HARE: Sharia Economic Review
Volume 3 No 1 Januari 2026
E-ISSN: 3110-0074

Analisis Kebocoran Data Pengguna Tokopedia Dan Implikasinya Terhadap Keamanan Siber Indonesia

Syahla' Fauziyyah Farhah[1], Hana Zakiya[2]
Universitas Siliwangi, Indonesia
241002111050@student.unsil.ac.id[1], 241002111052@student.unsil.ac.id[2],

ABSTRACT.
This study aims to analyze the 2020 Tokopedia user data breach, its causes, its impact on national cybersecurity, and the Islamic perspective on personal data protection. The method used is qualitative research with content analysis techniques based on literature and interview data. The findings indicate that the breach was caused by weaknesses in encryption, access management, and the absence of strong data protection regulations. The impact includes a decline in public trust and increased risk of cybercrime. From an Islamic perspective, data breaches constitute a violation of trust (amanah) and the right to privacy. There is a need for stricter regulations and heightened awareness regarding the importance of personal data protection.

Keywords: Data Breach, Cybersecurity, Tokopedia, Data Protection, Islamic Perspective.

ABSTRAK.
Penelitian ini bertujuan untuk menganalisis kebocoran data pengguna Tokopedia pada tahun 2020, penyebabnya, dampaknya terhadap keamanan siber nasional serta pandangan Islam terkait perlindungan data pribadi. Metode yang digunakan yaitu penelitian kualitatif dengan teknik analisis konten berdasarkan data dari literatur dan wawancara. Hasil penelitian menunjukkan bahwa kebocoran disebabkan oleh kelemahan enkripsi dan pengelolaan akses serta kurangnya regulasi perlindungan data. Dampaknya mencakup penurunan kepercayaan publik dan meningkatnya risiko kejahatan siber. Dalam pandangan Islam, kebocoran data melanggar amanah dan hak privasi. Diperlukan regulasi yang lebih ketat dan kesadaran tinggi tentang pentingnya perlindungan data pribadi.

Kata kunci: Kebocoran Data, Keamanan Siber, Tokopedia, Perlindungan Data, Pandangan Islam.

PENDAHULUAN

Di era digital seperti ini, data pribadi pengguna menjadi komoditas yang sangat berharga. Perkembangan teknologi informasi membawa dampak besar terhadap berbagai kehidupan termasuk dalam transaksi ekonomi dan pengguna platform digital. Seiring dengan kemajuan tersebut, ancaman terhadap keamanan siber semakin meningkat. Insiden besar yang pernah terjadi yaitu kebocoram data pengguna Tokopedia pada tahun 2020 yang mengejutkan publik dan menimbulkan kekhawatiran luas tentang perlindungan data pribadi di Indonesia. Tokopedia sebagai salah satu e-*commerce* terbesar di Indonesia mengalami insiden kebocoran data besar-besaran yang melibatkan lebih dari 91 juta akun pengguna.

Data yang bocor meliputi nama pengguna, email, nomor telepon dan hashed *password*, meskipun pihak Tokopedia mengklaim bahwa informasi sensitif seperti transaksi dan kartu

kredit tetap aman. Kejadian ini mengungkapkan kelemahan sistem keamanan digital dan lemahnya perlindungan data pribadi di Indonesia. Masyarakat pun semakin bergantung pada teknologi dan platform digital dalam menjalankan aktivitas sehari-hari. Menimbulkan pertanyaan besar terkait sejauh mana keamanan siber di Indonesia dapat menjamin perlindungan terhadap data pribadi masyarakat.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode deskriptif analitis. Dipilih untuk menggali secara mendalam penyebab, dampak dan implikasi dari kebocoran data Tokopedia pada tahun 2020 serta menganalisisnya dari segi teknis, sosial dan perspektif Islam.

Jenis data yang digunakan dalam penelitian ini yaitu data sekunder yang mencakup laporan-laporan terkait insiden kebocoran data, artikel ilmiah, berita dan dokumen resmi yang diterbitkan oleh Tokopedia dan lembaga terkait. Teknik pengambilan sampel dilakukan dengan menggunakan teknik purposive sampling di mana data diambil dari sumber-sumber yang relevan dan memiliki informasi mendalam terkait kebocorand ata seperti para ahli di bidang keamanan siber, pengelola platform digital serta dokumen resmi dari Tokopedia.

Waktu penelitian dilakukan pada bulan April 2025. Tempat penelitian berfokus pada pengelolaan data di Indonesia dengan perhatian khusus pada platform digital Tokopedia sebagai objek studi. Teknik analisis data yang digunakan yaitu analisis konten. Teknik ini melibatkan pengkategorian dan interpretasi data yang diperoleh dari dokumen dan wawancara dengan tujuan untuk menarik kesimpulan yang berkaitan dengan kebocoran data, penyebab, dampak dan pandangan Islam terhadap perlindungan data pribadi. Analisis ini dilakukan secara mendalam dengan mempertimbangkan sosial teknis dan hukum.

HASIL DAN PEMBAHASAN

Hasil Penelitian

Penelitian ini menunjukkan bahwa kebocoran data Tokopedia pada tahun 2020 terjadi akibat lemahnya sistem keamanan digital perusahaan dalam aspek enkripsi data dan manajemen kontrol akses. Berdasarkan analisis dokumen publik dan laporan keamanan siber, ditemukan bahwa data pengguna yang bocor mencakup nama lengkap, *email*, tanggal lahir dan *hash password* yang kemudian diperjualbelikan di forum *dark web.* Insiden ini berdampak pada sekitar 91 juta akun pengguna. Berdasarkan data dari Badan Siber dan Sandi Negara (BSSN, 2020), serangan siber selama tahun tersebut meningkat hingga lebih dari 290 juta kali dan Tokopedia menjadi salah satu target terbesar dengan tingkat kerentanan yang tinggi.

Tidak adanya regulasi perlindungan data pribadi yang kuat pada saat insiden terjadi menyebabkan keterlambatan dalam penanganan termasuk tidak adanya kewajiban hukum bagi perusahaan untuk memberitahukan pengguna secara transparan. Mengakibatkan kepercayaan masyarakat terhadap platform digital nasional menurun drastis. Studi ini juga menemukan bahwa tanggapan manajerial Tokopedia terhadap insiden tersebut bersifat defensif dan kurang responsif yang memperparah persepsi publik. Dalam wawancara dengan pakar keamanan siber, ditegaskan bahwa kelemahan sistem keamanan dan ketiadaan penilaian risiko berkala menjadi faktor utama yang memperbesar dampak kebocoran. Mereka juga menyebut bahwa perusahaan digital Indonesia umumnya masih melihat keamanan siber sebagai biaya tambahan, bukan sebagai kebutuhan strategis. Hasil analisis juga memperlihatkan bahwa banyak pengguna menggunakan ulang kredensial di berbagai platform sehingga kebocoran dari satu layanan dapat menciptakan efek domino terhadap layanan digital lainnya.

Penelitian ini juga mengangkat pandangan Islam terhadap perlindungan data pribadi. Berdasarkan kajian literatur keislaman, ditemukan bahwa menjaga privasi merupakan bagian dari ajaran moral Islam yang berkaitan erat dengan amanah dan larangan untuk menyakiti sesama melalui pelanggaran hak privasi. Kebocoran data bukan hanya persoalan teknis, tetapi juga pelanggaran terhadap prinsip keadilan dan etika Islam.

Tabel 1. Statistik Serangan Siber di Indonesia Tahun 2020

Jenis Serangan Siber	Jumlah Terdeteksi	Keterangan
Total Serangan Siber	495.337.202	Meningkat 41% dari tahun 2019 (290 juta serangan)
Ransomware	1.011.209	Mengancam privasi dan keamanan data pribadi
Advanced Persistent Threat (APT)	4.001.905	Aktivitas serangan siber tingkat lanjut
Insiden Siber	9.000	Serangan yang berhasil menembus sistem

Sumber: Badan Siber dan Sandi Negara (BSSN), 2020

Data di atas menunjukkan bahwa Indonesia mengalami lonjakan dalam jumlah serangan siber pada tahun 2020 dengan total lebih dari 495 juta serangan yang terdeteksi. Jenis serangan yang paling menonjol yaitu *ransomware* dan *Advanced Persistent Threat* (APT) yang menunjukkan peningkatan kompleksitas dan intensitas ancaman siber. Meskipun jumlah serangan sangat tinggi hanya sekitar 9.000 yang dikategorikan sebagai insiden siber yaitu serangan yang berhasil menembus sistem dan menyebabkan kerusakan atau kebocoran data. Statistik ini menekankan pentingnya peningkatan sistem keamanan siber di Indonesia, baik dari sisi teknologi, regulasi maupun kesadaran pengguna. Perusahaan dan institusi perlu melakukan evaluasi dan pembaruan terhadap protokol keamanan mereka untuk menghadapi ancaman yang semakin canggih dan terorganisir.

Pembahasan

Kelemahan Sistem Keamanan Tokopedia

Kebocoran data Tokopedia pada tahun 2020 menjadi bukti lemahnya sistem keamanan internal yang digunakan perusahaan (Liliana, 2023). Berdasarkan analisis forensik dari komunitas keamanan siber dan pernyataan resmi Tokopedia, ditemukan bahwa enkripsi kata sandi yang digunakan hanya berupa hash statis tanpa garam (salt) sehingga rentan terhadap serangan brute force dan rainbow table. Manajemen akses tidak menerapkan prinsip least privilege secara efektif, membuat data pengguna dapat diakses dengan tingkat otorisasi yang relatif rendah (Kurniawan, 2021). Memperbesar risiko eksploitasi jika terjadi pelanggaran sistem. Kelemahan sistem keamanan Tokopedia yang terbongkar dalam insiden kebocoran data 2020 menunjukkan adanya kegagalan mendasar dalam penerapan prinsip-prinsip dasar keamanan siber (Tarumingkem, 2021). Sistem enkripsi yang hanya menggunakan hash statis tanpa salt memperlihatkan minimnya upaya perusahaan dalam melindungi data sensitif pengguna secara kriptografis, padahal teknologi salting dan key stretching seperti bcrypt atau Argon2 telah menjadi standar industri yang direkomendasikan (Kurniawan, 2021). Ketiadaan salting menjadikan seluruh hash password pengguna rentan terhadap serangan rainbow table di mana penyerang dapat mencocokkan hash dengan basis data hash publik yang telah dipetakan sebelumnya.

Kegagalan dalam menerapkan prinsip least privilege yakni pemberian akses sistem seminimal mungkin yang dibutuhkan oleh pengguna atau aplikasi mengindikasikan lemahnya pengelolaan otorisasi internal (Pardosi.et.al, 2024). Ketika akses terhadap data sensitif dapat diperoleh oleh pihak dengan level otorisasi rendah, maka setiap celah pada akun tersebut secara otomatis menjadi celah keamanan bagi seluruh sistem. Selaras dengan defense in depth dalam keamanan siber, di mana tiap lapisan harus memiliki pembatas dan proteksi yang memadai. Kegagalan ini tidak berdiri sendiri melainkan berkaitan langsung dengan lemahnya

tanggung jawab manajerial dan sistemik seperti telah dijelaskan sebelumnya (Kriswandaru.et.al, 2024). Manajemen Tokopedia gagal mengintegrasikan keamanan siber sebagai bagian dari strategi korporasi yang menyeluruh. Tidak adanya audit keamanan berkala, kurangnya incident response plan serta lemahnya budaya keamanan internal turut memperparah dampak dari insiden ini. Menunjukkan absennya regulasi yang memaksa perusahaan untuk menerapkan standar minimum keamanan siber.

Ketiadaan Regulasi Perlindungan Data

Faktor yang memperparah dampak kebocoran data ini yaitu ketiadaan regulasi perlindungan data pribadi yang kuat di Indonesia saat insiden terjadi (Kriswandaru.et.al, 2024). Meskipun RUU Perlindungan Data Pribadi telah lama dibahas, saat itu belum disahkan menjadi undang-undang. Mengakibatkan tidak ada kewajiban hukum bagi Tokopedia untuk melaporkan insiden kepada publik secara cepat dan transparan. Menurunkan tingkat kepercayaan masyarakat terhadap penyedia layanan digital dalam negeri (Putra.et.al, 2025). Ketiadaan regulasi perlindungan data pribadi yang memadai pada saat insiden kebocoran data Tokopedia tahun 2020 menjadi salah satu yang memperbesar skala dan dampak dari kejadian tersebut.

Meskipun Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP) telah mulai dibahas sejak beberapa tahun sebelumnya, lambannya proses legislasi membuat tidak adanya dasar hukum yang kuat yang mewajibkan perusahaan digital untuk melakukan mitigasi dan pelaporan insiden secara terbuka dan sistematis. Berbeda jauh dari praktik di negara-negara dengan undang-undang privasi data yang ketat seperti Uni Eropa dengan GDPR yang mensyaratkan pelaporan insiden maksimal dalam 72 jam setelah diketahui. Ketiadaan kewajiban hukum ini memberi ruang bagi perusahaan seperti Tokopedia untuk mengambil pendekatan defensif dan minim akuntabilitas dalam menangani krisis. Respons yang

lambat dan tidak transparan tersebut mengganggu pemulihan kepercayaan konsumen dan juga berdampak sistemik pada stabilitas ekosistem digital nasional. Keengganan untuk mengakui kelemahan sistem secara terbuka menyebabkan publik tidak mendapat informasi yang memadai tentang risiko yang sedang mereka hadapi, termasuk potensi penyalahgunaan data pribadi mereka di dark web atau untuk kejahatan rekayasa sosial.

Tidak adanya kerangka hukum yang mengatur perlindungan dan pemrosesan data pribadi menyebabkan lemahnya pengawasan dan rendahnya standar keamanan yang diterapkan oleh perusahaan digital (Kriswandaru.et.al, 2024). Mengakibatkan tidak hanya Tokopedia yang terdampak, tetapi juga kredibilitas pemerintah dalam menjamin keamanan ruang siber nasional turut dipertaruhkan. Sebagaimana diperkuat dalam data BSSN tahun 2020, meningkatnya jumlah serangan siber hingga lebih dari 495 juta kali menunjukkan urgensi regulasi yang mampu mengatur pengelolaan data secara menyeluruh baik oleh sektor publik maupun swasta.

Dampak terhadap Kepercayaan Publik dan Keamanan Nasional

Dampak dari insiden ini sangat luas dari sisi individu maupun sistemik. Masyarakat mengalami keresahan karena kredensial mereka beredar bebas di dark web yang dapat digunakan untuk kejahatan seperti phishing, rekayasa sosial dan pencurian identitas (Rahmawati.et.al, 2024). Pemerintah harus menghadapi kenyataan bahwa infrastruktur digital nasional belum cukup siap dalam menangani serangan berskala besar. Menurut data dari Badan Siber dan Sandi Negara (BSSN) lebih dari 290 juta serangan siber terjadi di Indonesia sepanjang tahun 2020 dan Tokopedia merupakan salah satu target terbesar. Dampak kebocoran data Tokopedia tahun 2020 tidak hanya mencederai rasa aman individu tetapi juga mengguncang fondasi kepercayaan publik terhadap penyedia layanan digital domestik dan mengindikasikan lemahnya kesiapsiagaan negara dalam menghadapi tantangan keamanan siber (Putra.et.al, 2025).

Masyarakat sebagai korban langsung, mengalami kegelisahan akibat data pribadi mereka seperti alamat email, nama lengkap, nomor HP hingga hash kata sandi tersebar di dark web dan dapat dimanfaatkan oleh aktor jahat untuk kejahatan digital seperti phishing, rekayasa sosial (*social engineering*), pembajakan akun hingga pencurian identitas (Rahmawati.et.al, 2024). Minimnya kesiapan dalam mitigasi risiko digital ini memperkuat urgensi pembentukan sistem keamanan nasional berbasis pendekatan menyeluruh (*total defense cyber strategy*) yang tidak hanya melibatkan sektor pemerintah, tetapi juga swasta, akademisi dan masyarakat sipil (Hermawan.et.al, 2022). Ketiadaan regulasi dan kerangka koordinatif yang kuat menjadikan insiden Tokopedia sebagai *wake up call* terhadap kelemahan mendasar dalam tata kelola digital Indonesia. Peran negara sangat krusial sebagai regulator, fasilitator sekaligus pelindung kepentingan warga negara di dunia digital.

Perspektif Islam terhadap Privasi dan Keamanan Data

Dalam perspektif Islam, menjaga privasi termasuk dalam kategori menjaga amanah. Al-Qur'an Surat Al-Hujurat ayat 12 menegaskan larangan tajassus (memata-matai) yang relevan dengan perlindungan data pribadi. Pelanggaran terhadap keamanan data dapat dikategorikan sebagai pelanggaran etika dan hukum syariat. Privasi bukan hanya hak digital tetapi juga hak moral yang dijamin oleh nilai-nilai keislaman. Penelantaran terhadap perlindungan data mencerminkan pengabaian terhadap amanah dan bisa dikategorikan sebagai bentuk kezaliman. Pemaknaan etika digital dalam Islam menuntut integrasi nilai-nilai moral dalam setiap proses pengelolaan data termasuk transparansi, akuntabilitas dan keadilan (Gamar & Maliki, 2025). Perusahaan digital semestinya tidak hanya berpikir tentang efisiensi dan keuntungan, tetapi juga harus menyadari tanggung jawab etik dan spiritual mereka kepada para pengguna. Negara pun berkewajiban memastikan perlindungan data sebagai bagian dari perlindungan terhadap hak asasi manusia yang dijamin baik dalam konstitusi maupun dalam kerangka nilai keagamaan. Tentunya ini sekaligus memperkuat urgensi penerapan regulasi perlindungan data pribadi yang tidak hanya bersifat legalistik, tetapi juga berakar pada nilai keadilan dan tanggung jawab sosial dalam bingkai keislaman. Dalam ajaran Islam, perlindungan atas privasi seseorang tidak sekadar merupakan urusan administratif atau teknis, melainkan termasuk dalam prinsip hifz al-`ird (penjagaan kehormatan) dan hifz al-amanah (penjagaan amanah) (Musthofa, 2023). Ketika seseorang menyerahkan data pribadinya kepada suatu institusi, seperti Tokopedia, maka secara implisit terjadi akad amanah yang mewajibkan pihak penerima data untuk menjaganya sebaik mungkin.

Tanggung Jawab Manajerial dan Sistemik

Tercermin dari lambatnya respons publik serta minimnya komunikasi krisis yang efektif. Pada tingkat nasional, belum tersedia lembaga pengawasan independen yang dapat mengaudit dan mengevaluasi kesiapan sistem keamanan digital dari perusahaan teknologi besar. Tanggung jawab terhadap perlindungan data seharusnya tidak hanya dibebankan kepada entitas teknis tetapi harus menjadi komitmen manajerial yang menyeluruh. Lemahnya respon Tokopedia turut diperparah oleh ketiadaan lembaga otoritatif yang memiliki fungsi pengawasan, evaluasi dan penegakan hukum secara independen dalam isu perlindungan data pribadi.

Ketika insiden terjadi, tidak ada badan yang secara resmi memaksa Tokopedia untuk melapor, mengaudit sistemnya atau memberikan ganti rugi kepada pengguna. Menunjukkan bahwa sistem nasional belum memiliki digital accountability infrastructure yang memadai. Tanggung jawab perlindungan data tidak boleh hanya menjadi beban unit teknologi informasi atau tim keamanan digital. Dalam kerangka enterprise risk management, keamanan siber harus dijadikan isu strategis yang dibahas dalam rapat dewan direksi, didanai secara proporsional dan dipantau sebagai indikator utama kinerja organisasi. Menjadi panggilan bagi negara untuk memperkuat lembaga-lembaga pengawas digital yang independen, memiliki

legitimasi hukum, serta didukung oleh sumber daya yang kompeten dan sistem forensik digital yang memadai. Ketika tanggung jawab ini tidak ditangani secara serius di dua level korporat dan negara maka bukan hanya data masyarakat yang terancam, tetapi juga integritas sistem ekonomi digital nasional yang lebih luas. Keamanan data merupakan pondasi dari transformasi digital yang berkelanjutan dan kegagalan Tokopedia harus dibaca sebagai alarm keras bahwa Indonesia masih membutuhkan pembenahan sistemik agar tidak terus menjadi target empuk kejahatan siber global (Hermawan.et.al, 2024).

KESIMPULAN DAN SARAN

Penelitian ini menyimpulkan bahwa kebocoran data pengguna Tokopedia pada tahun 2020 merupakan akibat dari kelemahan sistem keamanan digital internal, terlebih pada enkripsi dan manajemen kontrol akses yang tidak memadai. Diperparah oleh belum adanya regulasi perlindungan data pribadi yang kuat di Indonesia pada saat kejadian sehingga respon hukum dan institusional terhadap insiden menjadi lambat dan tidak transparan. Kebocoran ini berdampak sistemik, mulai dari penurunan kepercayaan publik terhadap platform digital hingga meningkatnya potensi kejahatan siber di tingkat nasional. Dalam perspektif Islam, insiden ini mencerminkan pelanggaran terhadap amanah dan hak privasi yang seharusnya dijaga sebagai bentuk tanggung jawab moral. Temuan ini mengafirmasi hipotesis dan tujuan awal penelitian bahwa perlindungan data pribadi membutuhkan kesadaran teknologi, hukum dan etika yang terpadu.

Penelitian ini juga membuktikan bahwa kebocoran data berdampak luas, baik secara sosial melalui menurunnya kepercayaan publik terhadap layanan digital maupun secara nasional dengan meningkatnya eksposur terhadap ancaman keamanan siber. Dalam normatif Islam, insiden ini memperlihatkan pelanggaran terhadap prinsip amanah dan perlindungan hak individu atas privasi, menandakan kegagalan moral dan spiritual dalam praktik bisnis digital. Penelitian ini berhasil menjawab hipotesis bahwa perlindungan data pribadi di era digital hanya dapat terwujud apabila ada integrasi antara kesadaran teknologi, regulasi hukum yang tegas serta tanggung jawab etis dari pelaku industri digital. Keberadaan kebijakan yang komprehensif dan pengawasan institusional yang independen sangat krusial untuk mencegah insiden serupa dan memastikan keamanan serta kepercayaan dalam ekosistem digital nasional.

Saran

Sebagai tindak lanjut dari temuan penelitian ini, disarankan agar pemerintah segera memperkuat implementasi Undang-Undang Perlindungan Data Pribadi melalui regulasi turunan yang jelas, serta membentuk lembaga pengawasan independen yang memiliki otoritas untuk mengaudit dan menindak pelanggaran terhadap perlindungan data. Bagi perusahaan digital, perlu dilakukan transformasi paradigma bahwa keamanan siber bukan sekadar biaya tambahan, melainkan investasi strategis. Diperlukan juga pelatihan berkelanjutan bagi pengembang dan manajer sistem mengenai etika digital dan prinsip keamanan data. Dalam keagamaan dan sosial perlu digalakkan edukasi publik berbasis nilai-nilai keislaman tentang pentingnya menjaga privasi dan amanah dalam ruang digital agar pengguna menjadi subjek aktif dalam melindungi datanya. Perusahaan digital seperti Tokopedia juga diharapkan mengubah orientasinya terhadap keamanan siber dari pendekatan reaktif menjadi proaktif.

Mencakup penerapan standar enkripsi terkini, sistem manajemen akses yang ketat serta pembentukan unit tanggap insiden yang dilatih untuk merespons kebocoran data secara cepat dan transparan. Transformasi ini tidak hanya bersifat teknis, tetapi juga menuntut internalisasi nilai etika digital dalam pengambilan keputusan manajerial. Untuk pengembangan sumber daya manusia, pelatihan keamanan informasi yang berkelanjutan harus diwajibkan bagi tim pengembang, administrator sistem dan manajemen puncak. Materi pelatihan hendaknya tidak hanya mencakup aspek teknis tetapi juga dimensi etika dan hukum agar lahir kesadaran komprehensif akan tanggung jawab menjaga data pengguna sebagai bagian dari amanah

profesional. Dari sudut pandang sosial dan keagamaan, edukasi publik mengenai pentingnya perlindungan data pribadi perlu diperluas melalui pendekatan berbasis nilai-nilai keislaman seperti prinsip menjaga amanah dan larangan tajassus.

Edukasi ini penting agar masyarakat tidak hanya menjadi objek yang dilindungi tetapi juga menjadi subjek aktif yang memahami hak, risiko dan tanggung jawab dalam ruang digital. Disarankan agar penelitian lebih lanjut menggali hubungan antara efektivitas regulasi data pribadi dan perilaku keamanan digital di kalangan pelaku industri serta pengguna. Pendekatan interdisipliner yang menggabungkan perspektif hukum, teknologi, manajemen dan etika keislaman akan memperkaya pemahaman dan solusi terhadap isu kebocoran data di masa depan.

DAFTAR PUSTAKA

Gamar, N., & Maliki, P. L. (2025). *Manajemen Lembaga Pend*

Hermawan, A., Hartati, T., & Wijaya, Y. A. (2022). Analisa Keamanan Data Melalui Website Zahra Software Menggunakan Metode Keamanan Informasi CIA Triad. *Jurnal Informatika: Jurnal Pengembangan IT*, *7*(3), 125-130.

Kriswandaru, A. S., Pratiwi, B., & Suwardi, S. (2024). Efektivitas Kebijakan Perlindungan Data Pribadi di Indonesia: Analisis Hukum Perdata dengan Pendekatan Studi Kasus. Hakim: Jurnal Ilmu Hukum dan Sosial, 2(4), 740-756.

Kurniawan, A. (2021). *Ethical Hacker–Menjadi Peretas yang Beretika*. PENERBIT KBM INDONESIA.

Liliana, D. Y., Arnanda, R., Adnan, A. I., & Yuliastuti, H. (2023, August). Policy Brief–Penguatan Implementasi Regulasi Perlindungan Data Pribadi Bagi Pelanggan Lokapasar di Indonesia. In *Seminar Nasional Inovasi Vokasi* (Vol. 2, pp. 33-38).Priliasari, E. (2023). Perlindungan Data Pribadi Konsumen Dalam Transaksi E-Commerce. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, *12*(2).

Musthofa, M. A. (2022). Aturan Sertifikasi Produk Halal Dalam Tinjauan Maqāṣid Al-Syarī'ah Jasser Auda. *Al-Faruq: Jurnal Hukum Ekonomi Syariah Dan Hukum Islam*, *1*(1), 13-26.

Pardosi, V. B. A., Deta, B., Nugroho, F., & Vandika, A. Y. (2024). Sistem Keamanan Informasi.

Putra, B. P. P., Judijanto, L., Apriyanto, A., Susilo, A., Kusumastuti, S. Y., Jamaludin, J., ... & Sari, F. H. (2025). *Tren Bisnis Digital:: Transformasi Dunia Bisnis Terkini*. PT. Sonpedia Publishing Indonesia.

Rahmawati, D., Mila, V., Giri, L., Rienzy, K., Wiratri, A., Rizki, A., ... & Aisyah, A. (2024). Waspada Kejahatan Phishing Attack!.

Tarumingkeng, R. C. Risiko Siber..