

Perlindungan Privasi dan Keamanan Siber E-Wallet: Analisis Fikih Muamalah Terhadap Risiko Kebocoran Data

Zul Asri Widiastuti¹, Alia Yulianti², Siti Nur Aisyah³, Nastiti Ratnadewati⁴, Syaeful Bahri⁵

¹Program Studi Ekonomi Syariah, Fakultas Ekonomi dan Bisnis Islam, UIN Sultan Maulana Hasanuddin Banten

Email: ¹zulasriwidiastuti@gmail.com, ²aliayulianti647@gmail.com, ³sitinuraisyah10104@gmail.com,
⁴ratnadewati491@gmail.com, ⁵syaeful.bahri@uinbanten.ac.id

ARTICLE INFO

Article history:

Received: June 23, 2026

Accepted: August 02,
2026

Published: August 18,
2026

Keywords:

Cybersecurity; Data
Breaches; E-wallets;
Islamic Commercial Law;
Descriptive Analysis

ABSTRACT

The digital landscape in Indonesia is undergoing rapid changes and poses serious security risks related to the potential leakage of personal data from today's digital financial devices. This descriptive quantitative study aims to thoroughly assess users' perceptions of the effectiveness of cybersecurity features and to analyze the fulfillment of consumer rights under Islamic commercial law (fikh muamalah). Data were collected through a structured questionnaire distributed to 57 respondents and carefully analyzed using SPSS. The results show that digital wallet users are predominantly women (63.2%) aged 19-21. The study shows that, although security features are considered adequate, concerns regarding potential data misuse by third parties remain high. From the perspective of muamalah fikh, the protection of personal data privacy is an essential component in the application of the principles of hifz al-mal and hifz an-nafs. That is why e-wallet providers bear full responsibility for losses resulting from system negligence in the interest of the public good.

PENDAHULUAN

Akselerasi transformasi digital setelah pandemi telah secara mendalam mengubah peta ekonomi global, memicu pergeseran dari cara transaksi tradisional ke sistem pembayaran tanpa uang tunai. Di Indonesia, perkembangan ini terlihat jelas dengan meningkatnya jumlah platform digital seperti DANA, OVO, GoPay, dan ShopeePay yang menawarkan efisiensi tinggi, akses cepat, dan kenyamanan dalam kegiatan transaksi sehari-hari masyarakat [1]. Integrasi fintech ini tidak hanya menjadi bagian dari gaya hidup modern, tetapi telah menjadi infrastruktur penting yang mendukung inklusi keuangan di tingkat nasional, memperlancar birokrasi pembayaran, serta menjangkau masyarakat yang belum pernah merasakan layanan perbankan formal [2].

Namun, di balik kemudahan dan kenyamanan yang hadir dari e-wallet, ada risiko sistematis yang mengancam privasi dan keamanan data pengguna. Penggunaan teknologi pembayaran digital pada dasarnya melibatkan pengumpulan, pengelolaan, dan penyimpanan data sensitif pengguna secara real time [3]. Hal ini menjadikan industri penyedia platform digital sebagai sasaran utama serangan siber, seperti penipuan phishing, penyebaran malware, peretasan server, dan kejahatan rekayasa sosial [4]. Kasus kebocoran data pribadi yang terjadi secara besar-besaran di berbagai platform digital nasional menekankan bahwa struktur keamanan siber dan perlindungan hukum konsumen di Indonesia masih lemah dan belum mampu menjamin perlindungan yang memadai [5].

Dari sudut pandang hukum sipil dan regulasi yang berlaku seperti Undang-Undang Perlindungan Data Pribadi (UU PDP) Nomor 27 Tahun 2022, penyedia layanan e-wallet memiliki tanggung jawab hukum yang penuh dalam menjaga kerahasiaan data yang mereka kelola [6]. Kegagalan sistem yang berujung pada kebocoran data dapat menyebabkan kerugian materiil, seperti hilangnya saldo rekening konsumen, serta kerugian immaterial, misalnya penyalahgunaan identitas untuk pinjaman online ilegal, pemasaran, dan pelanggaran privasi yang serius [7]. Sayangnya, kenyataan menunjukkan adanya ketidakseimbangan posisi tawar antara konsumen dan perusahaan penyedia e-wallet. Dalam banyak ketentuan standar dalam perjanjian elektronik, sering kali tanggung jawab atas kegagalan keamanan dilimpahkan sepihak kepada pengguna, sehingga membuat konsumen berada dalam posisi rentan ketika terjadi kebocoran data pribadi [8].

Di sisi lain, sebagian besar pengguna platform digital di Indonesia termasuk dalam kategori usia yang produktif dan generasi muda (Gen Z) yang sangat terpengaruh oleh inovasi digital, namun terkadang memiliki tingkat kesadaran akan keamanan yang tidak merata. Meskipun secara umum pengguna mengerti pentingnya menjaga kerahasiaan kata sandi atau Personal Identification Number (PIN), pemahaman mereka tentang risiko berbagi data dengan pihak ketiga dan hak privasi digital masih dianggap setengah hati [9]. Ketidakseimbangan antara tingginya penggunaan platform digital dengan pemahaman menyeluruh tentang risiko siber menciptakan potensi kerentanan yang mengkhawatirkan untuk keamanan data nasional [10].

Menanggapi perkembangan tersebut, studi akademis seharusnya tidak hanya mengandalkan pendekatan hukum positif dari Barat atau regulasi teknis semata, tetapi juga penting untuk menggabungkan nilai-nilai etis-teologis yang diambil dari hukum Islam, khususnya dalam Fikih Muamalah. Islam sebagai sistem nilai yang menyeluruh menyatakan bahwa setiap aktivitas ekonomi dan transaksi digital harus berlandaskan pada prinsip keadilan, transparansi, amanah, serta terhindar dari unsur ketidakpastian yang merugikan [11]. Dalam perspektif Fikih Muamalah modern, data pribadi konsumen diakui memiliki nilai ekonomi dan kehormatan yang setara dengan aset, sehingga perlindungannya wajib. Kebocoran data karena kelalaian atau cacat pada sistem keamanan siber dari penyedia platform merupakan pelanggaran terhadap akad amanah yang dapat menimbulkan tuntutan kompensasi demi menjaga kepentingan publik [12].

Walaupun ada beberapa literatur sebelumnya yang meneliti efektivitas keamanan dompet digital, kebanyakan penelitian tersebut masih terperangkap dalam pendekatan normatif-hukum atau analisis kepuasan konsumen secara umum tanpa mengaitkannya dengan realitas persepsi risiko pengguna dan tinjauan Fikih Muamalah secara menyeluruh [13]. Oleh karena itu, penelitian ini hadir untuk menjembatani kekurangan akademis tersebut dengan merumuskan dua pertanyaan pokok. Pertama, bagaimana pandangan pengguna aplikasi dompet digital terhadap efektivitas fitur keamanan siber dan perlindungan privasi data pribadi mereka saat ini? Kedua, bagaimana analisis Fikih Muamalah mengenai perlindungan privasi dan pemenuhan hak-hak pengguna terkait risiko kebocoran data berdasarkan pengalaman nyata responden? Dengan menggunakan pendekatan kuantitatif deskriptif yang didasarkan pada data kuesioner empirik dan analisis statistik dengan SPSS, diharapkan penelitian ini bisa memberikan kontribusi teoretis dan praktis yang berarti untuk pengembangan hukum ekonomi syariah digital di Indonesia.

METODOLOGI PENELITIAN

Penelitian ini menggunakan metode kuantitatif dengan cara yang deskriptif dan analitis. Pendekatan ini dipilih untuk memberikan fakta-fakta serta hubungan antar fenomena yang diteliti berkaitan dengan pandangan penggunaan terhadap fitur siber e-wallet dan pengaruhnya dalam fikih muamalah. Oleh karena itu, jumlah deskripsi yang dikumpulkan tidak cukup untuk diproses dan disajikan untuk menjelaskan karakteristik sebenarnya dari kelompok yang diteliti, yang merupakan kebutuhan dari kompleks hipotesis asosiasi atau sebab akibat. Peserta atau kelompok umum ini adalah mereka yang menggunakan aplikasi kartu elektronik di Indonesia. Pilihan peserta berikut ini adalah metode pengambilan yang tidak mungkin, terutama karena kesalahan yang disengaja. Kriteria penyertaan bagi individu yang biasa menggunakannya kurang dari platform kartu digital dalam aktivitas keuangannya. Setelah menyebarkan pertanyaan secara online, 57 responden yang memenuhi syarat dan akan dijadikan sebagai unit analisis utama dalam penelitian.

Sumber data penelitian ini dibagi menjadi dua kategori. Pertama, data primer diperoleh langsung dari tanggapan kuesioner yang diisi oleh 57 responden. Instrumen kuesioner disusun dengan indikator yang dimodifikasi dari model kesadaran keamanan informasi, yang meliputi dimensi pengetahuan, sikap, dan perilaku konsumen digital. Kedua, data sekunder berupa literatur tentang Fikih Muamalah Kontemporer, Fatwa dari Dewan Syariah Nasional-Majelis Ulama Indonesia, buku-buku hukum islam klasik, serta regulasi hukum yang berlaku seperti UU Perlindungan Data Pribadi Nomor 27 Tahun 2022. Teknik pengumpulan data dilakukan melalui penyebaran kuesioner tertutup, dimana setiap pertanyaan disertai pilihan jawaban

terstruktur untuk memudahkan responden serta menjaga keharmonisan data. Selain itu, dilakukan juga studi dokumentasi terhadap syarat dan ketentuan beberapa platform e-wallet untuk menganalisis asimetri informasi serta klausul yang merugikan secara sepihak.

Untuk memastikan keabsahan data, penelitian ini sepenuhnya dilakukan dengan perangkat lunak statistik SPSS menggunakan metode analisis frekuensi. Tahapan pengolahan data menggunakan SPSS mencakup:

1. Pengeditan dan Pengkodean Data, yakni memeriksa kelengkapan jawaban kuesioner dari 57 responden serta melakukan pengkodean angka terhadap karakteristik demografi seperti jenis kelamin dan umur, dan juga nilai total jawaban kuesioner.
2. Entri Data, yakni memasukkan data mentah yang telah dikodekan ke dalam tampilan data di SPSS
3. Proses Deskriptif Statistik, yakni menerapkan fungsi analisis frekuensi untuk menghasilkan table distribusi frekuensi, nilai persentase, persentase valid, dan persentase kumulatif dari masing-masing variabel demografi maupun akumulasi skor jawaban responden.
4. Interpretasi Data, yakni menganalisis secara deskriptif hasil dari SPSS yang kemudian dikontekstualisasi dan dianalisis menggunakan teori dhaman, konsep milkiyah al-ma'lumat, serta pilar Maqashid Syariah dalam Fikih Muamalah modern.

HASIL DAN PEMBAHASAN

1. Analisis Karakteristik Demografi Peserta Melalui SPSS

Dengan memproses data dari SPSS, terhadap 57 responden (N=57) yang secara aktif memanfaatkan platform e-wallet, diperoleh Gambaran deskriptif tentang karakteristik partisipan penelitian yang berhubungan dengan jenis kelamin (JK) dan usia. Informasi ini penting untuk memahami seberapa besar variasi demografi memengaruhi perkembangan sikap dalam penggunaan transaksi digital [9].

Tabel 1. Distribusi Frekuensi Berdasarkan Jenis Kelamin (Output SPSS)

Jenis Kelamin	Frekuensi	Persentase %	Persentase Valid %	Persentase Kumulatif
Laki-Laki	21	36,8	36,8	36,8
Perempuan	36	63,2	63,2	100,0
Total	57	100,0	100,0	

Sumber: *Data Primer diolah (2026)*

Tabel 1 memperhatikan bahwa pengguna yang berjenis kelamin Perempuan mencapai 63,2% (36 responden), sementara pengguna laki-laki memiliki persentase 36,8% (21 responden). Tingginya partisipasi Perempuan ini sesuai dengan hasil penelitian Bimo Cokro utomo dan Atep Aulia Rahman [10] yang menyebutkan bahwa Perempuan lebih aktif dalam menggunakan dompet digital untuk keperluan sehari-hari dan sama, mereka juga lebih rentan terhadap ancaman rekayasa sosial.

Tabel 2. Distribusi Frekuensi Berdasarkan Umur Responden (Output SPSS)

Umur (Tahun)	Frekuensi	Persentase %	Persentase Valid %	Persentase Kumulatif
15	1	1,8	1,8	1,8
17	1	1,8	1,8	3,5
18	1	1,8	1,8	5,3
19	12	21,1	21,1	26,3
20	21	36,8	36,8	63,2
21	13	22,8	22,8	86,0
22	3	5,3	5,3	91,2
23	1	1,8	1,8	93,0
24	2	3,5	3,5	96,5
25	1	1,8	1,8	98,2
30	1	1,8	1,8	100,0
Total	57	100,0	100,0	

Sumber: *Data Primer diolah (2026)*

Analisis yang terdapat pada Tabel 2 menunjukkan bahwan seberapa besar partisipan berada dalam kategori yang produktif untuk penggunaan teknologi, yaitu pada usia 19 tahun (21,1%) 20 tahun (36,8%), dan 21 tahun (22,8%). Total persentase kumulatif untuk usia 19 hingga 21 tahun mencapai 80,7% dari seluruh sampel. Angka ini secara nyata menunjukkan bahwa pengguna e-wallet Sebagian besar berasal dari generasi Z. Dikutip dari jurnal studi keislaman [16], Generasi Z dikenal memiliki kemampuan beradaptasi dengan teknologi yang tinggi, tetapi sering kali terjebak dalam gaya hidup cepat tanpa memperhatikan perlindungan berlapis pada privasi perangkat mereka.

2. Analisis Distribusi Total Skor Kesadaran Keamanan Informasi

Dalam rangka menilai tingkat pemahaman dan kewaspadaan responden terhadap potensi kebocoran data pada e-wallet, data dari kuesioner dijumlahkan. Hasil dari SPSS menunjukkan bahwa skor total responden bervariasi dari nilai terendah 31 hingga nilai tertinggi 60.

Tabel 3. Segmentasi Akumulasi Skor Total Responden (Sintesis Distribusi SPSS)

Rentang Skor Total	Frekuensi	Persentase %	Kategori Kesadaran Keamanan
31,00 – 50,00	8	14,1	Rendah (Vulnerable)
52,00 – 58,00	18	31,6	Cukup Berwaspada (Cautionary)
59,00 – 60,00	31	54,3	Tinggi (Security Aware)
Total	57	100,0	

Sumber: *Data Primer diolah (2026)*

Data yang terdapat di Tabel 3 menunjukkan bahwa mayoritas peserta survei (54,3% atau 31 individu) meraih skor tertinggi (skor 59 dan 60), Dimana nilai yang paling sering muncul (modus) ada di skor tertinggi 60,00 dengan total responden (15,8%). Temuan kuantitatif ini memberikan bukti bahwa dalam konteks ini, konsumen digital memiliki harapan yang tinggi terhadap keandalan sistem serta memiliki pemahaman yang baik tentang hak privasi data pribadi mereka [14].

Namun, ada 14,1% responden yang memiliki skor di kisaran rendah (31-50). Kelompok kecil ini mendukung teori paradoks digital siber yang diusulkan oleh Putri Ernisa dkk [1], di mana kenyamanan dalam transaksi cepat mengalahkan rasionalitas dalam perlindungan data. Oleh karena itu, kelompok ini berisiko menjadi korban eksploitasi siber karena kurangnya perhatian terhadap penggantian kata sandi atau penyalahgunaan akses aplikasi.

3. Celah Keamanan Siber E-Wallet sebagai Bentuk Gharar Kontemporer

Di Indonesia E-wallet merupakan bagian penting dari alat pembayaran dizaman sekarang yang mana telah diatur langsung oleh Peraturan Bank Indonesia [18]. Dalam persepektif Fikih Muamalah modern, keabsahan transaksi non-tunai (termasuk yang menggunakan e-wallet atau QRIS terpusat) tergantung pada kemurnian akad dari unsur gharar (ketidakpastian) dan gharar (risiko/kerugian). Diketahui 14,1% pengguna yang memiliki perlindungan yang lemah, yang jika dikaitkan dengan kondisi sistem IT platform, menunjukkan adanya celah kerentanan yang signifikan [15].

Saefuddin Zuhri mengungkapkan bahwa tidak adanya interaksi fisik dalam transaksi digital mengharuskan adanya jaminan keamanan yang absolut sebagai pengganti kejelasan fisik objek (ta'yin al-maqud'alaih) [11]. Jika penyelenggara e-wallet tidak dapat memastikan keamanan data pengguna sehingga memicu kebocoran akun atau kegagalan sistem autentikasi, maka unsur gharar otomatis akan terintegrasi dalam transaksi tersebut. Ketidakjelasan tentang keamanan data pengguna atau potensi penyalahgunaan data pribadi oleh pihak ketiga untuk aktivitas kriminal, merusak dasar kerelaan timbal balik yang diwajibkan oleh syariah dalam islam.

4. Praktik Monetisasi Data Sepihak dalam Perspektif Milkiyah Al-Ma'lumat

Satu lagi fenomena yang di temukan dalam kajian terhadap teks kontrak elektronik dompet digital Adalah adanya pemaksaan klausul persetujuan untuk pengelolaan data pribadi pada saat pendaftaran aplikasi. Pengguna tidak memiliki pilihan untuk menolak yang mengakibatkan asimetri informasi hukum [6].

Dalam analisis kritis yang dilakukan oleh Zaenal Fanani, Bustanul Arifin, dan Fadwa Aly Elsayed Mohamed, Tindakan Perusahaan yang mengumpulkan, mengelola, dan memonetisasi atau membagikan data sensitif nasabah kepada pihak ketiga tanpa persetujuan yang jelas dan sukarela melanggar prinsip Milkiyah al-Ma'lumat (hak kepemilikan penuh atas informasi pribadi) [17]. Dalam konteks hukum ekonomi islam, data privasi seorang muslim di anggap berharga (mutaqawwim) dan bagian dari kehormatan yang harus dilindungi. Memanfaatkan data tersebut demi

keuntungan sepihak Perusahaan tanpa adanya akad bagi hasil atau izin eksplisit dianggap cacat hukum menurut syariah karena mencakup elemen ketidakjelasan.

5. Tanggung Jawab Hukum (Dhaman)

Korporasi atas kebocoran data nasabah Ketika sistem mengalami masalah yang mengakibatkan saldo pelanggan hilang atau akun diretas akibat kebocoran data masif, penentuan pihak yang bertanggung jawab atas kerugian menjadi hal yang sangat penting [7]. Hukum positif sipil di Indonesia dianggap masih lamban dan tidak adil dalam memberikan kompensasi yang nyata bagi para korban [5].

Fikih Muamalah modern memberikan alternatif untuk penerapan hukum yang lebih adil dengan menggunakan prinsip dharman al-Fi'li (tanggung jawab penuh atas Tindakan atau kelalaian) dan Fatwa DSN-MUI mengenai uang elektronik [13]. Moch.Hafido Fahmi menjelaskan bahwa posisi Perusahaan penyelenggara e-wallet syariah Adalah sebagai penyimpan data dan dana pelanggan berdasarkan akad Wadi'ah Yad Dhamanah atau Wakalah bil Ujrah [8]. Sebagai pihak yang dapat dipercaya, Perusahaan harus menerapkan standar keamanan tertinggi secara internasional untuk melindungi benda yang dipercayakan [4].

Jika terjadi kebocoran data atau saldo hilang akibat serangan peretas yang berhasil menembus sistem keamanan Perusahaan, maka dalam pandangan syariah, hal ini masuk dalam kategori taqsir (kelalaian yang signifikan dalam kewajiban perlindungan). Dengan demikian, posisi Perusahaan beralih dari penyimpan Amanah menjadi penanggung resiko yang harus bertanggung jawab (dhamin). Perusahaan diwajibkan untuk mengembalikan seluruh saldo hal yang hilang dan sepenuhnya memulihkan hak privasi pelanggan. Pelaksanaan sanksi Ganti rugi menurut syariah didasarkan pada kerangka kerja makro sistem Maqashid Syariah Jasser Auda, yang bertujuan untuk melindungi harta (hifz al-mal) dan melindungi hak asasi serta kehormatan jiwa manusia dari anacam kejahatan digital [3]

KESIMPULAN

Berdasarkan analisis yang telah dilakukan dan tambahan referensi yang mendasar, hasil penelitian dapat disimpulkan bahwasannya, Ekosistem pengguna e-wallet di dominasi oleh perempuan (63,2%) dan sebagian besar dari generasi Z berusia 19-21 tahun (80,7%). Mayoritas responden (54,3%) memiliki pemahaman yang baik mengenai keamanan. Namun, 14,1% terjebak dalam "paradoks siber," lebih memilih efisiensi transaksi dibandingkan perlindungan data pribadi [10]. Ada celah keamanan IT yang menyebabkan hilangnya dana nasabah. Berdasarkan Hukum Perdata, perusahaan bertanggung jawab penuh jika terjadinya kegagalan sistem [19]. Kebocoran data pribadi menyebabkan masalah hukum terkait pemenuhan kontrak [5]. Pembuatan klausul baku dalam dokumen pendaftaran dinilai merugikan konsumen dan tidak sesuai dengan prinsip syariah [3]. Ketidakpastian perlindungan siber mengandung gharar dan dharar yang dapat merusak validitas transaksi digital [11]. Monetisasi data pengguna tanpa adanya transparansi melanggar hak informasi pribadi [17]. Transaksi digital haruslah bebas biaya tersembunyi dan harus menerapkan tranparansi informasi [12].

Perlindungan data dalam transaksi non-tunai seperti QRIS merupakan bagian dari maqashid syariah terutama dalam menjaga kekayaan (hifz al-mal) dan melindungi jiwa (hifz an-nafs) [15]. Perlindungan konsumen merupakan hal utama yang harus diatur dengan regulasi yang bertujuan untuk kemaslahatan masyarakat [20]. Nilai-nilai syariah amat penting dalam enkripsi dapat mengurangi perilaku konsumtif dan hak keuangan konsumen dilindungi secara menyeluruh [16]. Penyedia dompet digital bertanggung jawab penuh akan semua keamanan aplikasi. Penegakan hukum perlindungan data memerlukan penguatan melalui sertifikasi dan pembentukan otoritas pengawas independen. Tidak dapat dipungkiri pula bahwa kebocoran data sering kali diperburuk dengan kelalaian pengguna, sehingga diperlukan reformasi yuridprudensi untuk penegakan hukum lebih baik di dunia siber.

UCAPAN TERIMA KASIH

Merupakan bentuk ucapan terima kasih dan penghargaan kepada pihak tertentu (badan, institusi, lembaga, organisasi, responden, dst) yang telah berkontribusi/mendanai/memberikan fasilitas/membantu penelitian dan lain sebagainya.

Penulis ingin mengungkapkan rasa Syukur dan pujian kepada Allah SWT atas segala anugrah-Nya, yang memungkinkan artikel ilmiah ini selesai dengan baik. Penulis menyadari bahwa penyusunan karya ini tidak terlepas dari bantuan, dukungan, dan bimbingan banyak pihak. Oleh karena itu, penulis mengungkapkan terima kasih yang mendalam kepada:

1. Orang tua dan Keluarga, untuk doa yang selalu mengalir, kasih sayang, serta dukungan moral dan materi yang menjadi sumber kekuatan utama bagi penulisan.
2. Dosen Pembimbing, yang telah meluangkan waktu, usaha, dan pemikiran untuk memberikan panduan, kritik yang membangun, serta pengarahan yang berharga dalam mendalami analisis Fikih Muamalah Kontemporer di artikel ini.
3. Pimpinan dan Civitas Academica UIN Sultan Maulana Hasanuddin Banten, atas sarana, fasilitas, dan lingkungan belajar yang mendukung selama masa perkuliahan.
4. Dewan Redaksi dan Reviewer Jurnal, berkat waktu, penilaian objektif, serta saran metodologis yang sangat membantu dalam memperbaiki kualitas dan kedalaman teori dalam artikel ini.
5. Semua Responden (57 Pengguna E-Wallet), yang telah meluangkan waktu untuk secara jujur mengisi kuesioner sehingga penulis memperoleh data primer yang valid untuk dianalisis.
6. Rekan-rekan seperjuangan dan semua pihak yang tidak bisa disebutkan satu per satu, terima kasih atas tempat berdiskusi, bantuan teknis dalam mengelola SPSS, serta semangat yang terus ada.

Sebagai penutup, semoga artikel ini dapat memberikan kontribusi nyata untuk meningkatkan literasi keuangan digital syariah, bermanfaat bagi penelitian dimasa depan, dan membawa kebaikan bagi Masyarakat luas. *Jazaakumullahu khairan katsiran*.

REFERENCES

- [1] P. Ernisa, C. A. Pratiwi, L. Trinanda, and K. P. Apandi, "E-Wallet dalam Rutinitas : dari Gaya Hidup Praktis Hingga Risiko Digital," *SINTAMA*, vol. 5, no. 3, pp. 352–360, 2025.
- [2] H. Hidayati, A. Malik, Bahtiar, and Suharti, "Transformasi Zakat melalui Aplikasi Digital: Upaya Membangun Literasi Keuangan Syariah di Era 5.0," *J. Pendidik. IPS*, vol. 15, no. 4, pp. 1569–1580, 2025, doi: <https://doi.org/10.37630/jpi.v15i4.3724>.
- [3] N. Adliyah, F. Jamaluddin, M. A. Kahfi, and Susisanti, "Perlindungan Data Pribadi Pengguna Dompet Digital Ovo," *Al-Ammwal*, vol. 6, no. 1, pp. 37–41, 2021.
- [4] F. Azhari, S. Sumarno, A. Fauzi, and D. R. Pratama, "Penerapan Manajemen Sekuriti Dalam Meningkatkan Keamanan Pengguna Pada Transaksi E-wallet," *, vol. 2, no. 2, pp. 138–147, 2024, doi: <https://doi.org/10.38035/jkmt.v2i2>.*
- [5] M. D. Maulindo and M. A. Antomy, "Tinjauan Yuridis Perlindungan Hukum terhadap

- Pengguna E- Wallet atas Kehilangan Dana Akibat Kebocoran Data dan Transaksi Tidak Sah dalam Perspektif Hukum Perdata,” *ALADALAH*, vol. 4, no. 2, 2026, doi: <https://doi.org/10.59246/aladalah.v2i4>.
- [6] A. Monica, C. Yulianti, and A. Nurintiara, “Upaya Penguatan Hukum Pelindungan Data Pribadi Dalam Keamanan Transaksi Menggunakan Dompot Elektronik Melalui Penerapan Zero-Knowledge Proof,” *Padjadjaran Law Rev.*, vol. 13, no. 1, pp. 73–87, 2025, doi: <https://doi.org/10.56895/plr.v13i1.2212> Submitted:
- [7] B. M. L. Putri, “Perlindungan Data Pribadi Atas Kebocoran Data Pengguna Pada Jual Beli Akun Dompot Digital (E-Wallet),” Universitas Lampung Bandar Lampung, 2025.
- [8] M. H. Fahmi, “Perlindungan Hukum Pengguna Dompot Digital Dan Hukum Islam,” UIN Kiai Haji Achmad Siddiq Jember, 2024.
- [9] M. S. Alif and A. R. Pratama, “Analisis Kesadaran Keamanan di Kalangan Pengguna E-Wallet Di Indonesia,” 2014.
- [10] B. C. Utomo and A. A. Rahman, “Analisis Kesadaran Keamanan Data Pribadi pada Pengguna E-Wallet DANA,” *JRST*, vol. 8, no. 2, pp. 155–166, 2024, doi: [10.30595/jrst.v8i2.21162](https://doi.org/10.30595/jrst.v8i2.21162).
- [11] S. Zuhri, “Fiqih Ekonomi Digital: Transaksi Online dalam Perspektif Syariah,” *EL MAKRIFAH*.
- [12] A. Rahmi, H. Bisri, A. Y. Rusyana, and H. Raharjo, “Penerapan Kaidah Muamalah dalam Transaksi Ekonomi Digital : Tinjauan Pustaka pada Paylater , E-Wallet , dan Marketplace,” *SALAM*, vol. 6, no. 2, pp. 347–365, 2025.
- [13] Z. Kamila and R. Efendi, “Perlindungan Hukum Atas Kehilangan Saldo Pengguna E-Wallet Dana di Tinjau Dari Fatwa DSN MUI No . 16 / Dsn Mui / Ix / 2017 Tentang Uang Elektronik Syariah (Studi Kasus Pengguna E-Wallet Dana di Kecamatan Medan Tembung , Kota Medan),” *UNES LAW Rev.*, vol. 6, no. 2, pp. 7185–7193, 2024, doi: <https://doi.org/10.31933/unesrev.v6i2>.
- [14] A. R. N. Isnaini and dkk, *RECHT: Journal of Legal Studies*, vol. 1, no. 1. LPKH FH Usakti, 2026.
- [15] A. A. Sholeh, M. Hasanah, and S. K. Nur, “Pengaruh Kemudahan dan Keamanan Terhadap Minat Penggunaan Pembayaran Non Tunai Quick Reaponse Code Indonesian Standard (QRIS) dalam perspektif Maqashid Syariah,” *IQTISHOD*, vol. 4, no. 2, pp. 164–181, 2025.
- [16] R. C. Anggara, Nurwahidin, and M. I. Muttaqin, “Perilaku Konsumen Generasi Z dalam Penggunaan E-Wallet: Perspektif Maqashid Syariah,” *KARTIKA*, vol. 5, no. 3, pp. 1855–1873, 2025.
- [17] Z. Fanani, B. Arifin, and F. A. E. Mohamed, *Monetisasi Data , Sentralisasi QRIS , dan Tantangan Integrasi Nilai Syariah dalam Sistem Pembayaran Digital Indonesia*, vol. 5, no. 1. 2025. doi: [10.30762/al-muhasib.v5i1.2388](https://doi.org/10.30762/al-muhasib.v5i1.2388).
- [18] S. Sunarsa and I. N. Fauzi, “Tinjauan Hukum Islam Tentang Mekanisme Transaksi E-Wallet,” *JHESY*, vol. 2, no. 1, pp. 1–14, 2023, doi: [10.37968/jhesy.v2i1.506](https://doi.org/10.37968/jhesy.v2i1.506).
- [19] M. F. Fauzadeli and R. Apriani, “Perlindungan Hukum Terhadap Nasabah E-Wallet Atas Kebocoran Data dan Kehilangan Sejumlah Dana,” *Ilm. Ilmu Huk. QISTIE*, vol. 15, no. 2, pp. 224–238, 2022.
- [20] H. Suhendar and M. Ulum, “Perlindungan Data Pribadi Penyelenggaraan Fintech Lending Syariah : Analisis Teori Sistem Maqosid Syariah Jasser Auda,” *el hisbah*, vol. 3, no. 1, pp. 1–16, 2023.