e-ISSN: 2686-4924, p-ISSN 2686-5246
DOI: https://doi.org/10.31933/jimt.v4i5
Received: 5 Februari 2023, Revised: 20 April 2023, Publish: 1 Mei 2023
https://creativecommons.org/licenses/by/4.0/

JIMT
JURNAL ILMU MANAJEMEN TERAPAN
https://dinastirev.org/JIMT
editor@dinastirev.org
0811 7401 455

Analisis Keamanan Data Pribadi pada Pengguna E-Commerce: Ancaman, Risiko, Strategi Kemanan (Literature Review)

Adisya Poeja Kehista[1], Achmad Fauzi[2], Annisa Tamara[3], Ivanida Putri[4], Nurul Afni Fauziah[5], Salma Klarissa[6], Vivi Bunga Damayanti[7]
[1] Universitas Bhayangkara Jakarta Raya, Indonesia, kehistaaraaa2605@gmail.com
[2] Universitas Bhayangkara Jakarta Raya, Indonesia, achmad.fauzi@dsn.ubharajaya.ac.id
[3] Universitas Bhayangkara Jakarta Raya, Indonesia, nisatamara19@gmail.com
[4] Universitas Bhayangkara Jakarta Raya, Indonesia, ivanidaputri8@gmail.com
[5] Universitas Bhayangkara Jakarta Raya, Indonesia, afnifauziah5765@gmail.com
[6] Universitas Bhayangkara Jakarta Raya, Indonesia, slmklarissa@gmail.com
[7] Universitas Bhayangkara Jakarta Raya, Indonesia, bungavivi80@gmail.com

Corresponding Author: Adisya Poeja Kehista

Abstract: *E-commerce is one of the trading activities carried out online by utilizing the internet in its business. Because the use of e-commerce is growing along with advances in technology, this allows for harmful crimes to occur. Use of personal data in e-commerce that is vulnerable to cyber-attacks. This article focuses on examining how the actions, risks, and security strategies described have an impact on the security of the personal data of e-commerce users. This research uses qualitative methods and a literature review (Library Research). The research results show that threats, risks, and security strategies influence the security of personal data on e-commerce users. This article is expected to contribute to the development of personal data security for e-commerce users.*

Keyword: *Data Security, Threats, Risk, Security Strategy.*

Abstrak: E-commerce merupakan salah satu kegiatan perdagangan yang dilakukan secara online dengan memanfaatkan internet dalam bisnisnya. Karena penggunaan e-commerce semakin berkembang seiring dengan kemajuan teknologi, hal ini memungkinkan terjadinya kejahatan yang merugikan. Penggunaan data pribadi dalam e-commerce yang rentan terhadap serangan cyber. Artikel ini berfokus pada pemeriksaan bagaimana tindakan, risiko, dan strategi keamanan yang dijelaskan berdampak pada keamanan data pribadi pengguna e-niaga. Penelitian ini menggunakan metode kualitatif dan kajian pustaka (Library Research). Hasil penelitian menunjukkan bahwa ancaman, risiko, dan strategi keamanan berpengaruh terhadap keamanan data pribadi pengguna e-commerce. Artikel ini diharapkan dapat berkontribusi dalam pengembangan keamanan data pribadi bagi pengguna e-commerce.

Kata Kunci: Keamanan Data, Ancaman, Risiko, Strategi Keamanan.

PENDAHULUAN

Teknologi saat ini berkembang sangat cepat dan menjadi semakin maju. Contoh dari teknologi tersebut adalah Internet. Padahal internet sendiri merupakan sistem komunikasi global yang menghubungkann komputerr dan jaringan komputerr di seluruh dunia. Penggunaan internet dan telepon seluler tidak hanya sekedarruntuk mencari berbagai informasi dan ngobrol, masyarakat saatt kini menjadikan internett terutama e-commerce. Menurut (Sabadmin, 2020) dampak positif menggunakan e-commerce yakni jangkauan pasar lebih luas, fleksibel, meningkatkan pendapatan dan mengurangi resiko biaya lainnya, pelayanan lebih maksimal, dan feedback berupa ulasan dari pembeli yang dapat dijadikan sebagai tolok ukur suatu usaha.

Perdagangan elektronik atau e-commerce di Indonesia adalah kegiatan mendistribusikan, menjual, membeli dan memperdagangkan barang (barang dan jasa) dengan menggunakan jaringan komunikasi seperti internet, televisi atau jaringan komputer lainnya. Meskipun e-commerce menawarkan kemudahan dan kenyamanan, namun juga membawa risiko keamanan. Pengertian keamanan sendiri yaitu suatu proteksi atau perlindungan pada sumber-sumber fisikkdan konseptual dari bahayaaalam atau manusia. Keamanan terhadap sumber konseptual meliputi data dan informasi. Isu teratas dalam lingkungan e-commerce saat ini, yaitu privasi dan masalah keamanan pada data pribadi (Yazdanifard et al., 2011). Data pribadi seperti nama, alamat, nomor telepon, dan informasi keuangan bisa dengan mudah dicuri atau disalahgunakann oleh pihak yang tidak bertanggung jawabb. Ancaman keamanan data pribadi pada pengguna e-commerce sangatlah beragam, termasuk serangan malware, phishing, hacking, dan pencurian identitas. Risiko yang ditimbulkan dari pelanggaran keamanan data pribadi tidak hanya dapat merugikan pengguna secara finansial, namun juga dapat merusak reputasi pengguna di masyarakat.

Teridentifikasi empat masalahhkeamanan utamaayang dihadapi industriiie-commerce berdasarkan 3 kriteria; platformmelektronik, pemilik, dan pengguna menurut (Kuruwitaarachchi et al., 2019). Empat isu keamanan tersebut adalah keamanan transaksi, privasi, keamanan sistem perdagangan, dan kejahatan dunia maya e-commerce. Oleh karena itu, penting bagi pengguna e-commerce untuk memahami risiko keamanan data pribadi dan mengambil tindakan yang tepat untuk melindungi informasi pribadi mereka. Jurnal ini akan membahas tentang ancaman dan risiko keamanan data pribadi pada pengguna e-commerce, serta strategi pengamanan yang dapat diimplementasikan oleh pengguna untuk melindungi data pribadi mereka saat bertransaksi secara online

Berdasarkan latar belakang, maka dapat di rumuskan permasalahan yang akan dibahas guna membangun hipotesis untuk riset selanjutnya yaitu:

1. Apakah ancaman berpengaruh terhadap keamanan data pribadi pada pengguna e-commerce?.
2. Apakah Risiko berpengaruh terhadap keamanan data pribadi pada pengguna e-commerce?.
3. Apakah Strategi Pengamanan berpengaruh terhadap keamanan data pribadi pada pengguna e-commerce?.

METODE

Dalam penelitian ini, penulis menggunakan metode penelitian kualitatif dan kajian pustaka (Library Research). Mengkaji Buku-buku literature dan jurnal sesuai dengan teori yang di bahas khusunya di lingkup Manajemen Sekuriti dan Keamanan Sistem Informasi. Semua artikel ilmiah yang di citasi bersumber dari Mendeley, Google Scholar, dan media

online lainnya. Salah satu alasan utama untuk melakukan penelitian kualitatif yaitu: bahwa penelitian tersebut bersifat eksploratif (Ali & Limakrisna, 2013).

Penelitian Kualitatif bersifat atau memiliki karakteristik bahwa datanya dinyatakan dalam keadaan kewajaran atau sebagimana adanya (natural setting) dengan tidak dirubah dalam bentuk simbol atau bilangan. Fokus dalam penelitian ini adalah: (1) Ancaman cybercrime pada data pribadi pengguna e-commerce. (2) Risiko keamanan data pribadi pada pengguna e-commerce. (3) Strategi pengamanan data pribadi pada pengguna e-commerce.

Tabel 1: Penelitian terdahulu yang relevan

No	Author (tahun)	Hasil Riset terdahulu	Persamaan dengan artikel ini	Perbedaan dengan artikel ini
1	(Nugroho et al., 2021)	Kebocoran privasi ini terjadi karena sistem perlindungan data yang digunakan pihak e-commerce lemah sehingga memungkinkan merchant dengan mudah mengakses dan mencuri data pelanggan e-commerce. Selain itu, kasus kebocoran informasi pribadi dapat terjadi karena tidak adanya undang-undang khusus mengenai perlindungan informasi pribadi yang bersifat wajib dan kuat.	Membahas penanggulangan untuk mencegah kebocoran data pribadi pada pengguna e-commerce guna memperkuat keamanan pada data pribadi.	Pada penelitian terdahulu menggunakan pengoptimalisasi regulatory blockchain sebagai startegi untuk keamanan data pribadi.
2	(Wicaksana et al., 2020)	Hasil penelitian menunjukkan Di Indonesia, peran dari karakter hero belum cukup kuat karena adanya villain dalam bentuk ketiadaan regulasi terpadu untuk perlindungan keamanan data pribadi dari ancaman serangan siber.	Membahas bagaimana strategi pengamana dapat berpengaruh terhadap perlindungan keamanan data pribadi dari serangan siber.	Pada penelitian tersebut memakai elemen naratif seperti hero (pihak yang mampu memecahkan masalah), villains (Pihak yang menyebabkan masalah), daan victims (pihak yang dirugikan)..
3	(Wajong & Putri, 2010)	Masih banyak celah untuk ancaman pada sistem keamanan e-commerce, termasuk ancaman yang terjadi pada keamanan data pribadii.uUntuk kedepannya diharapkann bisnis E-Commerceedapat terus berkembangg tentunya sejalan dengan perkembangan keamanannya.	Menjelaskan jenis-jenis ancaman yang dapat terjadi, memberikan perencanaan solusi untuk sistem keamanan e-commerce serta menjelaskan pengaruhnya pada keamanan data di e-commerce.	Dalam penulisan tersebut menjelaskan lebih mendalam tentang Dimensi dan Metode yang Digunakan pada Keamanan E-commerce.
4	(Mustika, 2020)	Membahas keamanan data pribadi pengguna pada website e-commerce dengan mengimplementasikan alogaritma AES sebagai strategi pengamanan. Startegi ini dirasa tepat	Penerapan strategi pengamanan data pribadi dengan mengimplementasikan alogaritma AES pada website e-commerce guna memperkuat keamanan data pada sistem e-commerce.	Penelitian tersebut hanya membahas strategi pengamanan keamanan data pribadi dengan menggunakan alogaritma kriptografi melalui metode AES.

		karena cukup sulit dipecahkan. Panjang kunci akan mempengaruhi lamanya proses enkripsi dan deskripsi, hal tersebut berpengaruh terhadap tingkat keamanannya.		
5	(Gull et al., 2022)	Hasil penelitian menunjukkan bahwa bahaya dari berbagai ancaman pada privasi data yang tampak negatif akan tentunya akan mempengaruhi persepsi keamanan data pribadi pada aplikasi e-commerce.	Membahas bagaimana Ancaman berpengaruh terhadap keamanan data pribadi pada e-commerce.	Persepsi positif mengenai keamanan aplikasi e-commerce berpengaruh terhadap loyalitas pelanggan.
6	(AHMED et al., 2021)	Dampat dari risiko yang dirasakan pada pengguna berpengaruh terhadap keamanan dan niat dalam berbelanja online (e-commerce). Ketika risiko yang dirasakan tinggi, maka niat untuk membeli secara online menurun. Secara risiko yang meningkat akan menurunkan tingkat kemanan data pada e-commerce.	Risiko mempengaruhi keamanan data pada e-commerce.	Tingkat keamanan yang rendah akan berpengaruh terhadap minat berbelanja pada e-commerce.

*Ket variabel: y1=Keamanan Data Pribadi; x1= Ancaman; x2= Risiko; dan x3= Strategi Pengamanan.

HASIL DAN PEMBAHASAN

Pengaruh Ancaman terhadap keamanan data pribadi pada pengguna e-commerce

Ancaman adalah segala bentuk tindakan atau upaya oleh individu atau kelompok tertentu yang dapat mengancam keselamatan satu atau kelompok lain. Ancaman terhadap keamanan data pribadi pengguna dalam e-commerce berupa kejahatan digital atau serangan yang mengancam keamanan, privasi, dan kejahatan pengguna. Ancaman utama sistem keamanan pada e-commerce yang terlihat akan berefek menghancurkan tidak hanya pada pelaku usaha akan tetapi juga konsumen (Nafi'ah, 2020) Penulis memiliki hipotesis bahwa ancaman ini pada dasarnya juga mempengaruhi keamanan data pribadi pengguna e-commerce karena semakin banyaknya atau berbahaya ancaman tersebut maka keamanan pada data pribadi pengguna semakin terancam.

Ancaman memiliki pengaruh besar terhadap keamanan data pribadi pada e-commerce. Hal ini dikarenakan e-commerce merupakan salah satu bentuk perdagangan yang dilakukan secara online, dimana para pelanggan melakukan transaksi dengan memberikan informasi pribadi seperti nama, alamat, nomor telepon, nomor kartu kredit, dan lain sebagainya. Jika informasi tersebut jatuh ke tangan yang salah, pengguna e-commerce dapat mengalami kerugian finansial dan bahkan identitas mereka dapat dicuri dan disalahgunakan oleh pihak yang tidak bertanggung jawab.

Sebelumnya, (Batmetan et al., 2019) juga pernah mengkaji tentang pengaruh cyber crime dan e-commerce dengan melakukan riset yang diikuti oleh 30 responden sebagai sampel untuk penelitian. Dalam riset tersebut menyatakan bahwa orang lebih memilih transaksi e-commerce dengan tingkat persentase sebesar 78%. Persentase lainnya sebesar 80% menyatakan jika beberapa marketplace sering terjadi fraud atau penipuan secara daring.

Tentunya hal ini menjadi bukti bahwa sebagian besar masyarakat memiliki kekhawatiran ketika mereka belanja dan transaksi secara daring pada *e-commerce*. Hal tersebut menunjukan bahwa faktor keamanan privasi data pengguna masih rentan terhadap ancaman kejahatan atau *cyber crime* yang menyerang pengguna e-commerce baik dari pihak penjual ataupun pembeli yang dimana hal tersebut menimbulkan kerugian karena penyalahgunaan informasi personal atau data pribadi.

Pengaruh Risiko terhadap keamanan data pribadi pada pengguna e-commerce

Menurut KBBI risiko mempunyai arti sebagai akibat yang kurang menyenangkan (merugikan, membahayakan) dari suatu perbuatan atau tindakan. Ancaman cyber crime yang terjadi pada data pribadi pengguna e-commerce tentunya merugikan pihak pengguna ataupun perusahaan. Tidak ada suatu tindakan yang terjadi tanpa adanya suatu risiko. Dalam konteks keamanan data pribadi pada e-commerce, risiko terkait dengan kemungkinan terjadinya kerusakan atau kehilangan data pribadi pelanggan, serta potensi dampak negatif terhadap perusahaan seperti reputasi buruk, sanksi hukum, atau kehilangan pelanggan. Penulis memiliki hipotesis bahwa risiko ini pada dasarnya juga mempengaruhi keamanan data pribadi pengguna e-commerce.

Risiko dapat berdampak pada keamanan data pribadi pengguna e-commerce karena dalam transaksi e-commerce, pengguna memberikan informasi pribadiiseperti nama, alamat, nomor telepon, dan nomor kartu kredit atau informasiiikeuangan lainnya. Risiko yang muncul pada keamanan data pribadi pengguna e-commerce dapat menyebabkan pelanggaran keamanan data yang dapat merugikan pengguna dan perusahaan yang menyediakan layanan e-commerce.

Seperti contoh kasus yang dibahas oleh (Raihan, 2023) dalam jurnalnya terjadi pada Tokopedia. Pada 17 April 2020, seorang hacker bernama 'Why So Dank' berhasil mencuri data pengguna dari Tokopedia. Berita tentang peretasan ini pertama kali diterima melalui akun Twitter @underthebreach yang mengklaim bahwa 15 juta akun Tokopedia telah diretas. Data yangdiambil mencakup email, password, dan nama pengguna. Namun, setelah penyelidikan lebih lanjut, jumlah akun yang diretas meningkat menjadi 91 juta akun pengguna dan 7 juta akun merchant. Ini berarti hampir semua akun di Tokopedia terpapar dan informasi mereka diambil.

Dari kasus risiko yang terjadi yaitu 91 juta pengguna Tokopedia telah diambil datanya oleh seseorang yang tidak bertanggung jawab. Risiko berpengaruh terhadap keamanan data pribadi pada e-commerce karena e-commerce melibatkan pengumpulan dan penyimpanan data sensitif pelanggan seperti informasi kartu kredit, alamat email, dan informasi pribadi lainnya. Korelasi antara risiko dan keamanan privasi data sangat penting, dan menyoroti pentingnya mengambil tindakan proaktif untuk mengatasi potensi risiko dan memastikan bahwa privasi data tetap terjaga. Pada penelitian (AHMED et al., 2021) Hasil penelitiannya didaptkan risiko berpengaruh terhadap niat beli, niat beli yang menurun ini dipengarungi oleh keamanan yang buruk. Dengan begitu risiko berpengaruh terhadap keamanan.

Oleh karena itu, risiko berpengaruh pada keamanan data pribadi pada e-commerce karena risiko tersebut dapat mengakibatkan kerugian finansial dan non-finansial hingga hilangnya kepercayaan pelanggan. Jika risiko tersebut tidak ditangani dengan baik, maka kemungkinan besar keamanan data pribadi pada e-commerce akan terancam.

Pengaruh Strategi pengamanan terhadap keamanan data pribadi pada pengguna e-commerce

Strategi diartikan sebagai proses seseorang membuat rencana yang dilakukan oleh seseorangggdengannnmaksud dan tujuan tertentuu. Kerentanan sistem dalam infrastruktur e-commerce dapat menjadi celah bagi penjahat cyber untuk mengakses data pelanggan, maka

dari itu pada penulisan ini membahas tentang strategi pengamanan terhadap ancaman pada data pribadi pengguna e-commerce. Penulis memiliki hipotesis bahwa strategi pengamanan ini mempengaruhi keamanan data pribadi pengguna e-commerce.

Strategi pengamanan sangat berpengaruh terhadap keamanan data pribadi pada pengguna e-commerce. Hal ini karena strategi pengamanan yang tepat dapat membantu melindungi data pribadi pengguna yang tentunya bersifat privasi dari ancaman keamanan. Semakin baik strategi yang digunakan maka akan semakin minim terjadinya kejahatan cyber pada data pribadi pengguna. Strategi pengamanan yang diterapkan oleh sebuah e-commerce sangat penting dalam menjaga keamanan data pribadi pada pengguna e-commerce. Seperti pada kasus Tokopedia, menurut (Pratama et al., 2022) dalam penelitiannya menyebutkan bahwa Tokopedia telah menggunakan strategi pengamanan OTP (One TimePassword) saat konsumen ingin masuk kedalam akunnya sebagai salah satu bentuk perlindungan Data Pribadi pengguna. Strategi pengamanan tersebut digunakan agar semakin terjaga keamanan pada data pribadi pengguna.

Dengan menerapkan strategi pengamanan yang tepat, pemilik e-commerce dapat memastikan bahwa data pribadi pelanggan dan informasi penting lainnya terlindungi dari serangan cyber. Namun tidak hanya pihak atau pemilik perusahaan e-commerce saja yang harus memiliki strategi pengamanan yang baik, dari pihak penggunapun harus mempunyai strategi bagaimana menjaga datanya agar tetap aman. Karena jika buruk strategi pengamanannya maka akan semakin tingkat kerentanan keamanan data pribadi terkena serangan siber.

Conceptual Framework

Berdasarkan rumusan masalah, kajian teori, penelitian terdahulu yang relevan dan pembahasan pengaruh antar variabel, maka di perolah rerangka berfikir artikel ini seperti di bawah ini.

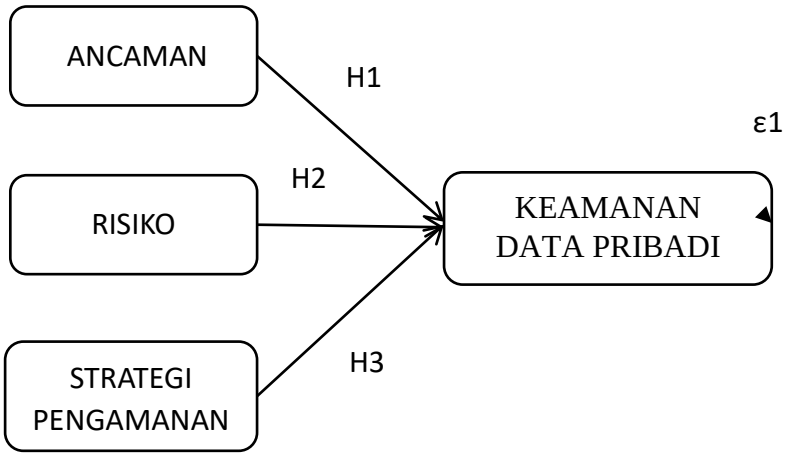

Figure 1: Conceptual Framework

Berdasarkan gambar conceptual framework di atas, maka: Ancaman, Risiko, dan Strategi Pengamanan berpengaruh terhadap Keamanan Data Pribadi.

Selain dari tiga variabel exogen ini yang mempengaruhi Keamanan Data Pribadi, masih banyak variabel lain yang mempengaruhinya diantaranya adalah:

a) Kesadaran pengguna : (Rohmah, 2022), (Chris et al., 2021)
b) Kebijakan dan regulasi: (Pratama et al., 2022a), (Wicaksana et al., 2020)

KESIMPULAN

Penggunaan e-commerce membawa ancaman dan risiko terhadap keamanan data pribadi pengguna. Pengguna e-commerce perlu mengambil tindakannpencegahan yang tepat untuk melindungi datapribadi mereka. Semakin besar ancaman yang ada pada sistem pengolahan data, semakin besar pula risiko terjadinya pelanggaran keamanan data pribadi pada pengguna e-commerce. Semakin baik dan tepat strategi pengamanan yang digunakan maka semakin terjaga keamanan data pribadi pengguna.

Berdasarkan hasil analisis literature review, maka dapat ditarik kesimpulan bahwa ancaman, risiko, dan strategi pengamanan memiliki pengaruh terhadap keamanan data pribadi pada pengguna e-commerce. Ancaman memungkinkan karena semakin banyaknya atau berbahaya ancaman maka keamanan pada data pribadi pengguna semakin rentan dan terancam. Sedangkan risiko yang muncul pada keamanan data pribadi pengguna e-commerce dapat menyebabkan pelanggaran keamanan data yang dapat merugikan pengguna dalam bentuk financial ataupun non-financial. Dan strategi pengamanan yang tepat dapat sangat berpengaruh terhadap perlindungan data pribadi sehingga keamanan data pribadi pengguna terjaga dengan baik privasinya.

REFERENSI

AHMED, S. Y., ALI, B. J., & TOP, C. (2021). Understanding the Impact of Trust, Perceived Risk, and Perceived Technology on the Online Shopping Intentions: Case Study in Kurdistan Region of Iraq. *Journal of Contemporary Issues in Business and Government*, *27*(3).

Ali, H., & Limakrisna. (2013). *Metode Penelitian Petunjuk Praktis untuk Memecahkan Masalah Bisnis, Penyusunan Skripsi, Tesis, Disertasi*.

Batmetan, J. R., Hensy, W., Leyri.N, & Avandi E.U. (2019). *Pengaruh Perilaku Cyber Crime Terhadap Pengguna Aplikasi E -ommerce*.

Chris, N., Susanti, T., Donglas, N., Yantson, C., & Vincent. (2021). Pengaruh Kesadaran Keamanan Informasi dan Privasi Jaringan Sosial Terhadap Perilaku Perlindungan Privasi pada Para Pengguna Jaringan Sosial. *Jurnal Ilmu Komunikasi*, *7*(2), 170–184.

Djafar, W., & Komarudin, A. (2014). *Perlindungan Hak Atas Privasi Di Internet-Beberapa Penjelasan Kunci* . ELSAM.

Gull, H., Saeed, S., Iqbal, S. Z., Bamarouf, Y. A., Alqahtani, M. A., Alabbad, D. A., Saqib, M., Qahtani, S. H. Al, & Alamer, A. (2022). An Empirical Study of Mobile Commerce and Customers Security Perception in Saudi Arabia. *Electronics*, *11*(3).

Mustika, L. (2020). *Implementasi Algoritma AES Untuk Pengamanan Login Dan Data Customer Pada E-Commerce Berbasis Web*. *7*(1).

Nafi'ah, R. (2020). PELANGGARAN DATA DAN PENCURIAN IDENTITAS PADA E-COMMERCE. *CyberSecurity Dan Forensik Digital*, *3*(1), 7–13.

Nugroho, I. I., Pratiwi, R., & Zahro, S. R. A. (2021). OPTIMALISASI PENANGGULANGAN KEBOCORAN DATA MELALUI REGULATORY BLOCKCHAIN GUNA MEWUJUDKAN KEAMANAN SIBER DI INDONESIA . *Toggle Navigation Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal*, *1*(2).

Pratama, B. A., Rani, M., & Nuraini, L. (2022a). PERLINDUNGAN HUKUM TERHADAP DATA PRIBADI KONSUMEN E-COMMERCE (Kajian Terhadap Kebijakan Privasi Shopee, Tokopedia, dan Lazada). *Student Online Journal (SOJ) UMRAH-Ilmu Sosial Dan Ilmu Politik*, *3*(1), 766–774.

Pratama, B. A., Rani, M., & Nuraini, L. (2022b). PERLINDUNGAN HUKUM TERHADAP DATA PRIBADI KONSUMEN E-COMMERCE (Kajian Terhadap Kebijakan Privasi Shopee, Tokopedia, dan Lazada). *Student Online Journal (SOJ)*, *3*(1), 766–774.

Raihan, M. (2023). PERLINDUNGAN DATA DIRI KONSUMEN DAN TANGGUNGJAWAB MARKETPLACE TERHADAP DATA DIRI KONSUMEN (STUDI KASUS: KEBOCORAN DATA 91 JUTA AKUN TOKOPEDIA) . *Jurnal Inovasi Penelitian*, *3*(10).

Ramadhan, I. H., & Nurnawati, E. K. (2022). *ANALISIS ANCAMAN PHISHING DALAM LAYANAN E-COMMERCE*.

Rohmah, R. N. (2022). Upaya Membangun Kesadaran Keamanan Siber pada Konsumen E-commerce di Indonesia. *Cendikia Niaga*, *6*(1), 1–11.

Sabadmin. (2020). *Dampak Positif dan Negatif E Commerce*.

Saputra, I. G. N. I., Sasmita, G. M. A., & Wiranatha, A. A. K. A. C. (2017). Pengembangan Sistem Keamanan untuk E-commerce. *Jurnal Ilmiah Merpati (Menara Penelitian Akademika Teknologi Informasi)*, *5*(1).

Wajong, A. M. R., & Putri, C. R. (2010). Keamanan Dalam Electronic Commerce. *Binus Journal Publishing*, *1*(2).

Wicaksana, R. H., Munandar, A. I., & Samputra, P. L. (2020). Studi Kebijakan Perlindungan Data Pribadi dengan Narrative Policy Framework: Kasus Serangan Siber Selama Pandemi Covid-19 . *Jurnal IPTEK-KOM (Jurnal Ilmu Pengetahuan Dan Teknologi Komunikasi)*, *22*(2).

Yazdanifard, R., Edres, N. A.-H., & Seyedi, A. P. (2011). Security and Privacy Issues as a Potential Risk for Further Ecommerce Development . *International Conference on Information Communication and Management , 16*, 23–27.