BAB 1
PENDAHULUAN

1.1. Latar Belakang

Perkembangan ilmu pengetahuan dan teknologi telah membawa perubahan fundamental dalam berbagai aspek kehidupan manusia, termasuk cara berinteraksi, bertransaksi, dan menjalankan bisnis.[1] Sejak ditemukannya *telegraf* pada tahun 1836, pola komunikasi masyarakat berangsur-angsur bergeser dari surat-menyurat dan tatap muka langsung menuju komunikasi yang membutuhkan perantara teknologi.[2] Revolusi ini terus berlanjut hingga komputer dan jaringan internet ditemukan, menandai dimulainya era baru di mana dunia seolah menciut, dan jarak serta ruang bukan lagi menjadi kendala utama dalam hubungan antar manusia.[3] Akibat dari pesatnya kemajuan ini, Teknologi Informasi dan Komunikasi (TIK) menjadi tulang punggung bagi hampir seluruh sektor, melahirkan konsep konvergensi yang memadukan telekomunikasi, media, dan informatika.[4]

Masifnya penggunaan teknologi digital, terutama komputer dan internet, telah menciptakan sebuah ruang virtual atau dunia siber (*cyberspace*) yang melampaui batas-batas fisik.[5] Dunia siber ini menjadi media penting yang

---

[1] Elza Noveliani, Dapid Aryando, and Sani Safitri, "Perkembangan Ilmu Pengetahuan Dan Teknologi : Menyongsong Era Baru Dalam Prespektif Ilmu Sosial," *PESHUM : Jurnal Pendidikan, Sosial Dan Humaniora* 4, *No.* 4 (2025). Hlm. 5984.

[2]Muhammad Irfan Hilmy, *Hukum Mayantara : Konstitusi Mayantara Hingga Pembentukan Kelembagaan*, Cetakan Pertama (Surabaya: Pustaka Aksara, 2021). Hlm 10.

[3] Krista Yitawati, *Hukum Dan Teknologi*, Cetakan I (Solo: Pustaka Iltizam, 2017). Hlm. 4.

[4] Sugeng, *Hukum Telematika Indonesia*, Edisi Pertama (Jakarta: Kencana Predana Media Group, 2020). Hlm. 21.

[5] Muhammad Husni Abdulah Pakarti et al., *Hukum Siber: Menyikapi Tantangan Hukum Di Era Digital* (PT. Nawala Gama Education, 2025). Hlm. 14.

memfasilitasi publik untuk melakukan berbagai interaksi sosial, ekonomi, dan politik, mengubah gaya hidup, komunikasi, serta pergeseran konteks ruang dan waktu bagi penggunanya. Keberadaan ruang siber yang terhubung secara global ini melalui miliaran komputer dan perangkat lain mendukung berbagai aktivitas mulai dari *e-commerce*, *e-government*, hingga *e-banking*.[6]

Namun, di balik kemajuan dan manfaat yang tak terbantahkan, teknologi juga menciptakan konsekuensi negatif, menjadikannya ibarat "pedang bermata dua".[7] Sejak komputer terhubung dalam jaringan, ia mulai menghadapi ancaman dari perangkat lunak berbahaya (*malware*) atau virus yang dirancang untuk merusak sistem, mencuri data, atau mengganggu fungsionalitas.[8] Kemunculan ancaman kejahatan siber (*Cybercrime*) secara signifikan pertama kali terjadi pada tahun 1988 ketika seorang mahasiswa berhasil menciptakan *worm* yang mematikan sekitar 10% dari total komputer yang terhubung ke internet saat itu.[9] Jenis-jenis kejahatan pun ikut berkembang pesat, mulai dari *hacking*, *carding*, hingga penyebaran virus, yang seluruhnya memanfaatkan kemudahan teknologi digital.

Dalam ekosistem kejahatan siber, aktor utama yang sering kali menjadi sorotan adalah peretas atau yang dikenal dengan istilah *hacker*. *Hacker* atau peretas didefinisikan sebagai sebagai individu atau kelompok dengan kompetensi tinggi dalam pemrograman, jaringan komputer, serta pemahaman mendalam mengenai

---

[6] Agus Wibowo, *Teknologi Informasi* (Semarang: Yayasan Prima Agus Teknik Bekerja sama dengan Universitas & Teknologi Komputer (Universitas STEKOM), 2025). Hlm. 4.

[7] Sugeng, *Hukum Telematika Indonesia*. Op. Cit. Hlm. 98.

[8] Tri Ginanjar Laksana and Sri Mulyani, "Pengetahuan Dasar Identifikasi Dini Deteksi Serangan Kejahatan Siber Untuk Mencegah Pembobolan Data Perusahaan," *Jurnal Ilmiah Multidisiplin* 3, *No.* 1 (2024). Hlm. 111.

[9] Hilmy, *Hukum Mayantara : Konstitusi Mayantara Hingga Pembentukan Kelembagaan*. Op. Cit. Hlm. 47.

perangkat keras.[10] Dalam ranah siber, keahlian ini memungkinkan mereka untuk mengeksplorasi hingga memanipulasi sistem keamanan pada berbagai perangkat, mulai dari komputer pribadi, ponsel, hingga infrastruktur jaringan seperti *router*. Penting untuk dipahami bahwa terminologi *hacker* tidak serta-merta berkonotasi negatif, istilah ini juga merujuk pada pengembang perangkat lunak (s*oftware developer*) atau ahli keamanan yang memiliki antusiasme tinggi terhadap sistem pertahanan digital. Perbuatan peretasan baru dikategorikan sebagai tindakan kriminal atau kejahatan siber apabila dilakukan dengan niat jahat yang menimbulkan kerugian bagi pihak lain.[11]

Salah satu bentuk kejahatan siber yang berevolusi paling cepat dan menjadi ancaman global yang sangat kompleks adalah *ransomware*. *Ransomware* pertama kali muncul pada akhir 1989 melalui program bernama "*AIDS Trojan*," yang dibuat oleh Joseph Popp. Serangan ini mengenkripsi data korban dan meminta tebusan untuk mengembalikannya. Dalam beberapa dekade terakhir, *ransomware* telah berevolusi menjadi ancaman global yang tidak hanya merugikan individu tetapi juga korporasi dan negara.[12]

Ransomware adalah jenis perangkat lunak berbahaya yang secara khusus diciptakan untuk memblokir akses pengguna ke sistem komputer atau data mereka sampai sejumlah tebusan dibayarkan.[13] Serangan ini umumnya diawali ketika

---

[10] Indah Sari, "Mengenal Hacking Sebagai Salah Satu Kejahatan Di Dunia Maya," *Jurnal Sistem Informasi Universitas Suryadarma* 10, *No.* 2 (2015). Hlm 173.

[11] Adelina Damayanti Anggarini et al., "Kajian Hukum Dan Regulasi Terkait Serangan Hacking Pada Platform Digital Di Indonesia Study Of Laws And Regulations Related To Hacking," *Multidisciplinary Indonesian Center Journal* 1, *No.* 2 (2024). Hlm 1047.

[12] Aliya Putri Novita et al., "Cyber Security Threats; Analisis Dan Mitigasi Resiko *Ransomware* Di Indonesia," Jurnal Ilmiah Sistem Informasi 3, *No.* 1 (2023). Hlm. 163.

[13] Budi Hartono, "*Ransomware*: Memahami Ancaman Keamanan Digital," *Bincang Sains Dan Teknologi* 2, *No.* 02 (2023). Hlm. 58.

pengguna tanpa disadari mengklik lampiran atau tautan yang bersifat berbahaya, yang pada akhirnya menginstal program jahat tersebut ke dalam perangkat korban. Setelah *Ransomware* terunduh dan diaktifkan, ia akan mengenkripsi semua berkas dan data, menjadikannya tidak dapat diakses sama sekali.

Dampak dari serangan *Ransomware* sangat luas dan kompleks, tidak hanya menyebabkan gangguan operasional tetapi juga menimbulkan implikasi serius di berbagai sektor penting, khususnya terhadap sektor-sektor kritis seperti layanan kesehatan, keuangan, dan pemerintahan.[14] Para pelaku akan menuntut pembayaran tebusan sering kali dalam bentuk mata uang kripto, seperti *Bitcoin* sebagai imbalan untuk memberikan kunci dekripsi.[15] Hal ini menempatkan organisasi pada posisi sulit, yaitu memilih antara membayar tebusan atau menghabiskan waktu dan biaya yang signifikan untuk pemulihan sistem dari cadangan data.

Kasus *ransomware* di Dunia bahkan di Indonesia menunjukkan tingkat kerentanan yang cukup tinggi. *Ransomware* telah terbukti sebagai ancaman utama yang melampaui *cybercrime* lainnya seperti phishing atau carding. Pada 2017, *WannaCry* melumpuhkan ribuan sistem di seluruh dunia dengan memanfaatkan kerentanan *EternalBlue* di *Windows*, sementara *NotPetya* , yang muncul di tahun yang sama, lebih fokus pada sabotase daripada pemerasan, menyebabkan kerugian besar bagi perusahaan seperti *Maersk*.[16]

---

[14] *Ibid*. Hlm. 3.

[15] Peizhi Yan and Tala Talaei Khoei, "Franklin Open Securing the Internet of Things : A Comprehensive Review of *Ransomware* Attacks , Detection , Countermeasures , and Future Prospects," *Franklin Open* 11, (2025). Hlm 3,.

[16] Amos Loh et al., "A Three-Level *Ransomware* Detection and Prevention Mechanism" *EAI Endorsed Transactions on Energy Web* 7, *No.* 26 (2020). Hlm. 2.

Ransomware lainnya seperti *GandCrab* (2018-2019), *Ryuk* (2018-sekarang), dan *REvil/Sodinokibi* (2019-sekarang) juga menimbulkan kerugian besar secara global, dengan metode penyebaran yang canggih dan target strategis. *REvil*, misalnya, mengadopsi teknik *double extortion*, mencuri data sensitif selain mengenkripsi sistem korban, membuat tekanan pada perusahaan untuk membayar tebusan.[17] Evolusi *ransomware* tidak berhenti di situ: muncul model *Ransomware-as-a-Service (RaaS)* yang membuat individu tanpa kemampuan teknis tinggi sekalipun dapat menyewa perangkat *ransomware* dari kelompok kriminal terorganisir.[18] Hal ini menunjukkan pergeseran dari kejahatan individu menjadi industri kriminal global yang memiliki struktur, pembagian keuntungan, dan bahkan sistem afiliasi layaknya perusahaan.

Kerugian akibat *ransomware* bukan hanya berupa pembayaran tebusan, tetapi jauh lebih kompleks. Perusahaan yang menjadi korban harus menanggung biaya pemulihan sistem, kehilangan produktivitas, kerusakan reputasi, dan hilangnya kepercayaan publik.[19] Beberapa korban bahkan memilih membayar tebusan demi menghindari kerugian lebih besar, padahal langkah tersebut justru memperkuat ekosistem kriminal dengan menyediakan aliran dana segar bagi pelaku. *Ransomware* termasuk dalam *organized transnational crime*. Pelaku sering kali beroperasi lintas negara, menggunakan *dark web* untuk berkomunikasi, dan

[17] Hartono, "*Ransomware*: Memahami Ancaman Keamanan Digital," 2023. Op. Cit. Hlm 58.
[18] Aldo Eko Syaputra and et al, *Keamanan Jaringan Komputer*, *Keamanan Jaringan Komputer* (Banten: Sada Kurnia Pustaka, 2025). Hlm. 237.
[19] Ferry Irawan Febriansyah, *Cybercrime: Kejahatan Di Balik Layar Digital* (Najaha, 2025). Hlm. 64.

memanfaatkan *cryptocurrency* seperti *Bitcoin* atau *Monero* untuk mengaburkan jejak keuangan.[20]

Dalam perspektif politik, *ransomware* juga dapat digunakan sebagai instrumen geopolitik. Serangan *NotPetya* misalnya, banyak disebut sebagai serangan dengan motif politik yang menargetkan Ukraina namun berdampak global. Dengan demikian, *ransomware* tidak hanya berdimensi ekonomi, tetapi juga berkaitan dengan keamanan nasional dan stabilitas internasional.[21]

Indonesia sebagai negara dengan pertumbuhan digital paling cepat di Asia Tenggara juga tidak lepas dari ancaman *ransomware*. Pada Mei 2017**,** ketika Rumah Sakit Dharmais dan Rumah Sakit Harapan Kita di Jakarta menjadi korban serangan global *WannaCry*. *Malware* tersebut mengenkripsi lebih dari 60 komputer di jaringan rumah sakit, mengunci akses terhadap sistem antrean, data pasien, dan catatan medis.[22] Akibatnya, operasional layanan kesehatan terganggu secara total dan harus beralih ke sistem manual. Pelaku menuntut tebusan dalam bentuk *Bitcoin*, namun pihak rumah sakit menolak membayar. Kasus ini menandai awal kesadaran nasional mengenai urgensi keamanan data dan sistem elektronik, khususnya di sektor pelayanan publik yang bersentuhan langsung dengan masyarakat.

Selanjutnya pada Desember 2021 hingga awal 2022, ketika kelompok *Conti Ransomware*, yang dikenal berafiliasi dengan jaringan kriminal dunia maya *Wizard*

---

[20] Dian Alan Setiawan, "Strategi Penanggulangan Kejahatan Ekonomi Berbasis Teknologi: Studi Komparatif Antara Indonesia, Amerika, Dan Eropa," *Masalah-Masalah Hukum* 53, *No.* 1 (2024). Hlm 87.

[21] Dina Anjelina, "Fenomena Serangan Siber Rusia Terhadap Ukraina: Sebagai Pembelajaran Bagi Indonesia Dalam Pengembangan Pertahanan Siber The Phenomenon Of Russian Cyber Attacks On Ukraine: Lessons For Indonesia In Cyber Defense Development," *Jurnal Pertahanan Dan Bela Negara* 13, *No.* 3 (2023). Hlm 231.

[22] Muhadi Sugiono, "Geopolitik Asia Dan Tantangan Diplomasi Struktural Indonesia," *JURNAL MAJELIS,* 2020. Hlm. 119.

Spider asal Rusia, menyerang Bank Indonesia (BI)**.** Peretas berhasil mencuri sekitar 13,88 GB data internal dan mengenkripsi sebagian sistem komputer BI. Meskipun data operasional utama diklaim tidak terdampak, insiden ini memperlihatkan bahwa lembaga keuangan tertinggi negara pun rentan terhadap serangan siber berskala internasional. Bank Indonesia kemudian memperkuat sistem keamanan siber dengan peningkatan protokol IT dan pelatihan ketahanan digital. Kasus ini menjadi preseden penting bahwa *ransomware* telah memasuki ranah keamanan ekonomi nasional**.**[23]

Satu tahun kemudian pada Mei 2023**,** Bank Syariah Indonesia (BSI) diserang oleh kelompok *ransomware LockBit*, yang mengklaim telah mencuri sekitar 1,5 *terabyte* data. dan menuntut tebusan lebih dari Rp200 miliar.[24] Serangan ini menyebabkan gangguan layanan digital banking selama beberapa hari, menimbulkan keresahan masyarakat, dan menggerus kepercayaan publik terhadap sistem keamanan perbankan nasional.

Puncak eskalasi ancaman *ransomware* terjadi pada Juni 2024**,** ketika varian *ransomware Brain Cipher* menyerang Pusat Data Nasional (PDN) milik Kementerian Komunikasi dan Informatika (Kominfo).[25] Serangan ini mengunci data milik ribuan instansi pemerintah, termasuk sistem imigrasi, perizinan, pendidikan, dan administrasi kependudukan**.** Dampaknya luar biasa, antrean

---

[23] R17 Kelola, *"Kasus Ransomware Di Indonesia: Ancaman, Contoh Kasus, Dan Cara Melindungi Bisnis Anda"* (R17, 2024), https://r17.co.id/id/blog/kasus-*ransomware*-di-indonesia-ancaman-contoh-kasus-dan-cara-melindungi-bisnis-anda. Diakses 30 Oktober 2025.

[24] B B C News Indonesia, *"BSI Diduga Kena Serangan Siber, Pengamat Sebut Sistem Pertahanan Bank 'Tidak Kuat,'"* 2023, https://www.bbc.com/indonesia/articles/cn01gdr7eero. Diakses 30 Oktober 2025.

[25] Syarifa Tommy and Muhammad Irwan Padli Nasution, "Evaluasi Manajemen Risiko Keamanan Siber Pada Infrastruktur Digital Pemerintah: Studi Kasus Pusat Data Nasional (PDN)," *Jurnal Manajemen Ekonomi Dan Bisnis* 4, *No.* 1 (2025). Hlm 20.

panjang terjadi di bandara karena sistem imigrasi *offline*, layanan publik di berbagai daerah terhenti, dan sebagian data strategis pemerintahan tidak dapat diakses. Pelaku menuntut tebusan sekitar USD 8 juta (setara Rp131 miliar) sebagai syarat pemulihan sistem.[26] Kasus PDN merupakan insiden siber terbesar dalam sejarah Indonesia dan menandai pergeseran *ransomware* dari ancaman kriminal individual menjadi ancaman terhadap kedaulatan digital negara**.**

Untuk memberikan gambaran yang lebih komprehensif mengenai eskalasi ancaman tersebut, berikut disajikan rekapitulasi kasus *ransomware* yang menargetkan sektor vital di Indonesia dalam beberapa tahun terakhir:

Tabel 1.1 Kasus *Ransomware* di Indonesia

No.	Tahun	Jenis *Ransomware*	Target Serangan	Dampak Serangan
1	2017	*Ransomware WannaCry*	Rumah Sakit Dharmais, Jakarta.	Sekitar 60 komputer di jaringan Rumah Sakit Dharmais terinfeksi *ransomware WannaCry* pada 13 Mei 2017. Sistem antrean dan data pasien terenkripsi, rumah sakit harus beroperasi manual, dan pelaku meminta tebusan dalam *Bitcoin* yang tidak dibayar.[27]
2	2017	*Ransomware WannaCry*	Rumah Sakit Harapan Kita, Jakarta Barat.	Bersamaan dengan serangan Dharmais, *WannaCry* juga menyerang sistem IT Rumah Sakit Harapan Kita, melumpuhkan layanan berbasis komputer. Pelaku menuntut tebusan dengan

[26] *Ibid*. Hlm. 11.

[27] Muhadi Sugiono, "Geopolitik Asia Dan Tantangan Diplomasi Struktural Indonesia," *JURNAL MAJELIS,* 2020. Hlm. 119

				ancaman penghapusan data.[28]
3	2022	*Ransomware Conti*	Bank Indonesia (BI).	*Ransomware* Conti menyerang jaringan internal BI, mencuri ±13,88 GB data, dan mengenkripsi server.[29]
4	2023	*Ransomware LockBit*	Bank Syariah Indonesia (BSI).	Pelaku *ransomware* mencuri ±1,5 TB data nasabah dan pegawai, mengunci sistem, serta mengancam menyebarkan data jika tebusan tidak dibayar.[30]
5	2024	*Ransomware Brain Cipher*	Pusat Data Nasional (PDN), Kementerian Komunikasi dan Informatika (Kominfo).	*Ransomware* mengenkripsi data ribuan instansi pemerintah, termasuk imigrasi dan pendidikan. Pelaku menuntut tebusan USD 8 juta.[31]

Sumber: Data hasil olahan peneliti tahun 2025.

Di level internasional, *Budapest Convention on Cybercrime* (2001) merupakan instrumen hukum *multilateral* pertama yang mengatur tindak pidana siber. Konvensi ini memuat kriminalisasi terhadap akses ilegal, gangguan sistem, serta penyalahgunaan perangkat lunak berbahaya, yang semuanya relevan untuk

[28] *Ibid*.

[29] R17 Kelola, *"Kasus Ransomware Di Indonesia: Ancaman, Contoh Kasus, Dan Cara Melindungi Bisnis Anda"* (R17, 2024), https://r17.co.id/id/blog/kasus-*ransomware*-di-indonesia-ancaman-contoh-kasus-dan-cara-melindungi-bisnis-anda. Diakses 30 Oktober 2025..

[30] B B C News Indonesia, *"BSI Diduga Kena Serangan Siber, Pengamat Sebut Sistem Pertahanan Bank 'Tidak Kuat,'"* 2023, https://www.bbc.com/indonesia/articles/cn01gdr7eero. Diakses 30 Oktober 2025.

[31] Syarifa Tommy and Muhammad Irwan Padli Nasution, "Evaluasi Manajemen Risiko Keamanan Siber Pada Infrastruktur Digital Pemerintah: Studi Kasus Pusat Data Nasional (PDN)," *Jurnal Manajemen Ekonomi Dan Bisnis* 4, *No.* 1 (2025). Hlm 20.

menjerat pelaku *ransomware*.[32] Namun, karena konvensi ini lahir sebelum ledakan *ransomware modern*, Dewan Eropa mengeluarkan *T-CY Guidance Note 12* (2022) untuk memperbarui interpretasi.[33]

Guidance ini menegaskan bahwa *ransomware*, termasuk modus *double extortion* dan *RaaS*, termasuk ke dalam lingkup tindak pidana yang diatur *Budapest Convention*. *Guidance Note 12* juga menekankan mekanisme penting seperti penyitaan aset digital dan kerja sama internasional dalam investigasi forensik. Indonesia hingga kini belum meratifikasi *Budapest Convention*, sehingga akses pada kerja sama hukum internasional melalui instrumen ini masih terbatas. Hal ini menimbulkan gap signifikan dalam kemampuan Indonesia menangani kasus *ransomware* lintas batas.

Berbeda dengan negara-negara maju menunjukkan bagaimana hukum pidana dapat merespons ancaman *ransomware* dengan tegas. Amerika Serikat melalui *LockBit Indictment* (2023) menjerat pelaku lintas negara dengan menggunakan *Computer Fraud and Abuse Act (CFAA), Wire Fraud Statute*, serta aturan penyitaan aset (*asset forfeiture*). Hukuman maksimalnya mencapai puluhan tahun penjara, ditambah penyitaan semua hasil kejahatan termasuk *cryptocurrency*, sehingga menciptakan efek jera yang kuat.[34] Di Jerman, *Strafgesetzbuch (StGB)* Pasal 303b secara spesifik mengatur sabotase komputer, sedangkan Pasal 202c

---

[32] Wahyu Rifqi Febrian, "Peran Hukum Internasional Dalam Menangani Kasus *Cybercrime* 1," *JURNAL SAHID DA'WATII* 03, no 02. (2024). Hlm.3.

[33] *Cybercrime* Convention Committee, *"T-CY Guidance Note # 12 Aspects of Ransomware Covered by the Budapest Convention,"* November (2022).

[34] Office of Public Affairs, *"Two Foreign Nationals Plead Guilty to Participating in LockBit Ransomware Group,"* 2024, https://www.justice.gov/archives/opa/pr/two-foreign-nationals-plead-guilty-participating-lockbit-*ransomware*-group. Diakses 31 Oktober 2025.

melarang pembuatan dan distribusi perangkat berbahaya. Regulasi ini secara jelas menargetkan elemen-elemen khas *ransomware*, memberikan kepastian hukum bagi penegak hukum, dan meminimalkan multitafsir.[35]

Sejumlah negara bagian di Amerika Serikat telah memiliki regulasi yang secara tegas mengatur tindak pidana *ransomware*, baik dalam aspek pemidanaan, pelaporan insiden, maupun mekanisme pencegahan. Banyak negara bagian, seperti California, Connecticut, Maryland, Michigan, dan Texas, secara tegas mengkriminalisasi tindakan memasukkan atau memiliki *ransomware*.[36] Selain itu, negara bagian seperti Florida, Indiana, dan Louisiana memberlakukan kewajiban pelaporan yang ketat bagi instansi pemerintah atau penyedia layanan siber saat terjadi insiden atau pembayaran tebusan. Aspek pencegahan juga diatur, misalnya larangan bagi lembaga negara untuk membayar tebusan di North Carolina, serta izin bagi pemerintah untuk membeli asuransi siber di Texas, yang semuanya menunjukkan keseriusan dalam memandang *ransomware* sebagai ancaman nyata terhadap integritas digital.[37]

Sementara itu, di Indonesia *Ransomware* sering dikaitkan dengan unsur-unsur tindak pidana sebagaimana diatur dalam Pasal 482 KUHP tentang Pemerasan dan Pengancaman.

Pasal 482 KUHP menyatakan bahwa:[38]

---

[35] ICLG, *"Cybersecurity Laws and Regulations Germany 2025"* (ICLG (The ICLG to: Cybersecurity Laws and Regulations), 2024, https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/germany. Diakses 31 Oktober 2025.

[36] National Conference of State Legislatures, *"Computer Crime Statutes"* (National Conference of State Legislatures (NCSL), 2022, https://www.ncsl.org/technology-and-communication/computer-crime-statutes. Diakses 31 Oktober 2025.

[37] *Ibid*.

[38] Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana. Pasal 482.

(1) Dipidana karena pemerasan dengan pidana penjara paling lama 9 (sembilan) tahun, Setiap Orang yang dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, memaksa orang dengan Kekerasan atau 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.
(2) Ketentuan sebagaimana dimaksud dalam Pasal 479 ayat (21 sampai dengan ayat (4) berlaku juga bagi pemerasan sebagaimana dimaksud pada ayat (1).

Pasal 483 KUHP:[39]

(1) Dipidana karena pengancaman dengan pidana penjara paling lama 4 (empat) tahun atau pidana denda paling banyak kategori IV, Setiap Orang yang dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan ancarnan pencemaran atau pencemaran tertulis atau dengan ancaman akan membuka rahasia, memaksa orang supaya: a. memberikan suatu Barang yang sebag'an atau seluruhnya milik orang tersebut atau milik orang lain; atau b. memberi utang, membuat pengakuan utang, atau menghapuskan piutang.
(2) Tindak Pidana sebagaimana dimaksud pada ayat (1) hanya dapat dituntut atas pengaduan Korban Tindak Pidana

Dalam serangan *ransomware*, pelaku memaksa korban untuk menyerahkan uang. Unsur "memaksa dengan ancaman kekerasan" dalam pasal 482 KUHP ini masih dimaknai sebagai kekerasan fisik. Sama halnya dengan pasal 483 KUHP, pada pemerasan, paksaan lebih bersifat fisik dan lahiriah, sedangkan pada Tindak Pidana pengancaman sarana paksaannya lebih bersifat nonfisik atau batiniah yaitu dengan menggunakan ancaman penistaan, baik lisan maupun tulisan atau dengan ancaman akan membuka rahasia.

Dalam kasus *ransomware*, pelaku menggunakan tipu muslihat dengan menyamarkan *malware* sebagai program yang sah atau menyebarkannya melalui

[39] *Ibid*. Pasal 483

metode penipuan seperti *phishing*. Pelaku kemudian mengunci akses data korban dengan tujuan memaksa korban menyerahkan uang tebusan sebagai gantinya. Sehingga *Ransomware* juga memenuhi unsur tindak pidana penipuan sebagaimana diatur dalam Pasal 492 KUHP yang menyatakan bahwa:[40]

> "Setiap Orang yang dengan maksud menguntungkan diri sendiri atau orang lain secara melawan hukum dengan memakai nama palsu atau kedudukan palsu, menggunakan tipu muslihat atau rangkaian kata bohong, menggerakkan orang supaya menyerahkan suatu Barang, memberi utang, membuat pengakuan utang, atau menghapus piutang, dipidana karena penipuan, dengan pidana penjara paling lama 4 (empat) tahun atau pidana denda paling banyak kategori V."

Keterbatasan daya jangkau Kitab Undang-Undang Hukum Pidana (KUHP) terhadap tindak pidana yang bertransformasi ke dalam ranah digital mengharuskan adanya analisis melalui peraturan perundang-undangan yang bersifat khusus seperti Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi untuk dapat menjangkau tindak pidana *Ransomware* ini.

Pasal 27B UU ITE menyatakan:[41]

(1) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan 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.

(2) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan Informasi Elektronik dan/atau Dokumen Elektronik, dengan maksud untuk menguntungkan diri sendiri atau orang lain

[40] *Ibid*. Pasal 492.

[41] Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pasal 27B.

> secara melawan hukum, dengan ancaman pencemaran atau dengan ancaman akan membuka rahasia, memaksa orang supaya:
> 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.

Unsur "mendistribusikan/mentransmisikan informasi" tidak menggambarkan perbuatan mengunci atau mengenkripsi data, yang menjadi esensi *ransomware*, lalu ketika merujuk pada pasal 45 ayat 9 yang menyatakan bahwasanya ketentuan dalam pasal 27B ayat (1) bila dilakukan dalam ruang lingkup keluarga maka akan menjadi delik aduan, dan pasal 45 ayat 11 yang menyatakan bahwasanya ketentuan dalam pasal 27B ayat (2) hanya dapat dituntut atas pengaduan korban tindak pidana (delik aduan).

Lebih lanjut ketika merujuk pada penjelasan pasal 27B ayat (1) yang memberikan batasan terhadap frasa "ancaman kekerasan" yang diartikan sebagai Informasi Elektronik dan/atau Dokumen Elektronik yang berisi muatan yang ditujukan untuk menimbulkan rasa takut, cemas, atau khawatir akan dilakukannya kekerasan. Kemudian pada penjelasan pasal 27B ayat (2) frasa "ancaman pencemaran" diartikan sebagai ancaman menyerang kehormatan atau nama baik orang lain dengan cara menuduhkan suatu hal dengan maksud supaya hal tersebut diketahui umum.

Sedangkan Pasal 32 ayat (1) UU ITE menyatakan:[42]

> "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik."

[42] *Ibid*. Pasal 32.

Secara yuridis, Pasal 32 ayat (1) UU ITE mampu menjerat tindakan teknis *ransomware* melalui pemenuhan unsur "mengubah", "menyembunyikan", dan "merusak", di mana proses enkripsi secara harfiah mengubah data asli menjadi *ciphertext* yang tidak dapat diakses sehingga merusak fungsionalitas informasi tersebut bagi pemiliknya. Kendati demikian, pasal ini mengandung kekaburan konsep karena hanya memandang *ransomware* sebagai tindak vandalisme digital atau perusakan data semata tanpa mampu mengakomodasi motif ekonomi (*financial motive*) yang menjadi inti dari tindak pidana pemerasan. Keterbatasan jangkauan norma ini mengakibatkan konstruksi hukum yang terbangun menjadi tidak utuh, di mana pelaku yang seharusnya diklasifikasikan sebagai penyandera data untuk tebusan justru hanya dijerat sebagai perusak data biasa, sehingga gagal merepresentasikan hakikat kejahatan *ransomware* secara komprehensif

Selain itu, pengaturan mengenai perlindungan data pribadi juga telah ditegaskan melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Pasal 65 UU PDP memuat ketentuan larangan terhadap setiap tindakan memperoleh, mengumpulkan, dan mengungkapkan data pribadi secara melawan hukum. Pasal 65 UU PDP menyatakan bahwa:[43]

> (1) Setiap Orang dilarang secara 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,
> (2) Setiap Orang dilarang secara melawan hukum mengungkapkan Data Pribadi yang bukan miliknya.

[43] Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Pasal 65.

Namun, ketentuan dalam pasal ini pada dasarnya hanya mencakup aspek perolehan dan pengungkapan data pribadi tanpa izin.

Meski sudah ada hukum positif di Indonesia yang dapat digunakan untuk menjerat tindak pidana *ransomware*, namun dari aturan yang ada tersebut hanya mencakup sebagian unsur tindak pidana *ransomware,* belum secara eksplisit dan komprehensif mencakup semua unsur dari tindak pidana *ransomware,* sehingga hal tersebut menyebabkan adanya ketidakpastian hukum dan menghambat aparat penegak hukum dalam menindaklanjuti tindak pidana *ransomware* ini.

Oleh karena itu, terdapat urgensi untuk melakukan tinjauan yuridis mendalam mengingat adanya indikasi ketidakjelasan konsep dan ambiguitas terminologis mengenai tindak pidana siber *ransomware* dalam hukum positif Indonesia. Konstruksi norma yang saat ini tersebar secara parsial ke dalam berbagai regulasi diduga memicu terjadinya kekaburan norma (*vagueness of norms*), yang pada akhirnya berpotensi mendistorsi penerapan pertanggungjawaban pidana serta menghambat terciptanya kepastian hukum terhadap karakteristik unik kejahatan siber tersebut. Berdasarkan hal tersebut, penelitian ini menjadi penting untuk mengevaluasi sejauh mana batasan hukum yang ada mampu mengakomodasi evolusi modus operandi *ransomware* demi menjamin ketahanan siber nasional.

1.2. Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan di atas maka muncul isu permasalahan yang dirumuskan sehingga dapat menjadi rujukan yang runut dan sistematis dalam pembahasan penelitian ini. Adapun pokok masalah yang

diformulasikan, yakni: Bagaimana Analisis Yuridis terhadap Tindak Pidana Siber *Ransomware* dalam Hukum Positif Indonesia?

1.3. Tujuan Penelitian

Adapun kesesuaian berdasarkan latar belakang dan rumusan masalah yang telah diuraikan sebelumnya, maka tujuan dari penelitian ini adalah untuk mengetahui dan menganalisis pengaturan hukum positif Indonesia terhadap tindak pidana siber *ransomware*. Penelitian ini bertujuan untuk menelaah peraturan perundang-undangan yang berlaku, khususnya Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP), Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya, dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, terhadap tindak pidana siber *ransomware*.

1.4. Manfaat Penelitian

Adanya penelitian ini akan memberikan manfaat baik secara teoritis maupun manfaat secara praktis:

1.4.1. Manfaat Teoritis

Secara teoretis, penelitian ini bertujuan memperluas wawasan dan cakrawala keilmuan dalam bidang hukum pidana, khususnya hukum pidana siber yang berkaitan dengan pengaturan hukum terhadap tindak pidana *ransomware*. Penelitian ini diharapkan dapat memberikan kontribusi akademik dalam

memperkuat kajian mengenai hukum positif Indonesia dalam menghadapi ancaman kejahatan siber modern seperti *Ransomware*.

1.4.2. Manfaat Praktis

a. Bagi Pemerintah

Penelitian ini memberikan rekomendasi bagi pemerintah untuk memperkuat kebijakan hukum pidana dalam menanggulangi *ransomware*. Penelitian ini menekankan pentingnya langkah-langkah strategis berupa melakukan revisi terhadap Undang-Undang Informasi dan Transaksi E;ektronik (ITE), peningkatan standar keamanan bagi penyelenggara infrastruktur informasi vital, serta penguatan literasi keamanan siber di sektor publik dan swasta.

b. Bagi Akademisi

Penelitian ini dapat menjadi sumber referensi yang relevan dan aktual dalam pengembangan keilmuan di bidang hukum, khususnya yang berkaitan dengan hukum pidana siber. penelitian ini diharapkan membuka ruang bagi diskusi akademis lebih lanjut mengenai efektivitas regulasi dan strategi penegakan hukum terhadap kejahatan siber.

c. Bagi Mahasiswa

Penelitian ini dapat menjadi sumber pembelajaran dan referensi yang mendalam bagi mahasiswa, khususnya yang menempuh studi di bidang hukum pidana dan hukum siber (*cyber law*). Penelitian ini memberikan pemahaman mengenai instrumen hukum (seperti KUHP, UU ITE dan UU PDP) dalam konteks kejahatan teknologi yang dinamis dan canggih. Selain

itu, hasil penelitian ini dapat dijadikan sebagai landasan awal atau inspirasi untuk kajian lebih lanjut dalam tugas akhir, skripsi, atau tesis, guna mengeksplorasi aspek-aspek spesifik terkait regulasi dan penegakan hukum *ransomware* di Indonesia

d. Bagi Masyarakat

Penelitian ini memberikan edukasi mengenai bahaya *ransomware* dan pentingnya perlindungan data pribadi. Selain itu, masyarakat juga diharapkan dapat memahami langkah-langkah preventif yang dapat dilakukan untuk melindungi diri dari ancaman *ransomware*. Dengan demikian, penelitian ini berkontribusi dalam meningkatkan kesadaran publik mengenai keamanan digital dan pentingnya kerja sama dengan pihak berwenang untuk mencegah kejahatan siber.