Al-Zayn: Jurnal Ilmu Sosial & Hukum e-ISSN 3026-2917
https://ejournal.yayasanpendidikandzurriyatulquran.id/index.php/AlZyn p-ISSN 3026-2925
Volume 4 Number 1, 2026
DOI: https://doi.org/10.61104/alz.v4i1.4093

Implementasi Kebijakan Keamanan Siber dalam Mencegah Cybercrime pada Layanan Shopee PayLater

T. Saiful Basri[1], Seri Mughni Sulubara[2]
Program Studi Hukum Hukum, Universitas Muhammadiyah Mahakarya Aceh[1-2]
Email Korespondensi: saifulelbasrie@gmail.com, serimughni@ummah.ac.id

Article received: 01 November 2025, Review process: 11 November 2025
Article Accepted: 25 Desmber 2025, Article published: 08 Januari 2026

ABSTRACT
The implementation of cybersecurity policies in preventing cybercrime on Shopee PayLater services is a crucial aspect as the use of this fintech service increases in Indonesia. Shopee PayLater offers easy payment with an attractive "buy now, pay later" system that attracts many users, especially the younger generation. The research method for the study on the Implementation of Cybersecurity Policies in Preventing Cybercrime on Shopee PayLater services uses a qualitative descriptive approach with case studies. The results of the study on the implementation of cybersecurity policies in preventing cybercrime on Shopee PayLater services show that Shopee has implemented various security technologies that are quite good, such as data encryption, two-factor authentication, and a strict monitoring system to protect users' personal data and transactions. However, despite the implementation of these security protocols, the study found several vulnerabilities, particularly in terms of application permissions and the verification process using OTP codes, which can still be exploited by cybercriminals. The conclusion of the implementation of cybersecurity policies in preventing cybercrime on the Shopee PayLater service is that these policies have provided an important foundation for protecting users' personal data and maintaining the security of digital transactions.
Keywords: *Cybersecurity; Cybercrime; Shopee; PayLater.*

ABSTRAK
Implementasi kebijakan keamanan siber dalam mencegah cybercrime pada layanan Shopee PayLater menjadi aspek krusial seiring dengan meningkatnya penggunaan layanan fintech ini di Indonesia. Shopee PayLater menawarkan kemudahan pembayaran dengan sistem "beli sekarang, bayar nanti" yang menarik banyak pengguna, khususnya generasi muda. Metode penelitian untuk studi tentang Implementasi Kebijakan Keamanan Siber dalam Mencegah Cybercrime pada Layanan Shopee PayLater menggunakan pendekatan deskriptif kualitatif dengan studi kasus. Hasil penelitian mengenai implementasi kebijakan keamanan siber dalam mencegah cybercrime pada layanan Shopee PayLater menunjukkan bahwa Shopee telah menerapkan berbagai teknologi keamanan yang cukup baik, seperti enkripsi data, autentikasi dua faktor (two-factor authentication), serta sistem pemantauan ketat untuk melindungi data pribadi dan transaksi pengguna. Namun, meski sudah diterapkan protokol keamanan tersebut, penelitian menemukan adanya beberapa celah kerentanan, terutama pada aspek perizinan aplikasi dan proses verifikasi menggunakan kode OTP yang masih dapat dimanfaatkan oleh pelaku kejahatan siber. Kesimpulan dari implementasi kebijakan keamanan siber dalam mencegah cybercrime pada layanan Shopee PayLater adalah bahwa

kebijakan ini telah memberikan landasan yang penting untuk melindungi data pribadi pengguna dan menjaga keamanan transaksi digital.
Kata Kunci: *Keamanan, Siber, Cybercrime, Shopee, PayLater.*

PENDAHULUAN

Implementasi kebijakan keamanan siber dalam mencegah cybercrime pada layanan Shopee PayLater menjadi aspek krusial seiring dengan meningkatnya penggunaan layanan fintech ini di Indonesia (S. M. Sulubara & Tasril, Virdyra, 2025). Shopee PayLater menawarkan kemudahan pembayaran dengan sistem "beli sekarang, bayar nanti" yang menarik banyak pengguna, khususnya generasi muda. Namun, tingginya jumlah transaksi juga membuka peluang besar bagi pelaku kejahatan siber untuk melakukan penyalahgunaan data dan serangan digital (S. M. Sulubara, Tasril, et al., 2025).

Penelitian dan analisis keamanan data pada aplikasi Shopee PayLater menunjukkan adanya beberapa celah kerentanan, terutama terkait perizinan aplikasi dan proses verifikasi melalui kode OTP yang bisa dimanfaatkan oleh pihak tidak bertanggung jawab (S. M. A. A. Sulubara, 2024). Hal ini menjadi tantangan serius yang harus diantisipasi melalui kebijakan keamanan siber yang tepat, termasuk penggunaan enkripsi data, autentikasi ganda, serta pengawasan dan audit reguler oleh otoritas terkait.

Selain itu, implementasi kebijakan harus mencakup edukasi pengguna untuk meningkatkan kesadaran menjaga keamanan akun dan data pribadi, serta transparansi kebijakan privasi agar pengguna memahami bagaimana data mereka digunakan dan dilindungi. Kebijakan keamanan juga perlu didukung oleh regulasi yang kuat dari pemerintah dan pengawasan ketat oleh lembaga seperti OJK untuk memastikan standar keamanan terpenuhi dan pelaku cybercrime dapat ditindak tegas (S. M. Sulubara, 2024b).

Dengan penerapan kebijakan keamanan siber yang menyeluruh dan dukungan dari berbagai pemangku kepentingan, layanan Shopee PayLater dapat meminimalkan risiko cybercrime sekaligus memperkuat kepercayaan dan perlindungan bagi para penggunanya, mendukung perkembangan ekosistem fintech yang aman dan berkelanjutan di Indonesia. Latar belakang penelitian mengenai implementasi kebijakan keamanan siber dalam mencegah cybercrime pada layanan Shopee PayLater sangat penting mengingat pesatnya perkembangan teknologi finansial (fintech) dan meningkatnya aktivitas transaksi digital di Indonesia (S. M. Sulubara, Fauzi, et al., 2025). Shopee PayLater, yang mulai diperkenalkan sejak 6 Maret 2019 oleh Shopee Indonesia bekerja sama dengan perusahaan fintech seperti PT. Lentera Dana Nusantara dan PT. Commerce Finance, memberikan kemudahan kepada pengguna untuk berbelanja dengan sistem “beli dulu bayar nanti”. Kemudahan ini menjadikan Shopee PayLater sangat diminati, terutama di kalangan milenial dan generasi Z, sehingga volume transaksi dan data pengguna yang dikelola layanan ini sangat besar.

Namun, perkembangan pesat ini juga membuka peluang bagi berbagai ancaman cybercrime yang dapat mengancam keamanan data pribadi pengguna dan kelangsungan layanan. Berbagai kasus pembajakan akun, pencurian data pribadi,

dan penipuan digital yang melibatkan pengguna Shopee PayLater telah muncul sebagai peringatan akan pentingnya kebijakan keamanan siber yang kuat dan efektif (Sulubara, Seri Mughni Lubis, Hidayati Purnama, Simbolon, 2024). Tidak hanya berdampak pada kerugian finansial pengguna, ancaman ini juga menimbulkan risiko penurunan kepercayaan publik terhadap layanan fintech dan e-commerce secara umum.

Oleh karena itu, implementasi kebijakan keamanan siber yang terstruktur dan komprehensif menjadi kebutuhan mendesak untuk mencegah dan menanggulangi risiko-risiko tersebut. Kebijakan ini harus mencakup aspek teknis seperti enkripsi data, autentikasi multi-faktor, serta pengawasan dan audit sistem secara berkala. Selain itu, aspek edukasi pengguna terkait kewaspadaan terhadap serangan siber dan transparansi penggunaan data juga merupakan bagian penting dari kebijakan keamanan. Dukungan regulasi dari pemerintah dan pengawasan dari lembaga seperti Otoritas Jasa Keuangan (OJK) menjadi fondasi utama guna memastikan kepatuhan dan perlindungan konsumen di ranah digital (Azrica & Sulubara, 2023).

Penelitian ini bertujuan untuk menganalisis sejauh mana kebijakan keamanan siber telah diterapkan dalam layanan Shopee PayLater dan bagaimana kebijakan tersebut efektif dalam mencegah cybercrime serta melindungi data pribadi pengguna. Dengan begitu, diharapkan hasil penelitian dapat memberikan rekomendasi strategis untuk memperkuat ekosistem fintech yang aman dan terpercaya di Indonesia.

METODE

Metode penelitian untuk studi tentang Implementasi Kebijakan Keamanan Siber dalam Mencegah Cybercrime pada Layanan Shopee PayLater menggunakan pendekatan deskriptif kualitatif dengan studi kasus. Metode ini cocok untuk memperoleh pemahaman mendalam mengenai praktik kebijakan keamanan siber yang diterapkan serta efektivitasnya dalam mencegah serangan cyber dan menjaga keamanan data pengguna. Analisis data dilakukan secara tematik (thematic content analysis) dengan fokus pada identifikasi praktik terbaik, hambatan, dan dampak kebijakan keamanan yang diterapkan. Analisis ini juga mengevaluasi bagaimana kebijakan ini berkontribusi dalam memitigasi risiko cybercrime yang dihadapi oleh layanan Shopee PayLater.

Metode studi kasus ini memungkinkan penelitian untuk menggambarkan situasi nyata di lapangan secara holistik, serta memberi rekomendasi strategis yang relevan dengan kebutuhan keamanan di sektor fintech Indonesia. Pendekatan ini juga didukung oleh kerangka teori dan standar internasional keamanan informasi seperti ISO/IEC 27001 dan NIST Cybersecurity Framework sebagai landasan evaluasi kebijakan.

HASIL DAN PEMBAHASAN

Hasil penelitian mengenai implementasi kebijakan keamanan siber dalam mencegah cybercrime pada layanan Shopee PayLater menunjukkan bahwa Shopee telah menerapkan berbagai teknologi keamanan yang cukup baik, seperti enkripsi

data, autentikasi dua faktor (two-factor authentication), serta sistem pemantauan ketat untuk melindungi data pribadi dan transaksi pengguna. Namun, meski sudah diterapkan protokol keamanan tersebut, penelitian menemukan adanya beberapa celah kerentanan, terutama pada aspek perizinan aplikasi dan proses verifikasi menggunakan kode OTP yang masih dapat dimanfaatkan oleh pelaku kejahatan siber (Sulubara, Seri Mughni, Lubis, Hidayati Purnama, Simbolon, Nanci Yosepin, Razi, 2024).

Analisis menggunakan metode hybrid yang menggabungkan digital forensik dan teknik reengineering terhadap aplikasi Shopee PayLater menunjukkan risiko penyalahgunaan data pribadi pengguna, terutama terkait verifikasi identitas dan keamanan aplikasi pada perangkat Android. Masih rendahnya kesadaran pengguna dalam menjaga keamanan data juga menjadi faktor penyebab meningkatnya kasus cybercrime yang menimpa pengguna PayLater (Riska, Seri Mughni Sulubara, 2025).

Dampak positif dari implementasi kebijakan keamanan siber ini adalah meningkatnya tingkat kepercayaan konsumen terhadap layanan Shopee PayLater, khususnya pada generasi muda yang banyak menggunakan fitur ini. Fitur keamanan seperti verifikasi biometrik dan penggunaan kode OTP dalam proses transaksi menjadi faktor utama yang meningkatkan keamanan dan kepercayaan pengguna. Namun, hasil penelitian juga menekankan perlunya penguatan berkelanjutan dalam kebijakan dan teknologi keamanan melalui audit rutin, edukasi pengguna, dan peningkatan sistem autentikasi untuk memastikan perlindungan maksimal terhadap tindakan cybercrime (Murthada Murthada & Seri Mughni Sulubara, 2022). Transparansi dalam kebijakan privasi dan penanganan insiden keamanan menjadi hal penting untuk menjaga kepercayaan dan loyalitas pelanggan di tengah berkembangnya ancaman keamanan digital.

Secara keseluruhan, implementasi kebijakan keamanan siber pada Shopee PayLater telah memberikan landasan yang kuat dalam menghadapi risiko cybercrime, namun masih perlu dilakukan perbaikan dan penyesuaian terhadap perkembangan teknologi dan modus kejahatan siber yang semakin canggih. Secara teknis, Shopee PayLater telah menerapkan teknologi keamanan yang meliputi enkripsi data, autentikasi dua faktor, dan sistem pemantauan transaksi untuk mencegah akses tidak sah serta penipuan digital. Namun, keberhasilan teknis ini sangat bergantung pada kesesuaian protokol yang digunakan dan kemampuan mitigasi terhadap modus serangan terbaru seperti pencurian kode OTP dan pembajakan akun (Sulubara, Seri Mughni, Tasril, Virdyra, 2025). Analisis keamanan menunjukkan bahwa walaupun ada perlindungan, tetap ditemukan beberapa celah yang dapat dieksploitasi, sehingga diperlukan peningkatan berkelanjutan dalam sistem keamanan dan audit rutin untuk menjaga integritas data pengguna.

Secara teknis, Shopee PayLater telah menerapkan teknologi keamanan yang meliputi enkripsi data, autentikasi dua faktor, dan sistem pemantauan transaksi untuk mencegah akses tidak sah serta penipuan digital (Seri Mughni Sulubara et al., 2023). Namun, keberhasilan teknis ini sangat bergantung pada kesesuaian protokol yang digunakan dan kemampuan mitigasi terhadap modus serangan terbaru seperti pencurian kode OTP dan pembajakan akun. Analisis keamanan

menunjukkan bahwa walaupun ada perlindungan, tetap ditemukan beberapa celah yang dapat dieksploitasi, sehingga diperlukan peningkatan berkelanjutan dalam sistem keamanan dan audit rutin untuk menjaga integritas data pengguna.

Dari sisi kebijakan, Shopee dan pemangku kepentingan lainnya perlu menegakkan kebijakan privasi yang transparan dan komprehensif, yang menjelaskan pengumpulan, penggunaan, dan perlindungan data pengguna. Kebijakan harus memenuhi standar peraturan nasional seperti Undang-Undang Perlindungan Data Pribadi (UU PDP) serta regulasi OJK dalam sektor fintech. Penguatan regulasi dan penegakan hukum menjadi pondasi bagi perlindungan konsumen dan pencegahan cybercrime di tingkat nasional.

Edukasi pengguna juga menjadi pilar penting dalam kebijakan keamanan siber. Kesadaran pengguna untuk menjaga kerahasiaan data pribadi, tidak membagikan kode OTP, serta mengenali potensi modus penipuan secara signifikan mengurangi risiko penyalahgunaan data dan serangan siber. Program edukasi yang terstruktur dan komunikasi yang efektif dari penyedia layanan dapat meningkatkan kewaspadaan pengguna dan memperkuat sistem keamanan secara keseluruhan.

Pengawasan dan peran regulator seperti OJK sangat krusial dalam memastikan implementasi kebijakan keamanan siber berjalan efektif. Audit dan pengawasan secara berkala selain menjamin kepatuhan juga memberikan tekanan bagi penyedia layanan untuk terus meningkatkan standar keamanan (S. M. Sulubara, 2024a). Regulator juga harus menyediakan mekanisme pengaduan dan penyelesaian sengketa yang memudahkan konsumen korban cybercrime untuk mendapatkan perlindungan dan pemulihan.

Implementasi kebijakan keamanan siber di Shopee PayLater adalah hasil sinergi berbagai aspek: teknologi yang handal, kebijakan yang jelas, edukasi pengguna, dan pengawasan regulator. Kombinasi ini merupakan kunci untuk menciptakan layanan fintech yang aman, meningkatkan kepercayaan pengguna, serta secara efektif mencegah dan menangani ancaman cybercrime yang terus berkembang. Upaya perbaikan berkelanjutan dan adaptasi terhadap tren serangan baru menjadi keharusan dalam menjaga ekosistem fintech yang sehat dan aman di Indonesia. Implementasi Kebijakan Keamanan Siber dalam Mencegah Cybercrime pada Layanan Shopee PayLater (S. M. Sulubara et al., 2024):

a. Teknologi Keamanan yang Diterapkan

Penggunaan enkripsi data, autentikasi dua faktor (2FA), dan sistem monitoring transaksi untuk mencegah akses tidak sah dan penipuan digital. Analisis menunjukkan peningkatan keamanan melalui proteksi pada verifikasi transaksi seperti OTP.

b. Kerentanan dan Tantangan Keamanan

Ditemukan beberapa celah pada aspek perizinan aplikasi dan autentikasi yang dapat dimanfaatkan pelaku kejahatan siber, menunjukkan perlunya penguatan sistem keamanan dan kontrol internal.

c. Regulasi dan Kebijakan Privasi

Pentingnya kepatuhan terhadap regulasi nasional seperti UU Perlindungan Data Pribadi (PDP) dan pengawasan oleh OJK untuk memastikan kebijakan keamanan dipatuhi serta perlindungan data pengguna terjaga.

d. Edukasi dan Kesadaran Pengguna

Upaya memberikan edukasi kepada pengguna mengenai risiko cybercrime, pentingnya menjaga kerahasiaan data pribadi, memverifikasi informasi resmi, dan tidak membagikan kode OTP kepada pihak lain.

e. Pengawasan dan Audit Berkala

Pelaksanaan audit sistem keamanan secara rutin oleh penyelenggara layanan dan lembaga pengawas untuk mendeteksi dan mengatasi potensi kelemahan keamanan.

f. Dampak Kebijakan Keamanan terhadap Kepercayaan Pengguna

Penerapan kebijakan keamanan yang efektif meningkatkan kepercayaan konsumen, terutama di kalangan generasi muda yang dominan menggunakan Shopee PayLater.

g. Perlindungan Hukum dan Mekanisme Pengaduan

Adanya mekanisme pengaduan dan penanganan insiden pada pengguna korban cybercrime untuk memberikan pemulihan dan sanksi kepada pelaku.

h. Rekomendasi Peningkatan Keamanan

Saran perbaikan mencakup peningkatan autentikasi multi-faktor, transparansi kebijakan privasi, serta kolaborasi antara penyedia jasa, regulator dan pengguna dalam menjaga keamanan layanan fintech.

Implementasi Kebijakan Keamanan Siber dalam Mencegah Cybercrime pada Layanan Shopee PayLater mencakup sejumlah kebijakan dan langkah strategis yang bertujuan melindungi data pribadi pengguna serta menjaga kelangsungan dan keamanan transaksi digital. Kebijakan ini meliputi penerapan teknologi enkripsi untuk melindungi data selama penyimpanan dan transmisi, penggunaan autentikasi multi-faktor seperti kode OTP untuk memastikan keamanan akses akun, serta sistem pemantauan dan deteksi dini terhadap aktivitas mencurigakan yang berpotensi menjadi ancaman siber (Sulubara, Seri Mughni, 2024).

Lebih lanjut, adanya kebijakan transparansi dan perlindungan privasi yang jelas membantu pengguna memahami bagaimana data mereka dikelola dan dilindungi, sekaligus memberikan kontrol terhadap penggunaan data tersebut. Edukasi dan sosialisasi keamanan bagi pengguna menjadi bagian penting dari implementasi kebijakan agar pengguna dapat lebih waspada terhadap potensi penipuan dan menjaga keamanan akun mereka. Selain itu, pengawasan ketat dari regulator seperti Otoritas Jasa Keuangan (OJK) dan Kominfo memastikan penerapan standar keamanan sesuai regulasi nasional serta penegakan hukum yang tegas terhadap pelaku cybercrime. Penyedia layanan diwajibkan melakukan audit keamanan secara rutin dan memiliki rencana kontinuitas bisnis serta pemulihan bencana untuk memastikan layanan tetap berjalan meski terjadi gangguan.

Implementasi kebijakan keamanan siber yang komprehensif tersebut menjadi kunci dalam membangun kepercayaan pengguna sekaligus mengurangi risiko kejahatan siber yang semakin berkembang di era digital, sehingga Shopee

PayLater dapat memberikan layanan fintech yang aman, handal, dan terpercaya di Indonesia.

SIMPULAN

Kesimpulan dari implementasi kebijakan keamanan siber dalam mencegah cybercrime pada layanan Shopee PayLater adalah bahwa kebijakan ini telah memberikan landasan yang penting untuk melindungi data pribadi pengguna dan menjaga keamanan transaksi digital. Meskipun Shopee PayLater sudah menerapkan berbagai teknologi keamanan seperti enkripsi data, autentikasi dua faktor, serta sistem pemantauan transaksi yang mampu mengurangi risiko akses tidak sah dan penipuan, masih terdapat beberapa celah kerentanan yang perlu diperkuat.Kebijakan transparansi dan edukasi pengguna juga berperan signifikan dalam mendorong kesadaran akan pentingnya menjaga keamanan data dan kewaspadaan terhadap modus penipuan digital, sehingga meningkatkan perlindungan secara menyeluruh. Selain itu, pengawasan dan regulasi dari OJK serta audit keamanan sistem secara rutin menjadi kunci untuk memastikan kebijakan dilaksanakan secara efektif dan terus diperbaharui mengikuti perkembangan ancaman cybercrime. Secara keseluruhan, implementasi kebijakan keamanan siber di Shopee PayLater telah berhasil meningkatkan kepercayaan pengguna dan memperkuat ketahanan layanan terhadap ancaman cyber. Namun, perhatian berkelanjutan dan peningkatan sistem keamanan mutakhir tetap diperlukan agar layanan fintech ini tetap aman, handal, dan dapat diandalkan di tengah tantangan cybercrime yang semakin kompleks di era digital.

DAFTAR RUJUKAN

Azrica, H., & Sulubara, S. M. (2023). Legalitas Transaksi E Commerce Dalam Platfortm Shopee Ditinjau Dalam Kitab Undang-Undang Hukum Perdata (Burgerlijk Wetboek), Undang-Undang Nomor: 8 Tahun 1999 Tentang Perlindungan Konsumen Dan Persfektif Fiqih Muamalah. *Hakim: Jurnal Ilmu Hukum Dan Sosial*, *1*(3), 296–318. https://doi.org/https://doi.org/10.51903/hakim.v1i3.1305

Murthada Murthada, & Seri Mughni Sulubara. (2022). Implementasi Hak Asasi Manusia di Indonesia berdasarkan Undang-Undang Dasar 1945. *Dewantara : Jurnal Pendidikan Sosial Humaniora*, *1*(4), 111–121. https://doi.org/10.30640/dewantara.v1i4.426

Riska, Seri Mughni Sulubara, N. (2025). *Analisis Hukum Peer To Peer Lending Pada Platform Shopee Paylater Perspektif Kontrak Elektronik dan Perlindungan Konsumen* (Tahta Media (ed.)). CV. Tahta Media Group.

Seri Mughni Sulubara, Yury Ulandary, Riska Riska, & Desi Purnama Sari. (2023). Gen Z Wajib Tau! Edukasi dan Penguatan Pasal-Pasal UUD 1945 bagi Generasi Z (Pasca Milenal) bagi Siswa-Siswi SMA Negeri 4 Takengon. *Karunia: Jurnal Hasil Pengabdian Masyarakat Indonesia*, *2*(4), 96–109. https://doi.org/10.58192/karunia.v2i4.1552

Sulubara, Seri Mughni, Lubis, Hidayati Purnama, Simbolon, Nanci Yosepin, Razi, F. (2024). *Teori Hukum Perdata (Studi Kasus: Transaksi E-Commerce Shopee Paylater* (Tahta Media (ed.); Edisi Pert). CV. Tahta Media Group.

Sulubara, Seri Mughni, Tasril, Virdyra, N. (2025). *Pengantar Hukum Siber (Cybercrime) di Indonesia*. CV. Meida Sains Indonesia.

Sulubara, Seri Mughni, I. (2024). Regulasi dan Lisensi Mengenai Perlindungan Hukum Investor di Platform Fintech Peer-To-Peer Lending dalam Hukum Konvensional. *Jurnal Hukum, Politik Dan Ilmu Sosial*, *3*(4), 431–442. https://doi.org/https://doi.org/10.55606/jhpis.v3i4.4499

Sulubara, Seri Mughni Lubis, Hidayati Purnama, Simbolon, N. Y. (2024). Legal Review of Electronic Commerce-Based Buying and Selling on the Shopee Platform Against Consumers Using Shopee PayLater. *Proceeding of IROFONIC 2024*, *Proceeding*(02), 392–402.

Sulubara, S. M. (2024a). Menyajikan Berbagai Insiden Cybercrime yang Terjadi di Indonesia , Termasuk Pencurian Data dan Peretasan Situs Web Pemerintah. *Konsensus: Jurnal Ilmu Politik Dan Komunikasi*, *1*(6), 199–206. https://doi.org/https://doi.org/10.62383/konsensus.v1i6.692

Sulubara, S. M. (2024b). Perlindungan Data Pribadi dalam Kasus Ransomware : Apa Kata Hukum ? *Eksekusi: Jurnal Ilmu Hukum Dan Administrasi Negara*, *2*(4), 426–434. https://doi.org/https://doi.org/10.55606/eksekusi.v2i4.1823

Sulubara, S. M. A. A. (2024). Legalitas Fintech Peer To Peer Lending Pinjaman Online dalam Aspek Hukum Konvensional. *MANDUB: Jurnal Politik, Sosial, Hukum Dan Humaniora*, *2*(2), 177–187. https://doi.org/https://doi.org/10.59059/mandub.v2i2.1184

Sulubara, S. M., Fauzi, H., Muslim, B., Ferdiansyah, M. F., & Musmulyadi, M. (2025). Judi Online Sebagai Cybercrime Serta Tantangan Penegakan Hukum Pidana di Era Digital : Antara Regulasi , Pembuktian , dan Ancaman Cybercrime. *Jurnal Riset Rumpun Ilmu Sosial, Politik Dan Humaniora*, *4*(2), 539–552. https://doi.org/https://doi.org/10.55606/jurrish.v4i2.4990

Sulubara, S. M., Lubis, H. P., & Simbolon, N. Y. (2024). Legality Of Shopee Paylater Payments For Shopee Platform E-Commerce Transactions In Conventional Law. *DELEGALATA Jurnal Ilmu Hukum*, *9*(2), 247–256. https://doi.org/10.30596/dll.v9i2.20414

Sulubara, S. M., & Tasril, Virdyra, N. (2025). Legal Protection Of Cybercrime Crimes From Ransomware Attacks And Evaluation Of The Cyber Security And Resilience Bill 2025 In Indonesia ' S Defense. *DE LEGA LATA: Jurnal Ilmu Hukum*, *10*(December), 287–297. https://doi.org/10.30596/dll.v10i2.25786

Sulubara, S. M., Tasril, V., & Nurkhalisah. (2025). *Perlindungan Hukum Tindak Pidana Cybercrime Dalam Cyberlaw Di Indonesia: Perkembangan Tekhnologi Dan Tantangan Hukum Dalam Mewujudkan Cybersecurity* (Edisi Pert). Tahta Media.