HEI EMA: Jurnal Riset Hukum, Ekonomi Islam, Ekonomi, Manajemen dan Akuntansi
E.ISSN: 2828-8033
https://jurnal.stisalhilalsigli.ac.id/index.php/jhei

PERLINDUNGAN HUKUM BAGI KORBAN *CYBER SABOTAGE* DAN *CYBER EXTORTION* DALAM PERSPEKTIF HUKUM POSITIF INDONESIA (STUDI KASUS: SERANGAN *RANSOMWARE WANNACRY* TERHADAP SISTEM INFORMASI TAHUN 2017)

Pramesti Refita Cahyani[1], Ravael Yehezkiel[2], Muhammad Adryan Maulana[3], Muhammad Zidan Ramadhan[4], and Bagas Arifianto[5]
Universitas Bina Sarana Informatika
E-mail: pramestirefitacahyani@gmail.com[1], ravaelyhz@gmail.com[2], adryanmaulana700@gmail.com[3], zdnrmd@gmail.com[4], bagasarifianto06@gmail.com[5]

Abstract

The rapid development of information technology has increased digital efficiency while simultaneously expanding exposure to cybercrimes, particularly cyber sabotage and cyber extortion. The 2017 WannaCry ransomware attack serves as a concrete example of these two modes operating simultaneously through data encryption and ransom demands. This study aims to analyze the legal protection afforded to victims of such attacks within the framework of Indonesia's positive law. Using a qualitative juridical-normative method, the research examines relevant regulations, including the Electronic Information and Transactions Law (UU ITE) and the Indonesian Criminal Code (KUHP), alongside academic literature and reports related to the WannaCry incident in Indonesia. The findings indicate that the attack significantly affected public institutions, particularly hospitals, whose operational performance was disrupted by encrypted data and system inaccessibility. Although UU ITE and KUHP provide a legal basis for electronic extortion and system interference, they do not explicitly regulate ransomware as a distinct offense. Victim protection both preventive and repressive remains insufficient due to the absence of clear mechanisms for restitution or compensation. This study highlights the need for regulatory reform, enhanced law enforcement capacity, and stronger national cybersecurity resilience to provide more effective and comprehensive protection for victims of modern cybercrimes.
Keyword: *Ransomware, Legal Protection, Cyber Extortion*

Abstrak

Perkembangan teknologi informasi membawa kemudahan signifikan bagi aktivitas digital, namun juga meningkatkan eksposur terhadap kejahatan siber, terutama cyber sabotage dan cyber extortion. Serangan ransomware WannaCry tahun 2017 menjadi contoh nyata bagaimana dua modus tersebut bekerja secara simultan melalui penguncian data dan tuntutan tebusan. Penelitian ini bertujuan menganalisis perlindungan hukum bagi korban kejahatan siber tersebut dalam perspektif hukum positif Indonesia. Metode penelitian yang digunakan adalah kualitatif yuridis-normatif melalui kajian peraturan perundang-undangan seperti UU ITE dan KUHP, serta literatur ilmiah dan laporan terkait insiden WannaCry di Indonesia. Hasil analisis menunjukkan bahwa serangan WannaCry memberikan dampak signifikan terhadap institusi publik, khususnya rumah sakit, yang mengalami gangguan operasional akibat enkripsi data. Dari aspek regulasi, UU ITE dan KUHP telah memberikan dasar hukum mengenai pemerasan dan gangguan sistem elektronik, namun belum secara eksplisit mengatur ransomware sebagai kategori kejahatan tersendiri. Perlindungan terhadap korban, baik preventif maupun represif, dinilai masih belum memadai karena belum adanya skema kompensasi atau restitusi yang jelas. Studi ini menegaskan perlunya pembaruan regulasi, peningkatan kapasitas aparat penegak hukum, serta penguatan ketahanan siber nasional agar perlindungan terhadap korban kejahatan siber dapat diimplementasikan secara lebih efektif dan komprehensif.
Kata Kunci: Ransomware, Perlindungan Hukum, Pemerasan Siber

PENDAHULUAN

Teknologi informasi yang berkembang pesat memberikan kemudahan luar biasa bagi aktivitas individu maupun institusi. Melalui digitalisasi, tugas rutin seperti komunikasi, penyimpanan data, dan transaksi bisnis dapat dilakukan dengan efisien dan cepat. Internet dan sistem *cloud* memungkinkan penyimpanan data secara praktis dan aksesibilitas yang tinggi, sementara *mobile banking* mendukung kenyamanan dalam aktivitas finansial (Ramadhan et al., 2023).

Namun, di balik kemudahan tersebut, muncul ancaman serius berupa kejahatan siber (*cybercrime*) yang semakin beragam dan kompleks. Penyalahgunaan teknologi informasi dapat mengakibatkan kerugian nyata, dari peretasan jaringan, pencurian data pribadi, hingga serangan seperti *Denial of Service* (DoS) yang mengganggu sistem operasional (Agustiono et al., 2024).

Dalam kerangka kejahatan siber, tindakan *sabotase* menjadi salah satu modus operasi utama. *Cyber sabotage* mencakup penguncian, perusakan, atau manipulasi data dan sistem korban misalnya dengan menyisipkan *malware* yang merusak jaringan dan mengganggu ketersediaan sistem kritis (Khakim et al., 2023). Sementara itu, *extortion digital* (pemerasan siber) kerap dilakukan melalui *ransomware* pelaku mengenkripsi data korban kemudian menuntut tebusan agar data bisa dipulihkan (Abdullah, 2023).

Dampak dari praktik *sabotase* dan *extortion* ini tidak hanya bersifat teknis, tetapi juga bersifat hukum dan sosial. Secara hukum, perlindungan data pribadi dan regulasi terkait kejahatan teknologi informasi menjadi sangat penting. Di Indonesia, misalnya, perkembangan pesat TI menekankan perlunya pembaruan regulasi pidana terkait transaksi *digital* dan kebocoran data pribadi (Sabadina, 2021).

Dari sisi sosial, rendahnya literasi *digital* masyarakat dan lemahnya kesadaran keamanan membuka celah besar bagi para pelaku *cybercrime* untuk mengeksploitasi korban. Sebagai contoh nyata, serangan *ransomware WannaCry* tahun 2017 menyasar institusi global dan inklusif di Indonesia, seperti rumah sakit, dengan modus mengunci data korban dan menuntut pembayaran tebusan (Anjelina et al., 2024). Hal ini menggambarkan kombinasi sabotase dan extortion sekaligus.

Dari perspektif hukum positif di Indonesia, terdapat regulasi yang mengatur kejahatan siber dan pemerasan, antara lain UU ITE (Pasal 27 ayat 4 jo Pasal 45 ayat 1) serta KUHP Pasal 368 tentang pemerasan. Namun muncul pertanyaan sejauh mana korban dari aksi *cyber sabotage/extortion* mendapatkan perlindungan hukum yang memadai (seperti restitusi, kompensasi, asistensi hukum) dan bagaimana efektivitas regulasi yang ada dalam menghadapi jenis kejahatan siber yang terus berkembang?

Artikel ini bertujuan menganalisis perlindungan hukum korban dalam kasus WannaCry di Indonesia, mengevaluasi kekuatan dan kelemahan regulasi yang ada, serta merumuskan rekomendasi agar perlindungan hukum bagi korban kejahatan siber tersebut dapat ditingkatkan. Penelitian ini urgen dan relevan dilakukan untuk mendeskripsikan *Cyber Sabotage* dan *Cyber Extortion* sebagai kejahatan digital secara masif yang dapat merugikan pihak korban tanpa memperoleh kompensasi dan perlindungan hukum yang pasti.

METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif yuridis-normatif dengan beberapa tahapan yang meliputi pengumpulan bahan hukum normatif seperti Undang-Undang (UU ITE, KUHP), regulasi pelaksana, kebijakan, serta literatur hukum dan jurnal terdahulu. Penggunaan pendekatan *yuridis normatif* dilakukan karena kajian dalam penelitian ini adalah kajian ilmu hukum. Oleh karena itu, aspek hukum menjadi bahan kajian dengan cara melihat dari segi peraturan-peraturan yang terkait dengan *cyber sabotage* dan *cyber extortion* (Soemitro, 1988).

Jenis penelitian ini merupakan penelitian kualitatif, yaitu prosedur penelitian yang menghasilkan data deskriptif berupa kata-kata tertulis atau lisan dari orang-orang dan perilaku yang dapat diamati (Moleong, 2001). Analisis dilakukan secara yuridis terhadap norma-norma hukum, khususnya UU ITE Pasal 27 ayat 4 dan Pasal 45 ayat 1 serta KUHP Pasal 368, untuk melihat bagaimana norma-norma tersebut dapat diterapkan dalam konteks kejahatan *ransomware* atau *extortion*. Selanjutnya, dilakukan analisis normatif untuk menelaah kesesuaian antara norma hukum dengan fenomena nyata, yaitu serangan *ransomware WannaCry* pada tahun 2017 di Indonesia, guna mengevaluasi apakah regulasi yang ada telah mengakomodasi kebutuhan perlindungan korban. Penelitian ini tidak melibatkan wawancara, survei, atau observasi lapangan, melainkan sepenuhnya didasarkan pada kajian pustaka melalui sumber-sumber seperti jurnal ilmiah, artikel berita, laporan resmi, dan peraturan perundang-undangan yang relevan.

LANDASAN TEORETIS

Cyber Sabotage dan *Cyber Extortion*

Cyber sabotage merupakan tindakan intentional yang merusak, mengunci, atau menyabot sistem/tata-kelola data/komputer korban melalui teknologi informasi sehingga operasional terganggu atau terhenti (Ferdiansyah, 2018). *Cyber extortion* merupakan tindakan pemerasan *digital* di mana pelaku menahan atau mengenkripsi data korban dan menuntut pembayaran tebusan (sering dalam kripto) agar akses dipulihkan atau ancaman tidak dilakukan (Ferdiansyah, 2018).

Kasus *ransomware* seperti *WannaCry* adalah bentuk gabungan *sabotase* (penguncian akses data) dan *extortion* (tuntutan tebusan). *Malware* mengeksploitasi kerentanan *Windows*, menyebar cepat dan mengunci banyak sistem (Ferdiansyah, 2018). Serangan *ransomware WannaCry* yang terjadi pada tahun 2017 memberikan dampak signifikan di berbagai negara, termasuk Indonesia. Berdasarkan jurnal *"*Challenges of Indonesian Defense Resilience in Facing Cyber Threats*"*, serangan ini menargetkan sejumlah infrastruktur penting, terutama sektor kesehatan. Rumah sakit menjadi salah satu sasaran utama di mana sistem komputer mereka terkunci dan tidak dapat diakses, sehingga menghambat pelayanan medis kepada Masyarakat (Wijaya et al., 2024). Kondisi ini menunjukkan bahwa serangan siber tidak hanya menimbulkan kerugian ekonomi, tetapi juga berdampak langsung terhadap aspek kemanusiaan dan pelayanan publik.

Selain pada sektor kesehatan, serangan *WannaCry* juga mengganggu sistem teknologi informasi di lembaga pemerintahan dan institusi pendidikan. Banyak komputer diinstalasi pemerintah yang terinfeksi, menyebabkan gangguan pada proses administrasi dan komunikasi internal. Dalam konteks ini, lemahnya sistem keamanan siber nasional pada saat itu memperlihatkan bahwa kesiapsiagaan Indonesia terhadap ancaman siber masih belum optimal. Hal ini menjadi titik tolak penting bagi pemerintah untuk memperkuat infrastruktur keamanan *digital* dan meningkatkan kesadaran serta kapasitas sumber daya manusia di bidang siber.

Tujuan *Cyber Sabotage* dan *Cyber Extortion*

Tujuan utama pelaku *ransomware* seperti *WannaCry* sangat jelas bersifat finansial mereka mengenkripsi data korban kemudian menuntut tebusan dalam bentuk mata uang kripto agar korban bisa mendapatkan kembali akses ke sistem atau data mereka. Metode pembayaran dengan kripto memberikan keuntungan ganda bagi pelaku, yakni anonimitas transaksi dan kemudahan pencucian dana. Pendekatan ini menegaskan bahwa motivasi utama serangan ransomware bukan ideologis atau politik, tetapi murni orientasi profit. Struktur bisnis *ransomware* telah berkembang menjadi ekosistem kriminal profesional dengan skema "*Ransomware-as-a-Service* (RaaS)", memungkinkan sindikat mengambil alih model operasi secara mirip dengan perusahaan legal demi keuntungan maksimal (Oosthoek et al., 2023).

Fenomena semacam ini mencerminkan pergeseran paradigma kejahatan siber dari serangan destruktif menjadi kegiatan kriminal yang sangat terorganisir dan menguntungkan secara ekonomi. Riset lain menunjukkan bahwa para penjahat ini memanfaatkan strategi harga dan diferensiasi tebusan untuk memaksimalkan pendapatan, sekaligus mempertimbangkan dampak kesejahteraan sosial dari serangan tersebut (Hernandez-Castro et al., 2020). Seiring dengan itu, kemudahan akses dan rendahnya biaya awal (modal) untuk meluncurkan serangan *ransomware* memperkuat motivasi ekonomi di balik aksinya.

Dengan demikian, *ransomware* dapat dikategorikan sebagai bentuk *cyber sabotage* karena menimbulkan gangguan dan kerusakan terhadap sistem digital, sekaligus sebagai *cyber extortion* karena adanya unsur pemerasan untuk memperoleh uang tebusan. Kedua bentuk kejahatan ini termasuk dalam ranah tindak pidana siber yang memerlukan penegakan hukum tegas dan kebijakan perlindungan siber yang komprehensif. Kasus *WannaCry* menjadi pembelajaran penting bagi Indonesia untuk memperkuat ketahanan *digital* nasional dan memperbarui regulasi yang mampu menjawab tantangan keamanan siber *modern*.

HASIL PENELITIAN DAN PEMBAHASAN

Kasus *WannaCry* (2017) Sebagai Studi Kasus

Serangan global *ransomware WannaCry* yang terjadi pada Mei 2017 merupakan salah satu serangan siber paling masif dalam sejarah, memengaruhi lebih dari 200.000 komputer di sekitar 150 negara di seluruh dunia (Wijaya et al., 2024). Serangan ini

memanfaatkan celah keamanan sistem operasi Windows dan menyebar secara cepat ke berbagai sektor penting seperti kesehatan, transportasi, dan administrasi publik. Dalam banyak kasus, sistem *digital* korban terkunci dan seluruh data menjadi tidak dapat diakses tanpa pembayaran tebusan, sehingga menyebabkan gangguan besar terhadap aktivitas operasional di berbagai negara.

Di Indonesia, meskipun data angka spesifik mengenai jumlah korban ransomware belum terdokumentasi secara komprehensif, sejumlah laporan akademik dan riset menunjukkan bahwa institusi publik, khususnya rumah sakit, pernah menjadi target serangan serius. Sebagai contoh, insiden *WannaCry* menyerang Rumah Sakit Harapan Kita dan Rumah Sakit Dharmais, mengakibatkan penguncian server dan mengganggu operasional pelayanan kesehatan (Kristalia et al., 2024). Gangguan semacam ini membahayakan aspek kemanusiaan karena rumah sakit adalah infrastruktur vital yang secara langsung menyentuh keselamatan pasien.

Kondisi ini menegaskan bahwa kesiapsiagaan siber di Indonesia pada saat itu masih tergolong rendah. Infrastruktur keamanan *digital* di banyak instansi publik belum cukup kuat untuk menghadapi serangan skala besar, baik dari sisi backup data maupun sistem tanggap darurat. Selain itu, lembaga kritikal seperti rumah sakit seringkali tidak memiliki protokol pemulihan data yang matang, sehingga begitu sistem terkena *ransomware*, pemulihan menjadi sangat sulit dan lama. Studi manajemen risiko keamanan siber juga menunjukkan bahwa pemerintah belum sepenuhnya memperkuat redundansi dan pemulihan bencana *digital*, yang menyebabkan risiko sosial meningkat jika layanan publik lumpuh (Tommy et al., 2025).

Dampak sosial dari serangan siber seperti ini juga menjadi sorotan dalam kajian hukum dan kebijakan. Penelitian tentang perlindungan hukum terhadap serangan *ransomware* menyatakan bahwa regulasi yang ada di Indonesia, seperti UU ITE dan UU PDP, belum secara khusus mengatur *ransomware* sebagai kejahatan digital terpisah (Sulubara et al., 2025). Karena itu, insiden serangan terhadap instansi publik dan rumah sakit turut menjadi panggilan bagi penguatan kebijakan keamanan siber nasional, baik dari segi regulasi maupun kesiapan infrastruktur *digital*.

Secara teknis, modus serangan *WannaCry* menggunakan exploit bernama "*EternalBlue*" yang awalnya dikembangkan oleh badan intelijen Amerika Serikat (NSA) namun kemudian bocor ke publik. Pelaku menyebarkan *ransomware* yang mengenkripsi seluruh data di perangkat korban dan menuntut pembayaran tebusan dalam bentuk Bitcoin agar dapat memberikan kunci dekripsi untuk memulihkan data yang terkunci (Ferdiansyah, 2018). Strategi ini menandai munculnya bentuk baru pemerasan digital yang sulit dilacak, karena transaksi *cryptocurrency* bersifat anonim dan lintas batas, sehingga menyulitkan aparat hukum dalam melakukan penegakan hukum terhadap pelaku.

Dampak dari serangan ini sangat luas, mencakup kerugian material seperti biaya pemulihan sistem, serta kerugian non-material seperti terganggunya pelayanan publik, menurunnya kepercayaan masyarakat terhadap institusi, dan rusaknya reputasi lembaga yang menjadi korban. Banyak institusi harus melakukan rasionalisasi anggaran untuk

memperbaiki infrastruktur *digital* dan memperkuat sistem keamanan. Dari perspektif korban, proteksi dan pemulihan sering kali tidak dapat dilakukan secara cepat karena keterbatasan sumber daya dan lemahnya koordinasi antarinstansi. Hal ini menunjukkan adanya kebutuhan mendesak untuk memperkuat perlindungan hukum terhadap korban kejahatan siber serta memperbarui kebijakan keamanan *digital* agar lebih adaptif terhadap ancaman yang terus berkembang.

Perlindungan Hukum Korban Menurut Hukum Positif Indonesia

1. Regulasi yang Relevan

Kerangka hukum di Indonesia yang mengatur kejahatan siber seperti *ransomware* dan pemerasan *digital* terutama diatur melalui UU ITE. Dalam Pasal 27 ayat (4) UU ITE diatur larangan mendistribusikan, mentransmisikan, atau membuat dapat diaksesnya informasi elektronik yang mengandung muatan pemerasan atau pengancaman, dan pelanggaran ini diancam dengan pidana penjara dan/atau denda menurut Pasal 45 ayat (4) UU ITE. Rumusan pasal ini bersifat "*rubber clause*" dan belum secara spesifik membedakan antara berbagai jenis kejahatan, sehingga menimbulkan problem kepastian hukum (Riyadh et al., 2024).

Selain itu, pertanggungjawaban pidana pelaku ransomware juga bisa dilihat melalui kombinasi UU ITE dengan KUHP. Serangan *ransomware* dapat memenuhi unsur "akses tanpa hak", "perusakan data", dan "pemerasan melalui sistem elektronik", sehingga dapat dijerat pasal-pasal UU ITE dan KUHP sekaligus (Sabillah et al., 2025). Regulasi saat ini dinilai masih belum memadai oleh sejumlah akademisi misalnya, analisis menyatakan bahwa undang-undang (UU ITE) belum mengatur secara eksplisit unsur "permintaan tebusan" pada kasus *ransomware*, sehingga diperlukan revisi untuk memperkuat kerangka hukum terhadap kejahatan ini (Alpajri et al., 2025).

Namun demikian, sejumlah penelitian menyoroti bahwa meskipun regulasi tersebut telah ada, substansinya masih memiliki kekosongan hukum terkait kasus *ransomware* yang secara teknis melibatkan elemen "permintaan tebusan" melalui enkripsi data. UU ITE cenderung fokus pada aspek gangguan terhadap sistem elektronik, tetapi belum mengatur secara eksplisit mekanisme pemerasan *digital* berbasis enkripsi. Hal ini menunjukkan perlunya pembaruan norma hukum agar dapat menyesuaikan dengan karakteristik kejahatan siber modern yang terus berkembang (Alpajri et al., 2025). Dalam konteks global, banyak negara telah memperbarui peraturan mereka untuk memasukkan terminologi seperti "*ransomware*", "data *encryption extortion*" dan "*cyber extortion*" sebagai tindak pidana tersendiri, sehingga Indonesia perlu menempuh langkah serupa untuk memperkuat sistem hukumnya.

2. Aspek Perlindungan bagi Korban: Preventif dan Represif

Dari sisi preventif, perlindungan terhadap korban kejahatan siber, termasuk *ransomware*, dapat dilakukan melalui penguatan regulasi dan kebijakan yang mewajibkan institusi publik maupun swasta melakukan langkah-langkah keamanan

siber yang memadai. Langkah tersebut meliputi kewajiban melakukan *data backup* secara rutin, pembaruan (*patching system*) terhadap perangkat lunak, serta peningkatan edukasi literasi siber bagi pegawai dan masyarakat. Infrastruktur *digital* di Indonesia masih belum sepenuhnya tangguh menghadapi ancaman *ransomware* karena rendahnya kesadaran keamanan dan minimnya investasi dalam sistem pertahanan siber (Wijaya et al., 2024). Oleh karena itu, pencegahan perlu difokuskan pada peningkatan kesiapan teknis serta penerapan standar keamanan nasional yang terukur dan wajib bagi seluruh penyelenggara sistem elektronik.

Sementara dari sisi represif, penegakan hukum menjadi aspek penting dalam memberikan perlindungan dan efek jera bagi pelaku. Kendala utama dalam penanganan kejahatan siber di Indonesia adalah keterbatasan kompetensi aparat penegak hukum, kurangnya fasilitas *cyber forensic*, serta lemahnya kerja sama internasional dalam pelacakan pelaku lintas negara (Arisandy, 2020). Untuk memperkuat aspek represif ini, diperlukan pembentukan unit khusus yang memiliki kemampuan teknis dan hukum dalam menghadapi kasus *ransomware*.

Selain itu, perlindungan korban secara hukum juga harus dijamin. Korban kejahatan siber secara prinsip memiliki hak yang sama dengan korban kejahatan konvensional, yaitu hak atas restitusi dan kompensasi. Namun, dalam praktiknya, kasus *ransomware* belum diatur secara khusus mengenai mekanisme restitusi bagi korban. Ketiadaan skema kompensasi yang jelas menyebabkan banyak korban tidak mendapatkan pemulihan atas kerugian yang diderita, baik secara finansial maupun non-finansial (Prasetyo, 2020). Hal ini memperlihatkan kesenjangan nyata antara norma hukum yang ideal dengan realitas implementasinya di lapangan.

3. Evaluasi dan Permasalahan

Evaluasi terhadap implementasi regulasi menunjukkan bahwa terdapat kesenjangan normatif antara ketentuan hukum dan praktik penegakan hukum di lapangan. UU ITE, misalnya, belum mengakomodasi secara spesifik unsur "permintaan tebusan" yang menjadi inti dari tindak *cyber extortion* seperti *ransomware*. Klausul yang ada masih terlalu umum dan tidak mencakup mekanisme digital berbasis enkripsi yang menjadi modus utama *ransomware* (Alpajri, 2025).

Di sisi lain, penegakan hukum terhadap kejahatan lintas negara masih menghadapi tantangan besar. Pelaku kejahatan siber sering kali beroperasi di luar yurisdiksi Indonesia, sehingga mempersulit upaya penangkapan dan proses hukum (Tobing et al., 2024). Selain itu, keterbatasan kapasitas *digital forensics* juga memperlambat proses pembuktian hukum.

Perlindungan terhadap korban *ransomware* di Indonesia memang dinilai belum optimal. Walaupun terdapat landasan hukum seperti UU ITE dan KUHP, mekanisme restitusi atau kompensasi untuk korban siber khususnya korban *ransomware* masih sangat umum dan tidak spesifik. Sebagian korban masih kesulitan memperoleh pemulihan kerugian finansial atau data, karena belum ada prosedur baku

dan peran pemerintah serta penyelenggara sistem elektronik dalam memberikan ganti rugi masih ambigu.

Dari perspektif akademis, penelitian menyatakan bahwa pendekatan keadilan restoratif bisa menjadi solusi dalam mengisi kekosongan perlindungan korban siber. Sebagai contoh, Flora et al., (2023) mengusulkan agar korban *cyber crime*, termasuk *ransomware*, mendapatkan asistensi, fasilitasi, dan kompensasi sebagai bagian dari pemulihan korban. Sementara itu, Sulubara et al., (2025) mengkritik regulasi saat ini seperti UU ITE dan UU PDP yang belum mengatur *ransomware* secara spesifik, sehingga perlindungan korban belum mencakup restitusi maupun tanggung jawab sistemik dari penyelenggara keamanan siber.

Selain permasalahan hukum dan penegakan, kesiapan institusional juga menjadi sorotan. Infrastruktur pertahanan siber di Indonesia masih lemah, dengan koordinasi antarlembaga yang belum optimal serta rendahnya pelatihan bagi petugas IT di sektor publik (Batu et al., 2025). Faktor lain yang memperumit situasi adalah ketidakjelasan yurisdiksi dan tantangan pembuktian *digital*, mengingat data dan pelaku sering berada di berbagai negara dengan sistem hukum berbeda. Akibatnya, korban sulit memperoleh keadilan secara cepat dan menyeluruh.

Dengan demikian, diperlukan langkah strategis berupa pembaruan regulasi yang lebih spesifik dan responsif terhadap pola kejahatan siber modern, termasuk penambahan pasal yang secara eksplisit mengatur tindakan *ransomware*, pemerasan *digital*, dan bentuk serangan berbasis enkripsi data. Pembaruan tersebut harus dibarengi dengan peningkatan kapasitas aparat penegak hukum, baik melalui pelatihan forensik *digital*, pemahaman teknis terhadap modus kejahatan siber, maupun koordinasi antarlembaga yang lebih solid. Tanpa kerangka hukum yang jelas dan aparat yang kompeten, respons terhadap insiden *ransomware* akan selalu terlambat dan tidak efektif.

Selain itu, penguatan sistem keamanan siber nasional menjadi agenda yang tidak dapat ditunda. Pemerintah perlu memperkuat infrastruktur *digital*, mekanisme deteksi dini, respons insiden (*incident response*), serta sistem pemulihan nasional yang mampu meminimalkan kerugian akibat serangan. Reformasi hukum yang adaptif dan komprehensif menjadi kunci agar Indonesia mampu menghadapi ancaman *ransomware* sekaligus menjamin perlindungan hak-hak korban secara lebih menyeluruh, baik pada aspek teknis, sosial, maupun hukum. Dengan kombinasi regulasi yang tepat, penegakan hukum yang kuat, serta kesiapsiagaan nasional yang baik, ancaman *ransomware* dapat ditekan secara signifikan.

Analisis Kebijakan dan Perbandingan Singkat

Indonesia saat ini tengah menggodok Rancangan Undang-Undang Keamanan dan Ketahanan Siber (RUU KKS / RUU Keamanan dan Ketahanan Siber) (Admin PP, 2025). Dalam jurnal *Legal Protection Against Cybercrime from Ransomware Attacks and Evaluation of the 2025 Cyber Security and Resilience Bill in Indonesia's Defense* dikemukakan bahwa RUU tersebut merupakan respons regulasi terhadap *ransomware*

extortion, dengan potensi memperkuat kewenangan otoritas siber, mewajibkan pelaporan insiden siber, dan memperketat sanksi bagi pelaku (Sulubara et al., 2025). Namun, RUU itu sendiri masih status draf dan belum berlaku penuh sebagai undang-undang.

Dibandingkan negara tetangga atau negara lain yang sudah lebih dulu memperkuat regulasi siber (misalnya memperkenalkan pasal khusus untuk *ransomware*, mekanisme pemulihan korban seperti restitusi atau dana kompensasi, dan lembaga penegakan siber yang mandiri), regulasi di Indonesia masih belum sekomprehensif itu. Ketiadaan pasal eksplisit mengenai "permintaan tebusan", "enkripsi data", atau "publikasi ancaman data" dalam UU yang berlaku memberi ruang kebingungan atau interpretasi hukum yang terbatas. RUU KKS bisa menjadi langkah maju, tapi efektivitasnya tergantung isi finalnya dan kemampuan lembaga pendukungnya.

Berdasarkan kondisi tersebut, beberapa rekomendasi kebijakan dapat diajukan:

1. Revisi UU ITE atau regulasi pendukung agar mencakup secara eksplisit unsur-unsur *ransomware*/*extortion digital* seperti "permintaan tebusan", "penguncian data (*enkripsi*)", dan "publikasi ancaman data".
2. Membentuk mekanisme restitusi korban kejahatan siber misalnya pembentukan dana pemulihan nasional atau jaminan kompensasi, agar korban dapat memperoleh kompensasi atas kerugian teknis maupun non-teknis (kerusakan data, *downtime* layanan, reputasi).
3. Penguatan kerjasama internasional dan institusional, misalnya antara Badan Siber dan Sandi Negara (BSSN), Kementerian Komunikasi dan Informatika, penegak hukum, lembaga forensik *digital* lintas negara, agar bisa menyelidiki pelaku dengan modus lintas batas.
4. Edukasi dan peningkatan kapasitas aparat penegak hukum dan infrastruktur teknis (*digital* forensik, tim *respons* insiden siber), agar ketika regulasi sudah diperkuat, aparat memiliki kemampuan untuk menerapkannya secara efektif.

Dengan demikian, meskipun RUU KKS menunjukkan niat memperkuat kerangka hukum terhadap serangan digital, masih perlu dipastikan bahwa pasal-pasalnya sesuai dengan modus operasi *ransomware modern*, adanya mekanisme perlindungan dan pemulihan korban yang nyata, serta kesiapan institusi penegakan hukum dan teknis agar regulasi tersebut bukan hanya norma di atas kertas, tetapi bisa dijalankan secara efektif di lapangan.

KESIMPULAN

Kasus *ransomware WannaCry* (2017) merupakan contoh nyata dari kejahatan siber yang tergolong dalam kategori *cyber sabotage* dan *cyber extortion*, dengan dampak signifikan terhadap berbagai institusi di Indonesia. Regulasi seperti UU ITE Pasal 27 ayat (4) jo Pasal 45 ayat (1) serta KUHP Pasal 368 memang dapat menjadi dasar hukum untuk menjerat pelaku pemerasan atau pengancaman *digital*, namun masih memiliki keterbatasan dalam menangani kasus ransomware yang melibatkan enkripsi data dan permintaan tebusan. Selain itu, perlindungan hukum bagi korban dalam bentuk restitusi, kompensasi, maupun asistensi hukum belum berjalan optimal karena regulasi belum

secara spesifik mengatur modus operandi *ransomware*, sementara penegakan hukum kerap menghadapi kendala teknis dan lintas yurisdiksi. Untuk memperkuat perlindungan terhadap korban kejahatan siber, diperlukan revisi regulasi yang mencakup ketentuan khusus mengenai ransomware dan *extortion*, serta pembentukan mekanisme pemulihan korban yang meliputi restorasi data, kompensasi finansial, dan bantuan hukum. Di samping itu, penguatan penegakan hukum, peningkatan kapasitas lembaga seperti BSSN dan Kominfo, serta kerja sama internasional perlu ditingkatkan untuk menghadapi ancaman lintas batas. Edukasi publik juga penting agar masyarakat dan institusi lebih siap dalam pencegahan dan respons terhadap serangan siber. Dengan demikian, efektivitas perlindungan hukum korban kejahatan *cyber sabotage* dan *extortion* hanya dapat tercapai melalui sinergi antara regulasi yang adaptif, penegakan yang kuat, pemulihan yang cepat, serta pencegahan yang proaktif.

DAFTAR PUSTAKA

Abdullah, Ifnu Abdul Aziz. "Pencegahan Ransomware Berbasis Edukasi Pengguna Dan Teknologi: Tinjauan Literatur." *DiJITAC : Digital Journal of Information Technology and Communication* 4, no. 1 (2023): 35–41. https://doi.org/10.21093/dijitac.v4i1.10325.

Admin PP. "PEMBAHASAN AWAL RUU KEAMANAN DAN KETAHANAN SIBER DIMULAI." DJPP, February 18, 2025. https://www.djpp.kemenkumham.go.id/publikasi/indeks-berita/pembahasan-awal-ruu-keamanan-dan-ketahanan-siber-dimulai.

Agustiono, Wahyudi, Dini Wulan Suci, and Novi Prastiti. "Analisis Forensik Digital Menggunakan Metode NIST Untuk Memulihkan Barang Bukti Yang Dihapus." *Jurnal Teknologi Dan Informasi* 14, no. 2 (2024): 174–85.

Alpajri, Muhammad, Erdianto Effendi, and Davit Rahmadan. "STRENGTHENING INDONESIA'S EIT LAW TO COMBAT RANSOMWARE THREATS: A LEGAL FRAMEWORK ANALYSIS." *JURNAL ILMIAH ADVOKASI* 13, no. 2 (2025): 402–13.

Arisandy, Yogi Oktafian. "Penegakan Hukum Terhadap Cyber Crime Hacker." *Indonesian Journal of Criminal Law and Criminology (IJCLC)* 1, no. 3 (2020): 162–69.

Batu, Dewi Pika Lbn, Parlaungan Gabriel Siahaan, Taufiq Ramadhan, and Agnes Irene Silitonga. "SERANGAN MALWARE RANSOMWARE DALAM PERSPEKTIF TRANSNATIONAL CRIME." *Bureaucracy Journal : Indonesia Journal of Law and Social-Political Governance* 5, no. 2 SE-Articles (June 6, 2025): 1197–1213. https://doi.org/10.53363/bureau.v5i2.615.

Chella Defa Anjelina, and Mahardini Nur Afifah. "Kilas Balik Ransomware WannaCry, Pernah Serang 150 Negara Termasuk Indonesia 7 Tahun Lalu." Kompas.Com, June 29, 2024. https://www.kompas.com/tren/read/2024/06/29/063000065/kilas-balik-ransomware-wannacry-pernah-serang-150-negara-termasuk-indonesia.

Ferdiansyah, Ferdiansyah. "Analisis Aktivitas Dan Pola Jaringan Terhadap Eternal Blue & Wannacry Ransomware." *JUSIFO (Jurnal Sistem Informasi)* 4, no. 1 SE-Articles (June 29, 2018): 37–48. https://doi.org/10.19109/jusifo.v4i1.2077.

Flora, H. S., Sitanggang, T., Simarmata, B., & Karina, I. (2023). Keadilan Restoratif dalam Melindungi Hak Korban Tindak Pidana Cyber: Manifestasi dan Implementasi. *Jurnal Ius Constituendum*, *8*(2), 169-184. https://doi.org/10.26623/jic.v8i2.6365

Hernandez-Castro, J, A Cartwright, and E Cartwright. "An Economic Analysis of Ransomware and Its Welfare Consequences." *Royal Society Open Science* 7, no. 3 (March 2020): 190023. https://doi.org/10.1098/rsos.190023.

Khakim, Shella Amalia, Rahma Kurnia, Cinta Perindu, and Wustari L Mangundjaya. "PERAN MANAJEMEN SEKURITI DALAM MENGATASI ANCAMAN KEAMANAN SIBER DI ERA DIGITAL: SEBUAH TINJAUAN LITERATUR." *Triwikrama: Jurnal Multidisiplin Ilmu Sosial* 7, no. 4 (2023): 2025.

Kristalia, B R M Yehizkia Y, and Indra Wisnu Wibisono. "Ancaman Siber Dan Penguatan Kedaulatan Digital Indonesia Dari Perspektif Geopolitik Digital." *Jurnal Ilmiah Multidisiplin* 3, no. 02 (2024): 83–93.

Moleong, L. J. (2001). *Metodologi Penelitian Kualitatif.* Bandung: Remaja Rusda Karya.

Oosthoek, Kris, Jack Cable, and Georgios Smaragdakis. "A Tale of Two Markets: Investigating the Ransomware Payments Economy." *Communications of the ACM* 66, no. 8 (2023): 74–83.

Prasetyo, Mujiono Hafidh. "Legal Protection as a Form of State Responsibility for Victims of Cyber Crime in Indonesia." *CCER*, 2020, 149. https://doi.org/10.4108/eai.26-9-2020.2302588.

Ramadhan, Muhammad, Dwi Oktafia Ariyanti, and Nita Ariyani. "Edukasi Hukum Implikasi Undang-Undang Informasi Dan Transaksi Elektronik Di Kelurahan Bener, Yogyakarta." *DAS SEIN: Jurnal Pengabdian Hukum Dan Humaniora (Journal of Legal Services and Humanities)* 3, no. 2 (2023): 119–30.

Riyadh, Muhammad Al, Sigid Suseno, and Rully Herdita Ramadhani. "Analisis Kebijakan Hukum Pidana Dalam Pasal 45 Ayat (4) Jo. Pasal 27 Ayat (4) UU ITE." *Indonesian Journal of Criminal Law and Criminology (IJCLC)* 5, no. 1 (2024).

Sabadina, Uni. "Politik Hukum Pidana Penanggulangan Kejahatan Teknologi Informasi Terkait Kebocoran Data Pribadi Oleh Korporasi Berbasis Online." *Lex Renaissance* 6, no. 4 (2021): 799–814.

Sabillah, Monica Mutmainah, Caecilia J. J. Waha, and Youla O. Aguw. "PERTANGGUNGJAWABAN PIDANA ATAS SERANGAN RANSOMWARETERHADAP DATA ASET INFORMASI NEGARA." *Lex CrimenJurnal Fakultas Hukum UNSRAT* 13, no. 2 (2025).

Seri Mughni Sulubara, Virdyra Tasril, & Nurkhalisah Nurkhalisah. (2025). Legal Protection Against Cybercrime from Ransomware Attacks and Evaluation of the 2025 Cyber Security and Resilience Bill in Indonesia's Defense. *Aliansi: Jurnal Hukum, Pendidikan Dan Sosial Humaniora*, *2*(5), 240–249. https://doi.org/10.62383/aliansi.v2i5.1234

Soemitro, R. H. (1988). *Metodologi Penelitian Hukum dan Jurimetri.* Semarang: Ghalia Indonesia.

Tobing, Clara Ignatia, Tiofanny Marylin Surya, Liris Roesa Selvias, Stepania Rehulina Girsang, Putri Berliana Azzahra, Lustri Yolanda Purba, Mahezha Agnia Putera, and Nurrahman Rusmana. "Globalisasi Digital Dan Cybercrime: Tantangan Hukum Dalam Menghadapi Kejahatan Siber Lintas Batas." *Jurnal Hukum Sasana* 10, no. 2 (2024): 105–23.

Tommy, Syarifa, 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): 1–26.

Wijaya, Mirza Mahbub, Naswa Bayu Tsabita, and Fathan Mubina Dewadi. "Challenges of Indonesian Defense Resilience in the Face of Contemporary Technology Advancement: What's Next?" *Pancasila: Jurnal Keindonesiaan* 4, no. 2 (2024): 235–50.