Al-Zayn: Jurnal Ilmu Sosial & Hukum e-ISSN 3026-2917
https://ejournal.yayasanpendidikandzurriyatulquran.id/index.php/AlZyn p-ISSN 3026-2925
Volume 3 Number 6, 2025
DOI: https://doi.org/10.61104/alz.v3i6.3594

Analisis Risiko *Cybercrime* pada Layanan *Shopee PayLater* dan Implikasi terhadap Keamanan Data Pengguna

Ramsi Meifati Barus[1], Desborn Rico Purba[2]
Fakultas Hukum, Universitas Darma Agung, Indonesia
Email Korespondensi: ramsibarus@gmail.com, desbornmutiarapurba@gmail.com

Article received: 07 November 2025, Review process: 15 November 2025
Article Accepted: 03 Desmber 2025, Article published: 20 Desember 2025

ABSTRACT
Shopee PayLater is a digital payment method that makes it easy for customers to purchase goods and pay for them later, either in installments or in a single payment the following month. However, the increase in the use of Shopee PayLater also poses potential digital security risks. Various cybercrime threats such as data theft, identity theft, and other cyber attacks increasingly threaten the security and privacy of users. The research method used in the analysis of cybercrime risks in the Shopee PayLater service and its implications for user data security is qualitative-descriptive with a case study approach. The results of the cybercrime risk analysis on the Shopee PayLater service reveal various vulnerabilities and serious threats that threaten user data security, as well as a real impact on consumer experience and trust. Cybercrime in the form of OTP code misuse, account hacking, and identity theft are major threats that must be watched out for in this fintech ecosystem. In addition to technical aspects, these risks have serious implications for user privacy, including data leaks and misuse of personal information. Suboptimal data management and protection increase the potential for losses and reduce consumer confidence. Shopee PayLater, as a service supervised by the OJK, is committed to maintaining data security, but cases of leaks and hacking demonstrate the need for continuous improvement in cybersecurity systems.
Keywords: *Risk Analysis; Cybercrime; Shopee PayLater; Data Security*

ABSTRAK
Shopee PayLater adalah metode pembayaran digital yang memberikan kemudahan bagi pelanggan untuk membeli barang dan membayarnya di kemudian hari, baik dengan cicilan ataupun satu kali pembayaran di bulan berikutnya. Namun, peningkatan penggunaan Shopee PayLater juga menimbulkan potensi risiko keamanan digital. Berbagai ancaman cybercrime seperti pencurian data, penyalahgunaan identitas, dan serangan siber lainnya semakin mengancam keamanan dan privasi pengguna. Metode penelitian yang digunakan dalam analisis risiko cybercrime pada layanan Shopee PayLater dan implikasi terhadap keamanan data pengguna ini bersifat kualitatif-deskriptif dengan pendekatan studi kasus. Hasil analisis risiko cybercrime pada layanan Shopee PayLater mengungkap berbagai kerentanan dan ancaman serius yang mengancam keamanan data pengguna, sekaligus dampak nyata terhadap pengalaman dan kepercayaan konsumen. Cybercrime dalam bentuk penyalahgunaan kode OTP, peretasan akun, dan pencurian identitas menjadi ancaman utama yang harus diwaspadai dalam ekosistem fintech ini. Selain aspek teknis, risiko tersebut berimplikasi serius terhadap privasi pengguna, termasuk kebocoran data dan

penyalahgunaan informasi pribadi. Pengelolaan dan perlindungan data yang belum optimal memperbesar potensi kerugian dan menurunkan kepercayaan konsumen. Shopee PayLater sebagai layanan yang diawasi OJK telah berkomitmen untuk menjaga keamanan data, namun kasus kebocoran dan peretasan menunjukkan perlunya peningkatan terus-menerus dalam sistem keamanan siber.
Kata Kunci: *Analisis_Risiko; Cybercrime; Shopee _PayLater; Keamanan _Data*

PENDAHULUAN

Shopee PayLater adalah metode pembayaran digital yang memberikan kemudahan bagi pelanggan untuk membeli barang dan membayarnya di kemudian hari, baik dengan cicilan ataupun satu kali pembayaran di bulan berikutnya (Riska, Seri Mughni Sulubara, 2025). Sistem ini berkembang pesat seiring meningkatnya transaksi e-commerce di Indonesia, menarik banyak minat konsumen karena kemudahan dan fleksibilitas yang ditawarkan (S. M. Sulubara et al., 2024). Pertumbuhan Shopee PayLater juga memicu munculnya berbagai risiko keamanan digital yang patut diwaspadai. Di tengah maraknya penggunaan layanan pay later, kejahatan siber seperti pencurian data, phishing, dan penyalahgunaan akun pengguna semakin sering terjadin (Sulubara, Seri Mughni, 2024). Hal ini mendorong perlunya analisis mendalam terhadap risiko cybercrime serta penerapan strategi cybersecurity yang efektif. Analisis risiko cybercrime pada layanan Shopee PayLater sangat penting untuk melindungi data pribadi dan transaksi pengguna (Sulubara, Seri Mughni, Lubis, Hidayati Purnama, Simbolon, Nanci Yosepin, Razi, 2024). Selain perlindungan teknologi seperti enkripsi dan verifikasi dua langkah, faktor edukasi pengguna dan kebijakan privasi juga menentukan efektivitas upaya keamanan. Penelitian ini bertujuan mengkaji berbagai ancaman siber yang mungkin terjadi serta implikasinya terhadap perlindungan data pengguna pada ekosistem pembayaran digital Shopee PayLater (Azrica & Sulubara, 2023).

Latar belakang penelitian ini berangkat dari perkembangan pesat layanan e-commerce di Indonesia, khususnya Shopee yang diluncurkan pada tahun 2015 di bawah naungan SEA Group. Shopee tidak hanya menyediakan platform jual beli, tetapi juga mengembangkan fitur pembayaran digital yang inovatif, yaitu Shopee PayLater, yang mulai diperkenalkan pada 6 Maret 2019. Fitur ini memungkinkan pengguna untuk membeli barang terlebih dahulu dan membayar di kemudian hari dengan sistem cicilan atau sekali bayar, sehingga memberikan kemudahan dan fleksibilitas dalam bertransaksi (S. M. Sulubara, 2024a).

Namun, peningkatan penggunaan Shopee PayLater juga menimbulkan potensi risiko keamanan digital. Berbagai ancaman cybercrime seperti pencurian data, penyalahgunaan identitas, dan serangan siber lainnya semakin mengancam keamanan dan privasi pengguna. Ancaman ini jika tidak ditangani dengan baik dapat mengakibatkan kerugian finansial dan menurunkan kepercayaan konsumen terhadap layanan digital. Oleh karena itu, analisis risiko cybercrime pada layanan Shopee PayLater menjadi sangat penting untuk memastikan keamanan data pengguna dan mendukung keberlanjutan layanan (Seri Mughni Sulubara et al.,

2023). Penelitian ini bertujuan mengidentifikasi ancaman utama yang dihadapi, serta mengevaluasi implikasi risiko tersebut terhadap keamanan data pengguna dalam platform Shopee PayLater. Langkah ini diharapkan mendorong penguatan sistem keamanan siber yang lebih efektif dan perlindungan pengguna yang lebih optimal.

Shopee PayLater bekerja sama dengan perusahaan fintech seperti PT. Lentera Dana Nusantara dalam menyediakan layanan pinjaman instan yang mendukung sistem cicilan tanpa kartu kredit. Dengan kemudahan akses dan proses yang singkat, layanan ini mendapat respons positif dengan jumlah pengguna yang terus meningkat. Namun, perkembangan pesat ini juga membawa risiko keamanan, terutama risiko cybercrime yang dapat mengancam data pribadi dan transaksi keuangan (Sulubara, Seri Mughni, Tasril, Virdyra, 2025).

Risiko dan ancaman tersebut memerlukan perhatian serius untuk menjaga kepercayaan pengguna dan mengamankan data dari potensi penyalahgunaan di era digital (Riska, Seri Mughni Sulubara, 2025). Oleh sebab itu, penelitian ini penting untuk menganalisis risiko cybercrime pada layanan Shopee PayLater dan bagaimana hal tersebut berimplikasi pada keamanan data pengguna sehingga dapat dihasilkan rekomendasi untuk meningkatkan sistem keamanan yang lebih efektif.

Analisis risiko cybercrime pada layanan Shopee PayLater dan implikasi terhadap keamanan data pengguna merupakan topik yang sangat relevan dan penting dalam era digital saat ini. Shopee, sebagai salah satu platform e-commerce terbesar di Indonesia, telah berkembang pesat sejak peluncurannya pada Desember 2015 di bawah naungan SEA Group. Perkembangan ini tidak hanya mencakup peningkatan jumlah pengguna dan transaksi, tetapi juga inovasi dalam fitur pembayaran digital seperti Shopee PayLater yang diluncurkan pada 6 Maret 2019. Fitur Shopee PayLater memberikan kemudahan bagi pengguna untuk melakukan pembelian dengan sistem bayar nanti, baik secara cicilan maupun sekaligus, yang meningkatkan fleksibilitas dan kenyamanan bertransaksi di platform Shopee.

Meski kemudahan ini membawa keuntungan bagi konsumen, terdapat risiko serius yang mengancam keamanan data pengguna, terutama risiko cybercrime. Layanan PayLater yang mengelola data sensitif seperti informasi pribadi, data transaksi, serta data finansial rentan terhadap serangan siber seperti pencurian identitas, phishing, malware, dan pencurian data internal. Ancaman-ancaman ini berpotensi menimbulkan kerugian finansial yang besar dan menurunkan kepercayaan pengguna terhadap layanan. Oleh karena itu, sangat penting untuk menganalisis risiko-risiko tersebut secara menyeluruh.

Selain risiko teknis, risiko privasi juga menjadi perhatian utama, dimana kebocoran data, penyalahgunaan data oleh pihak internal maupun eksternal, dan kurangnya transparansi dalam pengelolaan data pengguna dapat mengancam privasi konsumen. Analisis risiko ini tidak hanya membantu dalam mengenali potensi ancaman, tetapi juga memberikan dasar bagi pengembangan sistem

keamanan siber yang lebih baik serta kebijakan perlindungan data yang efektif. Penelitian ini akan mengkaji secara mendalam berbagai aspek risiko cybercrime yang menimpa Shopee PayLater dan bagaimana risiko tersebut berdampak pada keamanan data pengguna, dengan tujuan akhir meningkatkan ketahanan sistem dan melindungi hak privasi pengguna di Indonesia.

METODE

Metode penelitian yang digunakan dalam analisis risiko cybercrime pada layanan Shopee PayLater dan implikasi terhadap keamanan data pengguna ini bersifat kualitatif-deskriptif dengan pendekatan studi kasus. Pendekatan ini dipilih untuk memperoleh pemahaman mendalam mengenai berbagai risiko cybercrime yang mengancam layanan PayLater serta bagaimana dampaknya terhadap keamanan data pengguna. Penelitian ini menggabungkan analisis literatur, pengumpulan data primer melalui wawancara, serta studi dokumentasi terkait kebijakan dan mekanisme keamanan Shopee PayLater. Tahap pertama metode ini adalah studi literatur yang komprehensif, dimana data dikumpulkan dari sumber sekunder seperti artikel jurnal, laporan industri, dokumentasi resmi Shopee, serta regulasi dan kebijakan perlindungan data di Indonesia. Studi literatur ini bertujuan untuk mengidentifikasi kerangka teori, jenis-jenis ancaman cyber, serta praktik terbaik dalam cybersecurity layanan keuangan digital.

Data yang terkumpul kemudian dianalisis menggunakan teknik analisis isi untuk mengidentifikasi tema-tema utama mengenai ancaman cyber, tingkat risiko yang dihadapi, serta efektivitas mekanisme keamanan. Analisis ini juga mencakup evaluasi terhadap implikasi risiko tersebut terhadap keamanan data pengguna, baik dari segi teknis maupun kebijakan privasi. Metode penelitian ini diharapkan menghasilkan pemahaman yang mendalam dan komprehensif mengenai risiko cybercrime pada Shopee PayLater serta memberikan rekomendasi strategis dalam pengelolaan keamanan data yang lebih baik bagi layanan e-commerce di Indonesia. Pendekatan kualitatif ini memungkinkan eksplorasi aspek teknis, perilaku pengguna, dan kebijakan yang tidak mudah diperoleh melalui metode kuantitatif saja, sehingga memberikan kontribusi signifikan pada pengembangan literatur dan praktik cybersecurity di bidang fintech

HASIL DAN PEMBAHASAN

Hasil analisis risiko cybercrime pada layanan Shopee PayLater mengungkap berbagai kerentanan dan ancaman serius yang mengancam keamanan data pengguna, sekaligus dampak nyata terhadap pengalaman dan kepercayaan konsumen (S. M. Sulubara & Tasril, Virdyra, 2025). Dari segi teknis, ditemukan bahwa aplikasi Shopee PayLater masih memiliki beberapa celah kerentanan, terutama terkait perizinan aplikasi, proses verifikasi melalui OTP (One Time Password), dan potensi aktivitas malware yang dapat dimanfaatkan oleh pelaku kejahatan siber untuk mengakses data pribadi pengguna tanpa izin. Misalnya, penyalahgunaan kode OTP berpotensi menjadi celah untuk pembajakan

akun yang memungkinkan transaksi ilegal dan pencurian identitas (S. M. Sulubara, Tasril, et al., 2025).

Risiko kebocoran data pribadi juga semakin meningkat seiring pertumbuhan pesat penggunaan layanan PayLater di Indonesia, yang pada 2025 mencatat volume transaksi dan nilai utang mencapai triliunan rupiah. Data pribadi yang bocor seperti nama, alamat, nomor telepon, dan data keuangan dapat disalahgunakan untuk penipuan, pengambilalihan akun, dan pembukaan kredit ilegal. Kejadian serupa telah terjadi dimana data pribadi pengguna dimanfaatkan oleh pihak tidak bertanggung jawab, menimbulkan kerugian finansial dan psikologis bagi pengguna.

Selain risiko teknis, risiko sosial dan privasi juga mengemuka. Pengguna Shopee PayLater menunjukkan kekhawatiran yang cukup tinggi terkait keterlambatan pembayaran, potensi denda, dan keamanan data pribadi mereka. Kurangnya transparansi dari penyelenggara layanan dalam menginformasikan pengguna mengenai pengelolaan data dan mekanisme perlindungan memperbesar kerentanan pengguna terhadap modus penipuan dan phishing (Murthada Murthada & Seri Mughni Sulubara, 2022). Penipuan melalui peniruan situs resmi dan penyamaran sebagai pihak resmi PayLater menjadi modus umum yang mengancam keamanan pengguna (Sulubara, Seri Mughni Lubis, Hidayati Purnama, Simbolon, 2024).

Di sisi mitigasi, Shopee PayLater melalui PT Commerce Finance telah berizin dan diawasi oleh Otoritas Jasa Keuangan (OJK), serta menerapkan berbagai protokol keamanan siber yang ketat. Namun, efektivitas keamanan ini sangat bergantung pada kesadaran dan kewaspadaan pengguna dalam melindungi data pribadi, seperti tidak membagikan kode OTP, memeriksa keaslian situs atau komunikasi yang diterima, serta memilih platform dengan legalitas jelas. Edukasi keamanan digital menjadi salah satu kunci untuk mengurangi risiko serangan cybercrime (S. M. Sulubara, Fauzi, et al., 2025).

Hasil penelitian ini menunjukkan perlunya peningkatan sistem keamanan, termasuk penguatan enkripsi data, audit berkala terhadap aplikasi, pengembangan fitur autentikasi multi-faktor, serta transparansi kebijakan privasi untuk membangun kepercayaan pengguna. Selain itu, keterlibatan pemerintah dan lembaga pengawas dalam mengatur dan mengawasi layanan paylater sangat penting untuk meminimalisir risiko cybercrime dan melindungi konsumen dalam ekosistem digital yang semakin kompleks ini. Dengan pemahaman mendalam terhadap risiko dan implementasi tindakan keamanan yang komprehensif, layanan Shopee PayLater dapat meningkatkan keamanan data pengguna dan memperkuat posisi sebagai inovasi pembayaran digital terpercaya di Indonesia

1. Risiko Cybercrime dan Penyalahgunaan Data

Ancaman utama berupa pencurian dan penyalahgunaan data pribadi, pembajakan akun melalui pengambilan kode OTP, dan penipuan digital merupakan risiko signifikan yang dialami pengguna. Lonjakan penggunaan Shopee PayLater yang mencapai nilai transaksi triliunan rupiah meningkatkan

peluang serangan siber dan dampak kerugian finansial. Risiko cybercrime yang dialami pengguna Shopee PayLater sangat nyata dan beragam, dengan ancaman utama berupa pencurian dan penyalahgunaan data pribadi yang dapat menyebabkan kerugian finansial besar. Salah satu modus yang sering terjadi adalah pembajakan akun melalui pengambilan kode OTP (One Time Password) yang kemudian digunakan untuk transaksi ilegal tanpa sepengetahuan pengguna. Kasus nyata terjadi seperti dialami seorang pengguna di Palembang yang akunnya dibobol dan terjadi transaksi Shopee PayLater tanpa izin, mengakibatkan tagihan besar yang bukan tanggung jawab pengguna tersebut (S. M. Sulubara, 2024b).

Lonjakan penggunaan Shopee PayLater yang mencapai nilai transaksi triliunan rupiah meningkatkan peluang bagi pelaku kejahatan untuk menargetkan sistem dan pengguna layanan ini. Kejahatan digital ini tidak hanya berdampak pada kerugian finansial tapi juga menimbulkan ketidakpercayaan pengguna terhadap keamanan platform. Keamanan data pribadi pengguna yang bocor dapat disalahgunakan untuk pembukaan kredit ilegal, tindakan penipuan, atau pencurian identitas. Selain itu, risiko keamanan data juga timbul dari celah teknis pada aplikasi, seperti kerentanan dalam proses perizinan dan autentikasi pengguna yang dapat dieksploitasi, serta potensi aktivitas malware. Walaupun Shopee sudah menerapkan protokol keamanan dan pengawasan regulasi dari OJK, implementasi keamanan harus terus ditingkatkan sesuai evolusi ancaman siber agar perlindungan data pengguna optimal (S. M. A. A. Sulubara, 2024).

Dari sisi hukum, perlindungan terhadap korban juga belum sepenuhnya memadai, dengan upaya penyelesaian sengketa dan penanganan kasus kebocoran data yang seringkali memakan waktu lama dan belum memberikan kepastian perlindungan penuh bagi pengguna. Edukasi dan kesadaran pengguna dalam menjaga keamanan akun, seperti tidak membagikan kode OTP dan memverifikasi aktivitas transaksi, menjadi krusial mengingat sisi teknis tidak dapat menjamin keamanan mutlak tanpa partisipasi aktif pengguna (S. M. Sulubara et al., 2023).

Contoh tuntutan hukum dan klaim ganti rugi terhadap platform e-commerce di Indonesia umumnya berkaitan dengan perlindungan konsumen yang diatur dalam Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen dan Undang-Undang Informasi dan Transaksi Elektronik (ITE). Konsumen memiliki hak untuk menuntut kompensasi dan ganti rugi apabila mengalami kerugian akibat perbuatan pelaku usaha, termasuk penyelenggara platform e-commerce seperti Shopee. Beberapa contoh kasus dan mekanisme tuntutan hukum meliputi:

a. Konsumen yang dirugikan oleh transaksi online buruk, seperti barang tidak sesuai atau cacat, bisa mengajukan gugatan perdata konvensional atau gugatan kelompok (class action) terhadap penyelenggara maupun penjual di platform e-commerce.
b. Badan Penyelesaian Sengketa Konsumen (BPSK) berwenang menyelesaikan sengketa konsumen melalui mediasi, arbitrase, atau konsiliasi sebelum proses pengadilan, termasuk memutuskan kewajiban ganti rugi bagi pelaku usaha.

c. Sanksi administratif dapat dijatuhkan kepada pelaku usaha berupa denda hingga Rp 200 juta serta perintah penghentian kegiatan yang merugikan konsumen.
d. Pengadilan juga dapat memerintahkan pembayaran ganti rugi, penarikan barang dari peredaran, atau bahkan pencabutan izin usaha bagi pelaku usaha yang terbukti melanggar hukum perlindungan konsumen

Dalam kasus tertentu, pengguna e-commerce juga dapat menuntut pertanggungjawaban platform e-commerce sebagai penyedia sistem elektronik jika terbukti gagal mengawasi dan menjaga keamanan transaksi atau data pengguna sehingga menimbulkan kerugian. Namun, tanggung jawab ini masih dalam perdebatan hukum dan memerlukan bukti keterlibatan atau kelalaian platform (Riska, Seri Mughni Sulubara, 2025). Sebagai contoh, Shopee pernah dituntut oleh konsumen yang rugi akibat transaksi penipuan atau produk cacat dan proses pengembalian dana yang tidak lancar. Konsumen dapat mengajukan klaim ganti rugi sesuai besaran kerugian dan prosesnya melalui mekanisme penyelesaian sengketa yang berlaku.

Secara umum, perlindungan hukum terhadap konsumen e-commerce mencakup hak atas informasi yang benar dan jelas, hak mendapat barang/jasa yang sesuai, serta hak untuk diperlakukan adil dan mendapatkan penyelesaian jika dirugikan, dan ini menjadi dasar pelaksanaan tuntutan hukum dan klaim ganti rugi terhadap platform e-commerce yang lalai atau bertanggung jawab atas kerugian konsumen (Seri Mughni Sulubara, Murthada, 2023).

2. *Rekomendasi Kebijakan dan Regulasi Perlindungan Data Pribadi di Fintech*

Rekomendasi kebijakan dan regulasi perlindungan data pribadi di sektor fintech, khususnya untuk layanan seperti Shopee PayLater, meliputi beberapa poin penting yaitu (Seri Mughni Sulubara, Hidayati Purnama Lubis, Nanci Yosepin Simbolon, 2024):

a. Penegakan Regulasi Data Pribadi yang Ketat, Pemerintah perlu memperkuat penerapan Undang-Undang Perlindungan Data Pribadi (UU PDP) dengan menetapkan standar teknis keamanan data yang wajib dipatuhi oleh penyelenggara fintech. Regulasi harus mencakup kewajiban pelaporan insiden kebocoran data kepada otoritas dan pengguna secara transparan dan cepat.
b. Pengawasan dan Audit Berkala, Otoritas seperti OJK dan KOMINFO harus rutin melakukan audit keamanan dan evaluasi kepatuhan terhadap peraturan perlindungan data, serta memberikan sanksi tegas bagi pelanggaran. Monitor dan evaluasi juga terhadap implementasi teknologi keamanan seperti enkripsi dan autentikasi multi-faktor.
c. Transparansi Kebijakan Privasi, Platform fintech wajib menyampaikan kebijakan privasi yang mudah dipahami oleh konsumen, menjelaskan jenis data yang dikumpulkan, tujuan penggunaannya, dan durasi penyimpanan data. Pengguna harus diberikan pilihan kontrol atas data pribadi mereka,

termasuk opsi untuk menghapus data (Sulubara, Seri Mughni, Lubis, Hidayati Purnama, Simbolon, Nanci Yosepin, Razi, 2024).

d. Edukasi Pengguna dan Literasi Digital, Program edukasi nasional dan kampanye literasi digital perlu digalakkan agar pengguna fintech memahami pentingnya menjaga keamanan data, mengenali modus penipuan, dan menggunakan fitur keamanan yang tersedia.
e. Mekanisme Penyelesaian Sengketa yang Efektif, Ketersediaan mekanisme penyelesaian sengketa konsumen yang sederhana, cepat, dan adil, termasuk mediasi dan arbitrase, khususnya untuk kasus kebocoran data dan penipuan digital di fintech.
f. Kolaborasi antar Stakeholder, Sinergi antara pemerintah, penyelenggara fintech, asosiasi industri, dan komunitas pengguna untuk mengembangkan standar keamanan, berbagi informasi ancaman, dan merespons insiden cyber secara kolektif.
g. Penegakan Hukum Terhadap Pelaku Kejahatan Siber, Perkuat kapasitas aparat penegak hukum dalam menangani kasus cybercrime khususnya yang melibatkan penyalahgunaan data pribadi di fintech, dengan koordinasi internasional untuk melacak pelaku lintas negara

Penguatan Regulasi Nasional: Perlu dilakukan penguatan undang-undang perlindungan data pribadi (seperti UU PDP) yang mencakup fintech dengan standar keamanan teknis yang jelas, kewajiban pelaporan insiden, dan mekanisme perlindungan yang menyeluruh. Pengawasan dan Audit Berkala: Otoritas seperti OJK dan KOMINFO harus rutin melakukan audit kepatuhan terhadap regulasi data pribadi dan keamanan siber, dengan pemberian sanksi tegas bagi pelanggaran (Sulubara, Seri Mughni Lubis, Hidayati Purnama, Simbolon, 2024). Transparansi dan Kontrol Pengguna: Platform fintech wajib memberikan informasi yang jelas dan transparan terkait pengumpulan, penggunaan, dan penyimpanan data. Pengguna harus memiliki kontrol penuh atas data pribadinya, termasuk hak untuk menghapus data.

Edukasi dan Literasi Digital: Mendorong program edukasi bagi konsumen fintech untuk memahami risiko dan cara melindungi data pribadi mereka, serta mengenali modus kejahatan siber. Penyelesaian Sengketa Efektif: Menyediakan mekanisme cepat dan adil untuk penyelesaian sengketa terkait pelanggaran data dan kerugian akibat tindakan cybercrime (Azrica & Sulubara, 2023). Kolaborasi Multi Pihak: Mendukung kerja sama antara regulator, penyedia layanan fintech, komunitas teknologi, dan penegak hukum untuk berbagi informasi dan memperkuat sistem keamanan secara kolektif. Penegakan Hukum: Meningkatkan kapasitas aparat dalam mengusut dan menangani kasus pelanggaran data serta cybercrime di sektor fintech, dengan koordinasi internasional bila diperlukan

SIMPULAN

Layanan Shopee PayLater yang menawarkan kemudahan transaksi "beli sekarang, bayar nanti" memiliki potensi risiko cybercrime yang signifikan. Kasus

nyata seperti pembajakan akun, pencurian data pribadi, dan transaksi tanpa izin telah terjadi, mengakibatkan kerugian finansial yang besar dan kerusakan kepercayaan pengguna terhadap platform. Cybercrime dalam bentuk penyalahgunaan kode OTP, peretasan akun, dan pencurian identitas menjadi ancaman utama yang harus diwaspadai dalam ekosistem fintech ini. Selain aspek teknis, risiko tersebut berimplikasi serius terhadap privasi pengguna, termasuk kebocoran data dan penyalahgunaan informasi pribadi. Pengelolaan dan perlindungan data yang belum optimal memperbesar potensi kerugian dan menurunkan kepercayaan konsumen. Shopee PayLater sebagai layanan yang diawasi OJK telah berkomitmen untuk menjaga keamanan data, namun kasus kebocoran dan peretasan menunjukkan perlunya peningkatan terus-menerus dalam sistem keamanan siber. Dari sisi hukum, masih terdapat tantangan dalam memberikan perlindungan menyeluruh kepada korban, termasuk proses pengaduan yang kompleks dan belum adanya perlindungan konsumen digital yang memadai. Edukasi kepada pengguna dan transparansi kebijakan menjadi kunci penting agar konsumen dapat memahami risiko dan cara melindungi diri mereka sendiri. Pendekatan mitigasi yang efektif mencakup peningkatan protokol keamanan seperti autentikasi multi-faktor, audit reguler, transparansi kebijakan privasi, serta penegakan regulasi dan sanksi tegas dari pemerintah dan regulator terkait. Kolaborasi antara penyedia layanan, regulator, dan pengguna sangat diperlukan untuk membangun ekosistem fintech yang aman, terpercaya, dan berkelanjutan.

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, Hidayati Purnama Lubis, Nanci Yosepin Simbolon, F. R. (2024). Shopee Paylater Transactions in the Shopee Application In Legal Perspective. Annual International Conference on Islamic Economics and Business, 1(2), 64–71.

Seri Mughni Sulubara, Murthada, A. (2023). Penegakan Hukum Terhadap White collar crime Insider Trading Dalam Pasar Modal. Jurnal Ilmiah Penegakan

Hukum, 10(2), 184–190. https://doi.org/http://dx.doi.org/10.31289/jiph.v10i2.10445

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., Basri, T. S., & . F. (2023). Legal Aspects of E-Commerce Agreements in Shopee Platform in The Civil Law Code (Burgerlijk Wetboek). International Journal of Research and Review, 10(6), 690–699. https://doi.org/10.52403/ijrr.20230683

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

