JOURNAL OF LAW AND SECURITY STUDIES

Volume 3 Issue 1, June 2026 | pp. 73-88
E-ISSN 3090-2312
Doi: https://doi.org/10.31599/jlss.v3i1.5123

Ransomware Sebagai Kejahatan Siber: Rekonstruksi Kebijakan Pemidanaan Dan Strategi Pemulihan Kerugian Korban

[1]Miharni Hanapi*, [2]Edi Saputra Hasibuan
[1] Fakultas Hukum – Universitas Bhayangkara Jakarta Raya
[2] Fakultas Hukum – Universitas Bhayangkara Jakarta Raya
*miharni.akpol2006@gmail.com
*edi.saputra@dsn.ubharajaya.ac.id

Received: 29 Jan 2026 Reviewed: 12 May 2026 Published: 29 Jun 2026

Abstract

Ransomware has shifted from a technical nuisance to a coercive cybercrime that can paralyze public services and private business operations, as illustrated by the 2024 disruption of Indonesia's temporary national data center. This article examines how Indonesian criminal policy should be reconstructed to address ransomware as a layered offence and how victims' losses can be effectively recovered. The study uses normative legal research with a statutory and conceptual approach, supported by qualitative legal reasoning on cybercrime, extortion, electronic evidence, corporate liability, and victim protection. The findings show that relying on scattered provisions risks fragmented indictments and weakens a follow-the-money strategy. Policy reconstruction is therefore directed toward: (i) positioning ransomware as an extortion-based core offence accompanied by supporting offences, or formulating a specific ransomware offence; (ii) integrating restitution and asset recovery as mandatory outcomes of criminal proceedings through early loss assessment, tracing, freezing, and forfeiture of proceeds; and (iii) strengthening compliance duties of electronic system operators to reduce systemic harm. An integrated punishment–recovery model is proposed to improve deterrence and measurable victim recovery.

Keywords: *ransomware; cybercrime; criminal policy; restitution; asset recovery.*

Abstrak

Ransomware berkembang dari gangguan teknis menjadi kejahatan siber yang memaksa korban melalui penguncian sistem dan ancaman lanjutan, sebagaimana tercermin pada gangguan layanan akibat insiden Pusat Data Nasional Sementara tahun 2024. Artikel ini menganalisis arah rekonstruksi kebijakan pemidanaan ransomware di Indonesia serta desain strategi pemulihan kerugian korban agar putusan tidak berhenti pada penghukuman pelaku. Penelitian menggunakan metode hukum normatif dengan pendekatan perundang-undangan dan konseptual, dianalisis secara kualitatif melalui penalaran hukum atas konstruksi delik, pembuktian elektronik, pertanggungjawaban korporasi, dan perlindungan korban. Hasil penelitian menunjukkan bahwa pemakaian pasal yang tersebar cenderung menghasilkan dakwaan terfragmentasi dan melemahkan strategi pelacakan hasil kejahatan. Rekonstruksi kebijakan diarahkan pada: (i) penegasan ransomware sebagai inti pemerasan berbasis sistem elektronik beserta delik pendukung, atau pembentukan delik khusus ransomware; (ii) integrasi restitusi dan pemulihan aset sebagai keluaran wajib perkara melalui penghitungan kerugian,

pelacakan, pembekuan, dan perampasan hasil kejahatan sejak dini; serta (iii) penguatan kewajiban kepatuhan keamanan PSE untuk menekan kerugian sistemik. Model pemidanaan–pemulihan yang terintegrasi diusulkan untuk meningkatkan daya cegah dan pemulihan korban yang terukur.

Kata kunci: ransomware; kejahatan siber; kebijakan pemidanaan; restitusi; pemulihan aset.

PENDAHULUAN

Ketergantungan penyelenggaraan layanan publik dan aktivitas ekonomi terhadap sistem elektronik membuat serangan siber tidak lagi dapat dipandang sebagai gangguan teknis semata, melainkan sebagai ancaman nyata terhadap keamanan nasional dan keselamatan masyarakat. Serangan *ransomware* terhadap Pusat Data Nasional Sementara (PDNS) pada tahun 2024 memperlihatkan bagaimana kelumpuhan layanan dapat terjadi secara sistemik, menimbulkan kerugian berlapis mulai dari terhentinya pelayanan, biaya pemulihan, hingga risiko kebocoran dan penyalahgunaan data. Fenomena tersebut sekaligus menegaskan bahwa tata kelola keamanan siber Indonesia masih menyisakan kelemahan struktural pada aspek regulasi, koordinasi kelembagaan, dan desain kebijakan penanggulangan ancaman siber yang komprehensif.[1]

Ransomware pada dasarnya merupakan perangkat lunak berbahaya yang mengunci atau mengenkripsi data/sistem korban, lalu pelaku menuntut pembayaran tebusan agar akses dipulihkan. Dalam praktik kontemporer, pola pemerasan ini berkembang menjadi pemerasan ganda (*double extortion*) pelaku tidak hanya mengunci sistem, tetapi juga mengancam akan membocorkan data yang dicuri apabila korban tidak membayar. Konsekuensinya, kerugian korban tidak semata bersifat ekonomis, melainkan juga mencakup kerugian reputasi, gangguan operasional, dan meningkatnya risiko pelanggaran hak privasi.[2]

Dalam perspektif hukum pidana, karakter pemaksaan melalui ancaman penguncian akses data dan/atau ancaman penyebaran data menempatkan *ransomware* dekat dengan konstruksi pemerasan (*afpersing*) dan perbuatan melawan hukum di ruang siber. Sejumlah kajian menilai bahwa unsur pemerasan dapat ditarik dari norma pemerasan dalam KUHP dan dipertautkan dengan ketentuan larangan pemerasan/ancaman melalui media elektronik dalam UU ITE, sehingga *ransomware* tidak berhenti pada isu keamanan teknologi, tetapi menjadi perbuatan pidana yang memiliki elemen ancaman dan pemaksaan untuk memperoleh keuntungan.[3] Meski demikian, problem mendasar muncul pada tataran kebijakan pemidanaan, apakah perangkat hukum yang tersedia telah memadai untuk mengkualifikasi, membuktikan, dan menjatuhkan pidana secara proporsional kepada pelaku ransomware, khususnya ketika modusnya melibatkan jaringan lintas negara, pembayaran aset kripto, dan penggunaan infrastruktur anonim. Studi terkini mengenai

[1] Habib Ferian Fajar, Afdhal Fadhila, & Muhammad Kevin Yades. "Redesain Kebijakan Hukum Keamanan Dan Ketahanan Siber: Studi Kasus Serangan Siber Pada Pusat Data Nasional Tahun 2024". *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*. Vol. 14 No. 2, 2025. Hlm 477 – 482.

[2] Shellma Riyaadhotunnisa. "Aktivitas Pedagang Fisik Aset Kripto yang Tidak Bersertifikat: Studi tentang Perlindungan Hukum bagi Investor". *TANDA Jurnal Hukum*. Vol 4 No. 2, 2022. Hlm 160-172.

[3] Gilang Ramadhan. "Perlidungan Hukum Bagi Korban Ransomware Wannacry". *Das Sollen: Jurnal Kajian Kontemporer Hukum Dan Masyarakat.* Vol. 1 No. 2, 2023. Hlm 205 – 218.

pertanggungjawaban pidana pelaku *ransomware* menunjukkan adanya persoalan kekosongan/ketidakjelasan pengaturan dan tantangan pembuktian, karena pengaturan yang digunakan masih bergantung pada konstruksi pasal-pasal yang tersebar (misalnya akses tanpa hak, gangguan sistem, pemerasan/ancaman), bukan pada perumusan delik yang secara eksplisit menamai dan mengantisipasi pola *ransomware*.[4]

Di sisi lain, penelitian terdahulu juga memetakan penerapan UU ITE untuk kasus WannaCry dengan menekankan aspek larangan akses ilegal dan gangguan terhadap sistem elektronik. Namun, fokus kajian semacam ini cenderung berhenti pada identifikasi delik dan ancaman pidana, sementara dimensi pemulihan kerugian korban (*recovery*) belum ditempatkan sebagai agenda utama kebijakan pemidanaan. Padahal, bagi korban, pemulihan kerugian dan pemulihan layanan sering kali lebih mendesak daripada semata-mata pemidanaan pelaku.[5]

Kesenjangan yang paling nyata terletak pada posisi korban dalam sistem peradilan pidana. Dalam praktik penegakan hukum konvensional, negara berorientasi pada penghukuman pelaku, sedangkan korban kerap berada pada posisi sekadar saksi kerugian. Padahal, hukum positif telah mengenal mekanisme pemulihan melalui restitusi bagi korban tindak pidana, termasuk melalui peran dan mekanisme yang difasilitasi lembaga terkait. Tantangannya adalah bagaimana mekanisme tersebut dioperasionalkan secara efektif dalam perkara kejahatan siber yang kerugiannya kompleks, lintas yurisdiksi, dan kerap menghilang melalui pencucian hasil kejahatan.[6] Kebutuhan rekonstruksi kebijakan pemidanaan *ransomware* menjadi relevan karena kebijakan hukum pidana tidak hanya berbicara soal berapa lama pidana atau berapa besar denda, melainkan juga menyangkut arah politik hukum, delik apa yang dirumuskan, bagaimana penegakan dilakukan, dan tujuan apa yang hendak dicapai. Dalam kerangka kebijakan hukum pidana, pembaruan seharusnya tidak semata memperkuat aspek represif, tetapi juga mengintegrasikan orientasi pemulihan (*restorative*) yang rasional, pemidanaan harus diarahkan agar mampu menekan kejahatan sekaligus memulihkan kerugian korban secara nyata.[7]

Pemulihan kerugian korban *ransomware* membutuhkan strategi yang melampaui putusan pidana penjara dan denda. Pembayaran tebusan (ransom) bukan strategi pemulihan yang ideal karena berpotensi memperkuat ekosistem kejahatan; karena itu, fokus pemulihan semestinya mengarah pada pelacakan, pembekuan, perampasan, dan pengembalian aset hasil kejahatan (*asset recovery*) melalui instrumen hukum yang relevan, termasuk pendekatan follow the money terhadap aliran dana digital. Dalam konteks ini, pemulihan

[4] Suci Wahyuning Robbi. "Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Ransomware dalam Perspektif Peraturan Perundang-Undangan". *PAMPAS: Jurnal Hukum Pidana.* Vol. 6 No. 2. Hlm 282–295.

[5] Irfan Arief Kurniawan. "Penyebaran Virus Ransomware Wannacry Berdasarkan Undang-Undang No. 11 Tahun 2008". *Jurnal Inovasi Penelitian*. Vol. 2 No. 2, Juli 2021. Hlm 427 – 432.

[6] Rita Puspita Sari. *"Kronologi Serangan Ransomware yang Lumpuhkan PDN".* https://www.cloudcomputing.id/berita/kronologi-serangan-pdn. Diakses pada tanggal 28 Januari 2026, Pukul 19:45 WIB.

[7] Elma Aulia Musllim. "New Method Of Money Laundering By Utilizing Blockchain Technology And Cryptocurrency". *UIN Law Review : Journal Law And Human Rights*. Vol. 1 No. 2, 2025. Hlm. 132-155.

korban perlu dibaca sebagai agenda kebijakan yang melekat pada penanggulangan kejahatan modern, terutama ketika hasil kejahatan mudah dipindahkan dan disamarkan.[8]

Selain pelaku, ekosistem *ransomware* juga menyoroti tanggung jawab penyelenggara sistem elektronik dan korporasi atas keamanan siber. Ketika kegagalan tata kelola keamanan siber membuka celah serangan yang merugikan masyarakat luas, perdebatan berkembang mengenai relevansi pertanggungjawaban pidana korporasi di bidang keamanan siber, termasuk kemungkinan adopsi konsep pertanggungjawaban korporasi yang lebih tegas terhadap kelalaian sistemik. Hal ini penting karena kebijakan pemidanaan yang efektif perlu menempatkan pencegahan (*compliance* dan *due diligence*) sebagai insentif sekaligus kewajiban yang bermakna.[9]

Kompleksitas di atas semakin kuat ketika ditautkan dengan potensi tumpang tindih kewenangan dan fragmentasi regulasi penanggulangan ancaman siber. Tanpa desain yang jelas, risiko konflik kewenangan dan lemahnya koordinasi dapat berdampak langsung pada keterlambatan respons insiden, ketidakpastian langkah pemulihan, dan tidak optimalnya perlindungan korban. Karena itu, rekonstruksi kebijakan pemidanaan ransomware perlu ditempatkan dalam lanskap yang lebih luas: pembenahan sistem perlindungan dari ancaman siber yang menuntut konsistensi norma, konsolidasi kelembagaan, dan kepastian prosedur pemulihan. Berdasarkan pemetaan tersebut, artikel ini menegaskan kebaruan (*novelty*) pada dua hal. Pertama, rekonstruksi kebijakan pemidanaan ransomware tidak hanya dibangun pada pemetaan pasal-pasal yang dapat digunakan, melainkan diarahkan pada desain pemidanaan yang proporsional, adaptif terhadap modus ransomware, dan selaras dengan kebutuhan pembuktian kejahatan siber modern. Kedua, artikel ini menempatkan strategi pemulihan kerugian korban sebagai pilar utama kebijakan, dengan mengintegrasikan restitusi, asset recovery, dan penguatan kepatuhan keamanan siber penyelenggara sistem elektronik, sehingga respons hukum tidak berhenti pada penghukuman, tetapi menghasilkan pemulihan yang terukur. Sejalan dengan ketentuan penulisan bagian pendahuluan pada naskah jurnal ini, uraian berikut diarahkan untuk menampilkan fenomena terkini, telaah penelitian terdahulu guna menunjukkan keterbatasannya, serta penegasan kontribusi ilmiah dan praktis dari artikel

Tabel 1. Peta Instrumen Hukum yang Relevan untuk Ransomware dan Agenda Pemulihan Korban

Fokus	Instrumen/Nalar Hukum yang Umum Digunakan	Titik Kritis bagi Pemulihan Korban
Kualifikasi perbuatan	Delik akses tanpa hak, gangguan sistem elektronik, pemerasan/ancaman	Kualifikasi "tersebar" berisiko menyulitkan konsistensi dakwaan dan pembuktian, sehingga pemulihan korban tidak menjadi fokus putusan

[8] Gilang Ramadhan. "Perlidungan Hukum Bagi Korban *Ransomware* Wannacry Tindak Pidana *Ransomware*". *Das Sollen: Jurnal Kajian Kontemporer Hukum dan Masyarakat*. Vol. 1 No. 2, 2023. Hlm 1 – 25.

[9] Mangkunegara & RM. Armaya. "Tanggung Jawab Pidana Korporasi untuk Keamanan Siber: Rechtsvinding dalam Mengadopsi Konsep Pembunuhan Korporasi di Indonesia*". Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional.* Vol. 14 No. 2, 2025.

Fokus	Instrumen/Nalar Hukum yang Umum Digunakan	Titik Kritis bagi Pemulihan Korban
Pembuktian & penelusuran hasil kejahatan	Pembuktian elektronik, penelusuran aliran dana, keterkaitan dengan tindak pidana pencucian uang	Tanpa strategi pelacakan aset sejak dini, kerugian korban sulit dipulihkan karena hasil kejahatan cepat dipindahkan/diaburkan
Pemulihan kerugian	Restitusi (mekanisme dan fasilitasi), pengembalian aset hasil kejahatan	Perlu desain prosedural yang memastikan restitusi dan pengembalian aset menjadi outcome perkara, bukan opsi yang jarang dipakai
Pencegahan & tanggung jawab ekosistem	Kepatuhan keamanan siber penyelenggara sistem elektronik/korporasi	Tanpa insentif dan sanksi yang efektif, standar keamanan cenderung reaktif; korban menanggung beban terbesar saat insiden terjadi

TINJAUAN PUSTAKA

Konseptualisasi Ransomware sebagai Kejahatan Siber dan Kejahatan terhadap Kepentingan Korban

Ransomware pada dasarnya merupakan serangan siber yang mengunci, mengenkripsi, atau membuat sistem/berkas tidak dapat diakses, lalu pelaku menuntut pembayaran agar akses dipulihkan. Ciri khasnya bukan semata intrusi digital, melainkan pemaksaan kehendak melalui ancaman kerugian (kehilangan data, terhentinya layanan, kebocoran informasi), sehingga karakter pemerasan dan penguasaan atas kontrol sistem menjadi inti yang membedakannya dari peretasan biasa. Dalam konteks Indonesia, literatur menekankan bahwa dampak *ransomware* sangat relevan dengan perlindungan data pribadi karena serangan sering berujung pada eksfiltrasi/penyanderaan data, yang menempatkan korban dalam posisi rentan, korban dipaksa memilih antara membayar tebusan atau menanggung risiko lebih besar akibat kebocoran data dan kerusakan reputasi.[10]

Untuk meletakkan *ransomware* sebagai objek kajian hukum pidana, konsep kejahatan siber perlu dipahami sebagai tindak pidana yang memanfaatkan sistem elektronik sebagai target maupun sarana, dengan konsekuensi adanya persoalan pembuktian, yurisdiksi, dan penelusuran hasil kejahatan. Pendekatan konseptual ini penting karena ransomware biasanya tidak berhenti pada satu bentuk perbuatan, ia merupakan rangkaian tindakan (akses tanpa hak, intervensi sistem, penguasaan data, dan tuntutan pembayaran), sehingga pemetaan unsur deliknya harus mempertimbangkan konstruksi perbuatan berlanjut dan keterkaitan peran pelaku.[11]

[10] Seri Mughni Sulubara. "Perlindungan Hukum Terhadap Kejahatan Siber dari Serangan Ransomware dan Evaluasi Rancangan Undang-Undang Keamanan dan Ketahanan Siber 2025 dalam Pertahanan Indonesia". *Aliansi: Jurnal Hukum, Pendidikan dan Sosial Humaniora*. Vol. 2 No. 5, 2025. Hlm 240–249.
[11] Budi Suhariyanto. *Tindak Pidana Teknologi Informasi (cybercrime): Urgensi Pengaturan dan Celah Hukumnya.* Jakarta : Raja Grafindo Persada, 2013.

Dalam praktik, karakter lintas batas (*cross-border*) *ransomware* memperumit penegakan hukum karena pelaku, infrastruktur serangan, dan korban dapat berada pada yurisdiksi yang berbeda. Literatur yurisdiksi tindak pidana siber menegaskan bahwa batas teritorial klasik sering tidak memadai untuk menjelaskan *locus delicti* dalam kejahatan siber dan konsekuensinya, penanganan perkara membutuhkan argumentasi yurisdiksi yang lebih fungsional (misalnya berbasis akibat atau keberadaan sistem/korban), serta koordinasi antarotoritas. Dengan kata lain, tinjauan yurisdiksi menjadi fondasi untuk merancang rekonstruksi kebijakan pemidanaan *ransomware* yang realistis dari sisi penegakan.

Konstruksi Delik: Akses Tanpa Hak, Gangguan Sistem, dan Pemaksaan Kehendak dalam *Ransomware*

Kajian terdahulu mengenai tindak pidana peretasan (*hacking*) di Indonesia menunjukkan bahwa unsur tanpa hak/melawan hukum dan tujuan perbuatan (mengakses, mengambil alih, atau mengubah sistem/data) menjadi titik sentral dalam menilai pertanggungjawaban pidana. Pola argumentasi ini relevan untuk *ransomware* karena fase awal *ransomware* hampir selalu diawali intrusi/peretasan, lalu eskalasi menjadi kontrol paksa atas sistem/berkas korban. Namun, keterbatasan kajian peretasan adalah kecenderungan fokus pada fase akses dan pengamanan sistem, sementara *ransomware* menuntut analisis yang lebih lengkap karena terdapat tuntutan pembayaran yang menempatkan korban sebagai subjek yang dipaksa, bukan hanya pemilik sistem yang dibobol.[12]

Di sisi lain, pembuktian pada kejahatan siber tidak bisa dilepaskan dari status alat bukti elektronik dan tata kelola validitasnya (integritas, autentikasi, serta rantai penguasaan bukti). Literatur menegaskan bahwa pemanfaatan informasi/dokumen elektronik sebagai alat bukti harus disertai tata cara yang menjamin reliabilitas, karena kerentanan manipulasi dan kompleksitas teknis dapat melemahkan pembuktian unsur delik. Dalam konteks *ransomware*, isu ini menjadi lebih tajam, dengan pembuktian harus menjangkau jejak digital intrusi, proses enkripsi/*lock*, komunikasi tuntutan tebusan, hingga aliran pembayaran. Jika struktur pembuktian tidak dirancang sejak awal, proses peradilan cenderung berhenti pada pembuktian serangan, sementara dimensi pemaksaan kehendak dan pemulihan korban menjadi tidak optimal.[13]

Kebijakan Pemidanaan Kejahatan Siber: Arah Rekonstruksi dan Rasionalitas Pemidanaan

Literatur kebijakan hukum pidana pada ranah siber memperlihatkan kebutuhan pembaruan orientasi pemidanaan, bukan sekadar memperbanyak pasal, melainkan merumuskan kebijakan penal yang mampu merespons modus, dampak sosial, dan kesulitan pembuktian. Kajian tentang kebijakan penal dalam penanggulangan *cyber-terorism*, misalnya,

[12] Azzahra Mazaya Khalisah. "Implementasi Norma Hukum Terhadap Tindak Pidana Peretasan (Hacking) di Indonesia". *Jurist Diction – Law Journal*. Vol. 5 No. 6, 2022. Hlm 2117 – 2132.
[13] Dewa Gede Giri Santosa. "Akuisisi Dan Penyajian Bukti Digital Dalam Persidangan Pidana Di Indonesia". *Jurnal Hukum dan Peradilan*. Vol. 11 No. 2, 2022. Hlm 195–218.

menekankan pentingnya desain kriminalisasi dan pemidanaan yang terukur, termasuk perumusan unsur delik yang adaptif terhadap evolusi teknologi, tanpa kehilangan kepastian hukum. Argumen ini paralel dengan *ransomware*, pemidanaan yang efektif membutuhkan rumusan yang menangkap rangkaian perbuatan dan dampak, bukan hanya satu fase serangan.[14]

Dalam kerangka rekonstruksi kebijakan pemidanaan, isu proporsionalitas pidana juga tidak dapat dilepaskan dari karakter korban dan besaran kerugian. *Ransomware* kerap menimbulkan kerugian ekonomi langsung (*downtime* operasional, biaya pemulihan sistem), kerugian tidak langsung (kepercayaan publik), serta risiko hak privasi (kebocoran data). Oleh sebab itu, kebijakan pemidanaan yang semata menekankan penjara tanpa mengaitkan pemulihan kerugian cenderung tidak menjawab problem utama korban. Pada titik ini, kebijakan pemidanaan *ransomware* seharusnya dipahami sebagai kebijakan yang menghubungkan penghukuman dengan hasil perkara berupa pemulihan yang terukur.

Pemulihan Kerugian Korban : Restitusi, *Asset Recovery*, dan Perampasan Aset Dari perspektif korban, literatur tentang restitusi menyoroti persoalan klasik: restitusi sering dipahami normatif sebagai hak korban, tetapi pada praktiknya mengalami hambatan prosedural, pembuktian kerugian, serta keterbatasan efektivitas eksekusi. Dalam kasus *ransomware*, hambatan itu menjadi berlipat karena kerugian korban sering bercampur antara kerugian ekonomi, kerugian data, dan kerugian *immateriil* (kehilangan privasi), sementara pelaku juga sering menyembunyikan hasil kejahatan secara cepat. Artinya, desain pemulihan korban harus diletakkan sejak tahap awal penanganan perkara, bukan sekadar tambahan pada akhir putusan.

Strategi pemulihan korban juga berkaitan dengan perluasan cara pandang dari restitusi semata menuju *asset recovery*. Gagasan perampasan aset tanpa pemidanaan (*non-conviction based asset forfeiture*) dipaparkan sebagai salah satu pendekatan untuk mengatasi situasi ketika penghukuman pelaku sulit dilakukan (misalnya karena pelaku tidak teridentifikasi, berada di luar negeri, atau proses pidana berlarut), sementara aset hasil kejahatan tetap perlu dipulihkan untuk kepentingan korban/negara. Dalam konteks *ransomware* yang sering lintas yurisdiksi dan menggunakan mekanisme penyamaran pendekatan ini relevan sebagai opsi kebijakan, meskipun tetap memerlukan batasan dan mekanisme kontrol untuk menjaga perlindungan hak pihak ketiga beritikad baik.[15]

Kajian perampasan aset dalam tindak pidana pencucian uang dari perspektif keadilan menambahkan argumentasi penting, kejahatan tidak boleh memberi keuntungan pada pelaku, sehingga perluasan instrumen perampasan (termasuk model in rem/*civil forfeiture*) menjadi rasional secara kebijakan. Argumentasi ini dapat ditarik ke ransomware karena pembayaran tebusan atau keuntungan ekonomi pelaku pada akhirnya merupakan *profit from*

[14] Aisitita Laila Furqoni. "Encouraging the Establishment of Asset Forfeiture Regulations in Indonesia as a Form of Commitment to Achieving the Goals of the United Nations Convention Against Corruption". *Jurnal de Jure.* Vol. 17 No. 2, Oktober 2025. Hlm 33 – 60.

[15] Dian Alan Setiawan. "Terorisme Siber dan Pencegahannya di Indonesia". *Jurnal Media Hukum*. Vol. 27 No. 2, Hlm 267–283.

crime yang harus diputus, dan pemutusan itu membutuhkan strategi hukum yang menjangkau aset pelaku, tidak hanya pemidanaan badan.[16]

Dalam era digital, literatur juga menekankan urgensi perampasan aset dalam perkara TPPU dengan memperhatikan karakter aset modern yang mudah dipindahkan dan disamarkan. Penekanan ini memperkuat argumen bahwa pemulihan kerugian korban ransomware membutuhkan integrasi kebijakan, sejak awal perkara, aparat harus menempatkan pelacakan dan pengamanan aset sebagai bagian dari strategi penanganan, sehingga pemulihan korban tidak berhenti pada pengakuan kerugian tetapi berujung pada pengembalian yang dapat dieksekusi.

Tanggung Jawab Ekosistem: Kewajiban Penyelenggara Sistem Elektronik dan Perlindungan Data Pribadi

Kajian mengenai implementasi aturan perlindungan data pribadi oleh penyelenggara sistem elektronik (PSE) menunjukkan bahwa perlindungan data pada sektor elektronik bukan hanya isu kepatuhan administratif, tetapi berkaitan langsung dengan pemenuhan hak dasar dan kepastian hukum. Literatur tersebut menilai bahwa kelemahan desain regulasi (terutama sebelum adanya kerangka yang kuat) menyebabkan penanganan kasus kebocoran data tidak optimal, sehingga korban sering menanggung beban terbesar saat terjadi insiden. Dalam konteks *ransomware*, argumen ini mengarah pada kebutuhan memperjelas standar kewajiban keamanan, tata kelola insiden, dan konsekuensi hukum bagi PSE yang lalai, agar pencegahan dan pemulihan tidak semata dibebankan kepada korban.[17]

Kerangka hukum perlindungan data pribadi dalam penyelenggaraan pemerintahan berbasis elektronik (SPBE) menegaskan bahwa tata kelola data pemerintah memerlukan struktur norma yang jelas, karena kebocoran data dan serangan siber pada sektor publik berdampak sistemik terhadap kepercayaan warga negara. Relevansinya bagi ransomware adalah ketika data publik atau layanan publik terganggu, korban tidak selalu individu semata, melainkan masyarakat luas sebagai pengguna layanan. Karena itu, rekonstruksi kebijakan tidak cukup hanya pada delik pelaku, tetapi juga perlu strategi pencegahan dan pemulihan yang berbasis tata kelola sistem dan standar keamanan yang dapat diaudit.

METODE PENELITIAN

Bagian metode penelitian ini disusun secara deskriptif-naratif untuk menjelaskan secara runtut model penelitian, sumber data/bahan hukum, teknik pengumpulan, serta teknik analisis yang digunakan dalam mengkaji *ransomware* sebagai kejahatan siber, arah kebijakan pemidanaan, dan strategi pemulihan kerugian korban. Penelitian ini merupakan penelitian hukum normatif (*doctrinal research*) dengan sifat preskriptif-analitis, yakni penelitian yang

[16] Gumilang Fuadi. "Tinjauan Perampasan Aset dalam Tindak Pidana Pencucian Uang dari Perspektif Keadilan". *Jurnal Penegakan Hukum dan Keadilan*. Vol. 5 No. 1, 2024. Hlm 53 – 68.

[17] Wenderlin Koswara. "Implementasi Aturan Perlindungan Data Pribadi Oleh Penyelenggara Sistem Elektronik Dikaitkan Dengan Teori Keadilan Dan Kepastian Hukum". *Jurnal Paradigma Hukum Pembangunan*. Vol. 7 No.2, 2022

tidak hanya memaparkan ketentuan hukum yang berlaku, tetapi juga memberikan argumentasi mengenai apa yang seharusnya (*ought to be*) dibangun dalam desain kebijakan pemidanaan dan pemulihan korban *ransomware*. Kerangka preskriptif diperlukan karena fokus artikel adalah rekonstruksi kebijakan, menilai kecukupan norma yang ada dan merumuskan perbaikan yang lebih fungsional bagi penegakan hukum dan kepentingan korban.[18]

Pendekatan yang digunakan mencakup, pendekatan perundang-undangan (*statute approach*) untuk menilai konsistensi dan kecukupan norma pidana terkait akses tanpa hak, gangguan sistem elektronik, pemerasan/ancaman, serta mekanisme pemulihan, pendekatan konseptual (*conceptual approach*) untuk memperjelas konsep ransomware sebagai rangkaian perbuatan pidana dan konsep kebijakan pemidanaan yang berorientasi perlindungan korban dan pendekatan perbandingan (*comparative approach*) secara terbatas untuk menilai relevansi model pengaturan dan strategi pemulihan pada konteks kejahatan siber modern, terutama ketika sifat kejahatan lintas yurisdiksi menjadi variabel penegakan.[19]

Jenis bahan hukum yang digunakan meliputi bahan hukum primer, yaitu peraturan perundang-undangan yang relevan (antara lain regulasi mengenai tindak pidana siber, pembuktian, perlindungan data, serta mekanisme pemulihan korban dan perampasan hasil kejahatan), bahan hukum sekunder berupa buku, artikel jurnal ilmiah, dan pendapat ahli hukum untuk membangun argumentasi kebijakan, serta bahan hukum tersier sebagai bahan penunjang (misalnya kamus/ensiklopedia hukum) untuk memastikan ketepatan istilah dan konseptualisasi. Klasifikasi ini penting agar analisis tidak bertumpu pada satu jenis sumber, melainkan bergerak dari norma primer menuju pendalaman argumentasi melalui literatur otoritatif.[20]

Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan (*library research*) dan studi dokumen, yakni penelusuran, seleksi, dan inventarisasi bahan hukum primer maupun literatur yang relevan, lalu disusun secara sistematis sesuai isu konstruksi delik *ransomware* dan pertanggungjawaban pelaku, desain kebijakan pemidanaan yang proporsional dan adaptif, serta model pemulihan kerugian korban melalui restitusi dan pemulihan aset hasil kejahatan. Metode kepustakaan dipilih karena objek kajian bersifat normatif berpusat pada norma, doktrin, dan argumentasi hukum sehingga validitas penelitian bertumpu pada ketepatan dan keluasan literatur hukum yang digunakan.[21]

Analisis bahan hukum dilakukan secara kualitatif dengan pola penalaran hukum (*legal reasoning*) yang menekankan bahwa interpretasi gramatikal untuk memastikan makna istilah normatif, interpretasi sistematis untuk menilai hubungan dan hirarki antar-norma, serta interpretasi teleologis untuk menilai kesesuaian tujuan pemidanaan dengan perlindungan korban dan efektivitas pemulihan. Setelah itu dilakukan konstruksi hukum untuk

[18] Peter Mahmud Marzuki. *Penelitian Hukum Edisi Revisi.* Jakarta : Kencana Prenada Media Group. 2017. Hlm 76.
[19] Soerjono Soekanto & Sri Mamudji. *Penelitian Hukum Normatif Suatu Tinjauan Singkat*. Jakarta : Rajagrafindo Persada, 2011. Hlm 128.
[20] Amiruddin & Zainal Asikin. *Pengantar Metode Penelitian Hukum*. Jakarta : Rajawali Press. 2018. Hlm 89.
[21] Soemitro & Ronny Hanitijo. *Metodologi Penelitian Hukum Dan Jurimetri.* Jakarta : Ghalia Indonesia, 1990.

merumuskan rekomendasi rekonstruksi kebijakan pemidanaan dan strategi pemulihan korban *ransomware* yang lebih operasional.[22]

Sebagai langkah penguatan metodologis, penelitian ini menempatkan metode normatif sebagai instrumen yang responsif terhadap dinamika perubahan regulasi khususnya pada isu siber dengan memastikan setiap simpulan dibangun dari konsistensi norma, koherensi doktrin, dan rasionalitas tujuan kebijakan. Dengan demikian, keluaran penelitian tidak berhenti pada inventarisasi pasal, melainkan berorientasi pada rancangan kebijakan yang dapat diuji secara argumentatif (rasional) dan ditautkan pada kebutuhan pemulihan korban.[23]

HASIL DAN PEMBAHASAN

Ransomware sebagai Kejahatan Siber Berlapis dan Dampak Hukumnya

Temuan pertama menunjukkan bahwa *ransomware* bukan satu perbuatan pidana yang berdiri sendiri, melainkan rangkaian tindakan yang umumnya mencakup infiltrasi akses, pengambilalihan kontrol, penguncian/penyanderaan data (*availability*), lalu pemerasan melalui ancaman tidak memulihkan sistem atau menyebarkan data. Konsekuensinya, kerugian korban bersifat majemuk berupa kerugian ekonomi (*downtime* layanan, biaya pemulihan, potensi pembayaran tebusan), kerugian keamanan (hilangnya integritas sistem), dan kerugian sosial (turunnya kepercayaan publik, khususnya bila menyerang layanan publik/*critical services*). Pola ini juga memperlihatkan mengapa ransomware perlu diposisikan sebagai *kejahatan siber berorientasi keuntungan* (*profit-driven cybercrime*) dengan risiko sistemik, bukan sekadar gangguan teknis yang diselesaikan lewat pemulihan TI saja.[24]

Temuan kedua memperlihatkan bahwa konstruksi delik *ransomware* dalam hukum positif Indonesia bergerak pada *model delik berlapis* (*multi-offence approach*). Dari sisi norma, elemen pemerasan/ancaman melalui sarana elektronik memperoleh basis yang semakin eksplisit melalui perubahan UU ITE,[25] yakni pengaturan perbuatan yang bermaksud menguntungkan diri sendiri/orang lain secara melawan hukum dengan memaksa orang lain memberi sesuatu (barang/uang/akses) melalui ancaman kekerasan atau ancaman pencemaran/penyiaran informasi elektronik yang merugikan. Selain itu, rezim baru juga memperkuat ruang tindakan cepat dalam proses penegakan, termasuk langkah pembatasan akses/pemutusan akses pada akun, rekening, uang elektronik, maupun aset digital tertentu sebagai langkah awal pengamanan proses dan hasil kejahatan. Dua hal ini penting karena *ransomware* bekerja cepat dan hasil kejahatan mudah dipindahkan lintas yurisdiksi.

Temuan ketiga menunjukkan bahwa fragmentasi norma (akses ilegal, gangguan sistem, pemerasan, penyalahgunaan data, pencucian hasil kejahatan) memiliki dua implikasi.

[22] Sudikno Mertokusumo. *Penemuan Hukum : Sebuah Pengantar.* Yogyakarta : Universitas Atma Jaya Yogyakarta, 2010. Hlm 72.
[23] Alfan Maulana. "Metode Penelitian Hukum Normatif Dalam Menjawab Tantangan Dinamika Peraturan Perundang-Undangan". Jurnal Penelitian Ilmiah Interdisipliner. Vol 9 No. 11 November 2025.
[24] Monica Mutmainah Sabillah. "Pertanggungjawaban Pidana Atas Serangan Ransomware Terhadap Data Aset Informasi Negara". Jurnal Lex Crimen - Jurnal Fakultas Hukum UNSRAT. Vol. 13 No. 2, 2025. Hlm 5.
[25] Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Pertama, dakwaan cenderung tersebar dan berorientasi pada pemenuhan unsur delik, bukan pada pemulihan korban. Kedua, tanpa benang merah kebijakan, penegakan hukum rentan kehilangan fokus pada *follow the money* serta pemulihan kerugian, padahal keduanya justru menentukan nilai keadilan substantif bagi korban. Dengan kata lain, masalah utamanya bukan ketiadaan pasal sama sekali, melainkan ketiadaan desain kebijakan yang mengikat pemidanaan dan pemulihan sebagai satu paket hasil perkara.[26]

Temuan keempat berkaitan dengan dinamika regulasi pemidanaan nasional yang berubah signifikan. Setelah pemberlakuan KUHP Nasional, ruang desain pemidanaan (jenis pidana, sistem denda, dan orientasi kebijakan) semakin menuntut penyesuaian agar delik siber terutama yang berdampak sistemik dapat memiliki parameter penuntutan dan pemidanaan yang konsisten. Perubahan kebijakan pemidanaan juga dipengaruhi oleh ketentuan penyesuaian pidana yang baru (terutama terkait struktur denda/kategori dan penataan kebijakan sanksi), sehingga rekonstruksi kebijakan *ransomware* perlu diletakkan dalam lanskap hukum yang mutakhir, bukan hanya mengandalkan pola lama.

Rekonstruksi Kebijakan Pemidanaan: dari "Penghukuman Pelaku" ke "Penghukuman dan Pemulihan"

Temuan kelima menegaskan bahwa rekonstruksi kebijakan pemidanaan *ransomware* harus dimulai dari penjernihan orientasi pemidanaan, bahwa pemidanaan bukan semata pembalasan, melainkan instrumen negara untuk melindungi masyarakat dan memulihkan ketertiban hukum yang dilanggar. Kerangka ini penting agar rancangan sanksi tidak berhenti pada pidana penjara/denda yang simbolik, tetapi diarahkan untuk mencegah pengulangan, melumpuhkan kapasitas pelaku, dan memaksimalkan pengembalian kerugian korban. Dalam doktrin hukum pidana, pemidanaan dipahami sebagai bagian dari sistem yang harus konsisten dengan tujuan perlindungan masyarakat; dan rumusan tindak pidana harus menegaskan subjek, perbuatan yang dilarang, serta ancaman pidana secara tegas untuk menjamin kepastian hukum dan efektivitas penegakan.[27]

Temuan keenam menunjukkan kebutuhan *rekonstruksi formulasi* (kebijakan formulatif) untuk *ransomware* melalui dua jalur yang dapat dipilih secara kebijakan:

1. **Penguatan model delik berlapis** dengan pedoman penuntutan dan pemidanaan yang menempatkan pemerasan-penyanderaan data sebagai inti (*core offence*), sementara akses ilegal/gangguan sistem sebagai rangkaian (*supporting offences*) yang memperberat; atau
2. **Pembentukan delik khusus *ransomware*** (*lex specialis*) yang mendefinisikan *ransomware* sebagai perbuatan menguasai/mengunci/menyandera sistem/data untuk tujuan memperoleh keuntungan melawan hukum, dengan pemberatan jika menyerang infrastruktur kritis, layanan publik, atau mengakibatkan kebocoran data massal.

[26] Zainuddin Kasim. "Kebijakan Hukum Pidana untuk Penanggulangan Kejahatan Cyber di Indonesia". *Jurnal Indragiri Law Review (ILR)*. Vol. 2 No. 1, 2024. Hlm 18 - 24.
[27] Andi Hamzah. *Sistem Pidana Dan Pemidanaan Indonesia.* Jakarta : Pradnya Paramita, 1993. Hlm 41.

Dari perspektif sistem peradilan pidana, jalur mana pun yang dipilih harus terintegrasi dengan desain penegakan (penyidikan–penuntutan–pemidanaan) agar putusan tidak terfragmentasi, melainkan menghasilkan *outcome* yang terukur berupa penghukuman yang proporsional dan pemulihan yang nyata.[28]

Temuan ketujuh menekankan dimensi pertanggungjawaban korporasi dan ekosistem. *Ransomware* kerap menimbulkan kerugian luas bukan hanya karena pelaku, tetapi juga karena kelemahan tata kelola keamanan siber pada penyelenggara sistem elektronik/korporasi yang mengelola data dan layanan. Karena itu, kebijakan pemidanaan perlu menyediakan jalur yang jelas untuk menilai: kapan peristiwa ransomware semata perbuatan pelaku eksternal, dan kapan terdapat kelalaian serius (*negligence*) atau kegagalan kepatuhan keamanan yang membuat kerugian membesar. Literatur hukum menegaskan bahwa pemidanaan korporasi tidak semata menghukum, tetapi mendorong kepatuhan, pencegahan, dan perlindungan masyarakat sebagai pengguna sistem elektronik.[29]

Temuan kedelapan terkait pembuktian bahwa keberhasilan pemidanaan *ransomware* sangat ditentukan oleh kualitas pembuktian elektronik (log, jejak akses, forensik perangkat, aliran transaksi). Tanpa standar pembuktian yang rapi (keaslian, integritas, rantai penguasaan/*chain of custody*), perkara mudah terjebak pada perdebatan formil dan menghambat pengembalian kerugian korban. Doktrin pembuktian siber menekankan bahwa pembuktian elektronik harus dipahami sebagai perluasan instrumen pembuktian pidana modern, dan karenanya prosedur pengamanan bukti sejak awal insiden adalah jantung perkara siber.

Strategi Pemulihan Kerugian Korban: Restitusi, Pemulihan Aset, Dan Tanggung Jawab Ekosistem

Temuan kesembilan menunjukkan bahwa jalur pemulihan korban yang paling dekat dengan sistem peradilan pidana adalah restitusi. Namun, praktik restitusi sering tidak optimal karena dianggap tambahan, bukan target utama perkara. Karena itu, strategi pemulihan harus direkonstruksi melalui desain prosedural yang membuat restitusi menjadi *default outcome*, yaitu sejak tahap penyidikan (penghitungan kerugian), penuntutan (pencantuman restitusi dalam tuntutan), hingga putusan (perintah restitusi yang dapat dieksekusi). Kajian atas pengaturan prosedural restitusi menekankan pentingnya standar penilaian kerugian dan tata cara permohonan yang sederhana, agar korban tidak menanggung beban pembuktian yang berlebihan.[30]

Temuan kesepuluh menegaskan bahwa pada *ransomware*, restitusi tidak akan efektif tanpa strategi pemulihan aset hasil kejahatan. *Ransomware* bekerja sebagai kejahatan

[28] Muladi. *Kapita Selekta Sistem Peradilan Pidana.* Semarang : Badan Penerbit Universitas Diponegoro. 2002. Hlm 37.
[29] Rony Mart Panjaitan. "Pertanggungjawaban Pidana Korporasi Sebagai Penyelenggara Sistem Elektronik Dalam Terjadinya Kebocoran Data Pengguna Sistem Elektronik". *Jurnal Hukum Adigama*. Vol. 4 No. 2, Desember 2021. Hlm 2624 – 2643.
[30] Risma Putri Sugiarto. "Restitusi Terhadap Istri Korban Kekerasan Dalam Rumah Tangga Pada Perkawinan Siri". *Jurnal Perspektif : Kajian Masalah Hukum dan Pembangunan*. Vol. 31 No. 1, 2026. Hlm 12 – 21.

keuntungan dalam bentuk hasil kejahatan (tebusan/transfer) dipindahkan cepat, sering melalui aset digital, *mixing*, atau lintas platform. Karena itu, kebijakan pemidanaan harus memasangkan restitusi dengan *asset tracing* dan *asset freezing* sejak dini, bukan setelah putusan. Literatur kebijakan pemulihan aset menekankan pendekatan *follow the money* sebagai syarat efektivitas pemulihan, termasuk integrasi analisis transaksi dan kerja sama lembaga yang mengawasi aliran dana.[31]

Temuan kesebelas menunjukkan bahwa pemulihan korban juga menuntut tanggung jawab ekosistem penyelenggara sistem elektronik (PSE). Dalam PSTE, PSE dibebani kewajiban untuk memastikan sistem yang andal dan aman, serta kewajiban respons insiden (termasuk pelaporan ketika terjadi gangguan/kegagalan) agar kerugian tidak meluas. Konsekuensinya, kebijakan pemulihan tidak cukup hanya mengejar pelaku melainkan negara perlu memastikan PSE menerapkan kehati-hatian dan tata kelola keamanan yang dapat diaudit, karena pencegahan dan mitigasi pada level PSE adalah faktor utama yang menentukan besar-kecilnya kerugian korban.[32]

Temuan kedua belas berkaitan dengan karakter lintas batas. Banyak operasi *ransomware* bersifat transnasional, yaitu pelaku, infrastruktur serangan, dan aliran dana dapat berada di yurisdiksi berbeda. Karena itu, pemulihan aset dan pembuktian memerlukan kerja sama internasional (*mutual legal assistance*, pertukaran informasi, dan pembekuan aset lintas negara). Literatur mengenai bantuan hukum timbal balik menegaskan pentingnya mekanisme permintaan yang cepat dan standar komunikasi antar lembaga agar bukti dan aset tidak hilang karena keterlambatan prosedur.[33]

Model Integratif: Pemidanaan yang Mengunci Pemulihan Kerugian Korban

Berdasarkan temuan di atas, model rekonstruksi yang paling rasional adalah **integrasi pemidanaan–pemulihan**. Dalam model ini, pemidanaan *ransomware* dirancang sebagai paket kebijakan sebagai berikut : (i) penjeraan dan pelumpuhan kapasitas pelaku (*incapacitation*), (ii) perintah pengembalian kerugian (restitusi) sebagai bagian dari putusan, (iii) perampasan hasil kejahatan untuk pemulihan korban, dan (iv) penguatan kewajiban kepatuhan keamanan pada PSE/korporasi agar kerugian sistemik tidak berulang. Dalam kajian hukum telematika, pendekatan ini sejalan dengan kebutuhan menghubungkan norma siber dengan kepastian pembuktian, tata kelola sistem elektronik, serta perlindungan kepentingan korban dalam ruang digital.[34]

---

[31] I Dewa Gede Dana Sugama. "Pengaturan Tindak Pidana Pencucian Uang Pada Peraturan Perundang-Undangan Di Indonesia". *Jurnal Media Akademik (JMA).* Vol. 4 No. 1, Januari 2026. Hlm 4

[32] Rai Mantili & Putu Eka Trisna Dewi. "Prinsip Kehati-Hatian Dalam Penyelenggaraan Sistem Elektronik Dalam Upaya Perlindungan Data Pribadi Di Indonesia". *Jurnal Aktual Justice.* Vol. 5 No. 2, Desember 2020. Hlm 132 – 145.

[33] Abizar Al Ghiffari. "Kejahatan Siber dan Tantangan Penegakan Hukum di Indonesia". *JPIM: Jurnal Penelitian Ilmiah Multidisipliner.* Vol. 02 No. 02, Tahun 2025. Hlm 1295 – 1299.

[34] Edmon Makarim. *Pengantar Hukum Telematika : Suatu Kompilasi Kajian*. Jakarta : RajaGrafindo Persada, 2005.

Tabel 2. Ringkasan Temuan dan Arah Rekonstruksi Kebijakan

Isu Kunci	Temuan Normatif	Arah Rekonstruksi yang Disarankan
Konstruksi delik	*Ransomware* adalah kejahatan berlapis (akses–penguncian–pemerasan) sehingga dakwaan mudah terfragmentasi	Tetapkan *core offence* (pemerasan-penyanderaan data) dan *supporting offences*, atau rumuskan delik khusus *ransomware*
Orientasi pemidanaan	Pemidanaan cenderung fokus pada pelaku, pemulihan korban belum menjadi *outcome* perkara	Terapkan *sentencing policy* yang mewajibkan restitusi dan perampasan hasil kejahatan sebagai satu paket
Pembuktian	Kualitas bukti elektronik menentukan keberhasilan perkara dan pemulihan	Standarkan pengamanan bukti digital dan integrasikan forensik dan penelusuran aset sejak awal
Pemulihan korban	Restitusi sulit efektif tanpa pembekuan/penelusuran aset	Jalankan *follow the money* dan pemutusan akses aset terkait sedini mungkin
Ekosistem PSE	Kerugian membesar bila tata kelola keamanan lemah	Tegaskan tanggung jawab PSE, audit kepatuhan, dan sanksi yang mendorong pencegahan
Transnasional	Pelaku dan aset lintas negara menghambat pemulihan	Optimalkan MLA dan koordinasi lintas yurisdiksi untuk bukti dan aset

SIMPULAN

Ransomware pada hakikatnya merupakan kejahatan siber berorientasi keuntungan yang bekerja melalui rangkaian perbuatan mulai dari penguasaan sistem/data, penguncian akses, hingga pemaksaan kehendak korban untuk memberikan sesuatu. Karena karakternya sebagai pemerasan berbasis sistem elektronik dengan modus operandi kompleks, penanganan hukum yang hanya memusat pada satu unsur delik cenderung tidak memadai untuk menangkap keseluruhan kesalahan dan dampak pada korban.[35]

Rekonstruksi kebijakan pemidanaan harus dipahami sebagai politik hukum pidana yang menata kriminalisasi, pembuktian, dan sanksi secara fungsional, bukan sekadar menambah ancaman pidana. Orientasi kebijakan yang tepat menempatkan pemidanaan sebagai instrumen perlindungan masyarakat sekaligus koreksi sistemik atas risiko berulangnya kejahatan siber, sehingga desain delik dan sanksi perlu disusun selaras dengan tujuan

[35] Nur Syamsi Tajriyani. "Pertanggungjawaban Pidana Tindak Pidana Pemerasan Dengan Modus Operandi Penyebaran Ransomware Cryptolocker". Jurnal Jurist Diction. Vol. 4 No. 2, 2021. Hlm 685–710

penanggulangan kejahatan modern.[36]

Pemulihan kerugian korban perlu diposisikan sebagai hasil perkara yang melekat pada penegakan hukum *ransomware*, bukan agenda tambahan di luar proses pidana. Kerangka normatif mengenai restitusi menyediakan dasar untuk menagih ganti kerugian korban melalui mekanisme yang diakui hukum, sehingga agenda pemulihan semestinya diintegrasikan sejak awal penanganan perkara. Penguatan kewajiban keamanan dan tata kelola insiden pada penyelenggara sistem elektronik (PSE) merupakan prasyarat pencegahan dan pembatasan kerugian korban. Norma penyelenggaraan sistem dan transaksi elektronik menegaskan pentingnya aspek keamanan dan keandalan sistem; konsekuensinya, kebijakan pemidanaan dan pemulihan perlu berjalan paralel dengan penguatan rezim kepatuhan keamanan agar korban tidak terus menanggung beban terbesar ketika terjadi insiden.[37]

Perumusan dan penegakan delik ransomware perlu diarahkan agar lebih korban-sentris: fokus tidak berhenti pada identifikasi akses ilegal atau gangguan sistem, melainkan memastikan perbuatan pemerasan, ancaman, serta dimensi kerugian korban terbaca jelas dalam konstruksi dakwaan dan pertimbangan putusan. Penguatan orientasi perlindungan korban dalam kajian *ransomware* menunjukkan urgensi menggeser fokus dari semata pemidanaan menuju perlindungan dan pemulihan.[38]

Strategi pemulihan kerugian korban perlu mengadopsi pendekatan pelacakan aliran dana secara sistematis (*follow the money*) agar pengembalian kerugian tidak berhenti pada pengakuan normatif, melainkan dapat dieksekusi melalui pembekuan, perampasan, dan pengembalian aset hasil kejahatan. Pendekatan ini relevan karena keuntungan *ransomware* lazim bergerak cepat melalui kanal digital dan lintas yurisdiksi.

Penegakan pertanggungjawaban korporasi perlu dioperasionalkan secara konsisten pada konteks ekosistem *ransomware*, khususnya ketika terdapat kelalaian sistemik dalam tata kelola keamanan yang memperbesar dampak korban. Pedoman penanganan perkara tindak pidana oleh korporasi dapat menjadi rujukan prosedural untuk memastikan korporasi tidak sekadar diposisikan sebagai korban pasif, melainkan juga dinilai kewajiban kepatuhan dan tanggung jawab hukumnya bila terbukti lalai.

Perlindungan layanan publik dan sektor vital perlu diperlakukan sebagai area prioritas dalam kebijakan pencegahan dan respons *ransomware*, termasuk standardisasi manajemen insiden, koordinasi lintas institusi, dan kontrol risiko pada infrastruktur informasi vital. Kerangka pelindungan infrastruktur informasi vital menegaskan pentingnya pendekatan terstruktur untuk mencegah gangguan sistemik yang memperluas jumlah dan tingkat kerugian korban.

Standarisasi pembuktian dan pengelolaan alat bukti elektronik harus diperkuat sejak tahap awal perkara, karena keberhasilan pembuktian *ransomware* bergantung pada

[36] Barda Nawawi Arief. Bunga Rampai Kebijakan Hukum Pidana : Perkembangan Penyusunan Konsep KUHP Baru. Jakarta :Kencana Prenada Media Group, 2010.
[37] Peraturan Pemerintah (PP) Nomor 7 Tahun 2018 tentang Pemberian Kompensasi, Restitusi, dan Bantuan Kepada Saksi dan Korban.
[38] Peraturan Pemerintah (PP) Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

integritas jejak digital, validitas prosedur forensik, dan reliabilitas alat bukti elektronik di persidangan. Literatur mengenai efektivitas alat bukti elektronik menegaskan bahwa kualitas dan tata kelola bukti digital menentukan efektivitas penegakan serta berpengaruh langsung pada kemungkinan pemulihan kerugian korban.

DAFTAR PUSTAKA

Ananta, Ahmad Rizal Roby, Demas Brian Wicaksono, Indrawati, Istikhomah, dan Zaskiya Amalina. "Potensi Konflik Kewenangan pada Perlindungan dari Ancaman Siber di Indonesia." Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional 14, no. 2 (2025): 233–252. doi:10.33331/rechtsvinding.v14i2.2199.

Fajar, Habib Ferian, Afdhal Fadhila, dan Muhammad Kevin Yades. "Redesain Kebijakan Hukum Keamanan dan Ketahanan Siber: Studi Kasus Serangan Siber pada Pusat Data Nasional Tahun 2024." Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional 14, no. 2 (2025). doi:10.33331/rechtsvinding.v14i2.2155.

Haditama, Talia Kallista, dan Fajar Sugianto. "A Comparative Analysis of Corporate Criminal Liability for AI-Based Malware: A Study of Indonesian and European Union Law." Indonesia Law Reform Journal 5, no. 2 (2025): 308–322. doi:10.22219/ilrej.v5i2.39901.

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

Kurniawan, Irfan Arief, Hadi Mahmud, dan Nourma Dewi. "Penyebaran Virus Ransomware Wannacry Berdasarkan Undang-Undang No. 11 Tahun 2008." Jurnal Inovasi Penelitian 2, no. 2 (2021). doi:10.47492/jip.v2i2.704.

Maharani, P., Hafrida, H., dan M. Rapik. "Pertanggungjawaban Pidana Hacktivist dalam Perspektif Hukum Pidana di Indonesia." PAMPAS: Journal of Criminal Law 5, no. 2 (2024). doi:10.22437/pampas.v5i2.33291.

Makhali, Imam. "Bentuk Pertanggungjawaban Pidana bagi Pelaku Tindak Pidana Mayantara." Jurnal Transparansi Hukum 6, no. 1 (2023): 31–43. doi:10.30737/transparansi.v6i1.4226.

Mangkunegara, RM. Armaya. "Corporate Criminal Liability for Cybersecurity: Rechtsvinding in Adopting the Concept of Corporate Manslaughter in Indonesia." Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional 14, no. 2 (2025). doi:10.33331/rechtsvinding.v14i2.2193.

Pansariadi, Rafi Septia Budianto, dan Noenik Soekorini. "Tindak Pidana Cyber Crime dan Penegakan Hukumnya." Jurnal Bina Mulia Hukum 12, no. 2 (2023). doi:10.37893/jbh.v12i2.605.

Putri, Nisa Nindia, Sahuri Lasmadi, dan Erwin. "Pertanggungjawaban Pidana Perusahaan Pers terhadap Pemberitaan yang Mencemarkan Nama Baik Orang Lain Melalui Media Cetak Online." PAMPAS: Journal of Criminal Law 2, no. 2 (2021). doi:10.22437/pampas.v2i2.14761.

Robbi, S. Wahyuning, Hafrida, dan Yulia Monita. "Pertanggungjawaban Pidana Terhadap

Pelaku Tindak Pidana Ransomware dalam Perspektif Peraturan Perundang-Undangan." PAMPAS: Journal of Criminal Law 6, no. 2 (2025): 282–295. doi:10.22437/pampas.v6i2.43967.

Tajriyani, Nur Syamsi. "Pertanggungjawaban Pidana Tindak Pidana Pemerasan dengan Modus Operandi Penyebaran Ransomware Cryptolocker." Jurist-Diction 4, no. 2 (2021). doi:10.20473/jd.v4i2.25785.

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

Arief, Barda Nawawi. *Bunga Rampai Kebijakan Hukum Pidana: Perkembangan Penyusunan Konsep KUHP Baru*. Jakarta: Kencana Prenada Media Group, 2010.

Husein, Yunus. *Penjelasan Hukum tentang Perampasan Aset Tanpa Pemidanaan dalam Perkara Tindak Pidana Korupsi*. Jakarta: PSHK Indonesia dan Puslitbangkumdil Mahkamah Agung RI, 2019.

Muhaimin. *Metode Penelitian Hukum*. Mataram: Mataram University Press, 2020.

Situmeang, Sahat Maruli T. *Cyber Law*. Bandung: Penerbit Cakra, 2020.

Mahkamah Agung Republik Indonesia. *Peraturan Mahkamah Agung Nomor 13 Tahun 2016 tentang Tata Cara Penanganan Perkara Tindak Pidana oleh Korporasi*.

Republik Indonesia. *Peraturan Pemerintah Nomor 7 Tahun 2018 tentang Pemberian Kompensasi, Restitusi, dan Bantuan kepada Saksi dan Korban*.

Republik Indonesia. *Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik*.

Republik Indonesia. *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik* (LNRI Tahun 2024 Nomor 1; TLNRI Nomor 6905).

Republik Indonesia. *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi* (LNRI Tahun 2022 Nomor 196; TLNRI Nomor 6820).

Republik Indonesia. *Undang-Undang Nomor 31 Tahun 2014 tentang Perubahan atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban* (LNRI Tahun 2014 Nomor 293).