

Analisis Tanggung Jawab Etis dan Hukum Perusahaan E-Commerce terhadap Perlindungan Data Pribadi Konsumen: Studi Kasus Kebocoran Data Tokopedia 2020

Hendra Saputra¹, Gevy Ketia G², Bonansa Situmorang³, Dhaet Fretty Napitupulu⁴, Yeny Elfina Siagian⁵, Cristine Natasia Sihalo⁶, Cindy B. Sitanggang⁷, Dhea Anandha Pinem⁸

Universitas Negeri Medan, Indonesia

evytiagins@gmail.com², bonansasitumorang3@gmail.com³,
dhaet.frettynapitupulu@gmail.com⁴, yenyelfinasiagian@gmail.com⁵,
cristinenatasia@gmail.com⁶, sitanggangcindy37@gmail.com⁷,
dheapinem98@gmail.com⁸
E-mail Korespondensi : hensap@unimed.ac.id¹

Submitted: 28th Nov 2025 | **Edited:** 18th Dec 2025 | **Issued:** 01st January 2026

Cited on: Saputra, H., Ketia G, G., Situmorang, B., Napitupulu, D. F., Siagian, Y. E., Sihalo, C. N., Sitanggang, C. B., & Pinem, D. A. (2026). Analisis Tanggung Jawab Etis dan Hukum Perusahaan E-Commerce terhadap Perlindungan Data Pribadi Konsumen: Studi Kasus Kebocoran Data Tokopedia 2020. *SCIENTIFIC JOURNAL OF REFLECTION: Economic, Accounting, Management and Business*, 9(1), 120-127.

ABSTRACT

The rapid expansion of Indonesia's e-commerce sector has increased the exposure of consumer data to security risks, as shown in the 2020 Tokopedia breach. This study examines the ethical and legal responsibilities of e-commerce companies in protecting personal data by assessing Tokopedia's compliance with digital business ethics principles and national regulations. Using a qualitative case study approach, the analysis draws on secondary sources such as legal documents, incident reports, and scientific publications. The findings show that Tokopedia did not fully meet the standards of transparency, honesty, and privacy, and that its preventive and responsive measures were insufficient to safeguard user data. The company also failed to satisfy key obligations outlined in consumer protection rules and the Personal Data Protection Law, which serve as the benchmark for evaluating accountability. These shortcomings contributed to declining public trust and reputational harm. This study highlights the need for stronger ethical governance and more consistent legal compliance in digital platforms and recommends the integration of privacy-by-design principles, regular security audits, and a dedicated data ethics function to strengthen consumer data protection in Indonesia.

Keywords : Data Breach, Digital Ethics, Personal Data Protection, Legal Responsibility, E-Commerce

PENDAHULUAN

Perkembangan teknologi informasi dalam satu dekade terakhir telah mendorong tumbuhnya ekosistem perdagangan digital di Indonesia. Platform e-commerce berkembang pesat dan menjadi ruang interaksi utama antara pelaku usaha dan konsumen. Namun, peningkatan aktivitas digital tersebut diiringi dengan tingginya risiko terhadap

keamanan data pribadi. Kesenjangan antara kemajuan teknologi dan kesiapan perusahaan dalam mengelola data konsumen masih terlihat jelas, terutama dari aspek etika bisnis dan kepatuhan terhadap regulasi. Kondisi ini menunjukkan bahwa perlindungan data belum sepenuhnya ditempatkan sebagai prioritas dalam tata kelola perusahaan digital (Putri & Fahrozi, 2021; Rini et al., 2025).

Insiden kebocoran data Tokopedia pada tahun 2020 menjadi contoh nyata kerentanan tersebut. Lebih dari 90 juta data pengguna diperjualbelikan secara ilegal, menandakan lemahnya sistem keamanan dan minimnya tindakan preventif (Ayu & Nasution, 2023). Penundaan perusahaan dalam menyampaikan informasi kepada publik semakin memperlihatkan kurangnya transparansi dan akuntabilitas. Dari sudut pandang etika bisnis digital, tindakan tersebut mencerminkan kegagalan dalam memenuhi asas kejujuran, keterbukaan, dan penghormatan terhadap privasi pengguna (Sudarmanto, 2024; Malhotra et al. dalam As-syiva & Nasution, 2024).

Selain aspek etika, persoalan ini menyingkap lemahnya implementasi regulasi perlindungan data, terutama sebelum Undang-Undang Perlindungan Data Pribadi diberlakukan. Sejumlah penelitian menunjukkan bahwa pelaku usaha belum sepenuhnya melaksanakan kewajiban hukum terkait keamanan data, termasuk pemenuhan hak informasi, pemberitahuan insiden, serta penyediaan kompensasi bagi konsumen (Septiriani et al., 2024; Anindya & Subiyanto, 2025). Kasus Tokopedia juga memperlihatkan lemahnya mekanisme pengawasan negara dan belum optimalnya standar keamanan yang diterapkan industri e-commerce.

Berbagai temuan tersebut menegaskan urgensi penelitian yang tidak hanya mengkaji aspek regulasi, tetapi juga menilai tanggung jawab etis perusahaan dalam mengelola data pribadi. Dibutuhkan telaah yang lebih menyeluruh untuk memahami sejauh mana perusahaan digital menjalankan kewajiban moral dan hukum dalam melindungi konsumen di ruang digital. Dengan menjadikan kebocoran data Tokopedia sebagai studi kasus, penelitian ini bertujuan mengevaluasi tanggung jawab etis dan hukum perusahaan e-commerce dalam perlindungan data pribadi konsumen, serta merumuskan rekomendasi strategis bagi penguatan tata kelola keamanan data di Indonesia.

Berdasarkan uraian tersebut, rumusan masalah penelitian adalah sebagai berikut:

1. Bagaimana bentuk tanggung jawab etis perusahaan e-commerce dalam melindungi data pribadi konsumen?
2. Sejauh mana kepatuhan Tokopedia terhadap ketentuan perlindungan data pribadi dan perlindungan konsumen?
3. Apa implikasi etis, hukum, dan reputasional dari insiden kebocoran data Tokopedia?
4. Rekomendasi apa yang diperlukan untuk memperkuat perlindungan data pribadi di sektor e-commerce?

LANDASAN TEORI

Etika Bisnis Digital

Etika bisnis digital merupakan seperangkat prinsip moral yang mengatur bagaimana perusahaan mengelola aktivitas berbasis teknologi, termasuk pemrosesan data pribadi konsumen. Dalam konteks e-commerce, etika tidak hanya mengatur perilaku perusahaan terhadap pelanggan, tetapi juga mencakup komitmen terhadap transparansi, kejujuran, dan perlindungan privasi. Menurut Tavani (2020), etika informasi berfokus pada hak individu atas kontrol data dan kewajiban perusahaan dalam memastikan data dikelola

secara bertanggung jawab. Prinsip ini selaras dengan pandangan Floridi (2019) yang menekankan bahwa perlindungan data merupakan komponen mendasar dari kepercayaan digital.

Transparansi menjadi pilar utama etika bisnis digital. Perusahaan wajib memberikan informasi yang jelas mengenai tujuan pengumpulan data, prosedur keamanan, dan risiko yang mungkin terjadi. Kejujuran juga menjadi landasan dalam hubungan perusahaan-konsumen, di mana penyampaian informasi harus dilakukan secara apa adanya dan tidak menyesatkan (Martin et al., 2020). Sementara itu, perlindungan privasi mengharuskan perusahaan mengelola data konsumen secara hati-hati, termasuk menerapkan prinsip kehati-hatian dalam penyimpanan, pemrosesan, dan distribusi data.

Tantangan etika digital muncul ketika perusahaan menempatkan kepentingan bisnis di atas keamanan data, yang kemudian berpotensi mengurangi kepercayaan publik. Beberapa studi menunjukkan bahwa pelanggaran privasi sering kali terjadi karena lemahnya integrasi etika ke dalam sistem teknologi serta kurangnya budaya perlindungan data dalam organisasi (Richards & Hartzog, 2021; Zeng et al., 2023). Oleh karena itu, etika bisnis digital menuntut perusahaan membangun nilai-nilai organisasi yang menempatkan keamanan data sebagai bagian dari tanggung jawab moral dan bukan hanya kewajiban administratif.

Perlindungan Data Pribadi Konsumen

Perlindungan data pribadi merupakan upaya sistematis untuk menjaga keamanan informasi yang dapat mengidentifikasi individu. Dalam ekosistem e-commerce, data pribadi seperti alamat, nomor telepon, rekam transaksi, dan preferensi pengguna menjadi aset yang sangat sensitif. Menurut Solove (2020), data pribadi memiliki nilai ekonomi sekaligus risiko hukum yang tinggi, sehingga perusahaan wajib memastikan perlindungan terhadap data tersebut dari penyalahgunaan dan akses ilegal.

Di Indonesia, perlindungan data pribadi dipertegas melalui berbagai regulasi—mulai dari PP PMSE hingga UU Perlindungan Data Pribadi. Regulasi ini menekankan prinsip perlindungan data seperti legality, purpose limitation, accuracy, confidentiality, dan accountability. Prinsip-prinsip tersebut sejalan dengan standar global seperti General Data Protection Regulation (GDPR) yang menekankan pentingnya hak pemilik data, keamanan pemrosesan, dan kewajiban pemberitahuan insiden (Bradshaw et al., 2020).

Dari perspektif konsumen, pelanggaran data dapat menimbulkan risiko pencurian identitas, penipuan finansial, dan hilangnya rasa aman dalam bertransaksi digital. Penelitian oleh Choi et al. (2021) menunjukkan bahwa persepsi keamanan data berpengaruh langsung terhadap kepercayaan dan niat menggunakan platform e-commerce. Oleh karena itu, perlindungan data tidak hanya kewajiban hukum, tetapi juga menjadi strategi bisnis yang menentukan loyalitas pelanggan.

Tanggung Jawab Hukum dalam Pengelolaan Data Pribadi

Tanggung jawab hukum berkaitan dengan kewajiban pelaku usaha dalam menjaga keamanan data serta pemenuhan hak-hak konsumen. Prinsip legal compliance mewajibkan perusahaan mengelola data sesuai standar hukum yang berlaku. Badruzaman (2021) menjelaskan bahwa hubungan konsumen dan pelaku usaha dalam transaksi elektronik harus dilandasi prinsip kehati-hatian dan jaminan keamanan sebagaimana diatur dalam peraturan perlindungan konsumen.

Undang-Undang Perlindungan Data Pribadi mengatur bahwa pengendali data wajib melakukan langkah preventif untuk menjaga kerahasiaan data, memberitahukan insiden pelanggaran, serta menyediakan upaya pemulihan. Tanggung jawab ini dapat bersifat administratif, perdata, maupun pidana sesuai tingkat pelanggarannya. Sebagaimana

disampaikan oleh Subiyanto dan Nurlaily (2023), kelalaian perusahaan dalam menyediakan sistem keamanan yang memadai dapat dikategorikan sebagai pelanggaran kewajiban hukum, terutama jika mengakibatkan kerugian bagi konsumen.

Selain tanggung jawab internal, perlindungan data juga melibatkan mekanisme pengawasan negara. Penelitian oleh Yuniarti (2022) menegaskan bahwa pengawasan regulatori yang lemah sering menjadi faktor meningkatnya insiden kebocoran data di sektor digital. Karena itu, integrasi tanggung jawab korporasi dan negara dalam mengawasi pemrosesan data menjadi elemen penting dalam memperkuat perlindungan data di Indonesia.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi kasus untuk menganalisis tanggung jawab etis dan hukum perusahaan e-commerce terhadap perlindungan data pribadi, dengan fokus pada insiden kebocoran data Tokopedia tahun 2020. Pendekatan studi kasus dipilih karena mampu memberikan pemahaman mendalam mengenai konteks, kronologi, serta faktor-faktor yang memengaruhi terjadinya pelanggaran data (Yin, 2020). Pengumpulan data dilakukan melalui kajian literatur sekunder yang mencakup dokumen regulasi, laporan keamanan siber, publikasi ilmiah, pemberitaan media kredibel, serta laporan lembaga pemerintah terkait keamanan data digital. Untuk memastikan kualitas sumber, penelitian ini menetapkan kriteria inklusi berupa: relevansi langsung dengan topik perlindungan data pribadi, diterbitkan dalam rentang waktu lima hingga enam tahun terakhir, dan berasal dari jurnal akademik, lembaga riset, atau laporan resmi pemerintah (Creswell & Poth, 2018; Sutton & Austin, 2019).

Proses analisis data dilakukan melalui teknik analisis isi dan analisis tematik. Analisis isi digunakan untuk mengidentifikasi konsep, aturan hukum, serta ketentuan etika yang relevan dalam dokumen regulasi dan literatur akademik. Sementara itu, analisis tematik digunakan untuk mengelompokkan temuan ke dalam tema utama seperti tanggung jawab etis, kewajiban hukum, kelalaian perusahaan, dan dampak kebocoran data (Braun & Clarke, 2021). Setiap data dikodekan secara manual melalui proses membaca berulang, kategorisasi, dan penarikan makna sesuai tujuan penelitian. Validitas temuan diuji melalui triangulasi sumber, yaitu membandingkan informasi dari berbagai dokumen dan literatur untuk memastikan konsistensi serta mengurangi bias interpretatif (Nowell et al., 2017). Pendekatan kualitatif ini memungkinkan penelitian menjelaskan keterkaitan antara aspek etika, hukum, dan praktik perusahaan secara komprehensif, sekaligus memberikan landasan yang kuat dalam merumuskan rekomendasi strategis.

HASIL PENELITIAN

Tanggung Jawab Etis Perusahaan dalam Pengelolaan Data Pribadi

Hasil penelitian menunjukkan bahwa insiden kebocoran data Tokopedia tahun 2020 mengungkap kelemahan mendasar dalam penerapan tanggung jawab etis perusahaan dalam mengelola data pribadi konsumen. Meskipun Tokopedia merupakan salah satu platform e-commerce terbesar di Indonesia, prinsip transparansi, kejujuran, dan perlindungan privasi belum dijalankan secara optimal. Kronologi peristiwa memperlihatkan bahwa peretasan telah terdeteksi sejak Maret 2020, namun informasi resmi baru disampaikan kepada publik pada 3 Mei 2020, setelah data lebih dari 90 juta akun diperjualbelikan di forum gelap. Keterlambatan ini menunjukkan bahwa perusahaan

lebih terfokus pada stabilitas citra dibanding memberi informasi yang dibutuhkan oleh pengguna untuk menjaga keamanannya.

Temuan penelitian ini sejalan dengan penelitian Martin et al. (2020) yang menyebutkan bahwa banyak perusahaan digital cenderung menempatkan kepentingan reputasional di atas kewajiban etis, terutama ketika menghadapi insiden keamanan. Selain itu, Richards dan Hartzog (2021) menegaskan bahwa akar lemahnya etika digital sering muncul dari kurangnya “privacy culture” dalam organisasi, di mana perlindungan data belum menjadi nilai dasar perusahaan. Penelitian Zeng et al. (2023) juga menguatkan bahwa kebocoran data pada platform digital sering berkaitan dengan rendahnya integrasi etika ke dalam desain sistem. Hal ini tampak pada Tokopedia, di mana prinsip *privacy by design* belum diterapkan pada periode sebelum kejadian.

Kondisi ini menunjukkan bahwa tanggung jawab etis bukan sekadar kewajiban moral, tetapi fondasi pembangun kepercayaan pengguna. Sebagaimana disampaikan oleh Choi et al. (2021), persepsi konsumen terhadap keamanan dan etika data memengaruhi tingkat kepercayaan mereka terhadap platform digital. Penurunan kepercayaan publik terhadap Tokopedia pascainsiden mengonfirmasi temuan tersebut.

Analisis Tanggung Jawab Hukum Berdasarkan UU PDP dan UUPK

Analisis hukum menunjukkan bahwa Tokopedia belum memenuhi sejumlah kewajiban sebagai pengendali data, baik yang diatur dalam Undang-Undang Perlindungan Data Pribadi maupun Undang-Undang Perlindungan Konsumen. UU PDP menegaskan bahwa perusahaan wajib menjaga keamanan data, menerapkan langkah preventif, serta memberitahukan insiden paling lambat 72 jam sejak terjadinya pelanggaran. Namun, hasil penelitian memperlihatkan bahwa pemberitahuan insiden dilakukan secara terlambat, tanpa penjelasan rinci mengenai jenis data yang terdampak, potensi risiko, atau langkah mitigasi.

Temuan ini konsisten dengan penelitian Septiriani et al. (2024), yang menunjukkan bahwa pelaku usaha e-commerce di Indonesia masih lemah dalam memberikan pemberitahuan insiden dan pemulihan hak konsumen. Sementara itu, studi Anindya dan Subiyanto (2025) menemukan bahwa dalam kasus kebocoran data Tokopedia, perusahaan belum melaksanakan kewajiban hukum secara efektif, terutama terkait kompensasi dan pemberitahuan yang memadai. Penelitian global seperti OECD Digital Security (2022) juga mencatat bahwa salah satu kelemahan utama bisnis digital adalah minimnya penerapan kewajiban hukum mengenai incident response.

Selain pelanggaran kewajiban notifikasi, aspek perlindungan hak atas keamanan dan hak atas informasi sebagaimana diatur dalam UUPK juga tidak terpenuhi. Tidak ada kompensasi yang diberikan kepada konsumen, dan informasi yang diberikan melalui rilis resmi relatif terbatas. Analisis ini memperkuat temuan Badruzaman (2021) yang menekankan bahwa perusahaan digital sering mengabaikan kewajiban perlindungan konsumen karena kurangnya pengawasan regulasi.

Dampak Kebocoran Data terhadap Kepercayaan Konsumen dan Reputasi Perusahaan

Kebocoran data Tokopedia berdampak langsung pada munculnya kecemasan pengguna terkait pencurian identitas, penipuan digital, serta penyalahgunaan akun. Rasa tidak aman tersebut tercermin dari meningkatnya keluhan publik dan penurunan sentimen positif terhadap platform di berbagai media sosial setelah insiden. Penelitian Choi et al. (2021) menunjukkan bahwa persepsi risiko data memiliki pengaruh signifikan terhadap kepercayaan dan niat konsumen dalam melanjutkan penggunaan layanan digital. Hal ini menjelaskan mengapa reputasi Tokopedia mengalami penurunan pascainsiden.

Secara lebih luas, insiden ini berdampak terhadap ekosistem e-commerce nasional. Kajian Harahap dan Nugroho (2021) menunjukkan bahwa kebocoran data berskala besar dapat menghambat pertumbuhan ekonomi digital karena menurunkan kepercayaan masyarakat terhadap sistem perdagangan elektronik. Kasus Tokopedia menjadi salah satu contoh nyata bahwa perlindungan data bukan hanya isu perusahaan, tetapi juga berkaitan dengan stabilitas sektor digital secara nasional.

Faktor Penyebab Terjadinya Kebocoran Data

Penelitian ini mengidentifikasi empat faktor utama penyebab insiden, yaitu faktor teknis, organisasi, etika, dan regulasi. Dari aspek teknis, sistem keamanan Tokopedia belum memiliki mekanisme deteksi dini dan belum sepenuhnya menerapkan pendekatan privacy by design. Hal ini selaras dengan temuan Tanczer et al. (2020) yang menyatakan bahwa banyak perusahaan digital Indonesia masih bergantung pada sistem keamanan reaktif, bukan preventif.

Dari aspek organisasi, belum adanya divisi khusus yang mengawasi perlindungan data memperkuat potensi risiko. Richards dan Hartzog (2021) menjelaskan bahwa ketiadaan struktur organisasi yang fokus pada etika data cenderung menghasilkan respons insiden yang lambat. Dari aspek regulasi, penelitian Walden (2020) menunjukkan bahwa kelemahan regulasi nasional sebelum UU PDP disahkan turut memperbesar peluang terjadinya pelanggaran data karena tidak adanya ancaman sanksi tegas.

KESIMPULAN

Penelitian ini menunjukkan bahwa insiden kebocoran data Tokopedia tahun 2020 tidak hanya mencerminkan lemahnya perlindungan teknis, tetapi juga ketidakterpenuhannya tanggung jawab etis dan hukum perusahaan dalam menjaga data pribadi konsumen. Dari aspek etika, Tokopedia belum sepenuhnya menerapkan prinsip transparansi, kejujuran, serta perlindungan privasi sebagaimana yang menjadi dasar etika bisnis digital. Hal ini tampak dari keterlambatan perusahaan dalam memberikan informasi kepada publik dan minimnya penjelasan mengenai risiko yang mungkin dialami pengguna.

Dari aspek hukum, hasil analisis mengungkap bahwa sejumlah kewajiban perusahaan sebagaimana diatur dalam regulasi perlindungan data dan perlindungan konsumen belum dilaksanakan secara memadai. Kewajiban preventif, pemberitahuan insiden, serta upaya pemulihan tidak dijalankan secara optimal. Kondisi tersebut berdampak pada menurunnya kepercayaan pengguna dan mengganggu reputasi perusahaan di sektor e-commerce.

Secara teoretis, penelitian ini memberikan kontribusi dengan mengintegrasikan perspektif etika bisnis digital dan kepatuhan hukum dalam satu kerangka analisis, sehingga menghasilkan pemahaman yang lebih komprehensif mengenai tanggung jawab perusahaan dalam pengelolaan data pribadi. Secara praktis, penelitian ini menegaskan pentingnya penerapan privacy by design, audit keamanan yang konsisten, pembentukan divisi etika data, serta peningkatan koordinasi antara perusahaan, regulator, dan pemangku kepentingan untuk memperkuat ekosistem perlindungan data nasional.

Penelitian ini memiliki keterbatasan karena menggunakan data sekunder, sehingga belum menggali perspektif langsung dari konsumen atau pihak internal perusahaan. Oleh sebab itu, penelitian selanjutnya dapat mengembangkan analisis melalui wawancara, survei, atau pendekatan komparatif dengan kasus kebocoran data pada platform lain, agar diperoleh gambaran yang lebih menyeluruh mengenai kesiapan industri digital dalam melindungi data pribadi.

DAFTAR PUSTAKA

- Anindya, R. P., & Subiyanto, A. E. (2025). Tanggung jawab platform Tokopedia dalam kasus kebocoran data menurut Undang-Undang tentang Perlindungan Data Pribadi. *Jurnal Hukum Siber Indonesia*, 4(3), 1105-1112.
- As-syiva, M. H., & Nasution, M. I. P. (2024). Privasi data dan keamanan informasi dalam e-commerce. *Jurnal Teknologi Informasi dan Keamanan Digital*, 3(9), 45-55.
- Ayu, S. S., & Nasution, M. I. P. (2023). Analisis kebocoran data privacy pada e-commerce Tokopedia. *JUEB: Jurnal Ekonomi dan Bisnis*, 2(3), 21-24.
- Badrulzaman, M. (2021). *Hukum perlindungan konsumen dalam transaksi elektronik*. Penerbit FH Press.
- Bradshaw, S., Millard, C., & Walden, I. (2020). Contracts for clouds: Privacy and data protection issues. *International Data Privacy Law*, 10(2), 100-115.
- Braun, V., & Clarke, V. (2021). *Thematic analysis: A practical guide*. Sage.
- Choi, H., Jung, Y., & Lee, J. (2021). The impact of data privacy concerns on consumer trust in e-commerce. *Journal of Retailing and Consumer Services*, 62, 102-112.
- Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). Sage.
- Floridi, L. (2019). *The logic of information: A theory of philosophy as conceptual design*. Oxford University Press.
- Harahap, D. A., & Nugroho, A. (2021). Keamanan data pada transaksi digital dan implikasinya terhadap perlindungan konsumen. *Jurnal Teknologi dan Hukum Siber*, 5(1), 34-48.
- Mana, J. T. (2023). Perlindungan data pribadi terhadap kebocoran data pelanggan e-commerce di Indonesia. *Jurnal Hukum dan Cybersecurity*, 4(1), 15-29.
- Martin, K., Shilton, K., & Smith, J. (2020). Business ethics in the era of data-driven decision making. *Journal of Business Ethics*, 164(2), 185-199.
- Nowell, L., Norris, J., White, D., & Moules, N. (2019). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods*, 18, 1-13.
- OECD Digital Security. (2022). *Digital security risk management for economic and social prosperity*. OECD Publishing.
- Putri, D. D. F., & Fahrozi, M. H. (2021). Upaya pencegahan kebocoran data konsumen melalui pengesahan RUU Perlindungan Data Pribadi. *Jurnal Legislasi Indonesia*, 18(1), 46-68.
- Rini, N., Santoso, G., Wiyana, H., Daffa, A., & Putra, S. (2025). Tantangan dan solusi dalam menerapkan etika bisnis di era digital. *JUBISDIGI: Jurnal Bisnis Digital*, 1(1), 52-63.
- Richards, N., & Hartzog, W. (2021). *Privacy's blueprint: The battle to control the design of new technologies*. Harvard University Press.
- Sary, F., Nurwati, N., & Prasetyo, A. (2020). Analisis keamanan informasi pada platform e-commerce di Indonesia. *Jurnal Sistem Informasi dan Keamanan Siber*, 7(2), 112-127.
- Septiriani, V., Sofyan, T., & Rosari, W. N. (2024). Tanggung jawab pelaku usaha terhadap kebocoran data pribadi konsumen dalam pelaksanaan perdagangan elektronik. *Jurnal Rechtsens*, 23(1), 127-136.

- Sudarmanto, E. (2024). *Konsep etika bisnis digital pada era informasi*. Pustaka Ilmu.
- Sutton, J., & Austin, Z. (2019). Qualitative research: Data collection and analysis. *The Canadian Journal of Hospital Pharmacy*, 72(3), 226-231.
- Tanczer, L., Steenmans, I., & Carr, M. (2020). Cybersecurity governance: A systematic framework for risk assessment. *Journal of Cyber Policy*, 5(1), 1-20.
- Tavani, H. T. (2020). *Ethics and technology: Controversies, questions, and strategies for ethical computing* (5th ed.). Wiley.
- Walden, I. (2020). Data protection, cybersecurity, and digital trust. *International Cybersecurity Review*, 3(1), 1-18.
- Yin, R. K. (2020). *Case study research and applications*. Sage.
- Yuniarti, S. (2022). Pengawasan pemerintah terhadap pengelolaan data pribadi dalam ekonomi digital. *Jurnal Kebijakan Publik*, 14(2), 98-112.
- Zeng, Y., O'Keefe, C., & Brown, M. (2023). Data governance and ethical risks in digital platforms. *Journal of Digital Ethics*, 2(1), 45-61.