STRATEGI KEAMANAN SIBER DAN ETIKA INFORMASI DALAM E-COMMERCE: TANTANGAN DAN SOLUSI DI INDONESIA

Zaskia Pulungan¹, Zuhra Quratul Aini², Rayyan Firdaus³

zaskia.230420043@mhs.unimal.ac.id¹, zuhra.230420141@mhs.unimal.ac.id²,

rayyan@unimal.ac.id³

Universitas Malikussaleh

ABSTRAK

Pertumbuhan e-commerce di Indonesia menghadirkan peluang ekonomi yang besar sekaligus memunculkan tantangan serius dalam keamanan siber dan etika informasi. Maraknya kasus phishing dan kebocoran data menunjukkan lemahnya perlindungan sistem digital, khususnya pada pelaku usaha kecil. Di sisi lain, praktik penyalahgunaan data tanpa persetujuan dan minimnya transparansi kebijakan privasi menandakan rendahnya kesadaran etis pelaku industri. Penelitian ini menggunakan pendekatan studi literatur dan analisis deskriptif kualitatif untuk mengkaji risiko dan solusi dalam pengelolaan data e-commerce. Hasil kajian menunjukkan bahwa penguatan infrastruktur keamanan, edukasi digital, implementasi Undang-Undang Perlindungan Data Pribadi, serta penerapan prinsip etika informasi sangat penting untuk membangun ekosistem digital yang aman dan terpercaya.

Kata Kunci: Keamanan Siber, E-Commerce, Etika Informasi, Perlindungan Data Dan Indonesia.

ABSTRACT

The growth of e-commerce in Indonesia presents great economic opportunities while also posing serious challenges in cybersecurity and information ethics. The rise of phishing and data leakage cases shows the weak protection of digital systems, especially for small businesses. On the other hand, the practice of misusing data without consent and the lack of transparency of privacy policies indicate the low ethical awareness of industry players. This research uses a literature study approach and qualitative descriptive analysis to examine the risks and solutions in e-commerce data management. The results show that strengthening security infrastructure, digital education, implementation of the Personal Data Protection Law, and application of information ethics principles are essential to build a safe and reliable digital ecosystem.

Keywords: Cybersecurity, E-Commerce, Information Ethics, Personal Data Protection, And Indonesian.

PENDAHULUAN

Perkembangan teknologi digital dalam beberapa tahun terakhir telah mengubah secara drastis pola konsumsi masyarakat Indonesia. Transaksi konvensional berangsur-angsur tergeser oleh aktivitas jual beli secara daring atau e-commerce, yang menawarkan efisiensi waktu, kemudahan akses, dan pilihan produk yang lebih luas. Laporan Google, Temasek, dan Bain & Company (2022) menyebutkan bahwa ekonomi digital Indonesia tumbuh pesat dan mencapai nilai sebesar USD 77 miliar pada tahun 2022, menjadikannya salah satu pasar e-commerce terbesar di Asia Tenggara.

Namun, pertumbuhan yang masif ini tidak lepas dari berbagai risiko yang menyertainya. Salah satu isu utama yang muncul adalah persoalan keamanan siber, yaitu ancaman terhadap sistem informasi dan data pribadi pengguna yang beredar dalam platform e-commerce. Kasus kebocoran data pribadi jutaan pengguna di beberapa platform besar menunjukkan lemahnya perlindungan terhadap sistem keamanan informasi. Rendahnya kualitas sistem keamanan siber, terutama pada pelaku e-commerce skala kecil, menjadi celah masuknya serangan siber yang berdampak pada kerugian konsumen dan menurunnya kepercayaan publik terhadap ekosistem digital.

Selain aspek teknis, muncul pula permasalahan mendasar yang berkaitan dengan etika

informasi. Banyak pelaku e-commerce yang masih memanfaatkan data pribadi pengguna tanpa persetujuan eksplisit, atau tanpa memberikan penjelasan yang transparan terkait pengelolaan data tersebut. Praktik seperti ini bertentangan dengan prinsip dasar etika informasi, yang mengharuskan penghormatan terhadap hak privasi dan keterbukaan dalam penggunaan informasi digital (Rahardjo, 2021).

Dalam rangka memberikan perlindungan yang lebih kuat, pemerintah Indonesia mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Regulasi ini menandai langkah penting dalam pembentukan tata kelola data yang lebih aman dan bertanggung jawab (Kementerian Komunikasi dan Informatika, 2022). Namun, pengesahan undang-undang saja tidak cukup tanpa diiringi dengan peningkatan kesadaran etis dari pelaku usaha, edukasi publik mengenai hak-hak digital, serta penguatan sistem keamanan informasi secara teknis.

Kemajuan teknologi seharusnya tidak hanya dilihat dari sisi inovasi dan efisiensi, tetapi juga dari sisi perlindungan hak dan kepentingan pengguna. Oleh karena itu, pendekatan terhadap e-commerce di Indonesia perlu memadukan strategi keamanan siber yang tangguh dengan penerapan nilai-nilai etika informasi yang bertanggung jawab.

TINJAUAN PUSTAKA

Penelitian ini berlandaskan pada kerangka teori keamanan informasi dan etika informasi sebagai fondasi konseptual dalam menelaah dinamika e-commerce di Indonesia. Teori keamanan informasi, sebagaimana dikembangkan dalam literatur klasik dan kontemporer, menekankan pentingnya pemeliharaan tiga elemen utama—confidentiality, integrity, dan availability—dalam pengelolaan sistem digital (Rahardjo, 2021). Ketidakmampuan sistem untuk menjaga aspek kerahasiaan dan integritas data akan membuka peluang bagi serangan siber seperti phishing, kebocoran data, dan manipulasi identitas, sebagaimana tercermin dalam insiden besar yang melibatkan Tokopedia dan Bukalapak (Kusuma, 2020; Milafebina et al., 2023).

Secara bersamaan, teori etika informasi juga menjadi kerangka sentral dalam penelitian ini. Etika informasi mengacu pada seperangkat prinsip moral yang mengatur pengumpulan, penyimpanan, dan pemanfaatan informasi digital, dengan menempatkan privasi individu sebagai hak yang inheren dan tidak dapat dikesampingkan demi efisiensi ekonomi semata (Syah, 2022). Teori ini berasumsi bahwa akses terhadap informasi bukan hanya persoalan teknis, melainkan juga relasional, yang menuntut adanya transparansi, persetujuan yang diinformasikan (informed consent), serta akuntabilitas terhadap setiap bentuk pengelolaan data.

Dari sisi normatif dan kelembagaan, kajian ini juga dikaji dalam perspektif data governance dan regulasi perlindungan data, khususnya melalui pendekatan *privacy as a fundamental right*. Kehadiran Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menandai pengakuan negara terhadap pentingnya proteksi hukum atas hak-hak digital individu (Kementerian Komunikasi dan Informatika, 2022). Regulasi ini merefleksikan pendekatan legalistik terhadap isu perlindungan data, namun dalam praktiknya masih menghadapi hambatan implementasi, baik dalam bentuk ketimpangan kapasitas teknis pelaku usaha maupun lemahnya mekanisme pengawasan yang efektif (Rahardjo, 2021). Oleh karena itu, tata kelola informasi dalam e-commerce menuntut integrasi antara pendekatan teknologis, etis, dan yuridis secara simultan dan berkesinambungan.

Dengan demikian, pendekatan teoritik yang digunakan dalam penelitian ini memungkinkan eksplorasi mendalam atas relasi antara keamanan sistem, prinsip moralitas digital, dan kerangka hukum nasional. Interseksi antara ketiganya diperlukan untuk

menjawab kompleksitas tantangan siber dan etika informasi dalam praktik e-commerce yang berkembang pesat, namun belum sepenuhnya matang dari sisi regulasi maupun kesadaran etiknya.

METODE PENELITIAN

Penulisan artikel ini menggunakan pendekatan studi literatur dengan metode analisis deskriptif kualitatif. Studi literatur dipilih sebagai metode karena memungkinkan penelusuran terhadap berbagai sumber bacaan dan dokumen yang relevan untuk memahami fenomena keamanan siber dan persoalan etika informasi dalam ekosistem e-commerce Indonesia. Studi literatur merupakan aktivitas sistematis dalam mengumpulkan, mencermati, dan mengolah informasi dari beragam sumber yang telah tersedia, untuk kemudian dianalisis secara mendalam guna menghasilkan pemahaman yang utuh terhadap topik yang dikaji.

Analisis deskriptif kualitatif digunakan untuk mengurai masalah secara naratif, menggambarkan karakteristik situasi dan isu-isu yang muncul di dalamnya, serta menafsirkan makna dan keterkaitan antar-aspek yang diteliti. Fokus pendekatan ini tidak terletak pada angka atau statistik, tetapi pada interpretasi kritis terhadap informasi yang diperoleh dari sumber bacaan (Moleong, 2017).

Data yang digunakan dalam kajian ini bersifat sekunder, yakni data yang tidak diperoleh secara langsung dari lapangan melainkan dari sumber-sumber yang sudah tersedia dalam bentuk tertulis maupun digital. Data tersebut meliputi artikel jurnal ilmiah, buku-buku kajian akademik, laporan riset dari lembaga kredibel, undang-undang dan peraturan pemerintah seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta laporan media daring yang memuat informasi aktual mengenai insiden serangan siber dan kebijakan platform digital (Sugiyono, 2018).

HASIL DAN PEMBAHASAN

Risiko Keamanan Siber dalam E-Commerce

Pertumbuhan pesat e-commerce di Indonesia telah menciptakan peluang besar bagi pelaku usaha, namun juga memunculkan berbagai tantangan dalam hal keamanan digital. Platform e-commerce menjadi target utama serangan siber karena tingginya aktivitas transaksi dan banyaknya data pribadi yang tersimpan. Maraknya kejahatan digital seperti peretasan, pencurian identitas, dan kebocoran data pelanggan menjadi ancaman nyata dalam perkembangan ini (Ramadhani & Nasution, 2024).

Phishing menjadi salah satu bentuk serangan yang paling sering terjadi. Sektor e-commerce di Indonesia menyumbang sekitar 32% dari kasus phishing, menunjukkan tingginya risiko di sektor ini. Banyak pengguna belum memahami cara membedakan situs resmi dan palsu, yang membuka celah bagi pelaku kejahatan untuk mengecoh korban dengan menyamar sebagai pihak terpercaya (Al Fadillah et al., 2024). Kerentanan ini diperparah dengan minimnya edukasi kepada pengguna mengenai cara melindungi data pribadinya.

Kasus kebocoran data Tokopedia pada Mei 2020 menjadi salah satu insiden terbesar dalam sejarah e-commerce Indonesia. Sebanyak 15 juta data pengguna dilaporkan bocor dan dijual di forum gelap. Meskipun Tokopedia mengklaim data penting seperti kata sandi telah dienkripsi, kebocoran informasi seperti nama, email, dan nomor telepon tetap berisiko tinggi karena dapat dimanfaatkan untuk penipuan lanjutan atau rekayasa sosial (Kompas, 2020). Insiden ini mencerminkan lemahnya sistem enkripsi dan manajemen keamanan internal dalam mengantisipasi serangan berskala besar.

Insiden serupa juga terjadi pada Bukalapak pada tahun 2021, yang mengindikasikan

bahwa bahkan platform e-commerce besar dengan banyak fitur keamanan tetap rentan terhadap serangan (Milafebina, et al., 2023). Data lebih dari 13 juta pengguna dilaporkan dijual di dark web. Meskipun Bukalapak menyatakan bahwa data yang bocor bukan data krusial seperti kata sandi atau informasi keuangan, tetap saja kejadian ini menimbulkan kekhawatiran publik terhadap efektivitas sistem keamanan perusahaan digital besar. Terlebih, pola serangan yang terjadi memiliki kemiripan dengan insiden di Tokopedia, yang berarti ada kemungkinan metode peretasan belum direspons dengan pendekatan berbeda. Kedua kasus besar tersebut memicu keprihatinan akan kurangnya sistem audit dan monitoring berkala terhadap keamanan siber di perusahaan teknologi.

Evaluasi menyeluruh terhadap prosedur pengamanan data serta kecepatan respons terhadap insiden siber menjadi sorotan tajam. Banyak pihak menilai bahwa perusahaan hanya melakukan tindakan reaktif setelah serangan terjadi, bukan melalui pendekatan proaktif dan pencegahan (Ramadhani & Nasution, 2024). Hal ini memperkuat urgensi penerapan standar keamanan yang ketat dan berkelanjutan di sektor digital.

Serangan siber juga berdampak signifikan pada UMKM yang mulai merambah platform digital. Tidak sedikit pelaku UMKM yang hanya fokus pada penjualan tanpa memperhatikan pentingnya perlindungan data konsumen. Kurangnya investasi dalam sistem keamanan, ditambah dengan minimnya literasi digital, menjadikan UMKM target empuk serangan (Rahmadi & Pratama, 2020). Beberapa pelaku UMKM bahkan mengelola sendiri situs dan media sosialnya tanpa memahami risiko dari tautan atau aplikasi pihak ketiga yang dapat mengakses data konsumen secara ilegal.

Tak hanya infrastruktur teknis, sumber daya manusia juga menjadi titik lemah dalam sistem keamanan e-commerce. Banyak pengelola toko daring, baik skala besar maupun kecil, belum memiliki pelatihan khusus dalam bidang keamanan siber. Ketidaksiapan ini menyebabkan respon terhadap serangan cenderung lambat dan tidak terstruktur. Hal ini menunjukkan bahwa perlindungan terhadap sistem digital tidak cukup hanya dengan membeli perangkat lunak keamanan, tetapi perlu didukung dengan SDM yang memahami ancaman serta langkah antisipasi yang tepat (Ramadhani & Nasution, 2024).

Masalah Etika dalam Pengelolaan Informasi

Dalam ekosistem digital saat ini, data telah menjadi komoditas penting yang memiliki nilai ekonomi tinggi, terutama dalam sektor e-commerce. Namun, seiring dengan meningkatnya ketergantungan pada data konsumen, muncul berbagai masalah etika yang berkaitan dengan bagaimana informasi tersebut dikumpulkan, disimpan, digunakan, dan dibagikan. Salah satu persoalan etis yang sering terjadi adalah penyalahgunaan data pelanggan tanpa izin. Banyak perusahaan e-commerce mengumpulkan data pengguna melalui berbagai cara, seperti cookies, formulir pendaftaran, hingga aktivitas pengguna di platform, lalu menggunakannya untuk kepentingan marketing, profiling, atau bahkan dijual kepada pihak ketiga tanpa persetujuan eksplisit dari pemilik data. Praktik ini jelas melanggar prinsip informed consent yang menjadi landasan etika privasi digital (Sari & Nasution, 2024).

Masalah etis lain yang juga sering terjadi adalah minimnya transparansi dalam kebijakan privasi. Sebagian besar platform lokal belum sepenuhnya menjelaskan secara terbuka bagaimana data pengguna diproses. Kalaupun ada, dokumen kebijakan privasi cenderung disampaikan dengan bahasa yang teknis dan sulit dipahami oleh masyarakat umum, yang pada akhirnya menyebabkan pengguna memberikan persetujuan tanpa memahami implikasi sebenarnya (Mahbubi, 2024). Hal ini menciptakan kesenjangan informasi antara pihak perusahaan dan pengguna, serta memperlemah posisi konsumen sebagai subjek data.

Etika dalam pengelolaan informasi semestinya tidak hanya berorientasi pada

kepatuhan hukum semata, tetapi juga pada nilai-nilai moral dan tanggung jawab sosial. Etika informasi mencakup prinsip kejujuran dalam menyampaikan informasi, akuntabilitas atas pengelolaan data, dan penghormatan terhadap hak privasi individu. Syah (2022) menjelaskan bahwa ketika perusahaan menerapkan prinsip etika bisnis secara menyeluruh, termasuk dalam aspek digital, maka mereka tidak hanya menghindari pelanggaran hukum, tetapi juga membangun kepercayaan jangka panjang dengan pelanggan. Namun pada kenyataannya, sebagian besar perusahaan e-commerce lebih menekankan aspek efisiensi dan keuntungan ekonomi dari penggunaan data, daripada memperhatikan nilai-nilai etika tersebut.

Persoalan ini semakin kompleks karena regulasi perlindungan data pribadi di Indonesia, hingga beberapa tahun terakhir, belum memiliki landasan hukum yang kokoh. Meski kini sudah ada UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, implementasinya masih menghadapi banyak tantangan, baik dari sisi kesiapan teknologi, sumber daya manusia, maupun kesadaran pelaku usaha akan pentingnya etika digital. Oleh karena itu, perlu adanya sinergi antara regulasi yang tegas, edukasi kepada pelaku bisnis dan masyarakat, serta integrasi nilai-nilai etika dalam setiap aspek pengelolaan informasi digital. Pengabaian terhadap etika informasi tidak hanya berpotensi melanggar hukum, tetapi juga merusak reputasi bisnis dan kepercayaan konsumen yang menjadi aset utama dalam industri digital.

Strategi Solutif dan Praktik Baik

Berbagai strategi solutif dibutuhkan untuk menjawab persoalan etika dalam pengelolaan informasi digital, khususnya pada sektor e-commerce yang sangat bergantung pada data pengguna. Dari sisi teknis, penerapan teknologi keamanan siber merupakan langkah utama. Otentikasi ganda, enkripsi end-to-end, dan sistem deteksi dini terhadap serangan (intrusion detection system) terbukti mampu mengurangi risiko kebocoran data (Sari & Nasution, 2024). Selain itu, prinsip privacy by design dan data minimization semakin penting untuk diterapkan dalam perancangan sistem informasi, guna memastikan bahwa perlindungan privasi menjadi bagian mendasar sejak awal.

Strategi lain adalah penggunaan teknologi blockchain yang menyediakan transparansi dan integritas dalam pencatatan dan penyimpanan data. Teknologi ini sudah mulai diadopsi oleh beberapa perusahaan digital besar sebagai solusi jangka panjang terhadap ketidakpercayaan publik terhadap pengelolaan data (Mahbubi, 2024).

Pendidikan literasi digital juga sangat penting untuk memperkuat keamanan informasi. Tidak jarang kebocoran data terjadi karena kelalaian manusia, misalnya penggunaan sandi lemah atau klik pada tautan berbahaya. Oleh karena itu, pelaku usaha wajib menyelenggarakan pelatihan internal dan menyampaikan panduan keamanan digital kepada pengguna (Syah, 2022). Inisiatif seperti kampanye keamanan digital oleh pemerintah dan lembaga swadaya masyarakat juga terbukti efektif dalam meningkatkan kesadaran masyarakat luas.

Di ranah regulasi, hadirnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menjadi tonggak penting yang memberikan legitimasi terhadap hak-hak subjek data dan tanggung jawab pengendali data. UU ini menekankan pentingnya persetujuan eksplisit, pembatasan akses data, serta pelaporan insiden keamanan (Kementerian Komunikasi dan Informatika RI, 2022). Untuk memperkuat efektivitasnya, dibutuhkan lembaga pengawas yang berwenang serta sanksi tegas untuk pelanggaran, agar kepatuhan tidak bersifat formalitas semata.

Selain teknis dan hukum, praktik etis juga wajib menjadi bagian dari kebijakan internal perusahaan. Pendekatan ini meliputi pengelolaan data berbasis persetujuan (informed consent), keterbukaan informasi, dan pelaksanaan audit internal berkala. Beberapa

perusahaan teknologi global telah mulai menerbitkan transparency reports, yaitu laporan publik mengenai bagaimana data pengguna digunakan dan dibagikan. Strategi lain yang berkembang adalah penerapan prinsip data stewardship, yaitu komitmen moral untuk mengelola data pengguna secara bertanggung jawab, bukan semata-mata sebagai aset ekonomi. Dengan pendekatan teknis, edukatif, regulatif, dan etis secara simultan, maka tantangan pengelolaan informasi di era digital dapat dihadapi secara berkelanjutan dan berkeadilan.

KESIMPULAN

Pesatnya pertumbuhan e-commerce di Indonesia membawa dampak positif terhadap efisiensi ekonomi digital, namun juga menimbulkan tantangan besar dalam hal keamanan siber dan etika informasi. Ancaman seperti phishing, peretasan, dan kebocoran data menjadi permasalahan serius, yang diperparah oleh rendahnya literasi digital serta lemahnya infrastruktur keamanan, terutama di kalangan pelaku UMKM. Selain persoalan teknis, pelanggaran terhadap prinsip etika informasi, seperti penggunaan data tanpa izin dan ketidaktransparanan kebijakan privasi, juga menjadi perhatian utama yang menggerus kepercayaan publik terhadap platform digital.

Upaya mengatasi tantangan ini menuntut pendekatan multi-dimensi. Strategi teknis seperti enkripsi, autentikasi ganda, dan sistem deteksi dini perlu diintegrasikan dengan edukasi berkelanjutan bagi pelaku usaha dan konsumen. Di samping itu, regulasi seperti Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi harus ditegakkan secara efektif untuk menjamin hak-hak subjek data. Tak kalah penting, pendekatan etis berbasis persetujuan pengguna, keterbukaan informasi, serta audit internal yang berkelanjutan harus menjadi bagian dari tata kelola data perusahaan.

Dengan sinergi antara teknologi, hukum, edukasi, dan etika, ekosistem e-commerce Indonesia dapat berkembang secara berkelanjutan dan terpercaya. Perlindungan terhadap data pribadi bukan semata isu teknis, melainkan bentuk komitmen moral terhadap hak digital masyarakat di era informasi.

Untuk itu, demi memperkuat keamanan siber dan etika informasi dalam e-commerce Indonesia, disarankan agar pelaku usaha, khususnya UMKM, meningkatkan investasi pada infrastruktur keamanan digital dan memberikan pelatihan berkala bagi sumber daya manusia. Pemerintah perlu memastikan implementasi efektif Undang-Undang Perlindungan Data Pribadi melalui pengawasan ketat dan sanksi yang tegas. Selain itu, integrasi nilai-nilai etika dalam pengelolaan data harus menjadi prioritas, agar kepercayaan konsumen terhadap platform digital dapat terjaga dan tumbuh secara berkelanjutan.

DAFTAR PUSTAKA

- Al Fadillah, M. A., Ramadhan, M. G., & Ariefiandi, M. E. (2024). Analisis ancaman phishing terhadap penggunaan e-commerce di Indonesia. *Journal of Informatic and Information Security*, 5(2), 85–96.
- Google, Temasek, & Bain & Company. (2022). *E-Conomy SEA 2022: Through the waves, towards a sea of opportunity*. <https://economysea.withgoogle.com>
- Kementerian Komunikasi dan Informatika Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*. <https://pdp.kominfo.go.id>
- Kusuma, A. (2020, Mei 3). Kebocoran data Tokopedia: Apa yang harus diperhatikan? Kompas. <https://www.kompas.com/tren/read/2020/05/03/113251565/data-15-juta-pengguna-tokopedia-diduga-bocor-ini-cara-proteksi-akun-di-e>
- Mahbubi, H. A. (2024, April 19). Mengatasi kesenjangan perlindungan privasi di platform e-commerce. Kompasiana. <https://www.kompasiana.com/humamafifalmahbubi8502/67164c2eed641567605093d2>

- Milafebina, R., Lesmana, I. P., & Syailendra, M. R. (2023). Perlindungan data pribadi terhadap kebocoran data pada Bukalapak. *Jurnal Tana Mana*, 4(1), 25–35.
- Moleong, L. J. (2017). *Metodologi penelitian kualitatif (Edisi revisi)*. PT Remaja Rosdakarya.
- Rahardjo, B. (2021). *Keamanan siber dan perlindungan data pribadi di era digital*. Prenadamedia Group.
- Rahmadi, G., & Pratama, A. R. (2020). Analisis kesadaran cyber security pada kalangan pelaku e-commerce di Indonesia. *Automata*, 2(1), 50–60.
- Ramadhani, N., & Nasution, M. I. P. (2024). Tantangan dan solusi keamanan siber dalam transaksi e-commerce. *Jurnal Penelitian Sistem Informasi*, 2(2), 134–144.
- Sari, S. I., & Nasution, M. I. P. (2024). Penyalahgunaan data pribadi konsumen terhadap pinjaman online ilegal. *Causa: Jurnal Hukum dan Kewarganegaraan*, 14(8), 91–100.
- Sugiyono. (2018). *Metode penelitian kualitatif, kuantitatif, dan R&D*. Alfabeta.
- Syah, M. K. (2022). *Analisis pengaruh prinsip etika bisnis terhadap penerapan kebijakan privasi perusahaan e-commerce di Indonesia (Skripsi, Universitas Gadjah Mada)*. Universitas Gadjah Mada Repository.