada tanggal 25 Mei 2025 pukul 18:18
[26] *Ibid.*, hal 59-60.

yang dimilikinya, dan peran apa yang harus dimainkan oleh mereka.

c. Prinsip ketiga; pemerintah harus dapat dan mampu menguji serta mengenali sifat ketergantungan satu sama lain berbagai infrastruktur kritis yang dimilikinya agar dapat meningkatkan perlindungan terhadap infrastruktur tersebut.
d. Prinsip keempat; pemerintah hendaknya mendorong program kemitraan dengan para stakeholder, baik sektor public maupun swasta, dalam membagi dan menganalisis informasi infrastruktur kritis dalam rangka penanggulangan, penyidikan, dan tindakan kerugian ataupun gangguan yang telah terjadi terhadap infrastruktur tersebut.
e. Prinsip kelima; pemerintah berkewajiban membentuk dan memelihara pusat jaringan informasi krisis (*Crisis Information Network*) serta menguji dan melindungi keandalannya dalam keadaan darurat.
f. Prinsip keenam; pemerintah hendaknya dapat menjamin bahwa kebijakan tentang keterbukaan informasi juga harus dapat mengacu kepada kebutuhan akan perlindungan terhadap infrastruktur informasi kritis Nasional.
g. Prinsip ketujuh; pemerintah harus memfasilitasi penyidikan terhadap gangguan terhadap infrastruktur informasi kritis Nasional, dan bila memungkinkan berbagi informasi hasil penyidikannya dengan negara- negara lain.
h. Prinsip kedelapan; pemerintah hendaknya harus dapat memfasilitasi berbagai bentuk pelatihan untuk meningkatkan kemampuan bereaksi serta menguji kesiapan dan rencana cadangan bilamana terjadi gangguan terhadap infrastruktur informasi kritis Nasional dan berkewajiban mendorong para stakeholder untuk melakukan kegiatan yang serupa.
i. Prinsip kesembilan; pemerintah harus dapat menjamin ketersediaan produk-produk hukum yang memayungi berbagai kegiatan di atas, aparat yang terlatih dan mampu melakukan penyidikan dan penindakan atas gangguan yang terjadi, dan mengoordinasikan penyidikan tersebut dengan pihak lain, termasuk negara-negara yang terkait dengan gangguan tersebut.
j. Prinsip kesepuluh; pemerintah harus aktif menjembatani kerja sama internasional untuk memperoleh berbagai informasi kritis, termasuk di dalamnya mengembangkan dan mengoordinasikan sistem peringatan darurat, berbagi dan menganalisis informasi kelemahan-kelemahan, ancaman dan kejadian terhadap infrastruktur kritis, serta melakukan koordinasi penyidikan itu dengan mengacu kepada ketentuan-ketentuan hukum yang berlaku.
k. Prinsip kesebelas; pemerintah hendaknya menjembatani berbagai kegiatan penelitian, baik secara nasional maupun internasional, serta mendorong penggunaan berbagai aplikasi pengamanan yang telah disertifikasi berdasarkan standar- standar internasional yang berlaku.

Hal yang lebih penting selain sebelas prinsip tersebut adalah perlu adanya koordinasi antara pemangku kebijakan, baik regulator maupun operator terkait infrastruktur informasi kritis agar terciptanya harmonisasi. Disamping itu, upaya lainnya adalah dengan membangun *culture of cyber security* itu sendiri yang harus dimulai dari kalangan pemerintah (regulator) agar masyarakat secara luas dapat juga mengikuti dan mencontoh budaya tersebut.[27]

Klasifikasi ini penting sebagai dasar hukum untuk pengamanan sistem informasi negara dan juga menjadi parameter pertanggungjawaban pidana dalam kasus pelanggaran, seperti serangan *ransomware*. Pelaku yang menyasar sistem yang memuat informasi strategis dapat dihadapkan pada ancaman pidana yang lebih berat karena menyangkut keamanan nasional.

B. Pertanggungjawaban Pidana Atas Serangan *Ransomware* Terhadap Data Aset Informasi Negara

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). 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

[27] *Ibid.*

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.

Tindak pidana *ransomware* pada dasarnya merupakan bentuk kejahatan siber yang dapat dikategorikan sebagai tindak pidana pemerasan. *Ransomware* bekerja dengan cara menyusup ke dalam sistem elektronik milik korban, mengunci atau mengenkripsi data, lalu pelaku menuntut sejumlah tebusan agar data tersebut dapat diakses kembali. Dalam praktiknya, unsur-unsur dari kejahatan *ransomware* memiliki kesamaan karakteristik dengan unsur-unsur pemerasan yang diatur dalam hukum pidana, khususnya dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Salah satu pasal yang memiliki relevansi dengan tindak pidana *ransomware* adalah Pasal 27B ayat (1) UU ITE. Pasal ini menyatakan:[28]

"Setiap Orang dengan kekerasan atau ancaman kekerasan, secara melawan hukum memaksa orang untuk memberikan atau menyerahkan sesuatu, membayar atau mengakui utang, dilakukan dengan menggunakan Sistem Elektronik."

Walaupun rumusan pasal ini tidak secara spesifik menyebut istilah "*ransomware*", namun secara substansial, unsur-unsurnya sangat erat kaitannya. Dalam serangan *ransomware*, pelaku menggunakan sarana sistem elektronik untuk memaksa korban memberikan sesuatu biasanya uang dalam bentuk aset digital (*cryptocurrency*) agar akses terhadap data mereka dikembalikan. Unsur "kekerasan atau ancaman kekerasan" dalam konteks digital dapat diartikan sebagai ancaman penghapusan data, penyebaran informasi sensitif, atau penguncian sistem yang mengganggu aktivitas korban dan menimbulkan rasa takut atau cemas.[29]

Penjelasan pasal tersebut juga menyatakan bahwa ancaman kekerasan yang dimaksud adalah setiap tindakan yang ditujukan untuk menimbulkan ketakutan, kecemasan, atau kekhawatiran akan adanya kekerasan. Dalam kasus *ransomware*, tindakan tersebut dilakukan bukan dalam bentuk kekerasan fisik, melainkan kekerasan digital, yang efeknya sama berbahayanya terhadap stabilitas psikologis dan keamanan data korban.[30] Selanjutnya, tindak pidana *ransomware* juga dapat dikaji dari Pasal 30 ayat (2) UU ITE**,** yang berbunyi:[31]

"Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengkases Komputer dan/atau Sistem elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik"

Dalam pasal ini, unsur yang paling jelas berkaitan dengan *ransomware* adalah akses tanpa hak ke sistem elektronik, yang biasanya dilakukan melalui *eksploitasi* kerentanan sistem atau melalui teknik rekayasa sosial seperti *phishing* (salah satu bentuk **kejahatan siber** (*cybercrime*) yang dilakukan dengan **menipu korban agar secara sukarela memberikan informasi pribadi atau rahasia,** seperti **kata sandi, nomor kartu kredit, data login, atau informasi sensitif lainnya,** dengan cara menyamar sebagai entitas yang terpercaya). Akses tersebut digunakan oleh pelaku untuk mengenkripsi file, yang pada dasarnya merupakan penguasaan ilegal terhadap informasi milik korban.

Akan tetapi, Pasal 30 ayat (2) ini masih memiliki keterbatasan, karena tidak mencakup unsur pemerasan atau ancaman. Tujuan dalam pasal ini hanya sebatas "memperoleh informasi elektronik", bukan memaksa korban untuk memberikan sesuatu. Oleh karena itu, pasal ini dapat dijadikan pasal pendukung atau dasar tindak pidana awal (delik pokok), sedangkan unsur pemerasan lebih tepat diakomodasi oleh Pasal 27B ayat (1). Kombinasi kedua pasal ini dapat digunakan untuk mengonstruksikan pertanggungjawaban pidana terhadap pelaku *ransomware* dalam konteks sistem hukum nasional Indonesia.

Di sisi lain, karena kejahatan *ransomware* menyangkut aspek perbuatan melawan hukum melalui sistem elektronik**,** maka unsur subjek hukum pidana juga menjadi penting untuk ditegaskan. Dalam hukum pidana Indonesia,

[28] Lihat dalam *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*, Pasal 27B ayat (1)

[29] Lihat penjelasan Pasal 27B ayat (1) UU ITE mengenai makna "ancaman kekerasan"

[30] *Ibid.*

[31] Republik Indonesia, *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*, Pasal 30 ayat (2)

sebagaimana tercermin dalam Kitab Undang-Undang Hukum Pidana (KUHP), subjek hukum pidana adalah manusia (individu) yang dapat dimintai pertanggungjawaban atas perbuatan melawan hukum yang dilakukannya.[32] Dengan demikian, pelaku kejahatan *ransomware* dapat dikenai pertanggungjawaban pidana secara pribadi, sepanjang unsur kesengajaan, kemampuan bertanggung jawab, dan adanya perbuatan pidana dapat dibuktikan di pengadilan.

Perlindungan data pribadi berhubungan dengan konsep privasi. Konsep privasi sendiri adalah gagasan untuk menjaga integritas dan martabat pribadi.[33] Pengumpulan dan penyebarluasan data privasi tanpa sepengetahuan pemiliknya merupakan pelanggaran terhadap privasi seseorang, karena hak privasi mencakup hak untuk menentukan, memberikan atau tidak memberikan data privasi[34]

Meskipun Indonesia belum sepenuhnya memiliki regulasi khusus yang komprehensif mengenai perlindungan data pribadi pada saat awal perkembangan era digital, jaminan terhadap hak atas privasi telah ditegaskan dalam Pasal 28G Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, yang memberikan perlindungan terhadap diri pribadi, keluarga, kehormatan, martabat, dan harta benda seseorang, serta hak atas rasa aman dari segala bentuk ancaman. Dalam konteks serangan ransomware terhadap aset informasi negara**,** ketentuan ini menjadi sangat relevan, karena data yang disimpan oleh negara tidak hanya mencakup informasi pemerintahan, tetapi juga sering kali berisi data pribadi masyarakat seperti data kependudukan, kesehatan, dan keuangan.

Tindak pidana di bidang informasi dan transaksi elektronik merupakan bentuk perbuatan yang dilarang oleh peraturan perundang-undangan yang berlaku. Pengaturan mengenai kejahatan ini secara khusus termuat dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang kemudian diperbarui melalui Undang-Undang Nomor 19 Tahun 2016. Kedua undang-undang ini memberikan dasar hukum bagi penindakan terhadap berbagai bentuk pelanggaran yang dilakukan melalui sarana elektronik atau sistem digital.

Salah satu ketentuan utama yang mengatur mengenai tindak pidana tersebut terdapat dalam Pasal 27 UU ITE, yang memuat larangan terhadap perbuatan yang menggunakan sistem elektronik untuk menyebarkan konten bermuatan penghinaan, pencemaran nama baik, pemerasan, atau muatan asusila. Ketentuan ini menunjukkan bahwa hukum nasional telah menyesuaikan diri dengan dinamika kejahatan berbasis teknologi informasi.

Undang-Undang Nomor 1 Tahun 2024, tindak pidana yang relevan dengan serangan *ransomware* tidak disebutkan secara eksplisit, namun UU ITE memberikan dasar hukum bagi penindakan terhadap tindak pidana berbasis teknologi yang menargetkan data strategi dan aset informasi negara. Serangan ransomwaee terhadap sistem milik negara tidak hanya berdampak pada kerugian operasional, tetapi juga dapat mengancam keamanan nasional, kedaulatan data negara dan stabilitas pemerintahan.

Aset informasi negara adalah bagian dari infrastruktur informasi kritis nasional (IIKN), yang apabila terganggu, dapat menyebabkan gangguan besarr terhadap fungsi negara. Dalam konteks ini, serangan *ransomware* terhadap sistem pemerintahan atau lembaga negara bukan hanya kejahatan terhadap data elektronik, tetapi juga merupakan ancaman terhadap integritas dan fungsi negara.

Adapun dalam prespektif hukum pidana, *ransomware* yang menyerang aset informasi negara harus dipandang sebagai bentuk kejahatan berat (serious cybercrime), karena selain memenuhi unsur akses tanpa hak dan pemerasan, juga menyasar sistem yang dilindungi oleh hukum. Oleh sebab itu, perlu ada penegakan hukum yang tidak hanya menggunakan UU ITE, tetapi juga mengintegrasikan regulasi lainnya seperti UU Perlindungan Data Pribadi (UU No. 27 Tahun 2022) dan kebijakan keamanan siber nasional**,** serta membangun sistem deteksi dini dan kolaborasi dengan otoritas internasional.

Tinjauan terhadap sanksi pidana terkait *ransomware* erat dengan beberapa pasal dalam UU No.1 Tahun 2024 dan dapat diterapkan, yaitu:[35]

"Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau

[32] Moeljatno, *Asas-Asas Hukum Pidana*, (Jakarta: Rineka Cipta, 2002), hal. 68.

[33] Wahyudi Djafar, Bernhard Ruben Fritz dan Blandina Lintang Sentiani, "*Perlindungan Data Pribadi Di Indonesia"*, (Jakarta: Lembaga Studi Advokasi Masyarakat (ELSAM), 2016), hal.3

[34] Shinta Dewi Rosadi, "*CYBER LAW- Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional*", (Bandung: PT Refika Aditama, 2015), hal.9.

[35] Republik Indonesia, *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*, Pasal 30 ayat (3)

sistem elektronik dengan cara apapun dengan tujuan untuk melanggar, menembus, melampaui, atau menjebol sistem pengamanan." (Pasal 30 ayat (3))

Relevansi Pasal 30 ayat (3) UU ITE sangat penting, terutama apabila serangan ditujukan pada sistem elektronik milik negara. Pasal ini mengatur mengenai perbuatan mengakses sistem elektronik dengan sengaja, tanpa hak, dan dengan cara melanggar, menembus, atau menjebol sistem pengamanan. Dalam praktiknya, serangan *ransomware* hampir selalu melibatkan pelanggaran sistem keamanan untuk menyusup ke dalam server atau komputer targer. Jika sistem yang diserang merupakan milik instansi pemerintah atau Lembaga negara yang mennyimpang aset informasi strategis, maka pelaku tidak hanya melanggar hak kepemilikan digital, tetapi juga mengancam keamanan data negara yang sudah mencakup unsur ilegalitas akses dan pelanggaran terhadap sistem pertahanan elektronik sebagai Langkah awal dalam rangkaian serangan siber.

"Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak RP12.000.000.000,00 (dua belas miliar rupiah)" (Pasal 46 ayat (3))

Sanksi yang diberikan dalam konteks serangan *ransomware* terhadap sistem elektronik milik negara, karena mencerminkan keseriusan negara dalam melindungi kepentingan public. Tingginya ancaman pidana tersebut bertujuan memberikan efek jera serta memperkuat aspek pencegahan (*deterrent effect*) terhadap pelaku kejahatan siber yang secara sistematis dan terorganisir mengancam keamanan data nasional.

Penanggulangan kejahatan *ransomware* terhadap aset informasi negara tidak bisa hanya mengandalkan pendekatan represif, melainkan harus dilakukan secara integratif antara upaya preventif dan represif**.** Negara harus hadir melalui penguatan regulasi, sistem keamanan nasional, peningkatan kapasitas SDM, serta kerja sama lintas negara untuk menjamin keamanan dan kedaulatan data digital nasional. Upaya penanggulangan kejahatan tersebut dapat berupa upaya preventif dan upaya represif:[36]

1. Upaya Preventif Upaya ini merupakan upaya pencegahan yang dilakukan guna mencegah timbulnya suatu kejahatan didalam lingkup masyarakat. Beberapa hal yang dapat dilakukan guna mencegah terjadinya suatu kejahatan adalah dengan melakukan edukasi terhadap masarakat, melakukan pemblokiran, membentuk Badan Siber dan Sandi Negara (BSSN). Contohnya: peningkatan sistem keamanan jaringan pada instansi strategis melalui *firewall*, *antivirus*, *enkripsi*, dan sistem deteksi dini (IDS/IPS) dan audit sistem digital pemerintahan secara berkala.
2. Upaya Represif Upaya ini merupakan salah satu upaya yang bersifat konsepsional, dimana upaya ini dilakukan setelah terjadinya suatu kejahatan. Upaya ini bertujuan untuk menindak pelaku kejahatan seperti penjatuhan sanksi atau penjatuhan pidana sesuai dengan pelanggaran yang telah dilakukan. Adapun dapat diberlakukannya penerapan Pasal 30, 32, 46, dan Pasal 27B UU ITE, peningkatan pada *forensic digital* dan investigasi siber dan Kerjasama internasional melalui *INTERPOL* dan *ASEAN Cybersecurity Cooperation.*

Pertanggungjawaban atas tindak pidana di bidang informasi dan transaksi elektronik (ITE) merupakan bentuk tanggung jawab hukum yang harus dibebankan kepada pelaku yang melakukan pelanggaran terhadap ketentuan hukum di bidang tersebut. Dasar dari pertanggungjawaban pidana ini adalah asas kesalahan, yang menyatakan bahwa tidak dapat dijatuhkan pidana tanpa adanya kesalahan. Artinya, seseorang hanya dapat dikenai sanksi pidana apabila dapat dibuktikan bahwa ia memiliki kesalahan dalam melakukan perbuatannya.

Untuk membuktikan seseorang dinyatakan bersalah melakukan tindak pidana, ada dua unsur yang harus terpenuhi yaitu :

- Unsur Setiap Orang;
- Unsur Dengan Sengaja;

Bahwa yang dimaksud disini dengan Setiap Orang dalam undang-undang nomoe 35 tahun 2009 adalah subyek hukum, yaitu orang atau korporasi, yang melakukan suatau perbuatan hukum dan mampu mempertanggung jawabkan perbuatannya.

Kemudian Dengan Sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah mengurangi, melakukan transmisi, merusak suatu informasi elektronik dan/atau Dokumen elektronik milik orang lain atau milik publik.

Sanksi yang dapat dijatuhkan dalam tindak pidana ITE dapat berupa pidana penjara, denda, atau bentuk hukuman lain sesuai ketentuan hukum yang berlaku. Penegakan pertanggungjawaban

[36] A.S.Alam dan Amir Ilyas, *Kriminologi Suatu Pengantar"*, (Jakarta: Prenamedia Group, 2018), hal. 28."

pidana atas pelanggaran ITE diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, termasuk perubahan-perubahannya, serta peraturan perundang-undangan lainnya yang relevan. Agar keadilan hukum dapat terwujud, setiap proses penegakan hukum terhadap tindak pidana ITE harus memperhatikan unsur-unsur yang membentuk pertanggungjawaban pidana. Hal ini penting untuk memastikan bahwa hanya individu yang benar-benar memenuhi unsur kesalahan yang dapat dinyatakan bersalah dan dijatuhi hukuman.

Undang-Undang ITE secara eksplisit menggunakan istilah "aset informasi negara", namun jika disandingkan dengan Peraturan Presiden Nomor 95 Tahun 2018 tentang Standar dan Tata Cara Pelaksanaan Audit Keamanan Sistem Pemerintahan Berbasis Elektronik (SPBE) dan Peraturan lainnya dari Badan Siber dan Sandi Negara; maka sistem elektronik yang dikelola pemerintah dan memuat informasi strategis adalah bagian dari infrastruktur informasi kritis nasional. Oleh karena itu, pelaku yang menyerang sistem ini dengan *ransomware* layak dikenai sanksi pidana berat sebagaimana diatur dalam Pasal 46 ayat (3) dan Pasal 48 ayat (2) UU ITE.

Putusan Pengadilan Negeri Banjarbaru Nomor 85/Pid.Sus/2022/PN.Bjb yang merupakan salah satu contoh penegakan hukum terhadap kejahatan siber di Indonesia yang berkaitan dengan kerja sama Internasional. Dalam kasus ini, terdakwa Riswanda Noor Saputra terbukti mengembangkan dan mengoprasikan platform *phishing-as-service* bernama "16Shop", yang menjual perangkat lunak dan membuat situs palsu (Phising) yang digunakan untuk mencuri data pengguna dari berbagai negara.[37]

Cara terdakwa membuat TOOL KIT tersebut dengan cara awalnya terdakwa beli Domain di *idcloudhost* dengan pembayaran menggunakan Gateway OVO. Kemudian terdakwa menyiapkan peralatan berupa computer, setelah itu terdakwa mendownload aplikasi XAMP lalu terdakwa mendownload aplikasi SUBLIME TEXT, selanjutnya terdakwa membuat akun di salah satu produk Apple, untuk mengetahui isi bentuk tampilan gambar di aplikasi produk tersebut, lalu selanjutnya Terdakwa melakukan inspect element untuk mengambil kode dessain atau tampilan salah satu produk Apple, lalu terdakwa memprogram produk apple menggunkan *HTML, PHP, JAVA SCRIPT,* dan *CSS* .

Adapun cara pembeli menipu dan mencuri akun orang lain Adalah setelah membeli *TOOL KIT* Bernama 16shop dari terdakwa yang menyerupai PayPal dll, kemudian spammer (pembeli aplikasi) dengan menggunakan pengiriman email secara banyak dengan sekali kirim ke ratusan ribu email para korban pengguna produk PayPal, Apple, Amazon lalu setelah terkirim pada korban akan menerima sebuah email yang beriskan kata bahwa akaun merekan "Akun terkunci, aktifitas tidak wajar di akun, pembelian produk" dan para korban yang mengira itu Adalah email dari aplikasi PayPal, Apple, Amazon akan meng klik link yang sudah tersedia di email tersebut dan akan langsung mengarah ke TOOL KIT.

Penegakan hukum terhadap terdakwa yang melibatkan bantuan teknis dan informasi dari Lembaga penegak hukum asing yaitu *FBI (Federal Bureau Of Investigation)* yang mendeteksi dan melaporkan aktivitas situs 16Shop kejaringan penegak hukum internasional, serta *NBC INTERPOL* Jakarta dan Interpol Pusat yang menyampaikan hasil pelacakan IP address, penyedia hosting, dan dompet digital yang digunakan terdakwa, ke Divisi Hubungan Internasional Polri. Dengan bantuan dari FBI dan NBC terungkap dari surat kedua yang diberikan oleh Kedutaan Besar Amerika Serikat Nomor: U//FOUO/REL TO USE, IDN juga memberikan informasi bahwa nama yang tertera di akun Apple adalah Riswanda Noor Saputra. [38]

Dengan demikian terdakwa terjerat pasal 50 Undang-Undang Nomor 19 tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik jo Pasal 34 ayat (1) huruf a Undang-Undang Nomor 19 tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang. Dan Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana serta Peraturan Perundang-Undangan lainnya yang bersangkutan, dan Terdakwa dipidana penjara selama 2 tahun 6 bulan dan denda sejumlah Rp500.000.000,00 (lima ratus juta rupiah).[39]

Kerja sama internasional dalam menangani tindak pidana *ransomware* sangat penting karena kejahatan ini melintasi batas negara dan

[37] Yuswardi A, Suud, *"Mulai Disidang, Riswanda sang Pembuat Alat Peretas 16Shop Disebut Raup Rp1,7 Miliar",* Cyberhreat.id, https://m.cyberthreat.id/read/13834/Mulai-Disidang-Riswanda-sang-Pembuat-Alat-Peretas-16Shop-Disebut-Raup-Rp17-Miliar.

[38] Dilihta pada Putusan Nomor 85/Pid.Sus/2022/PN.Bjb

[39] *Ibid.*

melibatkan jejaring global. Salah satu bentuk kerjasama yang utama adalah saling berbagi informasi intelijen antar negara, seperti data tentang pelaku, cara serangan dilakukan, dan sistem digital yang digunakan, agar penanganannya bisa lebih cepat. Negara-negara lain juga saling memberikan bantuan hukum timbal balik (Mutual Legal Assistance Treaties/MLATs) misalnya, untuk mengekstradisi pelaku, menyita aset digital seperti uang kripto, dan mengumpulkan bukti yang berada di luar wilayah hukum masing-masing. Selaian itu, aparat penegak hukum dari berbagai negara sering bekerja sama dalam operasi bersama untuk membongkar jaringan kelompok *ransomware*. Operasi ini biasanya melibatkan lembaga seperti Europol, INTERPOL, FBI, dan Badan Siber lainnya yang saling membantu dalam menangkap pelaku, memastikan server pengendali, dan menghancurkan sistem digital milik para peretas. Contoh nyata dari kerja sama ini adalah operasi internasional terhadap kelompok *ransomware Revil* dan *LockBit,* yang berhasil melemahkan jaringan mereka dan menangkap anggotanya di beberapa negara sekaligus.

Selain itu, aparat penegak hukum dari berbagai negara sering bekerja sama dalam operasi gabungan untuk membongkar jaringan *ransomware*. Biasanya, operasi ini melibatkan lembaga seperti Europol, INTERPOL, FBI, dan badan keamanan siber lainnya. Mereka bekerjasama untuk menangkap pelaku, mematikan server kendali, dan menghancurkan sistem digital milik kelompok *ransomware Revil* dan *LockBit,* yang berhasil menghentikan aktivitas mereka dan menangkap beberapa anggotanya diberbagai negara.

Kerjasama internasional juga dilakukan melalui organisasi global seperti *INTERPOL, Europul EC3,* dan *UNODC,* yang memberikan dukungan teknis pelatihan, serta koordinasi antar negara. Selain itu, kerja sama antara pemerintah dan pihak swasta, seperti perusahaan keamanan siber dan penyedia layanan teknologi, memiliki peran penting dalam mendeteksi, menganalisis, dan menangani serangan. Kolaborasi ini semakin diperkuat dengan adanya inisiatif global seperti *No More Ransom Project*, yang menawarkan alat dekripsi gratis untuk membantu korban ransomware.[40] Dengan adanya kerja sama lintas sektor dan antar negara ini. Upaya penanggulangan ransomware bisa dilakukan secara menyeluruh dan efektif.

Salah satu contoh kerja sama internasional dalam menangani tindakan pidana *ransomware* yang sangat menonjol adalah Operasi *Cronos*, yang diterbitkan pada awal tahun 2024. Operasi ini merupakan Upaya baguman antara Lembaga penegak hukum dari berbagai negara termasuk *Europol*, *FBI (*Amerika Serikat), *National Crime Agency* (Inggris), serta otoritas dari Prancis, Jerman, Jepang, Australia, Kanada, dan negara lainnya.[41] Targer utama dari operasi ini adalah kelompok peretas *ransomware LockBit, ransomware LockBit,* yang selama bertahun-tahun dikenal sebgai salah satu jaringan *ransomware* yang paling canggih dan produktif di dunia, bertanggungjawab atas ribuan serangan terhadap institusi publik dan swasta di berbagai negara.[42]

Melalui koordinasi yang intensif dan berbasis pada pertukaran data intelijen, operasi ini berhasil mencapai sejumlah hasil penting. Beberapa anggota inti dari kelompok *LockBit* ditangkap di Eropa dan Asia, sementara infrastruktur teknis mereka seperti *server command and control*, domain, serta perangkat lunak enkripsi berhasil disita atau dimatikan. Selain itu, sejumlah besar aset keuangan dalam bentuk *cryptocurrency* juga berhasil dibekukan atau disita, yang diduga merupakan hasil pembayaran tebusan dari para korban. Tidak hanya itu, aparat juga berhasil memperoleh kunci dekripsi dari sistem *LockBit*, yang kemudian digunakan untuk membantu ribuan korban mengakses kembali data mereka tanpa perlu membayar uang tebusan.[43]

Kerja sama ini menjadi bagian penting dari pertanggungjawaban pidana dalam sistem global, karena meskipun pelaku tidak berada di dalam negeri, negara yang menjadi korban tetap bisa melakukan proses hukum dengan bantuan jaringan internasional. Tanpa Kerjasama internasional, pembuktian terhadap aktivitas siber lintas Negara ini akan sulit dilakukan oleh aparat penegak hukum nasional secara mandiri. Peran INTERPOL tidak hanya sebagai fasilitator Red Notice atau ekstradisi, tetapi untuk pembuktian sebagai jembatan penukaran data digital untuk pembuktian hukum di pengadilan nasional.

[40] Tentang Proyek*, "Penafian Situs Web",* https://www.nomoreransom.org/id/about-the-project.html.

[41] Kate Whiting, "*LockBit: How an international operation seized control of 'the world's most harmful cybercrime group",* https://www.weforum.org/stories/2024/02/lockbit-ransomware-operation-cronos-cybercrime/, 2025 July.

[42] *Ibid.*

[43] Europol. (2024, February 20). "*CRONOS: LockBit ransomware group disrupted in international operation*." Diakses dari: https://www.europol.europa.eu/newsroom/news/cronos-lockbit-ransomware-group-disrupted-in-international-operation.

Berbeda dengan kasus *ransomware* PDNS 2024 yang hingga saat ini belum memiliki putusan pengadilan. Mengingat *Brain Cipher* diduga beroprasi dari luar negeri, penggunaan mekanisme serupa yang melibatkan INTERPOL dapat dijadikan pembanding dengan kasus phishing global yang telah diputus oleh pengadilan dalam konteks hukum siber transnasional di Indonesia. Dengan membandingkan dua kasus tersebut, dapat dilihat bahwa bukti elektronik merupakan kunci dalam menuntaskankejahatan siber agar dapat dibawa keranah hukum positif melalui proses peradilan yang transparan dan akuntabel.

PENUTUP

A. Kesimpulan

1. Peraturan hukum terkait perlindungan terhadap data aset informasi milik negara merupakan hal yang sangat krusial karena berkaitan langsung dengan keamanan negara dan kedaulatannya. Di Indonesia, dasar hukum mengenai perlindungan aset informasi milik negara sebenarnya sudah tersedia, namun masih tersebar di berbagai regulasi yang berbeda-beda. Beberapa peraturan penting yang mengatur hal ini antara lain: Undang-Undang tentang Informasi dan Transaksi Elektronik (UU ITE), yang mengatur mengenai penggunaan serta keamanan sistem informasi elektronik, Undang-Undang Perlindungan Data Pribadi (UU PDP), yang mengatur perlindungan terhadap data pribadi, termasuk data milik aparatur pemerintah, Peraturan Presiden mengenai Sistem Pemerintahan Berbasis Elektronik (SPBE), yang mengatur pengelolaan sistem elektronik dalam layanan pemerintahan, Peraturan dan kebijakan dari Badan Siber dan Sandi Negara (BSSN), yang memiliki tugas utama menjaga keamanan siber, termasuk perlindungan terhadap data strategis negara. Walaupun berbagai aturan tersebut telah diberlakukan, pelaksanaannya di lapangan masih menghadapi berbagai tantangan. Di antaranya adalah belum meratanya kemampuan instansi pemerintah dalam membangun sistem keamanan data yang memadai, adanya tumpang tindih kewenangan antar lembaga, serta belum adanya satu payung hukum yang secara khusus dan menyeluruh mengatur perlindungan data milik negara.
2. Bagaimana pelaksanaan pertanggungjawaban pidana atas serangan ransomware dapat diterapkan melalui ketentuan dalam UU ITE, khususnya Pasal 30, 32, 46, dan Pasal 27B. Pelaku yang terbukti melakukan akses tanpa hak, perusakan data, dan pemerasan secara elektronik dapat dijatuhi pidana sesuai asas kesalahan dalam hukum pidana Indonesia. Tindak pidana *ransomware* memenuhi unsur-unsur seperti akses tanpa hak, perusakan data, serta pemerasan melalui sistem elektronik. Pertanggungjawaban pidana didasarkan pada asas kesalahan dan mensyaratkan adanya unsur perbuatan melawan hukum serta niat jahat (mens rea) dari pelaku. Upaya penanggulangan terhadap kejahatan *ransomware*, baik dari aspek preventif maupun represif, masih menghadapi sejumlah tantangan, antara lain minimnya kesadaran keamanan digital pada lembaga pemerintahan, keterbatasan sumber daya penegakan hukum siber, dan belum adanya regulasi komprehensif terkait pengamanan aset informasi negara.

B. Saran

1. Pemerintah perlu memperkuat regulasi dan pengawasan terhadap keamanan infrastruktur informasi negara, termasuk membuat kebijakan khusus mengenai proteksi terhadap aset informasi strategis agar terlindung dari ancaman serangan siber seperti *ransomware*. Untuk itu, langkah-langkah strategis yang perlu dilakukan pemerintah guna memperkuat perlindungan data negara seperti: merancang dan menerapkan regulasi yang lebih terpadu dan spesifik mengenai perlindungan informasi milik negara, meningkatkan sinergi dan koordinasi antara instansi terkait seperti Kominfo, BSSN, dan lembaga pemerintahan lainnya, mendorong peningkatan kapasitas sumber daya manusia dalam bidang keamanan data dan teknologi informasi, memastikan bahwa insrastruktur digital pemerintah menerapkan standar keamanan yang tinggi dan muktahir. Dengan penerapan langkah-langkah tersebut, perlindungan terhadap data dan informasi milik negara dapat dilakukan secara optimal, sehingga mampu meminimalkan resiko kebocoran, peretasan, dan penyalahgunaan oleh pihak yang tidak bertanggungjawab.
2. Memperkuat regulasi nasional yang secara spesifik mengatur mengenai tindak pidana serangan siber, terutama *ransomware* yang telah mengancam sistem informasi negara. Regulasi tersebut perlu mencangkup penegasan bentuk pertanggungjawaban

pidana bagi pelaku perorangan maupun korporasi, serta memperjelas sanski pidana yang dapat dikenakan. Selain itu, peninkatan kapasitas aparat penegak hukum dalam hal pemahaman dan keterampilan teknik terhadap kejahatan siber. Sangat penting agar proses penyidikan dan penuntutat dapat dilakukan secara efektif dan akurat. Serta meingkatkan kerja sama lintas batas dari kejahatan ransomware, kerja sama internasional dalam bentuk bantuan hukum timbal balik (mutual legal assistance), ekstradisi, serta kolaborasi dengan lembaga internasional seperti INTERPOL juga harus diperkuat. Dalam hal korporasi atau lembaga yang bertanggungjawab atas pengelolaan data aset informasi negara, menerapkan prinsip *strict liability* dan *corporate criminal responsibility* yang dapat digunakan sebgai dasar pertanggungjawaban pidana ats kelalaian atau pembiaran yang mengakibatkan terjadinya serangan siber. Pentingnya, perlu adanya mekanisme pemulihan dan kompensasi kepada pihak-pihak yang terkena dampak oleh serangan ini, baik dalam bentuk pengganti kerugian, pemulihan data, maupun mengembalikan kepercayaan publik terhadap keamanan informasi negara.

DAFTAR PUSTAKA

Buku

Abidin, A. Z. (1993). *Hukum Pidana I.* Jakarta: Sinar Grafika.

Alam, A. S., & Ilyas, A. (2018). *Kriminologi Suatu Pengantar.* Jakarta: Prenamedia Group.

Ali, M. (2011). *Dassar-Dasar Hukum Pidana.* Jakarta: Sinar Grafika.

Djafar, W., Fritz, B. R., & Sentiani, B. L. (2016). *Perlindungan Data Pribadi Di Indonesia.* Jakarta: Lembaga Studi Advokasi Masyarakat (ELSAM).

Ishaq. (2022). *Hukum Pidana.* Depok: Raja Grafindo Persada.

Mansur, D. M., & Gultom, E. (2009). *Cyber Law: Aspek Hukum Teknologi Informasi.* Bandung: PT Refika Aditama.

Maskun. (2013). *Kejahatan Cyber.* Jakarta: Kencana.

Moeljatno. (2002). *Asas-Asas Hukum Pidana.* Jakarta: Rineka Cipta.

Rohman, M. M., Purwoto, A., & Amalia, M. (2023). *Asas-Asas Hukum Pidana.* Paddang: Global Eksekutif Teknologi.

Rosadi, S. D. (2015). *CYBER LAW - Aspek Data Privasi Menurut Hukum Internasional.* Bandung: PT Refika Aditama.

Safaruddin, M. S. (2016). *Virus Komputer A-Z.* Sleman: Deepublish.

Sangalang, R. S., Rizki, & Farina , T. (2024). *Hukum Pidana Cyber*. Medan: PT. Media Penerbit Indonesia.

Simorangkir, J. (2004). *Aspek-Aspek Hukum Kejahatan Komputer.* Bandung: Alumni.

Soekanto, S. (2019). *Pengantar Penelitian Hukum.* Jakarta: Universitas Indonesia.

Wahyuni, S., & Khoirudin, R. (2020). *Pengantar Manajemen Aset.* Makassar: Nas Media Pustaka.

Peraturan Perundang-Undangan

Kitab Undang-Undang Hukum Pidana.

peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.

Peraturan Pemerintah Nomor 38 Tahun 2008 tentang Perubahan Atas Peraturan Pemerintah Nomor 6 Tahun 2006 Tentang Pengelolaan Barang Milik Negara Daerah.

Peraturan Presiden Nomor 174 Tahun 2024 tentang Kementerian Komunikasi dan Digital.

Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara.

peraturan Presiden Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital.

Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Jurnal/Web

discus.com: https://www.qiscus.com/id/blog/aset-digital/

Channel, I. (Director). (2024). *Pembangunan Pusat Data Nasional, Bagaimana Progresnya?* [Motion Picture]. Retrieved from https://youtu.be/-1KhSwkBKEg?si=mXn8hU7eyDdT tPf

CRONOS: LockBit ransomware group disrupted in international operation. (2024, februari 20). Retrieved from Europol: https://www.europol.europa.eu/newsroom/ne

ws/cronos-lockbit-ransomware-group-disrupted-in-international-operation.

Fadlian, A. (2020). Pertanggungjawaban Pidana Dalam Suatu Kerangka Teoritis. *Jurnal Hukum Positium, 5 no.2*, 13.

Freed, A. M. (n.d.). *Sejarah Singkat Evolusi Ransomware*. Retrieved from cybereason.com: ", https://www-cybereason-com.translate.goog/blog/a-brief-history-of-ransomware evolution?_x_tr_sl=en&_x_tr_tl=id&_x_tr_hl=id&_x_tr_pto=tc,

Hardiansyah, Z. (2024). *Kronologi Serangan Ransomware ke PDN dan Penanganannya yang Tak Kunjung Usai.* Kompas.com. Retrieved Februari 5, 2025, from https://tekno.kompas.com/read/2024/07/10/12350077/kronologi-serangan-ransomware-ke-pdn-dan-penanganannya-yang-tak-kunjung-usai

Hartono, B. (2024). Ransomware: Memahami Ancaman Keamanan Digital. *Bincang Sains dan Teknologi, 2 no.2*, 56.

Indonesia, C. (n.d.). *Kronologi Peretasan PDNS Diawali Pembobolan Windows Defender.* cnnindonesia.com. Retrieved from https://www.cnnindonesia.com/teknologi/20240626004744-192-1114133/kronologi-peretasan-pdns-diawali-pembobolan-windows-defender

Krismiyarsi. (2018). Sistem Pertanggungjawaban Pidana Individual. *Pustaga Magister*, 27.

Laksana, T. G., & Mulyani, S. (2024). Pengetahuan Dasar Identifikasi Dini Deteksi Serangan Kejahatan Siber Untuk Mencegah Pembobolan Data Perusaahaan. *Jurnal Ilmiah Multidisiplin, 3. no.01*, 109-22. Retrieved Mei 2025, from https://doi.org/10.56127/jukim.v3i01.1143

LANSKAP KEAMANAN SIBER TAHUN INDONESIA 2024. (2024). Retrieved from Diskominfo: https://diskominfo.tubankab.go.id/entry/lanskap-keamanan-siber-tahun-indonesia-2024,

Lasmadi, S. (2014). Pengaturan Alat Bukti Dalam Tindak Pidana Dunia Maya. *Jurnal Ilmu Hukum*, 1-23. doi:https://media.neliti.com/media/publications/43274-ID-pengaturan-alat- bukti-dalam-tindak-pidana-dunia-maya.pdf.

LockBit Takedown: Global Cooperation Hits Ransomware Syndicate. (2024, februari 21). Retrieved from FBI: https://www.fbi.gov/news/stories/lockbit-takedown-global-operation

Microsoft. (2025, Februari 5). *Apa itu Ransomware?* Retrieved from microsoft.com: https://www.microsoft.com/id-id/security/business/security-101/what-is-ransomware?utm_source=chatgpt.com,

Nasrudin, E. (2015). Efektifitas Sistem Informasi Manajemen dan Akuntansi Barang Milik Negara (SIMAK-BMN) Terhadap Pengelolaan Aset Negara. *Jurnal Akuntansi Universitas Jember, 13 no.2*, 49.

Penafian Situs Web. (2021). Retrieved from No More Ransom: https://www.nomoreransom.org/id/about-the-project.html

Pusinfokomnas. (2015). Kajian Strategi Pengamanan Infrastruktur Sumber Daya Informasi Kritis. *Laporan Peneliti*, 2-3. Retrieved from medianeliti.com: https://media.neliti.com/media/publications/41201-ID-kajian-strategi-pengamanan-infrastruktur-sumber-daya-informasi-kritis-study-of-c.pdf.

Putra, C. R., Sugiartha, I. N., & Widyantara, I. M. (2024). Analisis Yuridis Atas Keabsahan Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Pembobolan Sistem Data keamanan Komputer (Cracking). *Jurnal Preferensi Hukum, 5 no.1*, 4.

S, D. H., L, S., J, G., & M, A. A. (2023). Perlindungan Data Pribadi di Era Digital: Mengapa Kita Perlu Peduli? *Sang Sewagati Jurnal*, 66-90.

Sejarah Ransomware: Lengkap Dari Awal Sampai Sekarang. (2025, Februari 5). Retrieved from ASDF.ID: https://www.asdf.id/sejarah-ransomware/

Suud, Y. A. (2022, maret 19). *Mulai Disidang, Riswanda sang Pembuat Alat Peretas 16Shop Disebut Raup Rp1,7 Miliar*. Retrieved from Cyberhreat.id: https://m.cyberthreat.id/read/13834/Mulai-Disidang-Riswanda-sang-Pembuat-Alat-Peretas-16Shop-Disebut-Raup-Rp17-Miliar

U, M., & R, M. (2020). Perlindungan Data Pribadi Sebagai bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi. *Indonesia Jurnal Of Law and Policy Studies, 1 no.1*, 42-54.

Whiting, K. (2024, 02 21). *LockBit: How an international operation seized control of 'the world's most harmful cybercrime group'*. Retrieved from World Ecomic Forum: https://www.weforum.org/stories/2024/02/lockbit-ransomware-operation-cronos-cybercrime/

Wijaya, F. N. (2019). Bitcoin Sebagai Digital Aset Pada Transaksi Elektronik di Indonesia (Studi pada PT. Indodax Nasional Indonesia). *Jurnal Hukum Bisnis Bonum Commune, 2 no.2*, 128.

Z, H., M, A. A., M, T., & A, R. M. (2024). PENANGGULANGAN TINDAK PIDANA PENIPUAN MELALUI TRANSFER MOBILE MBANKING. *Jurnal Harmoniora, Sosial dan Bisnis, 2 no.5*, 475-482.