KAMPUS AKADEMIK PUBLISING
Jurnal Multidisiplin Ilmu Akademik
Vol.2, No.6 Desember 2025
e-ISSN: 3032-7377; p-ISSN: 3032-7385, Hal 951-958
DOI : https://doi.org/10.61722/jmia.v2i6.7379

PERLINDUNGAN HUKUM BAGI KONSUMEN TERHADAP PENYALAHGUNAAN DATA PRIBADI DALAM TRAKSAKSI ONLINE

Daffa Satya Pratiwi
Fakultas Hukum dan Ilmu Politik, Universitas Muhammadiyah Surakarta
Astin Putri Lestariyani
Fakultas Hukum dan Ilmu Politik, Universitas Muhammadiyah Surakarta
Yasmin Safinatunnajah
Fakultas Hukum dan Ilmu Politik, Universitas Muhammadiyah Surakarta
Elvia Ghina Nismara
Fakultas Hukum dan Ilmu Politik, Universitas Muhammadiyah Surakarta
Alamat: Jl. A. Yani, Mendungan, Pabelan, Kec. Kartasura, Kabupaten Sukoharjo, Jawa Tengah 57169
Korespondensi penulis: c100230229@student.ums.ac.id, c100230376@student.ums.ac.id, c100230031@student.ums.ac.id, c100230011@student.ums.ac.id

Abstrak. *This research increases the risk of use of consumers personal data by businesses. The purpose of this research is to analyze the legal protectionprovided to consumers regarding the use of personal data in online transaction, especially whitin the framework of Indonesian law. The research method used is normative juridical research, which includes the study of Law Number 11 of 2008 on Information and Eletronic Transaction (ITE Law), Law Number 27 of 2022 on Personal Data Protection (PDP Law), as well as comparisons with international regulation such as GDPR. The research result show that although the PDP Law provides a strong basis for perotecting personal data, the implementation of the Law still faces various challenges, such as law consumer awareness, limitations in law enforcement, and imperfections in the compensation mechanism. The research also suggests strengthening regulations, increasing consumer awareness, and the active role of supervisory authorities to prevent unauthorized use of personal data, thereby increasing consumer trust in online transactions. The research conclution emphasizes the inportance of aligning national law with international standards to create more effective legal protection for consumers.*
Keywords: *consumer protection, personal data, online transactions*

Abstrak. Penelitian ini meningkatkan resiko penggunaan data pribadi konsumen oleh pihak usaha.Tujuan dari penelitian ini adalah menganalisis perlindungan hukum yang diberikan kepada konsumen terkait penggunaan data pribadi dalam transaksi online, terutama dalam rangka hukum Indonesia.Metode penelitian yang digunakan adalah penelitian yuridis normatif, yang mencakup pengkajian Undang-Undang Nomor 11 Tahun 2008 tentang informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), serta perbandingan dengan regulasi internasional seperti GDPR. Hasil penelitian menunjukan bahwa meskipun UU PDP menyediakan dasar yang kuat untuk melindungi data pribadi, penerapan Undang-Undang tersebut masih menghadapi berbagai tantangan, seperti rendahnya kesadaran konsumen, keterbatasan dalam penerapan hukum, dan ketidaksempurnaan mekanisme pengganti pengganti kerugian.Penelitian juga menyarankan perkuatan regulasi, peningkatan kesadaran konsumen, serta peran aktif ototritas pengawas untuk mencegah penggunaan data pribadi yang tidak sah, sehingga meningkatkan kepercayaan konsumen terhadap traksaksi online.Kesimpulan penelitian menegaskan pentingnya penyelarasan hukum nasional dengan standar internasional untuk menciptakan perlindungan hukum yang lebih efektif bagi konsumen.
Kata Kunci: *Perlindungan konsumen, data pribadi, transaksi online*

PENDAHULUAN

Pesatnya perkembangan teknologi informasi dan kominikasi telah mengubah lanskap perdagangan secara fundamaental, memicu lonjakan masif dalam transaksi *online*

Received Oktober 28, 2025; Revised November 30, 2025;Desember 05, 2025
* Daffa Satya Pratiwi, c100230229@student.ums.ac.id

atau *e-commers.* Fenomena ini memberikan kemudahan dan efisiensi yang luar biasa bagi konsumen dalam mengakses berbagai produk dan layanan. Namun, di balik kemudahan tersebut, terdapat risiko yang semakin kompleks, terutama terkait pertukaran informasi pribadi. Dalam setiap interaksi digital mulai dari pendaftaran akun, pembelian produk, hingga penggunaan layanan. Konsumen secara tidak terhindarkan menyertakan sejumlah besar data pribadinya kepada pihak penyelenggara sistem elektronik. Ketergantungan pada platform digital ini menjadikan data pribadi sebagai aset yang sangat berharga sekaligus rentan, sehingga menjadi target utama bagi pihak yang tidak bertanggung jawab.

Munculnya ancaman berupa kebocoran data, pencurian identitas, dan pemanfaatan data konsumen tanpa izin untuk berbagai tujuan seperti pemasaran agresif maupun penipuan (phishing) semakin sring terjadi dan menjadi perhatian publik. Kondisi ini tidak hanya menimbulkan kerugian materiil bagi konsumen, tetapi juga dampak non-materiil seperti pelanggaran rpivasi dan berpotensi diskriminasi. Reisiko-risiko ini menciptakan celah kerentanan yang memerlukan perhatian lebih dalam menjaga keamanan data pribadi dalam ekosistem digital yang sangat dinamis dan berisiko tinggi.

Dalam menghadapi konsumen risiko digital tersebut, perlindungan hukum bagi konsumen menjadi pilar esensial untuk menjaga kepercayaaan publik terhadap sistem perdagangan elektronik. Tanpa jaminan perlindungan yang memadai, konsumen berpotensi ragu untuk berpartisipasi dalam transaksi online, yang dapat menghambat ekonomi digital nasional. Meskipun indonesia telah mengeluarkan berbagai regulasi sektoral terkait perlindungan data pribadi, seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang mengatur hak subjek data dan kewajiban pengendalian dta, implementasi dan integrasi regulasi tersebut dalam konteks transaksi online masih menghadapi tantangan. Kekosongan dan ketidak jelasan norma hukum spesifik membuat penegakan hukum dan pemulihan hak konsumen menjadi sulit.

Berangkat dari latar belakang tersebut, jurnal ini bertujuan untuk menganalisis perlindungan hukum yang tersedia bagi konsumen terhadap penyalahgunaan data pribadi dalam transaksi online, terutama pasca pemberlakuan Undang-Undangan Perlindungan Data Pribadi terbaru. Penelitian ini akan menilai efektivitaas regulasi yang ada, menyoroti kendala dalam implementasi serta penegakan hukum, dan mengkaji pertanggungjawaban hukum penyelenggara sistem elektonik. Dengan demikian, diharapkan hasil penelitian dapat memberikan rekomendasi strategis untuk memperkuat kerangka hukum yang adaptif dan komprehensif demi menjamin hak konstitusional konsumen atas perlindungan atas pribadi di ranah digital.

KAJIAN TEORI

A. Teori Perlindungan konsumen

Teori Perkembangan Konsumen dikembangkan oleh para ahli seperti Philip Kotler dan Gary Armstrong, yang menekankan bahwa konsumen memiliki hak untuk mendapat produk dan layanan yang aman, jujur, dan transparan.Dalam konteks transaksi online, teori ini diperluas oleh Undang-Undang Perlindungan Konsumen

yang mengakui konsumen sebagai pihak yang lemah dalam hubungan dengan pelaku usaha.Penyalahgunaan data pribadi dapat dianggap sebagai pelanggaran hak konsumen atas privasi dan keamanan, sebagaimana dijelaskan dalam teori "Consumer Sovereignty" oleh Adam Smith, dimana konsumen harus memiliki kendali penuh atas informasi pribadi mereka.Teori ini menjadi dasar untuk menganalisis bagaimana hukum Indonesia, seperti UU PDP, bertujuan melindungi konsumen dari eksploitasi data oleh platfrom digital.

B. Teori Privasi Data dan Hak asasi Manusia

Teori privasi data berakar dari hak asasi manusia, Hak atas privasi sebagaimana tercantum dalam pasal 17 Deklarasi Universal Hak Asasi Manusia (DUHAM) PBB. Ahli seperti Warren dan Brandeis dalam artikel " The Right to Privacy" (1890) mendefinisikan privasi sebagai hak individu untuk dibiarkan sendiri, yang meliputi konytrol atas data pribadi. Dalam era digital, Teori ini berkembang menjadi "Data Protection Theory" oleh Viktor Mayer-Schonberger, yang menekankan perlunya regulasi untuk mencegah penyalahgunaan data oleh entitas komersil. Penyalahgunaan data pribadi dalam transaks online dapat mengancam hak-hak fundamental seperti kebebasan berekspresi dan keamaan pribadi, sehingga teori ini mendukung argumentasi bahwa UU PDP di Indonesia harus diimplementasikan secara ketat antara inovasi teknologi, dan perlindungan individu.

C. Teori Transaksi Elektronik dan Resiko Digital

Berakar dari hak asasi manusia, khususnya Hak atas Privasi sebagaimana tercantum dalam Pasal 17 Deklarasi Universal Hak asasi Manusia,(DUHAM) PBB. Ahli seperti Warren dan Brandies dalam artikel "The Right to Privacy" (1890) mendefinisikan privasi sebagai hak individu untuk dibiarkan sendiri, yang meliputi kontrol atas data pribadi. Dalam era digital, teori ini berkembang menjadi "Data Protection Theory" oleh Victor Mayer Schonberger, yang menekankan perlunya regulasi untuk penyalahgunaan data oleh entitas komensil. Penyalahgunaan data pribadi dalam transaksi online dapat mengancam hak fundamental, seperti kebabasan berekspresi dan keamanan pribadi, sehingga teori ini mendukung argumentasi bahwa UU PDP di Indonesia harus diimplementasikan secara ketat untuk menjaga keseimbangan antara inovasi teknologi dan perlindungan individu.

D. Teori Transaaksi Elektronik dan Digital

Teori transaksi elektronik dikembangkan oleh Cristopher Milliard dan Lan walden, yang menggambarkan transaksi online sebagai bentuk kontrak digital yang rentan terhadap resiko seperti cybercrime dan kebocoran data. Dalam teori "Risk Society" oleh Ulrich Beck, masyarakat modern menghadapi resiko global yang tidak terlihat, termasuk penyalahgunaan data pribadi yang dapat menyebabkan kerugian sistematik. Teori ini relevan dengan fenoma transaksi online di Indonesia, di mana peningkatan penggunaan e-commerce meningkatkan resiko eksploitasi data oleh pihak usaha.

METODE PENELITIAN

Makalah ini disusun menggunakan metode penelitian kepustakaan (*library research*) berbasis pendekatan normatif, dengan menelaah klasik dan kontemporer yang relevan, di antaranya kitab-kitab fiqih jinayah, buku-buku hukum, peraturan perundang undangan indonesia (KUHP dan undang udang terkait), serta artikel-artikel jurnal nasional dan internasional. Data dianalisis secara deskriptif-analitis kasus nyata dengam menghubungkan peraturan perundang-undangan di Indonesia

HASIL PENELITIAN DAN PEMBAHASAN

1. Bentuk Perlindungan Hukum terhadap Penyalahgunaan Data Pribadi dalam Transaksi Online di Indonesia.

Perlindungan hukum bagi data pribadi konsumen dalam transaksi online di Indonesia kini menjadi fokus utama, terutama setelah disahkannya Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). UU PDP mengakui hak individu yang menjadi subjek data (dalam hal ini konsumen) untuk mendapatkan perlindungan terhadap data pribadi yang dikelola oleh penyelenggara sistem elektronik, seperti situs e-commerce dan penyedia layanan digital. Perlindungan ini mencakup kewajiban bagi pengelola data untuk mengumpulkan, menyimpan, menggunakan, dan mengungkapkan data pribadi dengan cara yang sah dan adil, sesuai dengan tujuan yang telah disepakati oleh konsumen.

Undang-Undang Perlindungan Data Pribadi (UU PDP) menekankan bahwa pengolahan data pribadi hanya dapat dilakukan jika ada persetujuan yang tegas dan untuk tujuan yang sah. Selain UU PDP, terdapat peraturan pendukung seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) nomor 19 tahun 2016 serta Peraturan Pemerintah Nomor 80 tahun 2019 yang mengatur perdagangan lewat sistem elektronik, yang juga memuat ketentuan penting mengenai perlindungan data di dunia digital. Secara prinsip, pelaku bisnis diwajibkan untuk mengimplementasikan langkah-langkah keamanan baik secara teknis maupun administratif, seperti enkripsi data serta pemantauan akses, guna mencegah kebocoran dan penyalahgunaan data. Namun, kenyataan di lapangan menunjukkan masih banyak kendala dalam penerapan peraturan ini.

Implementasi Undang-Undang Perlindungan Data Pribadi menghadapi berbagai masalah teknis, peraturan, dan aspek budaya organisasi yang dapat memengaruhi sejauh mana perlindungan data dapat dilakukan. Dari segi teknis, organisasi perlu menyesuaikan infrastruktur teknologi informasi serta sistem aplikasi yang mereka miliki untuk mematuhi standar keamanan tertentu seperti enkripsi data, penerapan kontrol akses yang ketat, dan persetujuan eksplisit dari pengguna. Tantangan lain adalah pemetaan jenis dan sumber data pribadi yang mereka kelola, mengingat data tersebut tersebar di berbagai sistem dan aplikasi. Dari sudut pandang regulasi, Undang-Undang Perlindungan Data Pribadi memiliki berbagai lapisan kompleks yang membutuhkan pemahaman yang mendalam serta interpretasi yang akurat agar dapat diterapkan dengan konsisten. Pentingnya pembuatan pedoman operasional yang jelas dan pelatihan untuk sumber daya manusia sangatlah vital untuk memastikan bahwa kepatuhan dapat berjalan dengan baik. Di samping itu, perlu ada penguatan harmonisasi Undang-Undang Perlindungan Data Pribadi dengan peraturan lainnya, seperti Undang-Undang Informasi dan Transaksi Elektronik serta regulasi di bidang perdagangan elektronik, untuk menciptakan kerangka hukum yang koheren dan tidak saling bertabrakan.

Tantangan lainnya muncul dari faktor budaya di dalam organisasi, di mana perubahan pola pikir dan budaya terkait privasi dalam organisasi tidaklah mudah untuk diterapkan. Penolakan

terhadap perubahan dari pihak-pihak yang sudah terbiasa dengan prosedur dan sistem yang lama menghalangi pelaksanaan optimal dari UU PDP. Oleh karena itu, perlu adanya manajemen perubahan yang efektif, disertai dengan komunikasi yang terbuka serta keterlibatan aktif semua pemangku kepentingan agar transformasi budaya privasi dapat berjalan dengan baik. Kesadaran serta pemahaman publik tentang pentingnya perlindungan data pribadi juga belum memadai, sehingga diperlukan peran aktif pemerintah dan organisasi untuk terus meningkatkan pemahaman dan kepatuhan melalui pendidikan dan sosialisasi. Dengan memperhatikan tantangan tersebut, perlindungan hukum terhadap data pribadi tidak hanya berfokus pada regulasi yang tertulis, tetapi juga membutuhkan pengelolaan risiko yang cermat, koordinasi lintas disiplin, dan kolaborasi yang kuat antara pemerintah, pelaku bisnis, dan masyarakat untuk mencapai perlindungan data pribadi yang efektif dan berkelanjutan.

Pada bulan Mei 2020, Tokopedia mengalami insiden kebocoran data yang sangat besar, melibatkan lebih dari 91 juta akun pengguna. Informasi yang bocor mencakup nama lengkap, alamat email, nomor ponsel, tanggal lahir, dan juga password yang, meskipun sudah dienkripsi, tetap menimbulkan ancaman serius bila sampai ke tangan yang salah. Kasus ini menunjukkan bahwa hanya mengandalkan regulasi tidak cukup tanpa adanya penerapan keamanan teknologi dan kebijakan internal yang ketat. Dalam hal tanggung jawab perlindungan data, perusahaan tidak hanya diharuskan melindungi data saat pengumpulan, tetapi juga selama seluruh siklus hidup data, termasuk setelah transaksi selesai. Kurangnya persiapan dan lemahnya kontrol internal sering menjadi penyebab utama terjadinya kebocoran. Kasus Tokopedia ini juga mendorong regulator dan perusahaan lain untuk meningkatkan standar keamanan informasi, dengan menerapkan standar internasional seperti ISO/IEC 27001 demi memperbaiki sistem keamanan data. Dari sisi hukum, perusahaan yang tidak mampu melindungi data pribadi dapat dikenakan sanksi administratif berupa denda, pembatasan kegiatan, bahkan sanksi pidana sesuai dengan UU PDP dan UU ITE. Namun, efektivitas penegakan hukum masih perlu ditingkatkan melalui penguatan kapasitas lembaga pengawas dan penegak hukum agar mereka dapat mengatasi pelanggaran secara sistematis.

2. Konsumen Upaya Pemerintah dan Masyarakat untuk Meningkatkan Kesadaran Hukum dan Mencegah Penyalahgunaan Data Pribadi dalam Transaksi Online.

Pemerintah Indonesia, melalui berbagai institusi seperti Kementerian Komunikasi dan Informatika (Kominfo) serta Otoritas Jasa Keuangan (OJK), telah menjalankan berbagai program untuk meningkatkan pemahaman mengenai hukum terkait perlindungan data pribadi dan meminimalkan kemungkinan penyalahgunaan data dalam transaksi online. Salah satu langkah krusial adalah pelaksanaan program literasi digital di seluruh negeri yang bertujuan untuk mengedukasi masyarakat, terutama konsumen dan pelaku UMKM, mengenai pentingnya menjaga keamanan data pribadi serta memahami hak-hak mereka sebagai konsumen di dunia digital. Edukasi ini meliputi pengetahuan mengenai cara melindungi data, cara mendeteksi penipuan digital, serta prosedur untuk melaporkan pelanggaran. Di samping itu, pemerintah juga menetapkan kewajiban bagi penyelenggara sistem elektronik (PSE) untuk menerapkan sistem keamanan yang berlapis, melakukan enkripsi data, dan menetapkan prosedur audit secara berkala. PSE yang tidak memenuhi kewajiban ini dapat dikenakan berbagai sanksi administratif, termasuk denda hingga penghentian layanan secara permanen. Penerapan regulasi ini dimaksudkan untuk memberikan efek jera dan mendorong industri digital untuk memperbaiki standar keamanan data pribadi.

Masyarakat pun terlibat secara aktif dalam pengawasan sosial serta melaporkan pelanggaran data pribadi kepada pihak berwenang atau lembaga perlindungan konsumen. Salah satu contohnya adalah laporan masif yang membantu Kominfo untuk menindak aplikasi atau platform yang tidak menjaga data dengan baik melalui pemeriksaan dan langkah hukum. Penguatan kolaborasi antara pemerintah, sektor swasta, dan organisasi masyarakat sipil sangat penting, misalnya melalui sertifikasi keamanan data oleh lembaga independen, pelatihan tentang keamanan siber untuk UMKM, serta kampanye publik yang luas mengenai hak dan kewajiban pengguna data. Namun, masih ada tantangan besar yang harus dihadapi, seperti kurangnya akses informasi, kekurangan sumber daya manusia yang terampil dalam keamanan data, dan perubahan yang cepat dalam pola kejahatan siber yang membutuhkan penyesuaian regulasi secara cepat.

Sebagai ilustrasi, setelah terjadinya kebocoran data di Tokopedia, pihak Kominfo segera melakukan audit keamanan dan mendorong semua platform digital untuk segera memperbaiki aspek keamanan serta transparansi dalam pengelolaan data. Di pihak masyarakat, semakin banyak konsumen dan komunitas digital yang aktif melaporkan dugaan pelanggaran melalui saluran pengaduan resmi, sehingga hal ini memberikan tekanan tambahan kepada pelaku usaha untuk mematuhi standar perlindungan data yang lebih ketat. Kampanye peningkatan kesadaran akan keamanan data melalui media sosial dan kerjasama dengan organisasi konsumen membantu memperkuat budaya perlindungan data pribadi di tingkat masyarakat. Selain itu, pemerintah dan sektor swasta semakin aktif mendorong penerapan sertifikasi keamanan data dan pembentukan tim tanggap insiden keamanan siber (CSIRT) agar respons terhadap kebocoran data dapat dilakukan dengan lebih cepat. Sebagai contoh, Bukalapak juga mengalami insiden kebocoran data pada tahun 2020, di mana hampir 13 juta data pengguna terungkap, sehingga mempercepat upaya untuk memperkuat pengamanan dan pengawasan. Bersama masyarakat, pemerintah berusaha menciptakan ekosistem digital yang aman secara hukum, teknologi, dan sosial, di mana konsumen memiliki pemahaman dan kekuatan untuk mengelola data pribadi mereka serta mendapatkan perlindungan hukum yang efektif saat terjadi pelanggaran.

KESIMPULAN

Perlindungan hukum untuk penyalahgunaan data pribadi dalam transaksi online di Indonesia telah mengalami perkembangan yang signifikan berkat adanya Undang-Undang Nomor 27 Tahun 2022 mengenai Perlindungan Data Pribadi (UU PDP), yang memberikan landasan hukum yang kuat untuk menjaga hak privasi konsumen. Peraturan ini menetapkan tanggung jawab yang jelas bagi penyelenggara sistem elektronik dalam pengelolaan data pribadi secara aman dan sesuai dengan izin dari konsumen, juga ditunjang oleh UU ITE serta aturan perdagangan elektronik yang relevan. Meski demikian, penerapan perlindungan data pribadi masih dihadapkan pada berbagai tantangan teknis, regulasi, dan budaya organisasi yang harus ditangani secara terintegrasi agar perlindungan dapat berlangsung dengan efektif.

Pemerintah aktif mengambil langkah-langkah melalui program peningkatan literasi digital, pengawasan yang ketat, dan penegakan hukuman bagi yang melanggar, sedangkan masyarakat mulai menunjukkan peran yang lebih signifikan dalam mengawasi dan melaporkan pelanggaran terhadap perlindungan data. Kasus kebocoran data besar seperti yang terjadi di Tokopedia dan Bukalapak mengingatkan kita akan pentingnya memiliki sistem keamanan yang handal serta transparansi dari pelaku usaha kepada konsumen. Kerjasama antara semua pihak dalam membangun ekosistem digital yang aman dan bertanggung jawab menjadi kunci utama dalam keberhasilan perlindungan data pribadi di Indonesia. Dan adapun sarannya yaitu:

1. Pemerintah perlu meningkatkan penyuluhan dan pendidikan mengenai perlindungan data pribadi untuk memastikan pemahaman masyarakat lebih merata.
2. Pengawasan dan penegakan hukum terhadap pelanggar Undang-Undang Perlindungan Data Pribadi harus diperkuat agar memberikan efek jera.
3. Pelaku usaha diwajibkan untuk mengadopsi standar keamanan data internasional seperti ISO/IEC 27001 demi menjaga data konsumen secara maksimal.
4. Organisasi perlu membangun budaya privasi melalui pelatihan dan manajemen risiko yang berkelanjutan.
5. Masyarakat didorong untuk memiliki tingkat literasi digital yang baik agar dapat melindungi data pribadi dan aktif melaporkan pelanggaran.
6. Kerja sama antara pemerintah, pelaku bisnis, dan masyarakat harus terus ditingkatkan dalam menciptakan ekosistem digital yang aman dan dapat dipercaya.

DAFTAR PUSTAKA

Jurnal.

Andini, N. (2025). *Perlindungan Data Pribadi Di Indonesia Berdasarkan Undang-Undang Nomor 27 Tahun 2022*. Jurnal Analisis Hukum, 6(1).

Dwiki, D.K.P. (2022). *Perlindungan Data Pribadi Konsumen Sebagai Pengguna Layanan E-Commerce (Kasus Kebocoran Data Tokopedia)*.

Priliasari, E. (2023). *Perlindungan Data Pribadi Konsumen dalam Transaksi E-Commerce*. Jurnal Rechtsvinding.

Rosadi, S.D., & Pratama, G.G. (Tahun tidak disebutkan). *Perlindungan Privasi Dan Data Pribadi Dalam Era Ekonomi Digital Di Indonesia*. Jurnal Veritas et Justitia.

Setiawan, H., Ghufron, M., & Mochtar, D.A. (2020). *Perlindungan Hukum Terhadap Data Pribadi Konsumen Dalam Transaksi e-Commerce*. MLJ Merdeka Law Journal, 1(2).

Setyawan, A., & Wijaya, B. (2018). *Perlindungan Konsumen dalam Transaksi E-Commerce Ditinjau dari Undang-Undang Perlindungan Konsumen*. Journal of Judicial Review, 19(2).

Suari, K.R., & Sarjana, I.M. (2024). *Menjaga Privasi Di Era Digital: Perlindungan Data Pribadi Di Indonesia*. Jurnal Analisis Hukum, 6(1).

VioIina, D., & Zahrani, H.T. (2020). *Perlindungan Data Pribadi Bagi Nasabah Korban Pembobolan Rekening Melalui Internet Banking*. Jurnal Kepastian Hukum Dan Keadilan, 2(1).

Warren, S.D. & Brandeis, L.D. (1890). *The Right to Privacy*. Harvard Law Review, 4(5), 193–220.

Watkat, F.X. (2024). *Perlindungan Data Pribadi Melalui Penerapan Sistem Hukum Pidana*. Jurnal Ilmiah Hukum dan Kebijakan.

Buku.

Aswandi, R., Muchsin, P.R.N., & Sultan, M. (2020). *Perlindungan Data Informasi Pribadi Melalui Indonesia Data Protection System (IDPS)*.

Beck, U. (1992). *Risk Society: Towards a New Modernity*. Sage Publications.

Kotler, P. & Armstrong, G. (2018). *Principles of Marketing*. Pearson.

Mayer-Schönberger, V. (2009). *Data Protection Law: Approaches and Principles*. Oxford University Press.

Milliard, C. & Walden, I. (2008). *Electronic Commerce and the Law*. Sweet & Maxwell.

Peraturan Perundang-undangan.

Deklarasi Universal Hak Asasi Manusia (DUHAM) PBB, Pasal 17.

General Data Protection Regulation (GDPR) Uni Eropa.

ISO/IEC 27001:2013 – *Information Security Management Systems*.

Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP).