

Kebocoran Data Tokopedia sebagai Krisis Komunikasi Digital

Iwan Samariansyah¹, Ihsan Suri²

¹Fakultas Ilmu Dakwah dan Ilmu Komunikasi, UIN Syarif Hidayatullah Jakarta

²Fakultas Ilmu Komunikaasi, Universitas Pancasila

¹Jl. Ir. H. Djuanda No. 95, Ciputat, Kota Tangerang Selatan, Banten, Indonesia

²Jl. Srengseng Sawah, Jagakarsa, Jakarta Selatan, Jakarta, Indonesia

Email: ihsansuri@univpancasila.ac.id

Diterima 30 April 2026, Disetujui 23 Mei 2026

ABSTRAK

Fenomena kebocoran data pribadi di era digital menjadi perhatian serius seiring meningkatnya penggunaan platform berbasis teknologi dalam berbagai aktivitas masyarakat. Kasus kebocoran data Tokopedia pada tahun 2020 merupakan salah satu insiden terbesar di Indonesia karena melibatkan jutaan data pengguna dan memunculkan persoalan terkait keamanan informasi, perlindungan privasi, serta menurunnya kepercayaan publik terhadap platform digital. Peristiwa ini tidak hanya menunjukkan adanya kelemahan teknis dalam sistem keamanan data, tetapi juga memperlihatkan pentingnya strategi komunikasi organisasi dalam menangani krisis secara transparan dan bertanggung jawab. Dalam konteks masyarakat digital, kegagalan komunikasi dapat memperburuk persepsi risiko dan memperdalam krisis kepercayaan publik. Penelitian ini bertujuan untuk menganalisis fenomena kebocoran data Tokopedia dalam perspektif privasi, perlindungan data, dan ilmu komunikasi dengan menekankan pada aspek krisis komunikasi serta kepercayaan publik. Penelitian menggunakan pendekatan kualitatif dengan metode studi kasus melalui teknik pengumpulan data berupa studi literatur, analisis dokumen, dan observasi media digital. Analisis data dilakukan menggunakan pendekatan analisis tematik dengan menjaga validitas melalui triangulasi sumber, audit trail, dan thick description. Hasil penelitian menunjukkan bahwa kebocoran data tidak hanya disebabkan oleh lemahnya sistem keamanan, tetapi juga oleh kegagalan komunikasi organisasi dalam mengelola krisis secara efektif. Strategi komunikasi yang lambat, kurang transparan, dan minim empati mempercepat erosi kepercayaan publik terhadap platform digital. Dalam perspektif agama, khususnya Islam, pelanggaran ini juga mencerminkan kegagalan dalam menjaga prinsip amanah sebagai tanggung jawab moral dalam pengelolaan data pengguna. Penelitian ini menegaskan bahwa perlindungan data harus dipahami secara multidimensional yang mencakup aspek teknologi, hukum, komunikasi, etika, dan spiritual dalam membangun kepercayaan di era digital.

Kata Kunci: Kebocoran Data; Kepercayaan Publik; Komunikasi Krisis; Privasi Digital; Tokopedia

Tokopedia Data Leak as a Digital Communication Crisis

ABSTRACT

The phenomenon of personal data breaches in the digital era has become a serious concern alongside the increasing use of technology-based platforms in various aspects of society. The Tokopedia data breach case in 2020 was one of the largest incidents in Indonesia, involving millions of user accounts and raising issues related to information security, privacy protection, and declining public trust in digital platforms. This incident not only demonstrated technical weaknesses in data security systems but also highlighted the importance of organizational communication strategies in managing crises transparently and responsibly. In the context of a digital society, communication failure can exacerbate risk perceptions and deepen the crisis of public trust. This study aims to analyze the Tokopedia data breach phenomenon from the perspectives of privacy, data protection, and communication studies, with a particular emphasis on crisis communication and public trust. The research employed a qualitative approach using a case study method through literature review, document analysis, and digital media observation. Data were analyzed using thematic analysis, while validity was ensured through source triangulation, audit trails, and thick description. The findings indicate that the data breach was caused not only by weak security systems but also by organizational communication failures in effectively managing the crisis. Slow, non-transparent, and less empathetic communication strategies accelerated the erosion of public trust in digital platforms. From a religious perspective, particularly in Islam, the breach also reflects a failure to uphold the principle of amanah (trustworthiness) as a moral responsibility in managing user data. This study emphasizes that data protection should be understood multidimensionally, encompassing technological, legal, communicative, ethical, and spiritual dimensions in building trust in the digital era.

Keywords: *Crisis Communication; Data Breach; Digital Privacy; Public Trust; Tokopedia*

PENDAHULUAN

Perkembangan teknologi digital telah mendorong transformasi besar dalam berbagai aspek kehidupan, termasuk dalam bidang ekonomi, komunikasi, dan interaksi sosial. Di Indonesia, pertumbuhan platform e-commerce seperti Tokopedia menjadi indikator kuat dari pesatnya digitalisasi masyarakat. Namun, di balik kemudahan dan efisiensi yang ditawarkan, muncul risiko baru yang berkaitan dengan keamanan dan privasi data pengguna. Salah satu kasus yang paling signifikan adalah kebocoran data Tokopedia pada tahun 2020 yang melibatkan jutaan akun pengguna.

Transformasi digital dalam dua dekade terakhir telah mengubah cara manusia berinteraksi, bertransaksi, dan membangun relasi sosial. Di Indonesia, perkembangan ekonomi digital berjalan sangat pesat, khususnya melalui platform e-commerce seperti Tokopedia, Shopee, dan Bukalapak. Platform-platform ini tidak hanya menjadi medium transaksi ekonomi, tetapi juga menjadi ruang produksi dan pertukaran data dalam skala besar. Setiap aktivitas para pengguna mulai dari pendaftaran akun, pencarian produk, hingga transaksi yang dilakukan menghasilkan jejak digital yang tersimpan dalam sistem platform. Dalam konteks ini, data pribadi telah menjadi komoditas baru yang memiliki nilai ekonomi tinggi sekaligus risiko yang signifikan.

Namun, perkembangan ini tidak selalu diiringi dengan kesiapan sistem perlindungan data yang memadai. Salah satu kasus yang paling menonjol di Indonesia adalah kebocoran data Tokopedia pada tahun 2020 dimana pengguna yang aktif dari tahun 2019 dan baru terungkap awal Mei 2020 melalui akun @underthebridge (Whysodank) yang mempublikasikan datanya di Raid Forum., yang dilaporkan melibatkan lebih dari 90 juta akun pengguna. Data yang bocor mencakup informasi sensitif seperti nama lengkap, alamat email, nomor telepon, hingga data yang berpotensi mengungkap identitas sosial dan preferensi individu. Bahkan beberapa studi menunjukkan bahwa data yang terekspos dalam ekosistem digital dapat mencakup kategori sensitif seperti agama, status sosial, dan kebiasaan konsumsi (Reni & Momo, 2025).

Kasus Tokopedia menjadi penting untuk dikaji karena beberapa alasan. Pertama, skala kebocoran yang besar menunjukkan kerentanan sistem keamanan data di Indonesia. Kedua, dampaknya tidak hanya bersifat teknis atau ekonomi, tetapi juga menyentuh aspek etika dan kepercayaan publik terhadap platform digital. Ketiga, kasus ini memperlihatkan adanya kesenjangan antara regulasi yang ada dengan implementasinya di lapangan. Meskipun Indonesia telah mengesahkan Undang-Undang Perlindungan Data Pribadi (UU PDP) pada tahun 2022, kasus-kasus kebocoran data menunjukkan bahwa perlindungan tersebut belum sepenuhnya efektif (Pawestri Maharani et al., 2025).

Fenomena ini tidak hanya menimbulkan kerugian secara teknis, tetapi juga memunculkan persoalan yang lebih kompleks terkait kepercayaan publik. Menurut (Coombs, 2007a), krisis organisasi tidak hanya berkaitan dengan kegagalan operasional, tetapi juga dengan bagaimana organisasi mengelola komunikasi kepada publik. Dalam konteks ini, kasus kebocoran data Tokopedia dapat dipahami sebagai kegagalan komunikasi organisasi dalam menjaga dan memulihkan kepercayaan publik. Komunikasi berperan penting dalam membangun makna, persepsi, dan kepercayaan, sehingga ketika terjadi kegagalan dalam pengelolaan komunikasi, dampaknya dapat memperburuk krisis yang terjadi.

Isu privasi dan perlindungan data tidak hanya berkaitan dengan aspek hukum, tetapi juga memiliki dimensi etika dan nilai sosial. Dalam masyarakat Indonesia yang plural dan religius, nilai-nilai moral berperan dalam membentuk kesadaran mengenai pentingnya menjaga informasi pribadi. Dalam perspektif Islam, prinsip *amanah* merepresentasikan tanggung jawab untuk menjaga kepercayaan dan informasi yang diberikan oleh pihak lain. Dengan demikian, pengelolaan data pribadi pada platform digital dapat dipahami sebagai bagian dari tanggung jawab etis dalam membangun dan mempertahankan kepercayaan publik (Saputra et al., 2022).

Dalam perspektif komunikasi, kebocoran data juga berkaitan erat dengan etika media digital. Platform digital tidak hanya berfungsi sebagai perantara informasi, tetapi juga sebagai aktor yang memiliki tanggung jawab moral terhadap data pengguna. Dalam konteks ini, kode etik media digital seharusnya mencakup prinsip transparansi, akuntabilitas, dan perlindungan terhadap privasi pengguna. Namun, dalam praktiknya, tekanan ekonomi dan kompetisi pasar seringkali membuat aspek etika menjadi terabaikan.

Studi kasus Tokopedia juga menarik karena memperlihatkan dinamika antara negara, korporasi, dan masyarakat dalam menghadapi krisis data. Negara memiliki peran sebagai regulator, tetapi seringkali tertinggal dalam mengantisipasi perkembangan teknologi. Korporasi memiliki kapasitas teknis untuk melindungi data, tetapi juga memiliki kepentingan bisnis yang dapat bertentangan dengan prinsip perlindungan privasi. Sementara itu, masyarakat sebagai pengguna seringkali berada dalam posisi yang lemah, dengan keterbatasan pengetahuan dan akses terhadap mekanisme perlindungan data.

Dari sudut pandang akademik, kajian ini menjadi penting untuk mengisi kekosongan literatur yang mengintegrasikan perspektif hukum, etika, dan agama dalam analisis perlindungan data di Indonesia. Sebagian besar penelitian sebelumnya cenderung fokus pada aspek hukum atau teknis, tanpa mengaitkannya dengan nilai-nilai normatif yang hidup dalam masyarakat. Padahal, dalam konteks Indonesia, pendekatan multidisipliner sangat diperlukan untuk memahami kompleksitas isu ini.

Selain itu, dalam konteks masyarakat Indonesia yang religius, isu privasi dan perlindungan data juga berkaitan dengan nilai-nilai moral dan agama. Konsep amanah dalam Islam menekankan pentingnya menjaga kepercayaan, termasuk dalam pengelolaan data pribadi. Dengan demikian, kebocoran data tidak hanya menjadi persoalan hukum dan teknologi, tetapi juga memiliki dimensi etika dan spiritual. Penelitian ini bertujuan untuk menganalisis kebocoran data Tokopedia sebagai krisis komunikasi dengan mengintegrasikan perspektif komunikasi, hukum, dan agama, serta mengkaji dampaknya terhadap kepercayaan publik sekaligus menganalisis secara mendalam isu privasi dan perlindungan data di era digital melalui studi kasus kebocoran data Tokopedia, dengan mengintegrasikan perspektif hukum, etika media digital, dan nilai-nilai agama. Analisis ini diharapkan dapat memberikan kontribusi baik secara teoritis maupun praktis dalam pengembangan kebijakan dan praktik perlindungan data di Indonesia.

Pembahasan mengenai privasi dan perlindungan data di era digital tidak dapat dilepaskan dari evolusi konsep privasi itu sendiri. Alan F. Westin dalam *Privacy and Freedom* mendefinisikan privasi sebagai hak individu untuk mengontrol informasi tentang dirinya, termasuk bagaimana dan sejauh mana informasi tersebut dibagikan (Westin, 2015 hlm. 7). Namun, dalam era digital, kontrol ini menjadi semakin kompleks karena data tersebar dalam sistem jaringan global yang sulit dikendalikan secara individual. Daniel J. Solove kemudian mengembangkan pendekatan taksonomi privasi yang lebih komprehensif, dengan mengklasifikasikan pelanggaran privasi ke dalam empat kategori: pengumpulan, pemrosesan, penyebaran, dan invasi informasi (Solove, 2006). Pendekatan ini relevan dalam kasus kebocoran data seperti Tokopedia, yang menunjukkan bahwa pelanggaran privasi merupakan hasil dari kegagalan sistemik dalam seluruh siklus pengelolaan data. Selanjutnya, (Nissenbaum, 2020 hlm. 2-3) melalui konsep *contextual integrity* menegaskan bahwa privasi bergantung pada kesesuaian aliran informasi dengan norma sosial dalam konteks tertentu, sehingga pelanggaran terjadi ketika data digunakan di luar konteks yang semestinya.

Dalam konteks ekonomi digital, Zuboff, (2019 hlm. 8-12) melalui konsep *surveillance capitalism* menjelaskan bahwa data pribadi telah menjadi komoditas ekonomi yang dieksploitasi secara sistematis. Hal ini memperluas isu privasi dari sekadar perlindungan individu menjadi persoalan struktural yang berkaitan dengan kekuasaan dan ekonomi politik digital. Dari perspektif komunikasi, kebocoran data dapat dianalisis melalui *Situational Crisis Communication Theory* (Coombs, 2007b), yang menekankan pentingnya strategi komunikasi dalam membentuk persepsi publik, serta *Trust Theory* yang menempatkan kompetensi, integritas, dan benevolence sebagai dasar kepercayaan (Mayer et al., 1995).

Dalam ranah etika, Floridi, (2015 hlm 87-90) melalui *information ethics* memandang data sebagai bagian dari identitas moral individu yang harus dihormati, sementara (Moor, 1985) menyoroti adanya *policy vacuum* akibat ketertinggalan regulasi dibandingkan perkembangan teknologi. Kajian komunikasi risiko kontemporer menunjukkan bahwa efektivitas komunikasi dalam situasi krisis sangat menentukan tingkat ketidakpastian dan respons publik terhadap suatu peristiwa. Malecki et al., (2021) menegaskan bahwa komunikasi yang tidak konsisten dan kurang transparan dapat meningkatkan kecemasan publik serta memperburuk persepsi risiko. Temuan serupa juga dikemukakan oleh Zhong et al., (2023), yang menjelaskan bahwa kejelasan pesan, kecepatan respons, dan kredibilitas sumber informasi menjadi faktor penting dalam menjaga kepercayaan publik selama krisis berlangsung, terutama dalam masyarakat jaringan yang ditandai oleh penyebaran informasi yang cepat dan tidak terpusat (Castells, 2010 hlm. 70-75).

Dari perspektif hukum, regulasi seperti GDPR menekankan prinsip transparansi, akuntabilitas, dan pembatasan tujuan dalam pengelolaan data (Walters et al., 2019). Namun, dalam praktiknya, tantangan utama terletak pada lemahnya penegakan hukum, sebagaimana terlihat dalam kasus Indonesia. Lebih jauh, privasi juga diakui sebagai bagian dari hak asasi manusia yang berkaitan dengan martabat dan kebebasan individu.

Dalam perspektif Islam, privasi memiliki dasar normatif yang kuat, seperti larangan memasuki ruang privat tanpa izin (QS. An-Nur: 27) serta konsep *maqasid al-shariah* yang menekankan perlindungan kehormatan (*hifz al-'ird*). Prinsip ini sejalan dengan nilai keadilan, tanggung jawab (*amanah*), dan larangan merugikan orang lain (Nidhom & Murtadho, 2025). Dengan demikian, data pribadi dapat dipandang sebagai amanah yang harus dijaga, dan pelanggaran merupakan bentuk pengkhianatan baik secara hukum maupun moral. Secara keseluruhan, kajian ini menunjukkan bahwa privasi dan perlindungan data merupakan isu multidimensional yang mencakup aspek teknologi, hukum, komunikasi, etika, dan agama. Oleh karena itu, pendekatan integratif menjadi penting untuk memahami kompleksitas serta merumuskan strategi perlindungan data yang lebih komprehensif di era digital.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan memanfaatkan dua jenis sumber data, yaitu data primer dan data sekunder. Data primer diperoleh melalui observasi terhadap pemberitaan media digital, pernyataan resmi Tokopedia, serta respons publik yang muncul di media sosial terkait kasus kebocoran data Tokopedia. Observasi dilakukan pada berbagai platform digital untuk memahami bagaimana informasi mengenai kebocoran data

disampaikan, diterima, dan didiskusikan oleh masyarakat. Data primer ini digunakan untuk melihat dinamika komunikasi krisis, persepsi risiko, serta bentuk respons publik terhadap kasus tersebut. Studi kasus dipandang relevan karena berfokus pada fenomena kontemporer dalam konteks nyata, di mana batas antara peristiwa dan lingkungan sosialnya sering kali saling beririsan (Yin, 2018; Creswell, 2013).

Sementara itu, data sekunder diperoleh melalui studi literatur dan analisis dokumen yang relevan dengan topik penelitian. Sumber data sekunder meliputi jurnal ilmiah nasional dan internasional, buku akademik, regulasi terkait perlindungan data pribadi, laporan lembaga resmi, artikel media kredibel, serta penelitian terdahulu yang membahas privasi digital, komunikasi krisis, dan perlindungan data. Literatur yang digunakan diprioritaskan berasal dari publikasi lima tahun terakhir untuk memastikan relevansi dan kebaruan data, meskipun beberapa teori klasik tetap digunakan sebagai landasan konseptual utama.

Jenis data yang digunakan dalam penelitian ini berupa data kualitatif dalam bentuk teks, narasi, dokumen, serta konten komunikasi digital. Data tersebut mencakup pernyataan resmi perusahaan, pemberitaan media, opini publik di media sosial, regulasi hukum, serta hasil penelitian akademik yang berkaitan dengan kebocoran data dan komunikasi krisis. Seluruh data kemudian dianalisis secara tematik untuk mengidentifikasi pola, makna, serta hubungan antarfenomena yang berkaitan dengan privasi, perlindungan data, dan kepercayaan publik di era digital.

Demi menjaga validitas penelitian, digunakan strategi triangulasi sumber, audit trail, dan *thick description*. Triangulasi memastikan konsistensi data dari berbagai sumber, audit trail mendokumentasikan proses penelitian secara transparan, sementara *thick description* memberikan gambaran kontekstual yang kaya terhadap fenomena yang dianalisis (Carcary, 2009; Lincoln & Guba, 1985). Dengan pendekatan metodologis ini, penelitian diharapkan mampu menghasilkan pemahaman yang komprehensif sekaligus kredibel mengenai isu privasi dan perlindungan data di era digital.

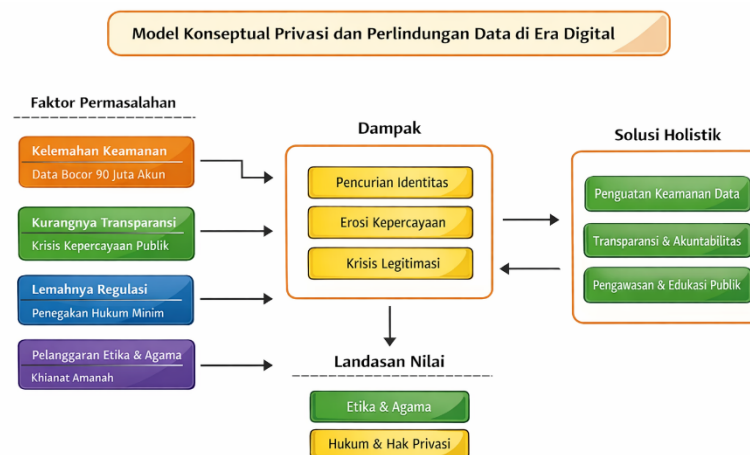
HASIL DAN PEMBAHASAN

Analisis terhadap kasus kebocoran data Tokopedia menunjukkan bahwa fenomena ini tidak dapat dipahami secara sempit sebagai kegagalan teknis semata, melainkan sebagai peristiwa multidimensional yang melibatkan aspek teknologi, hukum, etika, komunikasi, dan bahkan nilai-nilai agama. Berdasarkan hasil pengolahan data melalui studi literatur, analisis dokumen, serta observasi media digital, ditemukan beberapa tema utama yang saling berkelindan, yaitu kelemahan sistem keamanan data, kurangnya transparansi platform,

keterbatasan regulasi, serta pelanggaran nilai etika dan agama. Keempat tema ini tidak berdiri sendiri, melainkan saling memperkuat dalam membentuk krisis kepercayaan publik terhadap ekosistem digital.

Model konseptual yang dikembangkan dalam penelitian ini menggambarkan bahwa kebocoran data Tokopedia bukan sekadar peristiwa teknis, melainkan sebuah krisis komunikasi multidimensional yang melibatkan interaksi kompleks antara sistem teknologi, strategi komunikasi organisasi, persepsi publik, serta nilai-nilai normatif yang hidup dalam masyarakat. Model ini disusun berdasarkan integrasi beberapa teori komunikasi utama, yaitu *Situational Crisis Communication Theory* (Coombs, 2007b), *Communication Privacy Management Theory* (Petronio, 2002), *Trust Theory* (Mayer et al., 1995), *Risk Communication Theory* (Reynolds & W. Seeger, 2005), serta *Networked Communication* (Castells, 2010).

Gambar 1. Model konseptual mengenai privasi dan perlindungan data di era digital



Sumber: Hasil Olahan Peneliti. 2026

Dalam model tersebut, proses dimulai dari konteks digital, di mana ekosistem *e-commerce* seperti Tokopedia beroperasi dengan mengandalkan pengumpulan dan pengolahan data dalam skala besar. Kondisi ini menciptakan potensi risiko yang tinggi, terutama ketika terdapat kelemahan dalam sistem keamanan. Faktor pemicu krisis, seperti celah teknis dan kurangnya kontrol akses data, menjadi titik awal terjadinya kebocoran yang kemudian berkembang menjadi krisis komunikasi.

Tahap berikutnya dalam model adalah proses komunikasi organisasi, yang mencakup bagaimana Tokopedia mendeteksi krisis, mengelola komunikasi internal, serta menyampaikan informasi kepada publik. Dalam perspektif *Situational Crisis Communication Theory*, strategi komunikasi yang dipilih organisasi sangat menentukan bagaimana krisis tersebut dipersepsikan

oleh publik. Temuan penelitian menunjukkan bahwa respons awal yang cenderung defensif dan kurang transparan tidak sesuai dengan karakteristik krisis yang memiliki tingkat tanggung jawab tinggi (*high responsibility crisis*), sehingga memperburuk persepsi publik

Kelemahan Sistem Keamanan Data sebagai Akar Permasalahan

Temuan pertama menunjukkan bahwa kebocoran data Tokopedia berakar pada kelemahan sistem keamanan data yang digunakan oleh platform. Data yang bocor dalam jumlah besar hingga mencapai lebih dari 90 juta akun mengindikasikan adanya celah struktural dalam sistem proteksi data, baik dari sisi enkripsi, manajemen akses, maupun monitoring aktivitas jaringan. Dalam perspektif teori privasi (Solove, 2006), kondisi ini dapat dikategorikan sebagai kegagalan dalam tahap pemrosesan dan penyimpanan informasi, di mana data tidak dilindungi secara memadai dari potensi akses ilegal.

Pratama Persadha sebagai pakar keamanan siber mengungkapkan “Pihak Tokopedia harus bertanggungjawab atas kejadian ini karena data penggunanya diambil dan diperjualbelikan. Pihak Tokopedia wajib secara berulang-ulang, dengan menggunakan segala sarana media yang ada, mensosialisasikan apa saja yang harus dilakukan oleh para penggunanya, seperti ganti password akun dan mengaktifkan OTP, sampai semua penggunanya menyadari kebocoran ini dan mau mengganti password-nya.” (cnn indonesia, n.d.)

Lebih jauh, kelemahan ini tidak hanya mencerminkan keterbatasan teknis, tetapi juga menunjukkan adanya ketimpangan antara pertumbuhan bisnis digital dan investasi dalam keamanan siber. Dalam konteks ekonomi digital, perusahaan seringkali lebih fokus pada ekspansi pengguna dan peningkatan transaksi, sementara aspek keamanan menjadi prioritas sekunder. Hal ini sejalan dengan kritik (Zuboff, 2019) mengenai *surveillance capitalism*, di mana data diperlakukan sebagai aset ekonomi tanpa diimbangi dengan tanggung jawab perlindungan yang memadai.

Pentingnya komunikasi risiko dalam mengelola krisis data. Dalam kasus Tokopedia, kurangnya informasi yang jelas dan edukatif mengenai langkah-langkah mitigasi risiko menunjukkan adanya kelemahan dalam strategi komunikasi risiko. Padahal, menurut (Reynolds & W. Seeger, 2005), komunikasi risiko yang efektif harus mampu memberikan panduan praktis kepada publik untuk melindungi diri mereka.

Kegagalan dalam komunikasi risiko ini menyebabkan meningkatnya ketidakpastian di kalangan pengguna. Banyak pengguna tidak mengetahui apa yang harus dilakukan setelah kebocoran terjadi, sehingga memperburuk dampak psikologis dari krisis tersebut. Hal ini

menunjukkan bahwa komunikasi tidak hanya berfungsi sebagai alat informasi, tetapi juga sebagai mekanisme untuk mengurangi kecemasan dan membangun rasa aman. Dari hasil data, ditemukan bahwa banyak pengguna tidak menyadari tingkat risiko yang dihadapi sebelum kebocoran terjadi. Hal ini menunjukkan adanya kesenjangan informasi antara platform dan pengguna. Dalam perspektif komunikasi, kondisi ini mencerminkan kegagalan dalam membangun literasi digital yang memadai, sehingga pengguna tidak memiliki kapasitas untuk melindungi dirinya secara mandiri.

Kurangnya Transparansi dan Krisis Kepercayaan Publik

Tema kedua yang muncul adalah kurangnya transparansi dari pihak platform dalam merespons kebocoran data. Berdasarkan analisis dokumen dan pemberitaan media, respons awal Tokopedia dinilai lambat dan tidak memberikan informasi yang cukup jelas mengenai skala dan dampak kebocoran. Dalam konteks etika media digital, transparansi merupakan prinsip fundamental yang harus dijaga oleh platform sebagai bentuk akuntabilitas kepada publik (Floridi, 2015).

Kurangnya transparansi ini berdampak langsung pada menurunnya tingkat kepercayaan pengguna. Kepercayaan merupakan elemen kunci dalam ekosistem digital, karena tanpa kepercayaan, interaksi ekonomi dan sosial dalam platform akan terganggu. Dalam perspektif teori komunikasi, kepercayaan dibangun melalui konsistensi informasi, keterbukaan, dan respons yang cepat terhadap krisis. Ketika elemen-elemen ini tidak terpenuhi, maka yang terjadi adalah erosi kepercayaan yang sulit dipulihkan. Hal ini terlihat apa yang disampaikan oleh pihak tokopedia melalui akun *@TokopediaCare*”Tokopedia memastikan tidak ada kebocoran data pembayaran. Seluruh transaksi dengan semua metode pembayaran, termasuk informasi kartu debit, kartu kredit terjaga keamanannya.(antaranews.com, 2020)

Observasi media sosial menunjukkan bahwa banyak pengguna merasa “dikhianati” oleh platform yang sebelumnya mereka percayai. Dalam konteks “dikhianati” ini tidak dimaknai secara literal, melainkan sebagai bentuk representasi psikologis dan emosional pengguna terhadap hilangnya rasa aman dan kepercayaan kepada platform digital. Dalam kajian komunikasi dan psikologi sosial, perasaan dikhianati muncul ketika ekspektasi terhadap integritas dan tanggung jawab suatu institusi tidak terpenuhi (Mayer et al., 1995). Pengguna memberikan data pribadi dengan asumsi bahwa platform memiliki kemampuan dan komitmen untuk melindungi informasi tersebut. Ketika terjadi kebocoran data, muncul persepsi bahwa platform gagal memenuhi kepercayaan yang telah dibangun sebelumnya. Dengan demikian, istilah ini menggambarkan erosi hubungan kepercayaan (*trust deterioration*) antara pengguna

dan penyedia layanan digital. Sehingga narasi ini sangat menarik karena menunjukkan bahwa hubungan antara pengguna dan platform tidak hanya bersifat transaksional, tetapi juga emosional dan simbolik. Platform digital dipandang sebagai ruang yang seharusnya aman, sehingga ketika terjadi pelanggaran, dampaknya tidak hanya bersifat praktis, tetapi juga psikologis.

Hal ini juga menempatkan publik sebagai aktor aktif dalam proses komunikasi. Informasi mengenai kebocoran data tidak hanya disampaikan oleh organisasi, tetapi juga disebarluaskan melalui media massa dan media sosial. Dalam konteks ini, teori *networked communication* menjelaskan bahwa arus informasi bersifat horizontal dan tidak terpusat, sehingga organisasi kehilangan kendali penuh atas narasi yang berkembang. Publik kemudian melakukan proses interpretasi terhadap informasi yang diterima, yang dipengaruhi oleh kredibilitas sumber, pengalaman sebelumnya, serta nilai-nilai sosial dan agama. Dalam kerangka *Communication Privacy Management Theory*, kebocoran data dipersepsikan sebagai pelanggaran terhadap batas privasi yang telah disepakati secara implisit antara pengguna dan platform. Akibatnya, muncul reaksi emosional seperti rasa kehilangan kepercayaan, kecemasan, dan bahkan kemarahan.

Kepercayaan muncul sebagai variabel sentral yang menghubungkan antara tindakan organisasi dan respons publik. Berdasarkan *Trust Theory*, kepercayaan dibangun atas tiga dimensi utama: kompetensi, integritas, dan *benevolence*. Kebocoran data Tokopedia menunjukkan kegagalan pada ketiga dimensi tersebut, di mana organisasi dianggap tidak mampu melindungi data (kompetensi), tidak transparan dalam komunikasi (integritas), dan kurang menunjukkan empati terhadap pengguna (*benevolence*).

Penurunan kepercayaan ini memiliki implikasi yang luas, baik pada tingkat individu maupun institusional. Pada tingkat individu, pengguna menjadi lebih berhati-hati dalam berbagi data dan cenderung mengurangi aktivitas digital. Pada tingkat institusional, penurunan kepercayaan dapat berdampak pada loyalitas pengguna dan reputasi perusahaan. Dalam kerangka *Uses and Gratifications Theory*, kondisi ini mendorong pengguna untuk mencari alternatif platform yang dianggap lebih aman dan dapat memenuhi kebutuhan mereka secara lebih baik.

Keterbatasan Regulasi dan Penegakan Hukum

Temuan ketiga berkaitan dengan keterbatasan regulasi dan penegakan hukum dalam perlindungan data di Indonesia. Meskipun Undang-Undang Perlindungan Data Pribadi telah disahkan, implementasinya masih menghadapi berbagai tantangan, terutama dalam hal

pengawasan dan pemberian sanksi. Dalam banyak kasus, perusahaan yang mengalami kebocoran data tidak mendapatkan konsekuensi hukum yang signifikan, sehingga tidak ada efek jera yang kuat.

Dalam perspektif hukum, kondisi ini mencerminkan adanya regulatory gap antara norma yang diatur dalam undang-undang dengan praktik di lapangan. Walters et al., (2019) menekankan bahwa efektivitas perlindungan data tidak hanya ditentukan oleh keberadaan regulasi, tetapi juga oleh mekanisme penegakan yang kuat dan konsisten. Tanpa penegakan hukum yang efektif, regulasi hanya akan menjadi simbol tanpa daya.

Selain itu, hasil analisis menunjukkan bahwa koordinasi antar lembaga juga menjadi tantangan tersendiri. Perlindungan data melibatkan berbagai aktor, termasuk pemerintah, perusahaan, dan masyarakat, sehingga membutuhkan pendekatan kolaboratif. Namun, dalam praktiknya, koordinasi ini seringkali tidak berjalan optimal, sehingga respons terhadap kasus kebocoran data menjadi lambat dan tidak terintegrasi.

Pelanggaran Etika dan Nilai-Nilai Agama

Salah satu temuan yang paling menarik dari penelitian ini adalah adanya dimensi etika dan agama dalam memahami kebocoran data. Dalam perspektif Islam, data pribadi dapat dipandang sebagai bagian dari kehormatan individu (*hifz al- 'ird*) yang harus dijaga. Kebocoran data, dalam hal ini, bukan hanya pelanggaran teknis atau hukum, tetapi juga pelanggaran moral yang berkaitan dengan prinsip amanah. Zuhri, n.d. dalam tulisannya menyampaikan bahwa lembaga ormas Islam terbesar di Indonesia yaitu NU melalui musyawarah nasional alim ulama 2025 memandang bahwa perlindungan data anak merupakan bagian dari perlindungan jiwa (*hifzhun nafs*), akal (*hifzhul aql*), dan kehormatan (*hifzhul 'irdh*).

Konsep amanah menekankan bahwa setiap pihak yang diberi kepercayaan memiliki kewajiban untuk menjaga dan mengelola kepercayaan tersebut dengan baik. Dalam konteks platform digital, data pengguna merupakan bentuk amanah yang harus dilindungi. Ketika data tersebut bocor, maka yang terjadi adalah bentuk pengkhianatan terhadap amanah tersebut. Hal ini diperkuat oleh temuan dalam observasi media, di mana banyak pengguna menggunakan istilah “kepercayaan” dan “pengkhianatan” dalam menggambarkan pengalaman mereka.

Lebih jauh, pelanggaran ini juga memiliki implikasi sosial yang lebih luas. Dalam masyarakat yang religius seperti Indonesia, nilai-nilai agama memiliki peran penting dalam membentuk persepsi dan sikap masyarakat. Oleh karena itu, pelanggaran terhadap nilai-nilai tersebut dapat memperkuat dampak negatif dari kebocoran data, baik secara individu maupun kolektif.

Integrasi Temuan

Untuk memperjelas hubungan antar temuan, berikut disajikan tabel hasil analisis yang merangkum keterkaitan antara aspek teknis, etika, hukum, dan agama:

Tabel 1. ini menunjukkan bahwa setiap aspek saling berkaitan dan tidak dapat dipisahkan. Kelemahan teknis memperburuk masalah etika, sementara keterbatasan regulasi memperkuat dampak negatif dari pelanggaran tersebut.

Aspek	Temuan Utama	Analisis	Implikasi
Keamanan Data	Kebocoran 90 juta akun	Kegagalan sistem proteksi	Risiko pencurian identitas
Transparansi	Respons lambat	Pelanggaran etika komunikasi	Turunnya kepercayaan publik
Regulasi	Penegakan lemah	Regulatory gap	Minim efek jera
Etika	Tidak menjaga data	Pelanggaran moral	Krisis legitimasi
Agama	Pelanggaran amanah	Khianat terhadap kepercayaan	Dampak sosial-spiritual

Sumber : Hasil Penelitian, 2025

Salah satu kontribusi utama dari pemahaman ini adalah integrasi antara teori komunikasi modern dengan nilai-nilai etika dan agama. Dalam konteks ini, komunikasi tidak hanya dinilai berdasarkan efektivitasnya, tetapi juga berdasarkan kesesuaiannya dengan prinsip moral. Konsep *amanah* menjadi landasan etis yang menuntut organisasi untuk tidak hanya menjaga data, tetapi juga berkomunikasi secara jujur dan bertanggung jawab.

Integrasi ini menunjukkan bahwa dalam masyarakat seperti Indonesia, pendekatan komunikasi yang mengabaikan dimensi nilai akan sulit diterima oleh publik. Oleh karena itu, strategi komunikasi digital harus mempertimbangkan aspek budaya dan religius sebagai bagian dari upaya membangun kepercayaan. Implikasi penting bagi praktik komunikasi digital. Pertama, organisasi perlu mengembangkan strategi komunikasi krisis yang berbasis pada transparansi dan akuntabilitas. Kedua, penting untuk memperkuat komunikasi internal agar respons terhadap krisis dapat dilakukan secara cepat dan terkoordinasi. Ketiga, organisasi perlu mengintegrasikan komunikasi risiko sebagai bagian dari strategi komunikasi yang berkelanjutan.

Selain itu, model ini juga menekankan pentingnya pendekatan holistik yang mencakup aspek teknologi, komunikasi, hukum, dan etika. Tanpa integrasi ini, upaya perlindungan data akan sulit mencapai hasil yang optimal. Untuk memastikan validitas penelitian, digunakan beberapa strategi yang telah dijelaskan dalam metodologi. Triangulasi sumber data menunjukkan konsistensi temuan antara literatur akademik, dokumen resmi, dan observasi media. Audit trail memastikan bahwa seluruh proses penelitian terdokumentasi dengan baik,

sehingga dapat ditelusuri kembali. Sementara itu, penggunaan thick description memungkinkan peneliti untuk menggambarkan fenomena secara mendalam dan kontekstual.

Pendekatan ini menghasilkan pemahaman yang lebih kaya dibandingkan analisis yang hanya berfokus pada satu dimensi. Dengan mengintegrasikan berbagai perspektif, penelitian ini mampu menunjukkan bahwa kebocoran data merupakan fenomena kompleks yang membutuhkan pendekatan multidisipliner. Hasil penelitian ini memberikan kontribusi penting dalam pengembangan teori privasi dan perlindungan data, khususnya dalam konteks masyarakat berkembang seperti Indonesia. Salah satu temuan utama adalah pentingnya integrasi antara perspektif hukum, etika, dan agama dalam memahami isu privasi. Pendekatan ini memperluas cakupan analisis yang selama ini cenderung didominasi oleh perspektif teknis dan hukum.

Selain itu, penelitian ini juga menunjukkan bahwa kepercayaan merupakan elemen kunci dalam ekosistem digital. Tanpa kepercayaan, keberlanjutan platform digital akan terancam. Oleh karena itu, perlindungan data tidak hanya harus dilihat sebagai kewajiban hukum, tetapi juga sebagai strategi untuk menjaga keberlangsungan bisnis. Dari sisi praktis, penelitian ini memberikan beberapa implikasi penting. Pertama, perusahaan perlu meningkatkan investasi dalam keamanan data sebagai prioritas utama. Kedua, transparansi harus menjadi bagian integral dari strategi komunikasi, terutama dalam menghadapi krisis. Ketiga, pemerintah perlu memperkuat mekanisme penegakan hukum untuk memastikan efektivitas regulasi. Keempat, edukasi masyarakat mengenai literasi digital perlu ditingkatkan agar pengguna lebih sadar akan risiko yang dihadapi.

Dalam perspektif ilmu komunikasi, kasus kebocoran data Tokopedia tidak dapat dipahami semata sebagai kegagalan teknologi atau kelemahan sistem keamanan, melainkan sebagai bentuk krisis komunikasi organisasi yang memengaruhi relasi antara platform dan penggunanya. Komunikasi dalam konteks ini tidak hanya berfungsi sebagai penyampaian informasi, tetapi sebagai proses simbolik yang membentuk makna, persepsi, serta kepercayaan publik. Ketika terjadi kebocoran data, yang terganggu bukan hanya sistem informasi, tetapi juga struktur kepercayaan yang selama ini dibangun secara komunikatif antara organisasi dan pengguna.

Menariknya, dalam konteks Indonesia yang religius, respons publik terhadap kebocoran data juga dipengaruhi oleh nilai-nilai agama. Konsep *amanah* dalam Islam memberikan dimensi moral terhadap pengelolaan data, di mana organisasi dipandang memiliki tanggung jawab etis untuk menjaga kepercayaan pengguna. Pelanggaran terhadap prinsip ini tidak hanya dipersepsikan sebagai kegagalan teknis, tetapi juga sebagai bentuk pengkhianatan moral.

Dengan demikian, krisis yang terjadi memiliki dimensi yang lebih dalam, yaitu krisis etika dan kepercayaan.

Secara keseluruhan, analisis ini menunjukkan bahwa kebocoran data Tokopedia merupakan krisis komunikasi yang kompleks, di mana kegagalan teknis diperparah oleh kelemahan dalam strategi komunikasi organisasi. Kepercayaan publik menjadi variabel kunci yang terdampak, dan pemulihannya sangat bergantung pada transparansi, kecepatan, serta integritas komunikasi. Oleh karena itu, perlindungan data di era digital perlu dipahami tidak hanya sebagai isu teknologi, tetapi juga sebagai praktik komunikasi yang beretika dan bertanggung jawab.

SIMPULAN

Berdasarkan keseluruhan hasil analisis yang telah dilakukan, penelitian ini menunjukkan bahwa isu privasi dan perlindungan data di era digital, khususnya dalam kasus kebocoran data Tokopedia, merupakan fenomena yang kompleks dan multidimensional. Ia tidak dapat dipahami hanya sebagai persoalan teknis terkait keamanan sistem, tetapi harus dilihat sebagai permasalahan yang melibatkan interaksi antara teknologi, hukum, etika, komunikasi, dan nilai-nilai agama. Pendekatan yang reduksionis justru berisiko mengabaikan akar permasalahan yang lebih mendalam, yaitu bagaimana data dipahami, dikelola, dan diposisikan dalam struktur sosial digital yang semakin berkembang.

Dari sisi teknis, kebocoran data Tokopedia memperlihatkan adanya kelemahan mendasar dalam sistem keamanan informasi yang digunakan oleh platform digital di Indonesia. Skala kebocoran yang sangat besar menunjukkan bahwa perlindungan data belum menjadi prioritas utama dalam pengelolaan platform. Hal ini mengindikasikan adanya ketimpangan antara pertumbuhan ekonomi digital dengan kesiapan infrastruktur keamanan siber. Dalam konteks ini, data pribadi cenderung diperlakukan sebagai komoditas ekonomi tanpa diimbangi dengan tanggung jawab perlindungan yang memadai, sebagaimana dikritik dalam literatur mengenai ekonomi data dan kapitalisme pengawasan.

Namun demikian, persoalan tidak berhenti pada aspek teknis. Penelitian ini juga menemukan bahwa kurangnya transparansi dalam respons terhadap kebocoran data menjadi faktor yang memperparah krisis kepercayaan publik. Platform digital tidak hanya dituntut untuk mampu melindungi data secara teknis, tetapi juga harus mampu berkomunikasi secara terbuka dan akuntabel ketika terjadi pelanggaran. Ketika transparansi tidak terpenuhi, maka kepercayaan yang menjadi fondasi utama dalam ekosistem digital akan terkikis. Dalam konteks

komunikasi, kepercayaan bukan sekadar hasil dari performa teknis, tetapi juga dari bagaimana institusi membangun relasi dengan publik secara jujur dan bertanggung jawab.

Dari perspektif hukum, penelitian ini mengungkap adanya kesenjangan antara regulasi dan implementasi. Meskipun Indonesia telah memiliki kerangka hukum perlindungan data, efektivitasnya masih terbatas karena lemahnya penegakan hukum dan kurangnya mekanisme pengawasan yang kuat. Beberapa studi menunjukkan bahwa kasus kebocoran data, termasuk Tokopedia, belum mendapatkan respons hukum yang memberikan efek jera yang signifikan (Muhammad Abdurrohman Sholih & Rika Santina, 2025; Arradhiya & Febriani, 2025). Hal ini menunjukkan bahwa keberadaan regulasi saja tidak cukup, melainkan harus didukung oleh sistem penegakan yang konsisten dan tegas.

Lebih jauh, penelitian ini menyoroti pentingnya perspektif etika dan agama dalam memahami isu perlindungan data. Dalam konteks masyarakat Indonesia yang religius, nilai-nilai agama memiliki peran penting dalam membentuk persepsi dan sikap terhadap privasi. Dalam Islam, misalnya, konsep *amanah* dan *hifz al-'ird* memberikan landasan moral yang kuat untuk menjaga data pribadi sebagai bagian dari kehormatan individu. Kebocoran data, dalam hal ini, tidak hanya merupakan pelanggaran hukum, tetapi juga bentuk pengkhianatan terhadap kepercayaan yang diberikan oleh pengguna. Perspektif ini memperkaya pemahaman kita bahwa perlindungan data tidak hanya berkaitan dengan hak individu, tetapi juga dengan tanggung jawab moral yang lebih luas (Saputra et al., 2022).

Selain itu, pendekatan integratif yang digunakan dalam penelitian ini menunjukkan bahwa perlindungan data harus dipahami sebagai isu yang melibatkan berbagai aktor, termasuk negara, korporasi, dan masyarakat. Negara memiliki peran sebagai regulator yang harus memastikan adanya perlindungan hukum yang efektif, sementara korporasi memiliki tanggung jawab teknis dan etis dalam mengelola data pengguna. Di sisi lain, masyarakat sebagai pengguna juga perlu memiliki literasi digital yang memadai untuk memahami risiko dan hak-haknya. Tanpa keterlibatan ketiga aktor ini secara seimbang, upaya perlindungan data akan sulit mencapai hasil yang optimal.

Implikasi dari penelitian ini bersifat teoretis dan praktis. Secara teoretis, penelitian ini memperkuat pentingnya pendekatan multidisipliner dalam kajian privasi dan perlindungan data. Integrasi antara teori privasi, etika media digital, hukum, dan agama memberikan kerangka analisis yang lebih komprehensif dibandingkan pendekatan yang hanya berfokus pada satu dimensi. Secara praktis, penelitian ini memberikan rekomendasi bagi berbagai pemangku kepentingan. Bagi perusahaan, penting untuk meningkatkan investasi dalam keamanan data dan menerapkan prinsip transparansi dalam komunikasi. Bagi pemerintah,

diperlukan penguatan mekanisme penegakan hukum serta pembentukan lembaga pengawas yang independen. Sementara itu, bagi masyarakat, peningkatan literasi digital menjadi kunci untuk menghadapi risiko di era digital.

Pada akhirnya, penelitian ini menegaskan bahwa perlindungan data di era digital bukan hanya soal teknologi, tetapi juga soal kepercayaan, etika, dan nilai-nilai kemanusiaan. Kasus Tokopedia menjadi cerminan bahwa tanpa pendekatan yang holistik, transformasi digital justru dapat menghadirkan risiko baru yang mengancam keamanan dan martabat individu. Oleh karena itu, diperlukan upaya bersama untuk membangun ekosistem digital yang tidak hanya inovatif, tetapi juga adil, aman, dan beretika.

DAFTAR PUSTAKA

- antaranews.com. (2020, March 3). *Kebocoran data Tokopedia ramai dibincangkan warganet*. Antara News. <https://www.antaranews.com/berita/1462167/kebocoran-data-tokopedia-ramai-dibincangkan-warganet>
- Arradhiya, M. R., & Febriani, H. (2025). *Legal Protection Of E-Commerce User Privacy In Indonesia From The Perspective Of Civil Law And Islamic Law*. 4(1).
- Carcary, M. (2009). *The Research Audit Trial—Enhancing Trustworthiness in Qualitative Inquiry*. 7(1), 11–24.
- Castells, M. (2010). *The rise of the network society* (Second edition with a new preface). Wiley-Blackwell. <https://doi.org/10.1002/9781444319514>
- cnn indonesia. (n.d.). *Kronologi Lengkap 91 Juta Akun Tokopedia Bocor dan Dijual*. Teknologi. Retrieved March 1, 2026, from <https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual>
- Coombs, W. T. (2007). Protecting Organization Reputations During a Crisis: The Development and Application of Situational Crisis Communication Theory. *Corporate Reputation Review*, 10(3), 163–176. <https://doi.org/10.1057/palgrave.crr.1550049>
- Creswell, J. W. (2013). *Qualitative inquiry and research design: Choosing among five approaches* (third edition). SAGE.
- Floridi, L. (2015). *The ethics of information*. Oxford University Press.
- Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry* (Nachdr.). Sage.
- Malecki, K. M. C., Keating, J. A., & Safdar, N. (2021). Crisis Communication and Public Perception of COVID-19 Risk in the Era of Social Media. *Clinical Infectious Diseases*, 72(4), 697–702. <https://doi.org/10.1093/cid/ciaa758>
- Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *The Academy of Management Review*, 20(3), 709. <https://doi.org/10.2307/258792>
- Moor, J. H. (1985). Whats Is Computer Ethics? *Metaphilosophy*, 16(4), 266–275. <https://doi.org/10.1111/j.1467-9973.1985.tb00173.x>
- Muhammad Abdurrohman Sholih & Rika Santina. (2025). Law and Ethics in The Use of Information Technology: A Study on Privacy and Data Security. *Journal of Law, Society and Living Norms*, 1(1), 44–51. <https://doi.org/10.66111/vzej4x78>
- Nidhom, M., & Murtadho, A. (2025). Does Islam Protect Digital Privacy? An Islamic Studies Approach to Personal Data Protection. *Al-Afham: Journal of Islamic Studies*, 2(2), 107–128. <https://doi.org/10.62509/ajis.v2i2.260>
- Nissenbaum, H. (2020). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press. <https://doi.org/10.1515/9780804772891>
- Pawestri Maharani, D., Kusumadara, A., Nur Widhiyanti, H., & Dewantara, R. (2025). Administrative legal liability for data breaches: Securing the right to compensation in Indonesia and the EU. *Law. Human. Environment*, 16(3), 173–190. <https://doi.org/10.31548/law/3.2025.173>
- Petronio, S. S. (2002). *Boundaries of privacy: Dialectics of disclosure*. State University of New York Press.
- Reni, W. O., & Momo, A. H. (2025). State Responsibility And Constitutional Protection Of Personal Data In Indonesia: Addressing Digital Challenges. . . *ISSN*, 27(3).
- Reynolds, B., & W. Seeger, M. (2005). Crisis and Emergency Risk Communication as an Integrative Model. *Journal of Health Communication*, 10(1), 43–55. <https://doi.org/10.1080/10810730590904571>

- Saputra, A. A., Fasa, M. I., & Ambarwati, D. (2022). Islamic-Based Digital Ethics: The Phenomenon of Online Consumer Data Security. *Share: Jurnal Ekonomi Dan Keuangan Islam*, 11(1), 105–128. <https://doi.org/10.22373/share.v11i1.11167>
- Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 154(3), 477. <https://doi.org/10.2307/40041279>
- Walters, R., Trakman, L. E., & Zeller, B. (2019). *Data Protection Law: A Comparative Analysis of Asia-Pacific and European Approaches*. Springer Singapore Pte. Limited.
- Westin, A. F. (2015). *Privacy and freedom* (New edition). IG Publishing.
- Yin, R. K. (2018). *Case study research and applications: Design and methods* (Sixth edition). SAGE.
- Zhong, W., Hu, Q., & Kapucu, N. (2023). Robust crisis communication in turbulent times: Conceptualization and empirical evidence from the United States. *Public Administration*, 101(1), 158–181. <https://doi.org/10.1111/padm.12855>
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power* (Paperback edition). Profile Books.
- Zuhri, M. K. (n.d.). *Perlindungan Data Pribadi Menurut Islam: Antara Martabat, Maslahat, dan Ancaman Digital*. NU Online. Retrieved March 1, 2026, from <https://nu.or.id/syariah/perlindungan-data-pribadi-menurut-islam-antara-martabat-maslahat-dan-ancaman-digital-u9FPx>