ACADEMOS
Jurnal Hukum dan Tatanan Sosial

E-ISSN: 2985-797X

Vol 4 / No 1 / June 2025 / Page 39-60

Upaya Penanggulangan Tindak Pidana Ransomware: Kajian Yuridis Terhadap PP No. 71 Tahun 2019 Tentang PSTE

Afriqil Wildan[1], Samsul Arifin[2]
[1,2] *University of Muhammadiyah Surabaya, Indonesia*

Article History;

Received

Revised

Accepted

ABSTRACT

This study analyzes and evaluates the effectiveness of Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PSTE) in combating ransomware crimes in Indonesia. The ever-evolving ransomware threat has triggered the need for regulations capable of adaptively responding to the dynamics of cybercrime. This study uses a normative juridical method with a qualitative approach to examine the urgency of implementation and obstacles in its implementation. The study results indicate that PP No. 71 of 2019 still faces various challenges, such as weak technical understanding, minimal coordination between agencies, limited legal sanctions, and a lack of technical guidance for prevention and mitigation. This study's recommendations include the development of detailed technical guidelines, strengthening the role of the National Cyber and Crypto Agency (BSSN), digital security education, and harmonization with the Personal Data Protection Law. A comprehensive and collaborative legal strategy is needed to build national cyber resilience in the face of ransomware threats.

Keywords: ransomware, cybersecurity, PSTE, regulation and Indonesia

INTRODUCTION

Perkembangan teknologi informasi dan komunikasi (TIK) di Indonesia telah mengalami kemajuan pesat dalam beberapa dekade terakhir (Huda, 2020). Inovasi di bidang digital, seperti internet, cloud computing, kecerdasan buatan (AI), dan Internet of Things (IoT), telah membuka peluang baru dalam berbagai sektor, mulai dari ekonomi, pendidikan, kesehatan, hingga pemerintahan (Muhammad Yusuf et al., 2023). Kemajuan ini juga mendorong transformasi digital di kalangan bisnis dan pemerintahan (Suryawijaya, 2023). Banyak perusahaan mulai beralih ke sistem digital untuk mengoptimalkan operasional mereka, sedangkan pemerintah juga memanfaatkan teknologi untuk meningkatkan kualitas layanan publik melalui konsep "e-government" (Sufianti, 2007). Penggunaan sistem elektronik dalam administrasi pemerintahan, misalnya, bertujuan untuk meningkatkan transparansi, mempercepat layanan kepada masyarakat, dan mengurangi birokrasi yang berbelit-belit. Perkembangan TIK

telah memberikan kontribusi signifikan terhadap pertumbuhan ekonomi dan pembangunan sosial di Indonesia (Novitasari, 2022).

Ancaman kejahatan siber terus berkembang seiring dengan meningkatnya penggunaan teknologi digital di berbagai sektor. Salah satu bentuk ancaman siber yang paling menonjol dan meresahkan adalah ransomware. Ransomware adalah jenis malware yang menginfeksi sistem komputer, mengenkripsi data penting, dan kemudian meminta tebusan kepada korban untuk mendapatkan kembali akses ke data tersebut. Serangan ini semakin sering terjadi karena para pelaku kejahatan siber menyadari potensi keuntungan besar dari metode ini, terutama jika targetnya adalah perusahaan atau instansi yang memiliki data sensitif dan tidak dapat menanggung gangguan operasional yang berkepanjangan. Metode pemerasan siber telah ada sejak tahun 1980-an. Sampel ransomware pertama berasal dari tahun 1989 dengan PC Cyborg Trojan (Taylor & Patel, 2017). Ransomware adalah jenis malware yang dirancang untuk memfasilitasi berbagai aktivitas jahat, seperti mencegah akses ke data pribadi kecuali tebusan dibayarkan (Khammas, 2020). Tebusan ini biasanya menggunakan mata uang kripto seperti Bitcoin, yang membuatnya sulit melacak penerima transaksi dan ideal bagi penyerang untuk menghindari lembaga penegak hukum (Kara & Aydos, 2020).

Pemerintah Indonesia telah mengambil langkah penting untuk mengatasi ancaman siber dengan mengeluarkan Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE). Meskipun Peraturan Pemerintah No. 71 Tahun 2019 telah mengatur penyelenggaraan sistem elektronik secara komprehensif, implementasinya di lapangan menghadapi beberapa tantangan mendasar. Salah satu isu utama adalah adanya kekosongan hukum mengenai penanganan kejahatan siber spesifik seperti ransomware, sehingga regulasi yang ada belum secara rinci mengatur mekanisme pencegahan maupun penanganannya. Kekosongan ini diperparah oleh kurangnya kesadaran dan kesiapan, baik di kalangan pelaku usaha maupun institusi pemerintah, dalam menghadapi risiko serangan ransomware. Di sisi lain, terdapat pula potensi benturan norma dengan regulasi lain, seperti UU ITE dan UU Perlindungan Data Pribadi, yang dapat menimbulkan kebingungan dalam implementasi di lapangan, terutama dalam hal pelaporan insiden dan perlindungan data yang terdampak serangan.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE) belum sepenuhnya mengakomodasi dinamika kejahatan siber terkini, khususnya dalam konteks ransomware. Meskipun PSTE mengatur berbagai aspek keamanan siber, implementasinya dalam menanggulangi kejahatan ransomware masih menghadapi tantangan. Berbagai jenis serangan ransomware, mulai dari yang menargetkan individu hingga infrastruktur kritis negara, menunjukkan keragaman metode dan dampak yang signifikan. Serangan ini memanfaatkan berbagai vektor, mulai dari email phishing yang mendistribusikan malware, hingga eksploitasi kerentanan sistem yang kurang terlindungi. Selain itu, perkembangan teknologi ransomware yang semakin canggih, seperti penggunaan enkripsi yang kuat dan teknik penyebaran yang lebih tersembunyi, menambah kompleksitas penanggulangannya. Meskipun UU ITE dan peraturan pelaksanaannya telah mengatur sanksi pidana bagi pelaku kejahatan siber, penegakan hukum masih menghadapi kendala, antara lain

kurangnya kesadaran masyarakat akan keamanan siber, terbatasnya sumber daya penegak hukum, dan kesulitan dalam melacak pelaku kejahatan transnasional. Oleh karena itu, diperlukan strategi yang komprehensif, yang meliputi peningkatan kesadaran masyarakat, peningkatan kapasitas penegak hukum, dan kolaborasi yang lebih erat antara pemerintah, sektor swasta, dan masyarakat dalam membangun ekosistem siber yang lebih aman dan tangguh untuk menghadapi ancaman ransomware yang terus berkembang.

Penelitian oleh Gilang Ramadhan (2023) membahas implementasi Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE) dalam menanggulangi kejahatan ransomware di Indonesia. Penelitian ini mengemukakan bahwa serangan ransomware, yang memberikan keuntungan finansial bagi para pelakunya, mendorong korban untuk membayar tebusan agar data mereka dipulihkan. Hal ini dapat menyebabkan kerugian finansial yang besar dan gangguan operasional bagi korban. Penelitian ini juga menyoroti bahwa serangan ransomware dapat menjadi kebiasaan bagi para pelaku kejahatan siber, karena mudahnya mengakses dan menyebarkan ransomware melalui internet. Dalam kajian yang lain, Aliya Putri Novita mengkaji dampak ransomware terhadap keamanan siber di Indonesia. Penelitian ini menjelaskan berbagai jenis ransomware, dampaknya terhadap individu dan organisasi, serta langkah-langkah pencegahan dan mitigasi yang dapat diambil.

Semua penelitian di atas menunjukkan bahwa ransomware merupakan ancaman serius terhadap keamanan siber di Indonesia, dengan dampak yang meluas, mulai dari kerugian finansial hingga gangguan operasional dan hilangnya data penting. Serangan ransomware juga menunjukkan kecenderungan untuk semakin mudah diakses dan disebarluaskan melalui internet, sehingga membutuhkan upaya yang lebih komprehensif untuk menanggulanginya. Namun dengan kenyataan bahwa masih banyak hukum yang kurang jelas dalam mengatur kejahatan ransomware di Indonesia, implementasi Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE) menjadi sangat penting, maka diperlukan lebih banyak lagi sumbangan akademis untuk menganalisis produk hukum yang ada. Dalam konteks ini, akan dilakukan analisis dan evaluasi terhadap Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE).

METHODS

Penelitian ini menggunakan metode yuridis normatif, yaitu penelitian hukum yang berfokus pada pengkajian norma-norma hukum yang berlaku, dengan pendekatan perundang-undangan, konseptual, dan kajian pustaka. Pendekatan perundang-undangan (statute approach) dilakukan dengan menganalisis ketentuan hukum yang relevan, khususnya Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE) serta Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya dalam Undang-Undang Nomor 19 Tahun 2016, guna memahami pengaturan mengenai kewajiban dan tanggung jawab penyelenggara sistem elektronik dalam mencegah dan menanggulangi ancaman ransomware. Pendekatan konseptual (conceptual approach) digunakan untuk mengkaji konsep-konsep keamanan siber, perlindungan data, dan

karakteristik serangan ransomware, sehingga memberikan pemahaman komprehensif mengenai dampak ancaman tersebut terhadap sistem elektronik serta penerapan prinsip-prinsip keamanan siber dalam kerangka hukum Indonesia. Selanjutnya, kajian pustaka (literature review) dilakukan dengan memanfaatkan berbagai sumber seperti buku, jurnal ilmiah, artikel akademik, laporan resmi, dan penelitian terdahulu yang relevan, guna memperkaya analisis dan memberikan perspektif teoritis maupun empiris terhadap permasalahan yang diteliti (Wiradipradja, 2015).

DISCUSSION AND RESULT

A. Urgensi Analisis dan Evaluasi Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE) dalam meningkatkan efektivitas pencegahan dan penanggulangan kejahatan ransomware di Indonesia

Urgensi analisis dan evaluasi terhadap Peraturan Pemerintah (PP) No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE) menjadi sangat krusial dalam konteks meningkatnya ancaman kejahatan siber, khususnya ransomware, di Indonesia. Perkembangan teknologi digital yang begitu pesat telah mendorong transformasi besar dalam kehidupan masyarakat, termasuk dalam bidang ekonomi, pemerintahan, hingga sosial budaya(Gulo et al., 2021). Namun, kemajuan ini juga membuka celah bagi pihak-pihak yang tidak bertanggung jawab untuk mengeksploitasi sistem elektronik demi keuntungan pribadi. Kejahatan ransomware, yakni jenis serangan siber yang mengenkripsi data dan meminta tebusan kepada korban, semakin marak terjadi dan menimbulkan kerugian signifikan baik secara finansial maupun strategis, khususnya bagi lembaga-lembaga vital seperti instansi pemerintahan, sektor kesehatan, pendidikan, dan perusahaan besar. Dalam konteks inilah, keberadaan regulasi seperti PP No. 71 Tahun 2019 menjadi penting untuk ditinjau kembali dari aspek efektivitasnya dalam memberikan perlindungan dan respons yang tepat terhadap kejahatan tersebut(Sulistyawati et al., 2022).

Peraturan Pemerintah No. 71 Tahun 2019 sebenarnya disusun untuk menggantikan PP No. 82 Tahun 2012 dan bertujuan untuk menyesuaikan regulasi dengan dinamika perkembangan teknologi dan kebutuhan hukum yang lebih adaptif terhadap transformasi digital. Peraturan ini memuat ketentuan mengenai penyelenggaraan sistem elektronik, perlindungan data pribadi, tanggung jawab penyelenggara sistem, serta pemenuhan prinsip keamanan sistem dan transaksi elektronik(Waron, 2023). Namun, dalam praktiknya, regulasi ini masih menghadapi tantangan serius dalam hal implementasi, pengawasan, dan integrasi dengan mekanisme perlindungan siber secara nasional. Kejahatan ransomware yang bersifat kompleks dan lintas batas, membutuhkan strategi penanganan yang tidak hanya berbasis pada norma administratif, tetapi juga menyentuh aspek teknis, penegakan hukum, serta kolaborasi multi-stakeholder secara terpadu(Wahyuni, 2021).

Evaluasi terhadap PP No. 71 Tahun 2019 menjadi mendesak karena regulasi ini belum secara eksplisit mengatur secara komprehensif mengenai jenis-jenis serangan siber seperti ransomware, mekanisme pencegahan dan

mitigasi, serta penanganan insiden yang terjadi. Meskipun peraturan ini menekankan pentingnya keamanan sistem dan perlindungan data, namun belum tersedia panduan teknis maupun standar nasional yang secara jelas mengarahkan penyelenggara sistem elektronik dalam membangun ketahanan siber yang memadai terhadap ancaman ransomware(F. Kurniawan et al., 2024). Hal ini membuat banyak penyelenggara sistem, terutama dari kalangan UMKM atau institusi non-teknis, masih belum memiliki kesiapan yang cukup dalam mengantisipasi serangan yang semakin canggih. Dalam konteks ini, diperlukan penguatan terhadap substansi regulasi yang lebih responsif terhadap dinamika ancaman siber kontemporer(Pratama Putra et al., 2023).

Dalam hal pengawasan dan penegakan hukum, PP No. 71 Tahun 2019 juga belum memberikan mandat yang kuat kepada otoritas siber nasional seperti Badan Siber dan Sandi Negara (BSSN) untuk bertindak secara proaktif dan terkoordinasi dengan lembaga lainnya dalam menangani insiden ransomware. Kejahatan siber yang bersifat masif dan cepat seperti ransomware membutuhkan respon yang tidak hanya reaktif, tetapi juga preventif melalui pemantauan sistem yang terintegrasi secara nasional(Angriani, 2021). Tanpa adanya kerangka kerja yang jelas dan kewenangan yang tegas, upaya pencegahan dan penanggulangan kejahatan ini akan selalu tertinggal dari modus operandi pelaku kejahatan yang semakin maju. Maka dari itu, urgensi revisi atau pembaruan regulasi dalam hal ini menjadi penting untuk memastikan adanya kepastian hukum, efektivitas koordinasi, serta respons yang cepat terhadap insiden.

Urgensi lainnya terletak pada perlunya integrasi PP No. 71 Tahun 2019 dengan kebijakan perlindungan data pribadi yang lebih kuat. Serangan ransomware kerap menargetkan data penting sebagai objek utama, dan regulasi yang tidak memberikan jaminan perlindungan data yang tegas dapat melemahkan kepercayaan publik terhadap sistem elektronik(Anugrah, 2020). Saat ini, meskipun Indonesia telah memiliki Undang-Undang Perlindungan Data Pribadi (UU PDP), harmonisasi antara UU tersebut dengan PP No. 71 Tahun 2019 harus segera diwujudkan agar tidak terjadi tumpang tindih ataupun kekosongan regulatif. Evaluasi ini juga harus memperhatikan praktik internasional dan standar global terkait cybersecurity, mengingat sifat serangan ransomware yang berskala global dan terhubung dengan jaringan siber internasional(Hilman, 2020).

Pentingnya analisis terhadap PP No. 71 Tahun 2019 juga berkaitan dengan perlunya pendekatan edukatif dan kolaboratif dalam upaya pencegahan ransomware. Regulasi seharusnya tidak hanya bersifat normatif, tetapi juga menjadi landasan bagi program literasi digital, peningkatan kapasitas SDM, dan pembangunan budaya keamanan siber di kalangan masyarakat dan sektor privat(Sinaga, 2022). Kejahatan siber seperti ransomware tidak hanya bisa dilawan dengan teknologi, tetapi juga dengan membangun kesadaran kolektif terhadap pentingnya keamanan data dan informasi. Peraturan ini perlu mengakomodasi ruang yang mendorong kolaborasi antara pemerintah, sektor swasta, akademisi, dan masyarakat sipil dalam memperkuat ekosistem keamanan digital nasional.

Dengan mempertimbangkan semua aspek tersebut, maka jelas bahwa analisis dan evaluasi mendalam terhadap PP No. 71 Tahun 2019 sangat diperlukan untuk menjawab tantangan baru di era digital. Ransomware bukan lagi ancaman masa depan, melainkan kenyataan yang tengah dihadapi saat ini oleh berbagai sektor penting di Indonesia. Ketika regulasi gagal mengikuti kecepatan evolusi ancaman digital, maka kerentanan terhadap serangan akan semakin besar(Khammas, 2020). Pemerintah perlu mengambil langkah strategis dengan merevisi, memperjelas, dan memperluas cakupan peraturan ini agar mampu menjadi instrumen hukum yang efektif dalam melindungi kepentingan nasional dari bahaya serangan ransomware. Tanpa pembaruan yang adaptif, risiko stagnasi hukum dan kerugian sistemik akan terus menghantui transformasi digital Indonesia.

Urgensi Penanggulangan Kejahatan Ransomware

Urgensi penanggulangan kejahatan ransomware menjadi isu yang semakin penting di era digital saat ini, di mana ketergantungan terhadap sistem informasi dan data elektronik menjadi fondasi utama dalam berbagai sektor kehidupan, baik pemerintahan, bisnis, pendidikan, hingga pelayanan publik. Ransomware merupakan salah satu bentuk serangan siber paling merugikan karena menyerang sistem komputer dengan mengenkripsi data penting milik korban, lalu meminta tebusan (ransom) sebagai syarat untuk mendapatkan kembali akses terhadap data tersebut(Utama, 2023). Kejahatan ini tidak hanya menyebabkan kerugian ekonomi yang besar, tetapi juga mengancam stabilitas operasional sebuah lembaga atau perusahaan, bahkan hingga pada level negara. Karena sifatnya yang destruktif dan kemampuannya menyebar secara cepat, maka penanggulangan kejahatan ini memerlukan pendekatan yang menyeluruh, sistematis, dan kolaboratif.

Ransomware tidak hanya menargetkan perusahaan-perusahaan besar, tetapi juga menyasar institusi pendidikan, fasilitas kesehatan, lembaga pemerintahan, bahkan individu. Ancaman ini meningkat seiring kemajuan teknologi yang membuka celah-celah kerentanan baru dalam sistem keamanan siber. Laporan dari berbagai lembaga keamanan digital menunjukkan bahwa serangan ransomware mengalami peningkatan signifikan dari tahun ke tahun, baik dari segi frekuensi maupun tingkat kerumitan serangannya. Hal ini menunjukkan bahwa para pelaku kejahatan siber juga semakin canggih dalam mengembangkan teknik dan strategi serangan. Urgensi penanggulangan ransomware tidak bisa lagi dianggap sebagai isu teknis semata, tetapi harus menjadi bagian dari strategi keamanan nasional dan korporasi yang lebih luas(Hartono, 2023).

Salah satu urgensi utama dalam penanggulangan kejahatan ransomware adalah perlindungan terhadap data. Di era digital, data merupakan aset yang sangat bernilai dan menjadi fondasi pengambilan keputusan. Kehilangan akses terhadap data, atau kebocoran data karena serangan ransomware, bisa berdampak pada reputasi organisasi, kepercayaan publik, dan kelangsungan operasional. Misalnya, dalam sektor pelayanan kesehatan, serangan ransomware terhadap sistem rumah sakit dapat menghambat pelayanan medis yang berdampak langsung terhadap

keselamatan pasien. Di sektor pendidikan, serangan terhadap sistem akademik bisa mengganggu proses belajar-mengajar dan distribusi informasi penting. Perlindungan data melalui strategi penanggulangan ransomware menjadi kebutuhan mendesak(McIntosh et al., 2023).

Urgensi penanggulangan ransomware juga menyangkut aspek ekonomi. Banyak organisasi dan individu yang mengalami kerugian finansial akibat keharusan membayar tebusan yang jumlahnya bisa mencapai ribuan hingga jutaan dolar AS. Biaya untuk pemulihan sistem, investigasi forensik digital, serta potensi denda hukum karena pelanggaran perlindungan data pribadi, semuanya merupakan konsekuensi ekonomi dari serangan ransomware. Tidak jarang pula, perusahaan kecil hingga menengah mengalami kebangkrutan akibat serangan ini karena tidak memiliki cadangan sistem yang memadai dan ketidaksiapan dalam menghadapi insiden siber. Pencegahan dan penanggulangan ransomware merupakan investasi penting dalam menjaga keberlanjutan ekonomi digital(Razaulla et al., 2023).

Urgensi penanggulangan ransomware juga berkaitan erat dengan upaya menjaga keamanan nasional. Ketika infrastruktur penting seperti sistem transportasi, jaringan listrik, sistem keuangan, hingga pertahanan negara menjadi target serangan siber, maka dampaknya bisa sangat serius terhadap stabilitas negara. Dalam konteks ini, ransomware tidak lagi hanya dilihat sebagai tindak kriminal biasa, melainkan sebagai potensi ancaman terhadap kedaulatan dan keamanan nasional. Negara-negara maju seperti Amerika Serikat dan Uni Eropa telah memasukkan isu serangan siber, termasuk ransomware, dalam kerangka kebijakan pertahanan dan keamanan nasional mereka. Indonesia pun perlu mengadopsi pendekatan yang serupa, termasuk penguatan kerangka hukum, pembentukan satuan siber nasional, dan kerja sama internasional dalam mengatasi kejahatan siber lintas batas(Mukhopadhyay & Jain, 2024).

Untuk merespons urgensi tersebut, strategi penanggulangan ransomware perlu dilakukan secara terintegrasi, dimulai dari aspek preventif hingga responsif. Aspek preventif mencakup edukasi dan peningkatan kesadaran pengguna mengenai pentingnya keamanan digital, pembaruan sistem keamanan secara berkala, penggunaan antivirus dan firewall yang kuat, serta penerapan kebijakan backup data yang efektif. Perusahaan dan lembaga pemerintahan juga perlu membangun kapasitas sumber daya manusia di bidang keamanan siber agar siap menghadapi ancaman siber secara tanggap dan cepat. Sementara pada aspek responsif, penting untuk memiliki prosedur tanggap darurat ketika terjadi serangan, termasuk tim respons insiden siber yang mampu mengisolasi, menganalisis, dan memulihkan sistem yang terkena dampak(Kapoor et al., 2022).

Di samping itu, regulasi yang mendukung penanggulangan ransomware perlu disempurnakan. Hukum positif di Indonesia terkait kejahatan siber memang telah diatur dalam UU ITE, namun implementasinya perlu diperkuat agar mampu menjangkau perkembangan modus kejahatan digital terbaru. Perlu juga ada peningkatan kerja sama antara pemerintah, sektor swasta, akademisi, dan komunitas teknologi

untuk membentuk ekosistem keamanan siber yang solid(Urooj et al., 2022). Koordinasi lintas sektor ini penting untuk mempercepat pertukaran informasi tentang potensi ancaman, teknik serangan terbaru, serta solusi penanggulangan yang efektif. Urgensi penanggulangan kejahatan ransomware tidak dapat dipandang sebelah mata. Ransomware bukan hanya persoalan teknis atau masalah keamanan jaringan, melainkan sudah menjadi isu multidimensi yang mencakup ekonomi, sosial, hukum, dan keamanan nasional. Pendekatan yang komprehensif, strategis, dan kolaboratif menjadi kunci dalam menghadapi dan menanggulangi ancaman ini secara efektif. Semakin cepat upaya ini dilakukan, semakin besar pula peluang untuk melindungi masyarakat dan infrastruktur digital dari kerugian yang tidak diinginkan(Cen et al., 2024).

Prosedur penanggulangan dan pencegahan

Prosedur penanggulangan dan pencegahan kejahatan siber, khususnya serangan ransomware, merupakan elemen kunci dalam menjaga integritas sistem informasi serta melindungi data dan aset digital dari kerugian yang sangat besar. Dalam konteks perkembangan teknologi informasi yang semakin masif, ancaman siber tidak hanya menjadi tanggung jawab teknisi atau departemen IT semata, melainkan sudah menjadi urusan strategis yang harus dijawab oleh semua level organisasi, termasuk pimpinan, pembuat kebijakan, serta individu pengguna(Ali, 2017). Prosedur penanggulangan dan pencegahan harus dirancang secara holistik dan berkesinambungan, dengan memperhatikan aspek teknis, kebijakan, dan kesadaran kolektif. Dalam merespons serangan ransomware, dibutuhkan suatu sistem prosedural yang mampu bekerja cepat dan tepat, mulai dari deteksi dini, respon insiden, hingga pemulihan pasca serangan. Demikian pula, upaya pencegahan perlu dirancang agar menyentuh akar permasalahan, termasuk celah keamanan dan perilaku pengguna yang rentan dimanfaatkan oleh pelaku kejahatan siber.

Tahap awal dalam prosedur penanggulangan dimulai dari kemampuan organisasi untuk melakukan deteksi dini terhadap adanya aktivitas mencurigakan dalam sistem. Deteksi dini sangat krusial karena semakin cepat ancaman dikenali, maka semakin kecil kerusakan yang ditimbulkan. Untuk mendukung hal ini, organisasi perlu mengimplementasikan perangkat lunak keamanan mutakhir seperti sistem deteksi intrusi (Intrusion Detection System/IDS), antivirus, firewall, dan alat monitoring jaringan secara real-time. Sistem ini harus dikonfigurasi dengan benar dan diperbarui secara berkala agar mampu mengenali varian ransomware terbaru yang terus berkembang. Selain perangkat lunak, peran tim keamanan siber juga penting dalam menganalisis pola-pola lalu lintas data dan memantau log aktivitas sistem untuk mencari indikasi serangan(Kapoh, 2020).

Apabila terdeteksi adanya serangan ransomware, maka langkah cepat yang harus dilakukan adalah isolasi terhadap sistem yang terinfeksi. Prosedur ini bertujuan untuk mencegah penyebaran ransomware ke perangkat atau jaringan lain. Sistem yang diserang harus segera diputus dari

jaringan internet dan intranet organisasi, serta dilakukan pemblokiran akses eksternal yang mencurigakan(Peraturan Pemerintah Republik Indonesia No 71, 2019). Setelah isolasi, tahap respon insiden harus dilaksanakan oleh tim tanggap darurat keamanan siber (Computer Security Incident Response Team/CSIRT) yang memiliki keahlian dalam menganalisis jenis ransomware yang menyerang, mengevaluasi tingkat kerusakan, serta menyusun strategi pemulihan. Tim ini juga bertanggung jawab untuk mendokumentasikan kronologi serangan, mengidentifikasi titik masuk, dan menilai celah keamanan yang dimanfaatkan pelaku. Dokumentasi ini penting tidak hanya untuk kebutuhan audit keamanan, tetapi juga sebagai pembelajaran guna memperkuat sistem di masa mendatang.

Setelah tahap respon insiden, organisasi harus segera masuk ke fase pemulihan data. Prosedur pemulihan ini akan sangat bergantung pada kesiapan organisasi dalam melakukan pencadangan data (backup). Jika backup dilakukan secara rutin dan disimpan di lokasi yang aman (baik offline maupun cloud), maka proses pemulihan dapat berjalan lebih cepat dan data dapat dikembalikan tanpa perlu memenuhi tuntutan pelaku ransomware. Salah satu prosedur pencegahan paling vital adalah implementasi kebijakan backup berkala yang disiplin dan aman(Prawesti, 2017). Backup data sebaiknya dilakukan secara otomatis dan diverifikasi secara rutin untuk memastikan integritas file tetap terjaga. Perlu ada pemisahan antara jaringan utama dengan media penyimpanan cadangan agar tidak ikut terinfeksi saat serangan terjadi.

Dalam konteks pencegahan yang bersifat jangka panjang, pembangunan budaya keamanan siber merupakan hal yang mutlak. Ini mencakup pelatihan dan edukasi berkala kepada seluruh pegawai atau anggota organisasi mengenai bahaya ransomware, cara mengidentifikasi email phishing, pentingnya menggunakan kata sandi yang kuat, dan larangan mengunduh perangkat lunak dari sumber yang tidak terpercaya. Edukasi ini penting karena banyak serangan ransomware berhasil karena kelalaian pengguna dalam mengklik tautan atau membuka lampiran yang mencurigakan. Literasi digital menjadi bagian dari prosedur pencegahan yang tidak kalah penting dibanding perangkat lunak keamanan(Hendratno et al., 2022).

Organisasi juga harus memiliki kebijakan keamanan yang tertulis dan terstruktur, termasuk prosedur standar operasional (SOP) saat menghadapi insiden, regulasi penggunaan perangkat kerja, pengaturan hak akses berdasarkan kebutuhan kerja, serta pengawasan terhadap aktivitas pengguna. Kebijakan ini harus dikaji ulang secara berkala agar selalu relevan dengan dinamika ancaman siber yang terus berkembang. Dalam implementasinya, perlu juga dilakukan audit keamanan informasi secara rutin oleh pihak internal maupun eksternal guna menilai efektivitas kebijakan serta mengidentifikasi potensi celah keamanan(Menko Perekonomian, 2020). Selain aspek internal organisasi, kolaborasi dengan pihak luar juga menjadi bagian penting dari prosedur penanggulangan dan pencegahan ransomware. Pemerintah, sektor swasta, penyedia teknologi, akademisi, hingga komunitas keamanan siber perlu menjalin kerja sama

untuk bertukar informasi mengenai pola-pola serangan terbaru, indikator kompromi (IoC), serta solusi teknis yang efektif. Pemerintah dalam hal ini berperan penting dalam menciptakan regulasi yang mendukung keamanan siber nasional, membentuk lembaga khusus yang bertugas menangani insiden, serta menyediakan kanal pelaporan yang responsif dan edukatif bagi publik(Sari et al., 2020).

Dapat disimpulkan bahwa prosedur penanggulangan dan pencegahan ransomware harus bersifat menyeluruh dan dijalankan secara berkelanjutan. Tidak cukup hanya mengandalkan teknologi, tetapi juga dibutuhkan kesadaran kolektif, kesiapan sistem, kapasitas sumber daya manusia, serta sinergi lintas sektor untuk membangun ketahanan siber yang tangguh. Di tengah meningkatnya kompleksitas ancaman siber, pendekatan yang proaktif dan adaptif menjadi kunci utama dalam menjaga keamanan informasi serta menjamin keberlangsungan operasional organisasi di era digital yang penuh risiko ini.

B. Evaluasi kendala dan tantangan dalam Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE) dalam menanggulangi kejahatan ransomware di Indonesia, dan bagaimana solusinya

Evaluasi terhadap Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE) mengungkap sejumlah kendala dan tantangan nyata dalam upaya penanggulangan kejahatan ransomware di Indonesia. Meskipun regulasi ini dirancang untuk memberikan kerangka hukum dalam penyelenggaraan sistem elektronik secara aman dan terpercaya, kenyataannya penerapannya di lapangan masih menghadapi berbagai hambatan(Wabnitz et al., 2018). Salah satu kendala utama adalah kurangnya pemahaman teknis di kalangan penyelenggara sistem elektronik, terutama di sektor-sektor non-teknis seperti lembaga pendidikan, pelayanan kesehatan, hingga usaha mikro, kecil, dan menengah (UMKM). Banyak institusi belum memiliki infrastruktur keamanan siber yang memadai dan tidak memahami secara rinci bagaimana membangun sistem yang tahan terhadap serangan ransomware. Ketentuan dalam PP No. 71 Tahun 2019 yang bersifat normatif dan umum belum cukup operasional untuk menjawab kebutuhan teknis di tingkat pelaksanaan. Misalnya, meskipun telah ditegaskan kewajiban penyelenggara sistem untuk menjamin kerahasiaan, keutuhan, dan ketersediaan informasi elektronik, namun tidak dijabarkan secara rinci standar keamanan minimal, mekanisme audit berkala, atau panduan teknis mitigasi ancaman ransomware(Mahira Dewantoro & Dian Alan Setiawan S.H., M.H., 2023).

Selain persoalan pemahaman teknis, tantangan lain yang muncul adalah lemahnya koordinasi antar instansi dalam penanganan insiden siber. Dalam konteks ransomware yang bersifat mendesak dan berdampak sistemik, respons yang terkoordinasi sangat krusial. Namun, evaluasi terhadap penerapan PP No. 71 Tahun 2019 menunjukkan bahwa tidak semua pihak, baik dari sektor publik maupun swasta, memiliki jalur komunikasi yang efektif ketika terjadi serangan(Takanjanji, 2021). Lembaga seperti BSSN

yang memiliki otoritas di bidang keamanan siber belum secara optimal dilibatkan dalam pengawasan dan bimbingan terhadap penyelenggara sistem elektronik yang rentan terhadap ransomware. Ketidakhadiran prosedur respons insiden yang terstandar dan disepakati lintas sektor menjadi celah besar dalam upaya penanggulangan secara menyeluruh. Ditambah lagi, tidak semua entitas memiliki kewajiban atau prosedur pelaporan insiden siber yang tegas, sehingga sering kali serangan ransomware tidak teridentifikasi secara sistematis, atau malah disembunyikan untuk menghindari reputasi buruk(Anisah & Eko Nurisman, 2022).

Tantangan lainnya adalah lemahnya penerapan sanksi hukum terhadap pelanggaran yang terkait dengan keamanan sistem elektronik. Dalam PP No. 71 Tahun 2019, mekanisme penegakan hukum terhadap penyelenggara sistem yang lalai atau gagal menjaga keamanan belum ditegaskan secara rinci dan implementatif(Munawaroh & Agasi, 2022). Hal ini menciptakan ruang abu-abu dalam tanggung jawab hukum, khususnya ketika ransomware menyerang dan menyebabkan kebocoran data atau kelumpuhan layanan publik. Akibatnya, tidak ada efek jera bagi penyelenggara sistem yang mengabaikan aspek keamanan siber, sehingga praktik pengelolaan sistem yang rentan terus berlangsung tanpa konsekuensi yang berarti. Dalam banyak kasus, pelaku ransomware juga sulit dilacak dan dihukum karena minimnya kerja sama internasional dalam penegakan hukum siber lintas negara.

Selain kendala struktural dan hukum, PP No. 71 Tahun 2019 juga menghadapi tantangan dalam konteks perkembangan teknologi yang sangat cepat. Ransomware terus berevolusi dalam bentuk dan cara penyebarannya, mulai dari teknik phishing yang lebih canggih hingga pemanfaatan celah keamanan dari sistem cloud atau Internet of Things (IoT). Namun, regulasi yang cenderung statis dan lambat menyesuaikan diri, membuat perlindungan hukum dan teknis yang diberikan menjadi usang dalam waktu singkat. Tanpa revisi regulasi yang dinamis dan berbasis risiko aktual, maka upaya perlindungan terhadap kejahatan siber termasuk ransomware akan selalu tertinggal(Ramadhani, 2023).

Untuk mengatasi berbagai kendala tersebut, perlu dirumuskan solusi yang bersifat holistik dan strategis. Salah satu solusi utama adalah perlunya penyusunan pedoman teknis yang lebih terperinci dan operasional sebagai turunan dari PP No. 71 Tahun 2019. Pedoman ini harus mencakup standar minimum keamanan siber, sistem audit dan pelaporan insiden, serta prosedur pemulihan pasca serangan ransomware(Zaenudin & Faridah, 2022). Pemerintah, melalui BSSN dan kementerian terkait, harus aktif menyosialisasikan dan memberikan bimbingan teknis secara berkala kepada penyelenggara sistem elektronik, terutama sektor-sektor vital yang belum memiliki kompetensi keamanan digital yang kuat. Edukasi dan pelatihan keamanan siber harus dijadikan program prioritas nasional yang menyasar berbagai lapisan penyelenggara sistem, baik dari sektor publik maupun swasta.

Solusi lainnya adalah memperkuat integrasi dan koordinasi lintas

instansi dalam hal pencegahan dan penanganan ransomware. Pemerintah perlu membentuk pusat koordinasi keamanan siber yang berfungsi sebagai titik temu antara regulator, penegak hukum, penyelenggara sistem elektronik, dan sektor swasta dalam merespons insiden siber secara cepat dan terarah(Yustitiana, 2021). Mekanisme pelaporan insiden harus dibuat wajib dan dilindungi, agar korban ransomware tidak ragu untuk melaporkan kejadian dan mendapatkan bantuan. BSSN sebagai lembaga otoritatif harus diberikan wewenang yang lebih luas untuk melakukan pemantauan langsung, memberikan rekomendasi kebijakan, dan menindak penyelenggara sistem yang melanggar prinsip keamanan siber.

Dari sisi penegakan hukum, PP No. 71 Tahun 2019 perlu diperkuat dengan perangkat hukum yang jelas terkait sanksi terhadap kelalaian keamanan sistem serta kerja sama internasional dalam pelacakan pelaku ransomware. Indonesia harus aktif membangun jaringan kerja sama global dalam penanggulangan kejahatan siber, mengingat pelaku ransomware sering kali berasal dari luar yurisdiksi nasional. Harmonisasi hukum nasional dengan konvensi internasional terkait cybercrime akan membantu mempercepat proses investigasi dan penindakan terhadap pelaku lintas negara(Fista et al., 2023).

Solusi jangka panjang yang tidak boleh diabaikan adalah membangun budaya keamanan digital di masyarakat. Ransomware kerap memanfaatkan kelengahan individu melalui email atau tautan yang tidak aman. Peningkatan literasi digital masyarakat secara luas menjadi fondasi penting dalam ekosistem keamanan siber(A. B. Kurniawan & Seskandhi, 2022). Pemerintah dan lembaga pendidikan harus berkolaborasi untuk memasukkan aspek keamanan digital dalam kurikulum, serta menyediakan kampanye publik yang masif tentang pencegahan kejahatan siber. Jika semua pihak dapat bekerja sama secara sinergis, maka tantangan yang dihadapi dalam implementasi PP No. 71 Tahun 2019 akan dapat diatasi dan regulasi ini akan benar-benar berfungsi sebagai instrumen perlindungan efektif dalam era digital yang penuh risiko.

Kelemahan Regulasi dan penegakan hukum

Kelemahan dalam regulasi dan penegakan hukum sering kali menjadi kendala utama dalam mencapai keadilan dan kepastian hukum di berbagai sektor kehidupan masyarakat, baik itu di ranah sosial, ekonomi, hingga dunia digital. Regulasi yang lemah dapat menyebabkan ruang bagi pelanggaran hukum, korupsi, atau ketidakadilan yang merugikan pihak tertentu, sementara penegakan hukum yang tidak tegas dan tidak konsisten mengurangi efektivitas dari peraturan tersebut(Alraizza & Algarni, 2023). Salah satu masalah utama dalam penerapan regulasi adalah kurangnya kejelasan dalam pembentukan kebijakan yang dapat diterima oleh seluruh lapisan masyarakat. Ketidakjelasan atau ambiguitas dalam aturan sering kali membuka peluang untuk interpretasi yang berbeda-beda, yang pada gilirannya menciptakan ketidakpastian hukum.

Regulasi yang ada sering kali tidak dapat mengikuti dinamika perkembangan zaman, terutama dalam menghadapi tantangan baru seperti perkembangan teknologi yang pesat. Misalnya, dalam hal kejahatan siber,

banyak peraturan yang belum sepenuhnya mengatur cara menangani tindak kejahatan digital, seperti peretasan, pencurian data, atau penyebaran informasi yang merugikan. Ketika peraturan tidak mampu mengikuti perkembangan tersebut, pihak yang terlibat dalam tindakan melawan hukum sering kali berhasil lolos dari jeratan hukum. Ini menunjukkan bahwa regulasi yang ada harus terus diperbarui dan disesuaikan dengan tantangan baru yang muncul(Begovic et al., 2023).

Masalah lain terkait kelemahan regulasi adalah ketidakserasian antara regulasi yang ada dengan implementasi di lapangan. Dalam banyak kasus, meskipun terdapat peraturan yang cukup baik di atas kertas, namun pada tingkat pelaksanaannya sering kali tidak berjalan dengan efektif. Hal ini bisa disebabkan oleh beberapa faktor, seperti kurangnya pemahaman atau pelatihan bagi aparat penegak hukum, kurangnya sumber daya untuk menjalankan tugas, atau bahkan adanya niat buruk di antara pihak-pihak yang diberi tanggung jawab untuk menegakkan peraturan(Humayun et al., 2021). Dalam beberapa situasi, aparat penegak hukum mungkin kurang memahami atau memiliki ketidakmampuan dalam menerapkan aturan yang berlaku dengan konsisten, yang menyebabkan terjadinya kesenjangan antara apa yang tertulis dalam regulasi dengan apa yang diterapkan di lapangan.

Kelemahan dalam penegakan hukum juga sering kali berhubungan dengan masalah birokrasi yang berlarut-larut. Prosedur yang panjang dan rumit dalam sistem hukum sering kali menghalangi upaya penegakan hukum yang cepat dan efektif. Proses yang memakan waktu lama tidak hanya merugikan pihak yang berperkara, tetapi juga dapat mengurangi efektivitas dari sanksi hukum itu sendiri. Dalam konteks ini, penegakan hukum yang lambat memberikan kesan bahwa hukum tidak bisa berfungsi sebagai alat yang mendidik masyarakat untuk mematuhi peraturan yang ada, sehingga menurunkan tingkat kepatuhan hukum dalam masyarakat(Oz et al., 2022). Tidak hanya itu, faktor lain yang turut memperburuk penegakan hukum adalah ketidaksesuaian antara jenis hukuman dengan kejahatan yang dilakukan. Dalam beberapa kasus, hukuman yang dijatuhkan dianggap tidak setimpal dengan kejahatan yang terjadi. Ini sering kali menciptakan ketidakpuasan publik dan menurunkan rasa keadilan dalam masyarakat. Misalnya, dalam kasus korupsi yang melibatkan pejabat tinggi negara, sering kali hukuman yang dijatuhkan tidak sebanding dengan kerugian yang ditimbulkan. Masyarakat akan merasa bahwa penegakan hukum hanya berlaku untuk kalangan tertentu, sementara mereka yang memiliki kekuasaan atau uang dapat dengan mudah menghindari hukuman yang setimpal. Ini menciptakan ketimpangan dalam sistem hukum dan merusak kepercayaan masyarakat terhadap institusi penegak hukum.

Lemahnya koordinasi antar lembaga yang bertanggung jawab dalam penegakan hukum turut berkontribusi pada ketidakefektifan penerapan regulasi. Banyak masalah hukum yang melibatkan lebih dari satu instansi atau sektor, dan jika koordinasi antar lembaga tersebut tidak terjalin dengan baik, maka penyelesaian masalah dapat tertunda atau bahkan terhambat. Misalnya, dalam kasus kejahatan yang melibatkan data pribadi atau

kejahatan dunia maya, dibutuhkan kolaborasi antara instansi kepolisian, regulator, dan perusahaan penyedia layanan internet untuk mengumpulkan bukti dan menghukum pelaku. Tanpa adanya koordinasi yang baik, kasus tersebut bisa menjadi tidak jelas atau bahkan tidak dapat diselesaikan. Lemahnya penegakan hukum juga dapat disebabkan oleh faktor politik dan ekonomi yang mempengaruhi keputusan-keputusan hukum(Mukhopadhyay & Jain, 2024). Dalam beberapa kasus, kepentingan politik atau ekonomi dapat menghalangi proses hukum yang seharusnya dijalankan dengan adil dan transparan. Tekanan dari pihak-pihak tertentu yang memiliki pengaruh dalam dunia politik atau ekonomi sering kali membuat penegakan hukum terdistorsi, baik itu dalam bentuk penundaan proses, pengaruh dalam penyelidikan, ataupun dalam penjatuhan hukuman yang tidak adil. Fenomena ini menunjukkan bahwa regulasi yang sudah ada tidak akan memiliki pengaruh signifikan tanpa adanya kemauan politik yang kuat untuk menegakkannya dengan penuh integritas dan ketegasan.

Masyarakat juga memegang peran penting dalam menilai dan memperbaiki kelemahan regulasi serta penegakan hukum. Jika masyarakat kurang peduli atau tidak memahami pentingnya sistem hukum yang berlaku, maka mereka cenderung mengabaikan aturan yang ada dan lebih banyak mengandalkan jalan pintas atau cara yang tidak sah. Penting bagi pemerintah dan lembaga hukum untuk terus menyosialisasikan pentingnya kepatuhan terhadap hukum serta meningkatkan pemahaman publik mengenai regulasi yang berlaku.

Keterbatasan Norma dalam Mengatur Pencegahan dan Penanggulangan Ransomware

Keterbatasan norma dalam mengatur pencegahan dan penanggulangan ransomware merupakan salah satu tantangan besar dalam menghadapi ancaman siber yang semakin berkembang pesat. Ransomware, yang merupakan jenis perangkat lunak berbahaya yang mengunci data korban dan meminta tebusan untuk membukanya, telah menjadi ancaman global yang merugikan banyak sektor, mulai dari individu hingga perusahaan besar dan bahkan lembaga pemerintahan. Namun, meskipun ransomware semakin sering muncul dan menimbulkan kerugian finansial serta merusak infrastruktur digital, regulasi yang ada masih terbatas dalam menangani ancaman ini secara efektif. Salah satu keterbatasan utama adalah ketidakmampuan norma hukum yang ada untuk mengikuti perkembangan teknologi yang begitu cepat(Pemerintah RI, 2019).

Di banyak negara, hukum siber dan regulasi terkait masih sangat terbatas dalam hal cakupan dan relevansi terhadap ancaman-ancaman baru, seperti ransomware. Banyak undang-undang dan kebijakan yang ada lebih berfokus pada kejahatan siber secara umum, seperti peretasan dan pencurian data, namun kurang memberikan penanganan yang khusus terhadap jenis kejahatan siber ini. Ransomware, dengan karakteristiknya yang terus berkembang dan berubah, tidak selalu dapat diatur secara efektif oleh hukum yang ada. Misalnya, adanya kesulitan dalam menilai siapa yang seharusnya bertanggung jawab, baik itu pelaku, penyedia layanan yang

tidak aman, atau pihak yang menerima tebusan. Pada kenyataannya, dalam banyak kasus ransomware, peraturan yang ada tidak dapat dengan jelas mengatur alur tindakan yang harus diambil oleh korban maupun pihak berwenang untuk menanggulangi ancaman tersebut(Rumlus & Hartadi, 2020).

Regulasi yang ada seringkali lebih berfokus pada dampak yang sudah terjadi, yaitu pemulihan setelah serangan, bukan pada pencegahan atau mitigasi sebelum serangan terjadi. Hal ini mengarah pada pendekatan yang reaktif, bukan proaktif. Seringkali, hukum baru akan bertindak setelah kerugian terjadi, misalnya setelah perusahaan atau individu menjadi korban ransomware. Upaya untuk mencegah serangan ini seringkali terhambat oleh kurangnya kewajiban bagi entitas yang memiliki data atau infrastruktur untuk secara proaktif mengimplementasikan sistem keamanan yang memadai(Utama, 2023). Meskipun beberapa negara telah mulai mengeluarkan kebijakan yang mengharuskan perusahaan untuk memperkuat proteksi data mereka, regulasi ini belum sepenuhnya mencakup masalah teknis yang lebih spesifik dalam pencegahan ransomware, seperti penggunaan perangkat lunak yang terus diperbarui dan sistem backup data yang memadai.

Keterbatasan norma juga tercermin dalam kurangnya kesepahaman internasional mengenai cara menangani ancaman ransomware. Kejahatan siber bersifat transnasional, artinya pelaku kejahatan tidak terikat pada batas negara, dan serangan dapat berasal dari luar negeri. Namun, hukum yang mengatur kejahatan siber seringkali bersifat lokal atau nasional, yang menyulitkan penegakan hukum di tingkat internasional. Negara-negara yang memiliki regulasi yang lebih ketat dalam menghadapi ransomware bisa jadi tidak dapat menegakkan hukum tersebut terhadap pelaku yang berada di negara dengan peraturan yang lebih longgar atau tidak ada sama sekali. Hal ini menyebabkan ketidakmampuan norma untuk mengatasi masalah yang lebih luas terkait dengan kejahatan siber lintas batas(Hartono, 2023).

Dalam banyak kasus, regulasi terkait pencegahan ransomware sering kali tidak memperhitungkan dampak sosial dan ekonomi yang lebih luas. Serangan ransomware dapat mengganggu operasional bisnis, merusak kepercayaan konsumen, serta merugikan sektor-sektor yang sangat bergantung pada data dan teknologi, seperti rumah sakit, lembaga pemerintahan, dan industri keuangan. Namun, norma hukum yang ada seringkali kurang memperhatikan aspek pemulihan yang lebih luas, seperti dukungan kepada korban untuk pulih dari dampak sosial dan ekonomi jangka panjang(McIntosh et al., 2023). Tanpa adanya regulasi yang menanggulangi dampak ini secara menyeluruh, korban mungkin hanya menerima kompensasi yang terbatas atau tidak sama sekali, sementara organisasi yang terlibat dalam penanggulangan serangan juga tidak mendapatkan perlindungan yang cukup untuk mengurangi kerugian yang terjadi.

Tantangan lain adalah keterbatasan sumber daya untuk menegakkan hukum yang mengatur kejahatan siber seperti ransomware. Penegakan

hukum terhadap serangan ransomware memerlukan sumber daya yang besar, mulai dari teknologi canggih untuk memantau dan melacak serangan, hingga pengembangan keahlian dan pelatihan bagi aparat penegak hukum(Peraturan Pemerintah Republik Indonesia, 2012). Namun, di banyak negara, terutama negara berkembang, keterbatasan anggaran dan infrastruktur membuat penegakan hukum terhadap kejahatan siber menjadi sangat sulit. Dalam beberapa kasus, aparat penegak hukum mungkin kurang terlatih atau tidak memiliki akses ke teknologi terbaru untuk mendeteksi dan mengatasi ancaman ransomware secara efektif. Banyak lembaga dan perusahaan yang juga tidak siap untuk menghadapi ancaman ini, mengingat kurangnya pemahaman tentang cara mengelola risiko ransomware, baik secara teknis maupun dalam hal kebijakan internal.

Keterbatasan norma juga tercermin dalam masalah etika terkait dengan pembayaran tebusan. Beberapa pihak berpendapat bahwa membayar tebusan kepada peretas hanya akan memberi insentif bagi mereka untuk terus melakukan serangan. Namun, dalam beberapa kasus, terutama bagi korban yang tidak memiliki salinan cadangan data atau infrastruktur yang cukup kuat, membayar tebusan mungkin dianggap sebagai satu-satunya jalan untuk memulihkan data yang hilang. Regulasi yang ada seringkali tidak dapat memberikan panduan yang jelas mengenai keputusan ini, sehingga organisasi sering kali terjebak dalam dilema etis yang besar.

Rekomendasi Penguatan dan Strategi Perbaikan Regulasi

Penguatan dan strategi perbaikan regulasi dalam menghadapi ancaman ransomware menjadi hal yang sangat penting untuk menjaga integritas dan keamanan sistem digital di berbagai sektor. Mengingat tingginya kerugian yang ditimbulkan akibat serangan ransomware, baik dari sisi finansial maupun reputasi, regulasi yang ada saat ini perlu diperbarui agar dapat memberikan perlindungan yang lebih efektif bagi individu, organisasi, dan negara. Salah satu langkah utama dalam penguatan regulasi adalah dengan mengadaptasi kebijakan hukum untuk mengikuti perkembangan teknologi yang terus berkembang. Regulasi yang ada saat ini sering kali terjebak dalam ketidakmampuan untuk mengikuti perubahan cepat di dunia siber, terutama dalam hal serangan siber yang lebih canggih seperti ransomware. Diperlukan perbaikan regulasi yang dapat mengakomodasi tantangan baru yang muncul akibat ancaman ransomware(Agusta, 2022).

Salah satu langkah awal dalam memperkuat regulasi adalah dengan memperbarui undang-undang yang ada terkait dengan kejahatan siber. Peraturan yang ada saat ini sering kali lebih berfokus pada jenis kejahatan siber yang lebih umum, seperti peretasan atau pencurian data, tanpa memberikan perhatian khusus pada ransomware yang memiliki karakteristik unik(Rumlus & Hartadi, 2020). Ransomware, yang sering kali melibatkan permintaan tebusan untuk data yang dikunci atau sistem yang dibajak, memerlukan pengaturan yang lebih rinci dan spesifik dalam hukum. Pemerintah perlu mengembangkan dan mengimplementasikan

regulasi yang tidak hanya mengatur tentang hukuman terhadap pelaku, tetapi juga tentang kewajiban bagi organisasi dan individu untuk mengimplementasikan langkah-langkah pencegahan yang lebih baik, seperti pembaruan perangkat lunak secara berkala, penguatan sistem backup, dan pelatihan keamanan siber yang komprehensif bagi seluruh pihak yang terlibat.

Strategi perbaikan lainnya adalah dengan memperkenalkan regulasi yang mendorong kerja sama internasional dalam menanggulangi ransomware. Kejahatan siber bersifat transnasional, yang berarti pelaku dapat beroperasi di luar batas-batas negara, mempersulit penegakan hukum yang bersifat nasional. Negara-negara harus bekerja sama lebih erat dalam menciptakan kerangka hukum internasional yang dapat mengatasi ancaman ransomware secara global. Regulasi internasional ini perlu mencakup aturan mengenai ekstradisi pelaku ransomware, prosedur untuk berbagi informasi mengenai serangan siber, serta pembentukan mekanisme respons bersama yang dapat mengurangi dampak serangan. Pembentukan kerangka kerja internasional ini akan memberikan dasar hukum yang lebih kuat untuk penegakan hukum terhadap pelaku ransomware yang beroperasi lintas negara(Perdana et al., 2022).

Penting juga untuk mengintegrasikan pendekatan pencegahan yang lebih komprehensif dalam regulasi yang ada. Regulasinya harus mencakup kewajiban bagi organisasi untuk mengimplementasikan kebijakan keamanan yang lebih ketat, termasuk enkripsi data, proteksi terhadap perangkat yang terhubung ke internet, serta pemantauan yang lebih intensif terhadap potensi ancaman. Peraturan juga harus memprioritaskan pelatihan dan kesadaran siber bagi seluruh anggota organisasi, dari tingkat manajerial hingga staf operasional(Asri Agustiwi, 2016). Sebagian besar serangan ransomware berhasil dilakukan karena kelemahan dalam kesadaran dan kebijakan keamanan yang kurang efektif. Regulasi yang mendorong kesadaran akan ancaman ini dan memberikan pedoman jelas tentang cara menanggulanginya sangat diperlukan. Regulasi yang mengharuskan pelatihan rutin dan evaluasi keberlanjutan kebijakan keamanan akan memperkuat ketahanan organisasi terhadap serangan ransomware.

Regulasi yang ada juga harus dapat mengatur dengan jelas soal pembayaran tebusan yang seringkali menjadi dilema bagi korban ransomware. Beberapa pihak berpendapat bahwa membayar tebusan hanya akan memperburuk situasi dan memberi insentif bagi pelaku untuk terus melanjutkan aksi mereka. Namun, dalam banyak kasus, korban merasa terpaksa membayar tebusan untuk mendapatkan kembali akses ke data atau sistem yang terkunci(Pemerintah Indonesia, 2019). Regulasi yang memperjelas posisi hukum terkait pembayaran tebusan dan memberikan pedoman bagi korban tentang langkah yang tepat dalam menghadapi ancaman ransomware sangat penting. Beberapa negara telah melarang pembayaran tebusan kepada pelaku kejahatan siber, tetapi regulasi ini harus diimbangi dengan kebijakan yang jelas mengenai langkah-langkah pemulihan dan dukungan bagi korban, sehingga mereka tidak merasa terjebak dalam pilihan yang hanya mengarah pada pemberian uang kepada

pelaku.

Strategi perbaikan regulasi lainnya adalah dengan mendorong penguatan pengawasan dan penegakan hukum. Pemerintah harus memastikan bahwa lembaga penegak hukum memiliki sumber daya dan keahlian yang cukup untuk menangani kasus-kasus ransomware secara efektif. Ini termasuk pelatihan khusus dalam hal kejahatan siber dan penanganan bukti digital. Penegakan hukum yang lebih ketat diperlukan untuk menanggulangi serangan ransomware, dengan memberikan sanksi yang lebih berat bagi pelaku, serta memberdayakan aparat penegak hukum untuk dapat mengidentifikasi dan mengejar pelaku secara lebih cepat. Regulasi juga perlu mengatur dengan lebih rinci mengenai mekanisme pemberian sanksi terhadap perusahaan atau organisasi yang gagal memenuhi standar keamanan siber yang ditetapkan oleh hukum(Sitokdana, 2019).

Penting untuk ditekankan bahwa perbaikan regulasi ini harus mengutamakan kolaborasi antara sektor publik dan swasta. Banyak sektor swasta yang mengelola data sensitif dan infrastruktur penting yang menjadi target utama ransomware, sehingga mereka memiliki peran yang sangat penting dalam memitigasi risiko ini. Regulasi yang mengharuskan sektor swasta untuk berinvestasi dalam sistem keamanan yang lebih baik dan untuk berkolaborasi dengan pihak berwenang dalam berbagi informasi mengenai ancaman siber akan sangat membantu dalam upaya pencegahan dan penanggulangan ransomware. Pemerintah juga dapat mendorong sektor swasta untuk mengembangkan teknologi yang lebih canggih dalam mendeteksi dan mencegah serangan ransomware.

CONCLUSION

Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE) merupakan regulasi penting yang memberikan kerangka hukum dalam penyelenggaraan sistem elektronik di Indonesia. Namun, dalam konteks pencegahan dan penanggulangan kejahatan ransomware, implementasi regulasi ini masih menghadapi berbagai kendala, mulai dari kurangnya pemahaman teknis, lemahnya koordinasi antar lembaga, minimnya mekanisme penegakan hukum yang tegas, hingga tantangan adaptasi terhadap dinamika teknologi yang terus berkembang. Ketentuan normatif dalam PP No. 71 Tahun 2019 belum cukup operasional untuk menjawab tantangan teknis dan praktis di lapangan. Kejahatan ransomware yang bersifat lintas batas dan terus berevolusi menuntut respons yang cepat, adaptif, dan berbasis kolaborasi yang kuat antar pemangku kepentingan. Efektivitas regulasi ini sangat bergantung pada keberanian pemerintah dalam mengevaluasi, memperbarui, dan memperkuat kebijakan secara komprehensif dan responsif terhadap perkembangan ancaman siber.

Saran

Untuk meningkatkan efektivitas PP No. 71 Tahun 2019 dalam menghadapi ancaman ransomware, diperlukan langkah-langkah strategis.

Pertama, pemerintah perlu menyusun pedoman teknis turunan yang lebih rinci dan implementatif, termasuk standar minimum keamanan sistem, prosedur penanganan insiden, serta mekanisme audit dan pelaporan yang wajib. Kedua, memperkuat kapasitas lembaga seperti BSSN dalam hal pemantauan, koordinasi, dan intervensi terhadap penyelenggara sistem elektronik yang rentan terhadap serangan siber. Ketiga, membangun sistem pelaporan insiden yang terintegrasi secara nasional serta memperluas edukasi dan literasi digital di berbagai sektor, termasuk pendidikan, pemerintahan, dan industri. Keempat, mempertegas sanksi hukum terhadap penyelenggara sistem yang lalai, sekaligus memperluas kerja sama internasional dalam rangka penegakan hukum terhadap pelaku kejahatan siber lintas negara. Terakhir, pemerintah dan seluruh elemen masyarakat harus berperan aktif dalam membangun budaya keamanan digital sebagai pilar utama ketahanan siber nasional di era transformasi digital yang kian kompleks.

REFERENCES

Agusta, H. (2022). Telaah Yuridis Aplikasi Zoom Dalam Mengumpulkan Data Pribadi Ditinjau Dari Peraturan Pemerintah No. 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik. *KRTHA BHAYANGKARA*, *16*(1). https://doi.org/10.31599/krtha.v16i1.1076

Ali, A. M. (2017). Aspek Pendokumentasian Rekam Medis Elektronim Ditinjau dari Peraturan Pemerintah Nomor 82 Tahun 2012 Tentang Penyelenggaraan SIstem dan Transaksi Elektronik (Studi Kasus Rumah Sakit Columbia Asia Semarang). In *Masters thesis, Unika Soegijapranata* (Issue 2).

Alraizza, A., & Algarni, A. (2023). Ransomware Detection Using Machine Learning: A Survey. In *Big Data and Cognitive Computing* (Vol. 7, Issue 3). https://doi.org/10.3390/bdcc7030143

Angriani, P. (2021). Perlindungan Hukum terhadap Data Pribadi dalam Transaksi E-Commerce: Perspektif Hukum Islam dan Hukum Positif. *DIKTUM: Jurnal Syariah Dan Hukum*, *19*(2), 149–165.

Anisah, A. P., & Eko Nurisman. (2022). Cyberstalking: Kejahatan Terhadap Perlindungan Data Pribadi Sebagai Pemicu Tindak Pidana. *KRTHA BHAYANGKARA*, *16*(1). https://doi.org/10.31599/krtha.v16i1.1047

Anugrah, D. (2020). PERLINDUNGAN HUKUM TERHADAP NASABAH KORBAN DUPLIKASI DATA BANK DI INDONESIA. *JURNAL AKTA YUDISIA*, *5*(1). https://doi.org/10.35334/ay.v5i1.1205

Asri Agustiwi, S. A. D. (2016). PERLINDUNGAN HUKUM TERHADAP KONSUMEN DALAM TRANSAKSI JUAL BELI SECARA ELEKTRONIK DI INDONESIA. *UNIFIKASI : Jurnal Ilmu Hukum*, *3*(2). https://doi.org/10.25134/unifikasi.v3i2.409

Begovic, K., Al-Ali, A., & Malluhi, Q. (2023). Cryptographic ransomware encryption detection: Survey. *Computers and Security*, *132*. https://doi.org/10.1016/j.cose.2023.103349

Cen, M., Jiang, F., Qin, X., Jiang, Q., & Doss, R. (2024). Ransomware early detection: A survey. In *Computer Networks* (Vol. 239). https://doi.org/10.1016/j.comnet.2023.110138

Fista, Y. L., Aris Machmud, & Suartini, S. (2023). Perlindungan Hukum Konsumen Dalam Transaksi E-commerce Ditinjau dari Perspektif Undang-Undang Perlindungan Konsumen. *Binamulia Hukum*, *12*(1). https://doi.org/10.37893/jbh.v12i1.599

Gulo, A. S., Lasmadi, S., & Nawawi, K. (2021). Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *PAMPAS: Journal of Criminal Law*, *1*(2). https://doi.org/10.22437/pampas.v1i2.9574

Hartono, B. (2023). Ransomware: Memahami Ancaman Keamanan Digital. *Bincang Sains Dan Teknologi*, *2*(02). https://doi.org/10.56741/bst.v2i02.353

Hendratno, L., Erly Pangestuti, & Aulia Rahman Hakim. (2022). Perlindungan Hukum Bagi Korban Transaksi Jual Beli Online Di Indonesia. *Yustitiabelen*, *8*(2). https://doi.org/10.36563/yustitiabelen.v8i2.565

Hilman, D. (2020). Tindak Pidana Agama Menurut Perspektif Hukum Islam, Hukum Positif dan Hak Asasi Manusia. *Mizan: Journal of Islamic Law*, *4*(1). https://doi.org/10.32507/mizan.v4i1.593

Huda, I. A. (2020). Perkembangan Teknologi Informasi Dan Komunikasi (Tik) Terhadap Kualitas Pembelajaran Di Sekolah Dasar. *Jurnal Pendidikan Dan Konseling (JPDK)*, *2*(1), 121–125. https://doi.org/10.31004/jpdk.v1i2.622

Humayun, M., Jhanjhi, N. Z., Alsayat, A., & Ponnusamy, V. (2021). Internet of things and ransomware: Evolution, mitigation and prevention. In *Egyptian Informatics Journal* (Vol. 22, Issue 1). https://doi.org/10.1016/j.eij.2020.05.003

Kapoh, S. J. (2020). KAJIAN HUKUM PENERAPAN KONTRAK BAKU ELEKTRONIK PADA TRANSAKSI E-COMMERCE. *LEX ET SOCIETATIS*, *8*(3). https://doi.org/10.35796/les.v8i3.30671

Kapoor, A., Gupta, A., Gupta, R., Tanwar, S., Sharma, G., & Davidson, I. E. (2022). Ransomware detection, avoidance, and mitigation scheme: A review and future directions. In *Sustainability (Switzerland)* (Vol. 14, Issue 1). https://doi.org/10.3390/su14010008

Kara, I., & Aydos, M. (2020). Cyber Fraud : Detection and Analysis of the. *2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON*, 0764–0769.

Khammas, B. M. (2020). Ransomware Detection using Random Forest Technique. *ICT Express*, *6*(4), 325–331. https://doi.org/10.1016/j.icte.2020.11.001

Kurniawan, A. B., & Seskandhi, H. (2022). Perlindungan Hukum Kepada Pengguna Elektronik Banking Atas Kejahatan Carding Ditinjau Dari Undang-Undang Informasi dan Transaksi Elektronik. *Supremasi Jurnal Hukum*, *5*(01).

Kurniawan, F., Suhariyanto, D., & Hartana. (2024). Perlindungan Konsumen Terhadap Pinjaman Online Atas Penyebaran Data Pribadi. *INNOVATIVE: Journal Of Social Science Research*, *4*(1), 2817–2829.

Mahira Dewantoro, N., & Dian Alan Setiawan S.H., M.H. (2023). Penegakan Hukum Kejahatan Siber Berbasis Phising dalam Bentuk Application Package Kit (APK) Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *Bandung Conference Series: Law Studies*, *3*(2). https://doi.org/10.29313/bcsls.v3i2.7247

McIntosh, T., Kayes, A. S. M., Chen, Y. P. P., Ng, A., & Watters, P. (2023). Applying staged event-driven access control to combat ransomware. *Computers and Security*, *128*. https://doi.org/10.1016/j.cose.2023.103160

Menko Perekonomian. (2020). UU Cipta kerja dorong pengembangan dan digitalisasi UMKM di Indonesia. *Siaran Pers*, *11*.

Muhammad Yusuf, Dwi Julianingsih, & Tarisya Ramadhani. (2023). Transformasi Pendidikan Digital 5.0 melalui Integrasi Inovasi Ilmu Pengetahuan dan Teknologi. *Jurnal MENTARI: Manajemen, Pendidikan Dan Teknologi Informasi*, *2*(1), 11–19. https://doi.org/10.33050/mentari.v2i1.328

Mukhopadhyay, A., & Jain, S. (2024). A framework for cyber-risk insurance against ransomware: A mixed-method approach. *International Journal of Information Management*, *74*. https://doi.org/10.1016/j.ijinfomgt.2023.102724

Munawaroh, M., & Agasi, E. E. K. (2022). Tindak Pidana Pelecehan Seksual di Media Sosial Perspektif UU ITE. *Rechtenstudent*, *3*(1). https://doi.org/10.35719/rch.v3i1.101

Novitasari, A. T. (2022). Kontribusi Umkm Terhadap Pertumbuhan Ekonomi Era Digitalisasi Melalui Peran Pemerintah. *JABE (Journal of Applied Business and Economic)*, *9*(2), 184. https://doi.org/10.30998/jabe.v9i2.13703

Oz, H., Aris, A., Levi, A., & Uluagac, A. S. (2022). A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions. *ACM Computing Surveys*, *54*(11s). https://doi.org/10.1145/3514229

Pemerintah Indonesia. (2019). Peraturan Pemerintah No. 71 tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. In *Pemerintah RI*.

Pemerintah RI. (2019). Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. *Pemerintah RI*.

Peraturan Pemerintah Republik Indonesia. (2012). PENYELENGGARAAN SISTEM DAN TRANSAKSI ELEKTRONIK. *PERATURAN PEMERINTAH REPUBLIK INDONESIA*, *Kolisch 1996*.

Peraturan Pemerintah Republik Indonesia No 71. (2019). Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik. *Media Hukum*, *7*(2).

Perdana, A. P., Muttaqin, A., & Arief, S. (2022). Perlindungan Hukum Konsumen dalam Jual Beli Online dengan Jasa Escrow. *Notary Law Journal*, *1*(2). https://doi.org/10.32801/nolaj.v1i2.14

Pratama Putra, R., Saputra, H., Perlindungan Privasi Yusuf Daeng, H., Linra, N., Darham, A., Handrianto, D., Risandy Sianturi, R., & Martin, D. (2023). Perlindungan Data Pribadi dalam Era Digital: Tinjauan Terhadap Kerangka Hukum Perlindungan Privasi. *Innovative: Journal Of Social Science Research*, *3*(6), 2898–2905.

Prawesti, I. (2017). Perlindungan Hukum Terhadap Konsumen Atas Penjualan Barang Bermerek Palsu Secara Online. *Kertha Semaya: Journal Ilmu Hukum*, *02*(01).

Ramadhani, F. (2023). Dinamika UU ITE Sebagai Hukum Positif di Indonesia Guna Meminimalisir Kejahatan Siber. *Kultura: Jurnal Ilmu Hukum, Sosial, Dan Humaniora*, *1*(1).

Razaulla, S., Fachkha, C., Markarian, C., Gawanmeh, A., Mansoor, W., Fung, B. C. M., & Assi, C. (2023). The Age of Ransomware: A Survey on the Evolution, Taxonomy, and Research Directions. *IEEE Access*, *11*. https://doi.org/10.1109/ACCESS.2023.3268535

Rumlus, M. H., & Hartadi, H. (2020). Kebijakan Penanggulangan Pencurian Data Pribadi dalam Media Elektronik. *Jurnal HAM*, *11*(2). https://doi.org/10.30641/ham.2020.11.285-299

Sari, A. G., Bahroni, A., & Murty, H. (2020). PERLINDUNGAN BAGI KONSUMEN PADA TRANSAKSI JUAL BELI SECARA ELEKTRONIK DITINJAU DARI HUKUM POSITIF. *Transparansi Hukum*, *3*(1). https://doi.org/10.30737/transparansi.v3i1.665

Sinaga, M. I. J. (2022). Penetapan Tersangka Dalam Penyidikan Tindak Pidana Transnational Cybercrime Menurut Sistem Hukum di Indonesia. *Jurnal Ilmiah Indonesia*, *7*(3).

Sitokdana, M. N. N. (2019). Rencana Strategis Penerapan Sistem Informasi Eksekutif e-Government Pemerintah Provinsi Papua. *Jurnal Komunika : Jurnal Komunikasi, Media Dan Informatika*, *8*(1). https://doi.org/10.31504/komunika.v8i1.1762

Sufianti, E. (2007). Aplikasi e-Government dalam Meningkatkan Kualitas Pelayanan Publik pada Beberapa Pemerintah Daerah Kota/Kabupaten di Indonesia. *Jurnal Ilmu Administrasi: Media Pengembangan Ilmu Dan Praktek Administrasi*, *4*(4), 3.

Sulistyawati, N. L. G., Suarjana, I. M., & Wibawa, C. I. M. (2022). Pengembangan Media Website Berbasis Google Sites pada Materi Statistika Kelas IV Sekolah Dasar. *Jurnal Pendidikan Dan Konseling*, *4*(4), 899.

Suryawijaya, T. W. E. (2023). Memperkuat Keamanan Data melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses dalam Transformasi Digital di Indonesia. *Jurnal Studi Kebijakan Publik*, *2*(1), 55–68. https://doi.org/10.21787/jskp.2.2023.55-68

Takanjanji, J. (2021). MEREFLEKSI PENEGAKAN HUKUM TINDAK PIDANA PENIPUAN ONLINE. *Widya Pranata Hukum : Jurnal Kajian Dan Penelitian Hukum*, *2*(2). https://doi.org/10.37631/widyapranata.v2i2.260

Taylor, A. J. P., & Patel, A. D. (2017). ransomware attacks prevention, monitoring and damage control. *International Journal of Research and Scientific Innovation (IJRSI)*, *2321–2705*.

Urooj, U., Al-Rimy, B. A. S., Zainal, A., Ghaleb, F. A., & Rassam, M. A. (2022). Ransomware Detection Using the Dynamic Analysis and Machine Learning: A Survey and Research Directions. *Applied Sciences (Switzerland)*, *12*(1). https://doi.org/10.3390/app12010172

Utama, A. S. (2023). Ransomware : Memahami Ancaman. *Bincang Sains Dan Teknologi*, *2*(02).

Wabnitz, C. C. C., Lam, V. W. Y., Reygondeau, G., Teh, L. C. L., Al-Abdulrazzak, D., Khalfallah, M., Pauly, D., Deng Palomares, M. L., Zeller, D., & Cheung, W. W. L. (2018). Climate change impacts on marine biodiversity, fisheries and society in the Arabian Gulf. *PLoS ONE*, *13*(5). https://doi.org/10.1371/journal.pone.0194537

Wahyuni, W. (2021). Aspek Hukum Terhadap Transaksi Pinjaman Online. *Tadayun: Jurnal Hukum Ekonomi Syariah*, *2*(1), 25–40. https://doi.org/10.24239/tadayun.v2i1.14

Waron, A. (2023). *Perlindungan Hukum Terhadap Data Pribadi Pihak Peminjam Yang Disebar Oleh Layanan Pinjaman Online Yang Berstatus Ilegal*. *8*, 17115–17132.

Wiradipradja, E. S. (2015). *Penuntun Praktis Metode Penelitian dan Penulisan Karya Ilmiah Hukum*. Keni Media.

Yustitiana, R. (2021). Pelaksanaan Pengaturan Hukum Tindak Kejahatan "Fraud Phising" Transaksi Elektronik sebagai Bagian dari Upaya Penegakan Hukum di Indonesia Dikaitkan dengan Teori Efektivitas Hukum [Implementation of the Criminal Act of Fraud Phising of Electronic Transaction as Part of the Law Enforcement Effort in Indonesia in Regard to the Effectiveness of Law Theory]. *Jurnal Hukum Visio Justisia*, *1*(1). https://doi.org/10.19166/vj.v1i1.3802

Zaenudin, F. R., & Faridah, H. (2022). Pertanggungjawaban Pidana Terhadap Afiliator Aplikasi Opsi Biner Ilegal Dalam Hukum Pidana Indonesia. *Jurnal Hukum Sasana*, *8*(1). https://doi.org/10.31599/sasana.v8i1.1066