Eksekusi: Jurnal Ilmu Hukum dan Administrasi Negara
Volume 2, Nomor 4, November 2024
e-ISSN: 2987-7113; p-ISSN: 2987-9124, Hal. 426-434
DOI: https://doi.org/10.55606/eksekusi.v2i4.1823
Available Online at: https://journal-stiayappimakassar.ac.id/index.php/Eksekusi

Perlindungan Data Pribadi dalam Kasus Ransomware: Apa Kata Hukum?

Seri Mughni Sulubara
Universitas Muhammadiyah Mahakarya Aceh, Indonesia

Korespondensi penulis: serimughni@ummah.ac.id

Abstract. *Ransomware attacks are an increasingly complex and costly global threat. International reports show a 300% increase in the frequency of ransomware attacks in the last five years (for example, data from IBM Security or Kaspersky). This threat not only blocks data access through encryption, but also jeopardizes privacy. This research will also examine the criminal law aspects associated with ransomware attacks, including the possible prosecution of the perpetrators of the attacks and the legal liability for victimized organizations. The theoretical study in the research titled "Personal Data Protection in Ransomware Cases: What Does the Law Say?" covers the theory of legal protection of personal data. The research method uses normative legal research that examines applicable regulations, namely the Criminal Code, ITE Law, PDP Law. This research refers to the case of a ransomware attack that hit Bank Syariah Indonesia (BSI), where the Lock Bit hacker group managed to steal the personal data of more than 15 million customers. This attack resulted in significant operational disruption to the bank's services. Ransomware is categorized as an act of extortion in accordance with Article 368 of the Criminal Code and Article 27 paragraph (4) of the ITE Law. The ITE Law and the Criminal Code are not considered to specifically regulate ransomware, although the articles (such as extortion and hacking) can be used to ensnare the perpetrators Collaboration between the government, the private sector, and the cybersecurity community is needed to build an early detection system for ransomware threats.*

Keywords: *Law, Personal Data Protection, Ransomware Case.*

Abstrak. Serangan ransomware merupakan ancaman global yang semakin rumit dan merugikan. Laporan internasional menunjukkan peningkatan frekuensi serangan ransomware hingga 300% dalam lima tahun terakhir (misalnya, data dari IBM Security atau Kaspersky). Ancaman ini tidak hanya memblokir akses data melalui enkripsi, tetapi juga membahayakan privasi. Penelitian ini juga akan meneliti aspek hukum pidana yang terkait dengan serangan ransomware, termasuk kemungkinan penuntutan pelaku serangan dan tanggung jawab hukum bagi organisasi yang menjadi korban. Kajian teoritis dalam penelitian berjudul "Perlindungan Data Pribadi dalam Kasus Ransomware: Apa Kata Hukum?" mencakup terori perlindungan hukum data pribadi. Metode penelitian menggunakan penelitian hukum normatif yang meneliti peraturan-peraturan yang berlaku yaitu KUHP, UU ITE, UU PDP. Penelitian ini mengacu pada kasus serangan ransomware yang menimpa Bank Syariah Indonesia (BSI), di mana kelompok peretas Lock Bit berhasil mencuri data pribadi lebih dari 15 juta pelanggan. Serangan ini mengakibatkan gangguan operasional yang signifikan pada layanan bank. Ransomware dikategorikan sebagai tindakan pemerasan sesuai dengan Pasal 368 KUHP dan Pasal 27 ayat (4) UU ITE. UU ITE dan KUHP dinilai tidak spesifik mengatur ransomware, meski pasal-pasalnya (seperti pemerasan dan peretasan) dapat digunakan untuk menjerat pelaku Diperlukan kolaborasi antara pemerintah, sektor swasta, dan komunitas keamanan siber untuk membangun sistem deteksi dini terhadap ancaman ransomware.

Kata Kunci: Hukum, Kasus Ransomware, Perlindungan Data Pribadi.

1. LATAR BELAKANG

Latar belakang penelitian berjudul "Perlindungan Data Pribadi dalam Kasus Ransomware: Apa Kata Hukum?" berfokus pada meningkatnya ancaman serangan ransomware yang menargetkan data pribadi dan dampaknya terhadap individu serta organisasi. Dalam era digital saat ini, data pribadi menjadi aset yang sangat berharga dan rentan terhadap serangan siber, termasuk ransomware, yang dapat mengunci akses ke data dan meminta tebusan untuk memulihkannya. Serangan ransomware telah meningkat secara signifikan dalam

Received Oktober 24, 2024; Revised November 05, 2024; Accepted November 27, 2024; Published November 30, 2024

beberapa tahun terakhir, dengan banyak kasus yang dilaporkan di Indonesia, termasuk serangan terhadap lembaga keuangan seperti Bank Syariah Indonesia (BSI) yang mengalami kebocoran data akibat serangan tersebut (Ramadhan, 2023).

Serangan ransomware merupakan ancaman global yang semakin rumit dan merugikan. Laporan internasional menunjukkan peningkatan frekuensi serangan ransomware hingga 300% dalam lima tahun terakhir (misalnya, data dari IBM Security atau Kaspersky) . Ancaman ini tidak hanya memblokir akses data melalui enkripsi, tetapi juga membahayakan privasi**.** Data pribadi korban (misalnya, informasi keuangan, kesehatan, atau identitas) seringkali digunakan untuk memaksa pembayaran tebusan. Menyebabkan kerugian finansial karena korban, baik individu maupun organisasi, sering dipaksa membayar tebusan (biasanya dalam cryptocurrency) atau mengalami penghentian operasional yang merugikan (Prayugah et al., 2024). Mengganggu stabilitas digital karena adanya serangan pada infrastruktur penting (rumah sakit, pemerintah, atau perusahaan) dapat membahayakan kehidupan dan keamanan publik. Di Indonesia, kasus ransomware juga meningkat, seperti yang dilaporkan oleh Kominfo dan Badan Siber dan Sandi Negara (BSSN). Namun, peraturan hukum yang relevan, seperti UU PDP, belum sepenuhnya dievaluasi dalam konteks serangan ini (Afifah, 2023).

Meskipun terdapat regulasi seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan ketentuan dalam Kitab Undang-Undang Hukum Pidana (KUHP), perlindungan hukum bagi korban ransomware masih dianggap kurang efektif. Penelitian ini bertujuan untuk mengeksplorasi tantangan dalam implementasi regulasi yang ada dan bagaimana hukum dapat lebih baik melindungi data pribadi. Banyak pengguna masih kurang sadar akan risiko yang terkait dengan pengelolaan data pribadi mereka. Penelitian ini juga menyoroti pentingnya pendidikan dan kesadaran tentang keamanan siber untuk mencegah serangan di masa mendatang. Dengan kemajuan teknologi, metode enkripsi dan perlindungan data terus berkembang, namun pelaku kejahatan siber juga semakin canggih. Penelitian ini akan membahas bagaimana hukum dapat beradaptasi dengan perkembangan teknologi ini untuk memberikan perlindungan yang lebih baik bagi individu dan organisasi (Mubarak et al., 2024).

Melalui penelitian ini, diharapkan dapat memberikan wawasan yang lebih dalam mengenai perlindungan hukum terhadap data pribadi dalam konteks serangan ransomware serta rekomendasi untuk perbaikan regulasi yang ada. Penelitian ini dilatarbelakangi oleh meningkatnya ancaman ransomware dan dampaknya terhadap perlindungan data pribadi. Serangan ransomware, yang melibatkan penyandian data dan permintaan tebusan, menimbulkan konsekuensi serius, termasuk pelanggaran privasi data dan kerugian finansial

yang signifikan. Penelitian ini akan menelaah aspek hukum yang relevan terkait perlindungan data pribadi dalam konteks serangan ransomware, khususnya di Indonesia (Annisa et al., 2025).

Undang-Undang Perlindungan Data Pribadi: Penelitian ini akan meneliti undang-undang dan regulasi perlindungan data pribadi yang berlaku di Indonesia, seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). UU PDP mengatur pengumpulan, pengolahan, dan penyimpanan data pribadi, serta hak-hak subjek data. Penelitian akan menganalisis bagaimana UU PDP melindungi data pribadi dalam situasi serangan ransomware. Perbandingan dengan hukum perlindungan data internasional seperti GDPR (General Data Protection Regulation) di Eropa dan CCPA (California Consumer Privacy Act) di Amerika Serikat juga mungkin dilakukan untuk memberikan perspektif yang lebih luas (Muhaimin et al., 2025).

Penelitian ini juga akan meneliti aspek hukum pidana yang terkait dengan serangan ransomware, termasuk kemungkinan penuntutan pelaku serangan dan tanggung jawab hukum bagi organisasi yang menjadi korban. Ini mencakup analisis pasal-pasal dalam KUHP yang relevan dengan kejahatan siber dan pelanggaran data. Penelitian ini akan memberikan kontribusi yang signifikan dalam memahami dan mengatasi tantangan hukum yang ditimbulkan oleh serangan ransomware terhadap perlindungan data pribadi di Indonesia. Hasil penelitian diharapkan dapat memberikan rekomendasi kebijakan dan praktik terbaik untuk melindungi data pribadi dan meminimalkan dampak serangan ransomware (Wahidin et al., 2022).

2. KAJIAN TEORITIS

Kajian teoritis dalam penelitian berjudul "Perlindungan Data Pribadi dalam Kasus Ransomware: Apa Kata Hukum?" mencakup beberapa aspek penting yang berkaitan dengan perlindungan hukum terhadap data pribadi, khususnya dalam konteks serangan ransomware. Berikut adalah beberapa poin utama yang dapat dijadikan dasar kajian teoritis:

1) **Teori Perlindungan Data Pribadi** (Aruan, 2024)**.**
    a. Hak Privasi: Data pribadi merupakan bagian dari hak privasi individu yang harus dilindungi. Teori ini menekankan bahwa setiap individu memiliki hak untuk mengontrol informasi pribadi mereka dan mencegah penyalahgunaan oleh pihak ketiga.
    b. Prinsip Perlindungan Data: Terdapat prinsip-prinsip yang mendasari perlindungan data pribadi, seperti prinsip pembatasan pengumpulan, kualitas data, spesifikasi tujuan, dan perlindungan keamanan. Prinsip-prinsip ini menekankan pentingnya

pengumpulan data yang sah dan adil, serta penggunaan data yang sesuai dengan tujuan yang telah ditetapkan.

2) Regulasi Hukum Terkait Cybercrime

a. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE): UU ITE mengatur tentang tindakan melawan hukum di ruang siber, termasuk pemerasan melalui ransomware. Pasal-pasal dalam UU ini memberikan landasan hukum untuk menuntut pelaku kejahatan siber.

b. Undang-Undang Perlindungan Data Pribadi (UU PDP): UU ini memberikan kerangka hukum yang lebih komprehensif untuk melindungi data pribadi di Indonesia. UU PDP mencakup sanksi bagi pelanggaran terkait pengumpulan dan penggunaan data pribadi secara ilegal

3) Dampak Ransomware Terhadap Data Pribadi

Serangan ransomware tidak hanya mengakibatkan kerugian finansial tetapi juga dapat menyebabkan hilangnya data pribadi yang sensitif. Hal ini dapat berdampak pada privasi individu dan reputasi organisasi yang terkena serangan.

4) Perlunya Kerjasama antara Pemerintah dan Masyarakat

Penelitian ini juga menyoroti pentingnya kolaborasi antara pemerintah dan masyarakat dalam menciptakan regulasi yang efektif untuk melindungi data pribadi. Kerjasama ini diperlukan untuk meningkatkan kesadaran tentang risiko kejahatan siber dan langkah-langkah pencegahan yang dapat diambil oleh individu dan organisasi.

5) Pendekatan Multidisiplin dalam Penanganan Ransomware

Penanganan ransomware memerlukan pendekatan multidisiplin, termasuk aspek hukum, teknologi informasi, dan pendidikan masyarakat. Penelitian ini berupaya mengeksplorasi bagaimana ketiga aspek tersebut dapat saling mendukung dalam upaya perlindungan data pribadi.

Melalui kajian teoritis ini, penelitian bertujuan untuk memberikan pemahaman yang lebih baik mengenai tantangan hukum dalam melindungi data pribadi dari ancaman ransomware serta rekomendasi untuk perbaikan regulasi yang ada.

3. METODE PENELITIAN

Penelitian ini menggunakan bahan hukum primer, bahan hukum sekunder dan bahan hukum tersier yang kemudian dianalisis dan diambil kesimpulannya. Bahan hukum primer bersifat autoritatif artinya mempunyai otoritas. Bahan hukum primer terdiri dari peraturan perundang-undangan yang terkait dengan masalah yang diteliti. Metode penelitian

menggunakan penelitian hukum normatif yang meneliti peraturan-peraturan yang berlaku yaitu Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Perlindungan Data Pribadi dan UU No. 1 Tahun 2024 tentang Keamanan Jaringan Nasional. Dengan demikian, kerangka hukum Indonesia untuk ransomware mencakup UU ITE, KUHP, dan UU PDP, namun perlu adaptasi terus-menerus untuk menjawab kompleksitas kejahatan siber. Metode penelitian menjelaskan secara rinci bagaimana penelitian dilakukan.

Metode penelitian yang digunakan adalah penelitian deskriptif kualitatif dengan pendekatan yuridis normatif. Penelitian deskriptif kualitatif dengan pendekatan yuridis normatif adalah penelitian yang berusaha mendeskripsikan suatu peristiwa atau kejadian yang terjadi secara langsung, nyata, realistis, aktual secara aturan-aturan yang ada. Teknik atau instrumen pengumpulan data yang digunakan adalah penelitian kepustakaan *(library research)* dengan cara mempelajari berbagai buku-buku sebagai literatur, dokumen-dokumen resmi, peraturan perundang-undangan, hasil-hasil penelitian terdahulu, dan sumber-sumber kepustakaan lainnya yang berkaitan dengan permasalahan yang diteliti (Soekanto, 2010).

Penelitian ini menggunakan pendekatan penelitian hukum yuridis normatif yang menggunakan teknik pengumpulan data yang terdiri dari studi kepustakaan yang berpedoman pada bahan hukum primer, sekunder, tersier dan kemudian dianalisis (Septiani & Zuhdy, 2020). Penelitian ini bertujuan untuk mengetahui "*Perlindungan Data Pribadi dalam Kasus Ransomware: Apa Kata Hukum"*

4. HASIL DAN PEMBAHASAN

Ransomware adalah jenis malware yang mengunci akses pengguna ke sistem komputer dan meminta tebusan untuk mengembalikan akses tersebut. Serangan ini dapat menyebabkan kerugian finansial dan kehilangan data pribadi yang signifikan. Indonesia merupakan salah satu negara dengan tingkat kejahatan siber yang tinggi, termasuk serangan ransomware, yang mengancam privasi dan keamanan data pribadi warga negara (Simorangkir, 2024).

Penelitian ini mengacu pada kasus serangan ransomware yang menimpa Bank Syariah Indonesia (BSI), di mana kelompok peretas Lock Bit berhasil mencuri data pribadi lebih dari 15 juta pelanggan. Serangan ini mengakibatkan gangguan operasional yang signifikan pada layanan bank. Ransomware dikategorikan sebagai tindakan pemerasan sesuai dengan Pasal 368 KUHP dan Pasal 27 ayat (4) UU ITE. Tindakan ini melanggar hukum dan dapat dikenakan sanksi pidana. UU Perlindungan Data Pribadi (PDP) memberikan kerangka hukum untuk melindungi data pribadi. Pelanggaran terhadap UU ini dapat dikenakan sanksi pidana, termasuk penjara dan denda yang signifikan (Hartati & Muhammad, 2023).

Dampak ransomware adalah data pribadi yang dicuri dapat disalahgunakan, mengakibatkan kerugian bagi individu. Serangan ransomware dapat merusak sistem dan perangkat yang digunakan. Biaya pemulihan dan tebusan dapat sangat tinggi. Penelitian ini menyoroti beberapa sanksi yang diatur dalam UU PDP, termasuk penjara hingga 5 tahun dan/atau denda hingga Rp5 miliar untuk pengumpulan data pribadi secara ilegal. Penjara hingga 6 tahun dan/atau denda hingga Rp6 miliar untuk pemalsuan data pribadi. Langkah-langkah pencegahan diantaranya meningkatkan kesadaran keamanan di kalangan pengguna, memperbarui sistem perangkat secara berkala dan menggunakan perangkat lunak keamanan yang kuat dan membuat cadangan data secara teratur dan berhati-hati saat mengunduh aplikasi.

Regulasi seperti UU ITE dan UU PDP belum sepenuhnya efektif melindungi data pribadi dalam kasus ransomware. Contoh kasus Bank Syariah Indonesia (BSI) menunjukkan bahwa kelemahan utama terletak pada aspek kelembagaan, seperti kurangnya koordinasi antarlembaga penegak hukum dan lambatnya respons institusi finansial saat terjadi serangan. Sanksi pidana dalam UU ITE (misal: Pasal 45 Ayat (4)) dinilai terlalu umum dan tidak mempertimbangkan tingkat kerugian akibat serangan ransomware.

Bank BSI dianggap melakukan perbuatan melawan hukum karena gagal memenuhi kewajiban perlindungan data nasabah sesuai UU PDP. Namun, pembuktian tanggung jawab bank secara hukum masih rumit akibat keterbatasan bukti digital dan kompleksitas teknis serangan ransomware. Serangan ransomware pada BSI (2023) mengakibatkan kebocoran 1,5 TB data nasabah, termasuk informasi sensitif seperti saldo rekening dan riwayat transaksi. Hal ini menurunkan kepercayaan nasabah meski tidak signifikan memengaruhi loyalitas mereka. Kerugian finansial mencapai Rp295,61 miliar untuk tebusan dan Rp131 miliar untuk pemulihan sistem (Sulistiadi & Salman, 2023).

Peneliti menekankan pentingnya integritas data, kerahasiaan informasi, dan tanggung jawab sosial bagi ahli keamanan siber dalam mencegah dan merespons serangan ransomware. UU ITE dan KUHP hanya mengkriminalisasi tindakan pemerasan dan peretasan, tetapi tidak secara spesifik mengatur mitigasi risiko ransomware atau kewajiban pemulihan data. UU PDP belum diintegrasikan dengan standar keamanan siber yang memadai, seperti kewajiban enkripsi data atau pelaporan kebocoran dalam waktu 72 jam. Bank BSI gagal menerapkan prinsip *security by design* dalam sistem IT-nya, seperti tidak adanya pemantauan real-time terhadap ancaman siber dan cadangan data (*backup*) yang terenkripsi (Jurnal et al., 2023). Penelitian merekomendasikan bank meningkatkan alokasi anggaran untuk teknologi *endpoint detection* dan pelatihan SDM guna mencegah serangan serupa. Serangan ransomware memiliki beberapa karakteristik umum, termasuk (Wahidin et al., 2022):

1) Enkripsi Data: Data korban dienkripsi sehingga tidak dapat diakses.
2) Permintaan Tebusan: Pelaku meminta tebusan untuk mengembalikan akses ke data.
3) Metode Penyebaran: Ransomware dapat disebar melalui berbagai cara, seperti email phishing, exploit kit, dan malware.

Dampak serangan ransomware terhadap perlindungan data pribadi meliputi (Novita et al., 2023):

1) Kebocoran Data: Data pribadi korban dapat bocor jika tebusan tidak dibayar atau jika pelaku gagal mengembalikan akses ke data.
2) Pelanggaran Privasi: Kebocoran data dapat menyebabkan pelanggaran privasi dan reputasi korban.
3) Kerugian Finansial: Korban dapat mengalami kerugian finansial yang signifikan akibat serangan ransomware.

Hasil penelitian ini menyoroti urgensi harmonisasi regulasi dan peningkatan kapasitas teknis untuk melindungi data pribadi dari ancaman ransomware yang semakin canggih. Penelitian ini menekankan bahwa perlindungan data pribadi adalah hal yang krusial dalam menghadapi ancaman ransomware (Ferdiansyah, 2018). Dengan adanya regulasi yang jelas dan langkah-langkah pencegahan yang tepat, diharapkan dapat mengurangi risiko serangan siber dan melindungi hak privasi individu (Yuniarti et al., 2023).

5. KESIMPULAN DAN SARAN

UU ITE dan KUHP dinilai tidak spesifik mengatur ransomware, meski pasal-pasalnya (seperti pemerasan dan peretasan) dapat digunakan untuk menjerat pelaku. Sanksi dalam UU ITE dianggap terlalu umum dan tidak mempertimbangkan skala kerugian. UU Perlindungan Data Pribadi (UU PDP) diakui sebagai langkah progresif, tetapi implementasinya masih menghadapi kendala seperti kurangnya integrasi dengan standar keamanan siber (misal: enkripsi wajib atau pelaporan kebocoran dalam 72 jam). Serangan ransomware pada BSI (2023) menyebabkan kebocoran 1,5 TB data nasabah dan kerugian finansial Rp426,61 miliar (tebusan + pemulihan). Ahli keamanan siber wajib menjaga integritas data, kerahasiaan informasi, dan tanggung jawab sosial dalam mencegah ransomware. Penelitian ini menyimpulkan bahwa perlindungan data pribadi dari ransomware memerlukan harmonisasi regulasi, peningkatan kapasitas teknis, dan kolaborasi multisektor. Tanpa langkah-langkah ini, ancaman ransomware akan terus membahayakan keamanan siber di Indonesia.

Penting untuk meningkatkan kesadaran masyarakat mengenai risiko kejahatan siber, termasuk ransomware. Program pelatihan dan seminar tentang keamanan siber dapat

membantu individu memahami cara melindungi data pribadi mereka. Diperlukan kolaborasi antara pemerintah, sektor swasta, dan komunitas keamanan siber untuk membangun sistem deteksi dini terhadap ancaman ransomware. Pembentukan pusat layanan keamanan siber nasional yang dapat memberikan dukungan teknis dan informasi kepada organisasi dalam menghadapi ancaman ransomware. Profesional di bidang teknologi informasi harus menjaga integritas dan tanggung jawab sosial dalam pengelolaan data pribadi, serta berkomitmen untuk melakukan tindakan pencegahan terhadap potensi serangan ransomware. Dengan menerapkan saran-saran ini, diharapkan perlindungan terhadap data pribadi dapat ditingkatkan secara signifikan, sehingga masyarakat lebih aman dari ancaman ransomware dan kejahatan siber lainnya.

DAFTAR REFERENSI

Afifah, D. (2023). Perlindungan konsumen di sektor jasa keuangan pada kasus serangan siber ransomware yang menimpa perbankan. *JIIP - Jurnal Ilmiah Ilmu Pendidikan*, *6*(11), 9318–9323. https://doi.org/10.54371/jiip.v6i11.3176

Annisa, S., Langi, A. R., Padang, U. N., & Terbuka, U. S. (2025). Evaluasi strategi reaktif pasca serangan ransomware pada pusat data nasional sementara 2 Surabaya 1. *Prosiding Seminar Nasional Sains dan Teknologi Seri III*, *2*(1), 680–691.

Aruan, J. E. S. (2024). Perlindungan data pribadi ditinjau dari teori perlindungan hukum dan teori perlindungan hak atas privasi. *Jurnal Globalisasi Hukum*, *1*(1), 1–22. https://doi.org/10.25105/jgh.v1i1.19499

Ferdiansyah. (2018). Analisis aktivitas dan pola jaringan terhadap Eternal Blue dan WannaCry ransomware. *JUSIFO (Jurnal Sistem Informasi*, *2*(1), 44–59. http://eprints.binadarma.ac.id/3873/1/Ferdiansyah-Analisis Aktivitas dan Pola Jaringan Terhadap Eternal Blue dan Wannacry Ransomware.pdf

Hartati, C. S., & Muhammad, A. (2023). Combating cybercrime and cyberterrorism in Indonesia. *Jurnal Hubungan Internasional*, *11*(2), 45–56. https://doi.org/10.18196/jhi.v11i2.15647

Jurnal, D., Ilmu, D., Pembangunan, U., Veteran, N., & Upnvj, J. (2023). Hukum pertahanan dan keamanan negara: State defense and security law. *Jurnal Dunia Ilmu Hukum dan Politik*, *1*(4), 56–67. https://doi.org/10.59581/doktrin.v1i4.1355

Mubarak, A. S., Insirat, M. N., & Lutfiya, M. N. (2024). Ransomware: Evolution, classification, attack phase, detection, and prevention. *Seminar Nasional Teknik Elektro, Sistem Informasi, dan Teknik Informatika*, 1–6.

Muhaimin, S., & Cokroaminoto, J. H. O. S. (2025). Analisis serangan ransomware pada sistem keamanan siber Bank Syariah Indonesia (BSI) terhadap customer trust. *Journal Transformation of Mandalika*, *6*(2), 67–72. https://doi.org/10.56741/bst.v2i02.353

Novita, A. P., Fatmanegara, F., Runtuwene, F. J. J., Samuela, J. T., & Syahbani, M. F. (2023). Cyber security threats: Analisis dan mitigasi risiko ransomware di Indonesia. *Jurnal Ilmiah Sistem Informasi, 3*(1), 160–169. https://doi.org/10.46306/sm.v3i1.91

Prayugah, M. I., Indahyanti, U., & Ariyanti, N. (2024). Analisis sentimen publik pada pemerintah dalam serangan ransomware dengan pendekatan SMOTE. *JOISIE (Journal of Information Systems and Informatics Engineering, 8*(2), 333–343. https://doi.org/10.35145/joisie.v8i2.4764

Ramadhan, G. (2023). Perlindungan hukum bagi korban ransomware WannaCry tindak pidana ransomware. *Jurnal Kajian Kontemporer Hukum dan Masyarakat, 1*(2), 1–15. https://doi.org/10.11111/dassollen.xxxxxxx

Simorangkir, A. (2024). Ransomware pada data PDN: Implikasi etis dan tanggung jawab profesional dalam pengelolaan keamanan siber. *Kampus Akademik Publishing, 2*(6), 324–331. https://doi.org/10.61722/jssr.v2i6.2966

Sulistiadi, & Salman, M. (2023). Ransomware attacks threat modeling using Bayesian network. *Digital Zone: Jurnal Teknologi Informasi dan Komunikasi, 14*(1), 43–56. https://doi.org/10.31849/digitalzone.v14i1.13788

Wahidin, G. W., Syaifuddin, S., & Sari, Z. (2022). Analisis ransomware WannaCry menggunakan aplikasi Cuckoo Sandbox. *Jurnal Repositor, 4*(1), 83–94. https://doi.org/10.22219/repositor.v4i1.1373

Yuniarti, D. R., Alfarizy, H. F., Siallagan, Z., & Rizkyanfi, M. W. (2023). Analisis potensi dan strategi pencegahan cyber crime dalam sistem logistik di era digital. *Jurnal Bisnis, Logistik dan Supply Chain (BLOGCHAIN, 3*(1), 23–32. https://doi.org/10.55122/blogchain.v3i1.714