Maliki Interdisciplinary Journal (MIJ) eISSN: 3024-8140
Volume 3, Issue Maret, 2025 pp. 556-561 http://urj.uin-malang.ac.id/index.php/mij/index

Pengaruh Ancaman, Risiko, dan Strategi Pengamanan Terhadap Keamanan Data Pribadi pada Pengguna E-Commerce

Siti Khotimah
[1]*Program Studi Manajemen, Universitas Islam Negeri Maulana Malik Ibrahim Malang*
*e-mail: *khot06jan04@gmail.com*

Kata Kunci:
e-commerce, keamanan, data pribadi

Keywords:
e-commerce, security, personal data

A B S T R A K

E-commerce adalah suatu bentuk perdagangan online di mana pelanggan memberikan informasi pribadi seperti nama, alamat, nomor telepon, nomor kartu kredit, dll. Apabila informasi itu jatuh ke tangan orang yang salah, maka pengguna bisa mengalami kerugian finansial atau bahkan identitasnya dicuri dan disalahgunakan oleh orang yang tidak bertanggung jawab. Ancaman terhadap keamanan informasi pribadi dalam e-commerce mencakup serangan kriminal atau tinkat lanjut yang mengancam keamanan, privasi, dan kejahatan pengguna. Dampak dari ancaman-ancaman ini terhadap keamanan data pribadi di e-commerce sangat besar dan berdampak baik bagi pemilik bisnis maupun pelanggan. Risiko yang terkait dengan keamanan data pribadi dalam e-commerce bisa menyebabkan pembobolan data yang bisa merugikan pengguna dan perusahaan penyedia layanan e-commerce. Penerapan strategi keamanan yang tepat dapat membantu melindungi data pribadidan informasi penting lainnya dari serangan siber. Penggunaan OTP (One Time Password)oleh Tokopedia merupakan salah satu contoh strategi keamanan yang dapat membantu melindungi data pribadi. Semakin membaik strategi keamanan yang digunakan, maka akan semakin rendah pula risiko kejahatan siber terhadap data pribadi. Oleh karena itu, baik pemilik bisnis e-commerce maupun pengguna harus memiliki strategi keamanan yang baik untuk menjamin keamanan data pribadi.

A B S T R A C T

E-commerce is a form of online commerce where customers provide personal information such as name, address, phone number, credit card number, etc. If that information falls into the wrong hands, then the user can suffer financial loss or even have their identity stolen and misused by irresponsible people. Threats to personal information security in e-commerce include criminal or advanced attacks that threaten users' security, privacy and crime. The impact of these threats to personal data security in e-commerce is substantial and impacts both business owners and customers. The risks associated with personal data security in e-commerce can lead to data breaches that can be detrimental to both users and e-commerce service providers. Implementing the right security strategies can help protect personal data and other critical information from cyber-attacks. Tokopedia's use of OTP (One Time Password) is one example of a security strategy that can help protect personal data. The better the security strategy used, the lower the risk of cybercrime against personal data. Therefore, both e-commerce business owners and users must have a good security strategy to ensure the safety of personal data.

Pendahuluan

Saat ini teknologi menjadi semakin maju dan berkembang sangat cepat. Salah satu bukti dari teknologi itu adalah Internet. Internet adalah sistem komunikasi global yang menghubungkan komputer ke jaringan komputer di seluruh dunia. Pemanfaatan internet dan telepon genggam tidak hanya sekedar untuk mencari berbagai informasi dan berkomunikasi, masyarakat saat ini menggunakan internet khususnya e-commerce.

Dampak positif dari penggunaan e-commerce adalah cakupan pasar yang lebih luas, fleksibilitas, peningkatan pendapatan dan pengurangan risiko biaya-biaya lainnya, pelayanan yang maksimal, serta feedback berupa review pembeli yang dapat dijadikan tolak ukur dalam bisnis. Selain sisi positifnya, E-commerce juga mempunyai sisi negatif yaitu rawan terhadap kejahatan cyber seperti pencurian identitas dan penipuan yang menipu pelanggan, kejahatan kartu kredit, phishing, spammer, dll. Ancaman keamanan ini akan menyebabkan customer menjadi takut untuk melakukan transaksi sehingga menyebabkan pelanggan kembali ke cara bisnis yang tradisional. Jika setiap pelaku bisnis e-commerce menyadari pentingnya keamanan sejak awal, masalah di atas bisa diperkirakan.

E-commerce di Indonesia mengacu pada aktivitas perdistribusian, penjualan, pembelian, dan perdagangan barang atau jasa. Dengan adanya penggunaan jaringan komunikasi seperti internet, televisi atau jaringan komputer lainnya. Meski memberikan kemudahan dan kenyamanan, tapi juga bisa membawa risiko terhadap keamanan. Keamanan mencakup perlindungan sumber fisik dan konseptual dari bahaya alam atau buatan manusia. Keamanan sumber daya konseptual seperti data dan informasi. Masalah utama dalam lingkungan e-commerce saat ini adalah masalah privasi dan keamanan mengenai data pribadi (Yazdanifard et al., 2011). Data pribadi seperti nama, alamat, nomor telepon, dan informasi lainnya dapat dengan mudah dicuri atau disalahgunakan oleh orang yang tidak mau bertanggung jawab. Ancaman keamanan terhadap pengguna e-commerce dari data pribadi bervariasi dan mencakup serangan malware, phishing, peretasan, dan pencurian identitas. Risiko yang ditimbulkan oleh pelanggaran keamanan data pribadi tidak hanya akan merugikan kepentingan ekonomi pengguna, namun juga merusak reputasi sosial mereka.

E-commerce menghadapi masalah keamanan dan privasi yang mengancam keselamatan konsumen. Penggunaan data pribadi dalam transaksi e-niaga dapat menyebabkan pelanggaran data, yang dapat membahayakan privasi konsumen. Kebocoran data pribadi dari perusahaan e-commerce merupakan ancaman nyata bagi konsumen. Oleh karena itu, perusahaan e-commerce perlu memastikan keamanan sistem mereka dan meningkatkan langkah-langkah keamanannya. Perlindungan data pribadi sangat penting untuk menjaga kepercayaan dan keyakinan konsumen terhadap e-commerce. Pemerintah perlu memberikan kepastian hukum dan menjamin perlindungan privasi konsumen. Pentingnya melindungi hak privasi individu didasarkan pada prinsip otonomi, kemandirian pribadi, dan martabat. Perusahaan e-commerce perlu memastikan privasi pelanggannya dengan melindungi identitas, kesetaraan, keamanan, dan kepercayaan mereka. Kurangnya kepercayaan antara pelanggan dengan perusahaan e-commerce dapat menyebabkan menurunnya transaksi e- commerce. Oleh karena itu, perusahaan e-commerce perlu mengatasi masalah privasi dan kepercayaan untuk menjaga kepercayaan konsumen.

Metode Penelitian

Penelitian ini menggunakan metode kajian pustaka dengan mencari sumber atau bahan dan informasi yang berhubungan dengan topik keamanan dan privasi e-commerce dari sumber-sumber secara literatur, baik dari buku, jurnal, dan artikel-artikel dari situs tertentu. Penelitian ini melibatkan analisis mendalam terhadap literatur yang membahas tentang faktor-faktor yang mempengaruhi keamanan dan privasi e-commerce atau perdagangan elektronik dan menganalisis sumber informasi yang ditemukan untuk menentukan hubungan antara faktor-faktor tersebut.

Manfaat Penelitian

Manfaat penelitian dari artikel ini adalah agar pembaca memahami dan menyadari pentingnya keamanan pada data pribadi pada penggunaan e-commerce serta memberikan pemahaman lebih mendalam bagaimana menjaga keamanan data pribadi di era teknologi saat ini.

Kajian teori

Dilihat dari prinsipnya, dapat dikatakan bahwa transaksi e-commerce mirip dengan transaksi jual beli pada umumnya, namun ada beberapa hal yang membedakannya yaitu mereka melakukannya melalui media online. Akibatnya keamanan transaksi e-commerce sering menjadi masalah utama. Salah satunya melalui metode penipuan. Baik pelaku usaha maupun konsumen yang buruk dapat melakukan penipuan ini. Penipuan adalah salah satu jenis kejahatan komputer. Penipuan jenis ini menjadi semakin umum. Secara khusus, banyak orang ingin memenuhi kebutuhan mereka dengan mudah dan menghemat waktu dan uang. Meskipun aktivitas ini dilakukan secara online, mereka dapat dikategorikan sebagai tindakan dan proses nyata. Penjahat dunia maya ini adalah penjahat yang memanfaatkan kelemahan dan kebiasaan keamanan orang saat menggunakan Internet.

Electronic commerce atau disingkat dengan e-commerce didefinisikan sebagai serangkaian proses jual beli, memasarkan produk yang berupa informasi, barang atau jasa, membentuk kontrak perjanjian mengenai harga dan produk serta menyelesaikan transaksi melalui sistem elektronik dan jaringan internet. E-commerce adalah transaksi komersial yang melibatkan pertukaran nilai melalui penggunaan teknologi digital antar individu. Proses transaksi bisnis pada e-commerce menggunakan berbagai jenis media seperti internet, WorldWide Web, browser maupun aplikasi pada perangkat seluler. Menurut pendapat (Ahmed, 2021)Dampak dari risiko yang dirasakan pada pengguna berdampak pada keamanan dan kemauan berbelanja online. Ketika risiko yang dirasakan lebih tinggi, niat membeli secara online menurun. Meningkatnya risiko akan menurunkan tingkat keamanan data pada e-commerce.

Menurut dari (Wajong, 2010) Masih banyak celah ancaman yang dihadapi sistem keamanan e-commerce, termasuk ancaman terhadap keamanan data pribadi. Ke depannya, diharapkan bisnis e-commerce dapat terus berkembang dan konsisten dengan perkembangan keamanan. Menurut (Nugroho, 2021) Mengatakan bahwa pelanggaran privasi ini terjadi karena sistem perlindungan yang dipakai e-commerce

lemah sehingga memungkinkan pedagang, yaitu individu atau perusahaan dengan mudah mencuri data pelanggan e-commerce. Selain itu, karena kurangnya undang-undang khusus yang wajib dan kuat untuk perlindungan informasi pribadi, kebocoran informasi pribadi juga dapat terjadi.

Hasil dan pembahasan

Ancaman mempunyai dampak yang besar pada keamanan data pribadi e-commerce. Karena e-commerce merupakan suatu bentuk perdagangan yang dilakukan online yang dimana pelanggan melakukan transaksi dengan memberi informasi seperti nama, alamat, No. telepon karti kreditnya dan lain-lain. Apabila informasi ini jatuh ke tangan orang yang tidak tepat, pengguna bisa mengalami kerugian finansial atau bahkan identitasnya bisa dicuri dan disalahgunakan. Dengan menerapkan kebijakan keamanan yang tepat, pemilik e-commerce dapat memastikan bahwa data dan informasi pribadinya tidak digunakan oleh orang lain. Yang penting terlindungi dari seranga siber. Namun, bukan hanya satu pihak saja atau pemilik perusahaan yang harus memiliki kebijakan keamanan yang baik, pengguna juga harus memiliki strategi bagaimana menjaga keamanan data. Karena jika kebijakan keamanan buruk, tingkat kerentanan keamanan data meningkat akibat serangan siber.

Pengaruh Ancaman

Ancaman bisa diartikan sebagai tindakan atau usaha yang dilakukan oleh individu atau kelompok tertentu yang berpotensi menimbulkan risiko ataupun ancaman kelompok lain. Dalam konteks e-commerce, ancaman terhadap data pribadi pengguna terjadi dalam bentuk kejahatan atau serangan siber yang mengancam privasi serta dapat memicu aksi kejahatan. Ancaman keamanan yang serius di sistem keamanan ini tidak hanya berdampak negatif pada pelaku bisnis, tetapi juga bagi konsumen yang mempercayakan data mereka (Nafi'ah, 2020). Penulis menyimpulkan bahwa makin meningkatnya ancaman ini dapat semakin berisiko terhadap keamanan data pribadi pengguna (Batmetan, 2019) Menjelaskan bahwa risiko terhadap keamanan data pribadi di e-commerce berpotensi membahayakan pengguna.

Sebagai platform perdagangan atau jual beli daring, Ancaman mempunyai dampak yang signifikan dalam keamanan data pribadi di e-commerce. Ini karena e-commerce adalah bentuk kegiatan jual beli yang secara online, yang di mana para pelanggan atau konsumen melakukan transaksi dengan memberikan informasi pribadi seperti nama pengguna, alamat, nomor telepon, ataupun nomor kartu kredit, dan lain-lain. Apabila informasi-informasi itu jatuh ke pihak yang salah atau tidak bertanggung jawab, pengguna e-commerce bisa mengalami kerugian finansial, bahkan indentitasnya bisa dicuri atau disalahgunakan. Sebelumnya, (Batmetan, 2019) juga mempelajari dampak cybercrime dan e-commerce melalui penelitian terhadap 30 responden sebagai sampel penelitian. Dalam penelitian menunjukkan bahwa 78% orang lebih menyukai transaksi e-commerce. 80% respinden mengatakan penipuan online sering terjadi di pasar tertentu.

Hal ini tentu menjadi bukti bahwa banyak masyarakat yang merasa khawatir saat berbelanja dan bertransaksi online melalui e-commerce. Hal ini menandakan bahwa unsur keamanan privasi pengguna masih rentan terhadap ancaman kejahatan dan

cybercrime yang menyerang pengguna baik dari pihak penjual maupun pembeli, yang dapat mengakibatkan kerugian akibat penyalahgunaan informasi personal atau data pribadi.

Pengaruh Risiko

Berdasarkan Kamus Besar atau KBBI risiko dipahami sebagai akibat yang bisa merugikan, atau membahayakan dari suatu tindakan atau perbuatan. Ancaman kejahatan dunia maya yang terkait dengan data pribadi bagi pengguna e-commerce tentu merugikan pihak pengguna dan pelaku bisnis. Tidak ada tindakan yang tidak disertai risiko. Terkait dengan keamanan data pribadi, terdapat risiko yang memungkinkan terjadinya kerusakan maupun hilangnya data pribadi, serta potensi dampak negatifnya terhadap bisnis seperti publisitas negatif, sanksi hukum, atau kehilangan pelanggan. Penulis berasumsi bahwa risiko ini secara mendasar juga berdampak pada keamanan data pribadi pengguna e-commerce.

Risiko itu dapat membahayakan keamanan informasi pribadi pengguna e-commerce karena dalam transaksi e-commerce, karena pengguna memberikan informasi pribadi iseperti nama, alamat, nomor telepon, dan nomor kartu kredit, dan informasi keuangan lainnya selama transaksi. Risiko terhadap keamanan informasi pribadi pengguna e-commerce dapat mengakibatkan pelanggaran keamanan data dan merugikan pengguna dan perusahaan penyedia layanan e-commerce.

Pengaruh Strategi Pengamanan

Strategi dijelaskan sebagai proses seseorang merencanakan untuk melakukan tugas untuk mencapai tujuan tertentu. Sistem yang rentan dalam infrastruktur e-commerce dapat diekspolitasi sebagai kerentanan oleh penjahat dunia maya untuk mengakses data pelanggan, artikel ini membahas tentang strategi keamanan terhadap ancaman data pribadi pengguna e-commerce. Penulis berhipotesis bahwa strategi keamanan ini mempengaruhi keamanan data pribadi pengguna.Keamanan data pribadi pengguna e-commerce dipengaruhi oleh kebijakan keamanan. Kebijakan keamanan yang tepat dapat membantu melindungi data pengguna dari ancaman keamanan. Jika kebijakan keamanan ditingkatkan, kejadian kejahatan dunia maya yang menargetkan keamanan data pribadi berkurang. Oleh karena itu, untuk strategi keamanan yang diterapkan pada e-commerce, sangat penting untuk menjaga keamanan data pribadi pengguna. Seperti halnya Tokopedia, menurut (Pratama, 2022) yang dalam analisisnya menyatakan bahwa Tokopedia menggunakan kebijakan keamanan OTP (one-time-password) sebagai bentuk perlindungan kebijakan ketika konsumen ingin, 1 login ke akun pengguna. Dengan menerapkan strategi keamanan ini, keamanan data pribadi pengguna semakin terjaga.

Jika strategi yang tepat diterapkan, pemilik e-commerce dapat menjaga data pribadi pelanggan dan informasi penting lainnya tetap aman dari serangan siber. Namun, tidak hanya pemilik perusahaan yang harus memiliki kebijakan keamanan yang baik, pengguna juga harus memiliki kebijakan keamanan untuk memastikan datanya aman. Sebab, jika kebijakan keamanan tidak baik maka tingkat keamanan data pribadi akan semakin rentan terhadap serangan siber. Pemilik e-commerce dapat memastikan bahwa data pribadi pelanggan dan informasi penting lainnya terlindungi dari serangan cyber

jika melakukan penerapan strategi yang tepat. Namun, bukan hanya pemilik perusahaan e-commerce saja yang harus memiliki strategi pengamanan yang baik, tapi dari pihak pengguna juga harus mempunyai strategi keamanan agar datanya tetap aman. Karena, jika strategi pengamanannya itu buruk, maka akan semakin besar rentan tingkat keamanan data pribadi terkena serangan cyber.

Kesimpulan dan Saran

E-commerce adalah suatu bentuk perdagangan yang dilakukan secara online atau daring yang dimana seorang pelanggan atau konsumen itu melakukan transaksi dengan memberikan informasi pribadi mereka. Oleh karena itu, keamanan data pribadi pengguna e-commerce menjadi isu penting. Dampak ancaman terhadap keamanan data pribadi pengguna dapat mengakibatkan kerugian finansial dan potensi bagi perusahaan. Kebanyakan orang merasa khawatir saat berbelanja online dan melakukan transaksi yang berani. Risiko yang mungkin terjadi mencakup kehilangan ataupun kerusakan dari data pribadi penggunanya, serta berpotensi akan berdampak negatif terhadap perusahaan, seperti publisitas atau reputasi buruk, sanksi hukum, atau hilangnya pelanggan. Strategi keamanan yang tepat akan membantu melindungi data pribadi pengguna dari ancaman keamanan. Di sisi pengguna, mereka harus mengembangkan strategi bagaimana menjaga keamanan data mereka. Jika kebijakan keamanan buruk, tingkat pelanggaran keamanan data yang terkena serangan siber akan meningkat. Namun, tidak hanya pihak atau pemilik perusahaan saja yang perlu memilik kebijakan yang baik, namun pengguna juga perlu untuk membantu meminimalkan risiko dan melindungi data pribadi. Pemerintah juga perlu memperkuat lingkungan transaksi yang lebih aman.

Daftar Pustaka

Adisya Poeja Kehista, A. F. (2023). Analisis dan keamanan, Data Pribadi Pada Pengguna E-Commerce : Ancaman, Risiko, dan Strateh=gi Keamanan. *Jurnal Ilmu Menejemen Terapan*, 627-630.

Ahmed, A. S. (2021). The Impact of Perceived Risks on Consumer Online Shopping Behavior. *Journal of E-Commerce Research*, 321-335.

Batmetan, J. R. (2019). Pengaruh Perilaku Cyber Crime.

Nafi'ah, R. (2020). Pelanggaran Data dan Pencurian Identitas Pada E-Commerce. *Cyber Security Dan Forensik Digital*, 7-13. Diambil kembali dari Cyber Security dan Forensik Digital.

Nugroho, B. A. (2021). Weak protection systems in e-commerce and the implications for user data privacy. *Journal of Cybersecurity and Digital Privacy*, 45-58.

Pratama, B. A. (2022). Perlindungan Hukum Terhadap Data Pribadi Konsumen E-Commerce (Kajian Terhadap Kebijakan Privasi Shopee, Tokopedia, dan Lazada). *Student Onnline Journal*, 766-774.

Setiani, R. S. (2022). *Pengantar Bisnis : teori dan Bisnis.* Malang: Maliki Press.

Wajong, M. &. (2010). Challenges in E-Commerce data Security System And Future Developments. *Indonesian Journal of Information Technology*, 112-118.