

Perlindungan Hukum Perdata Terhadap Korban Kebocoran Data Pribadi Dalam Transaksi Digital Pasca Berlakunya Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi

Limrogate Immanuel¹, Mhd. Raihan Rizqullah², Sabda Abdillah Lubis³

¹ Program Studi Hukum, Universitas Nusa Cendana

^{2,3} Program Studi Hukum, Universitas Deztron Indonesia

e-mail: limrogate.immanuel@staf.undana.ac.id

Abstrak

Perkembangan teknologi informasi dan komunikasi telah mendorong transformasi berbagai aktivitas masyarakat ke dalam ruang digital, termasuk kegiatan perdagangan elektronik, layanan keuangan digital, transportasi daring, pelayanan kesehatan elektronik, serta berbagai bentuk transaksi berbasis internet lainnya. Kemudahan yang ditawarkan oleh ekosistem digital tersebut di sisi lain menimbulkan risiko baru berupa meningkatnya ancaman terhadap keamanan data pribadi pengguna. Dalam beberapa tahun terakhir, Indonesia menghadapi berbagai kasus kebocoran data pribadi yang melibatkan instansi pemerintah maupun sektor swasta, sehingga menimbulkan kerugian materiil dan immateriil bagi masyarakat sebagai subjek data. Kehadiran Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi merupakan langkah strategis pemerintah dalam membangun sistem perlindungan data yang komprehensif dan memberikan kepastian hukum bagi masyarakat. Penelitian ini bertujuan untuk menganalisis bentuk perlindungan hukum perdata terhadap korban kebocoran data pribadi dalam transaksi digital pasca berlakunya Undang-Undang Pelindungan Data Pribadi serta mengkaji efektivitas mekanisme pertanggungjawaban perdata yang dapat ditempuh oleh korban. Penelitian menggunakan metode normatif-empiris dengan pendekatan perundang-undangan, pendekatan konseptual, dan pendekatan kasus. Data diperoleh melalui studi kepustakaan terhadap berbagai peraturan perundang-undangan, jurnal ilmiah, putusan pengadilan, serta data empiris mengenai kasus kebocoran data pribadi di Indonesia. Hasil penelitian menunjukkan bahwa Undang-Undang Pelindungan Data Pribadi telah memberikan dasar hukum yang lebih kuat bagi korban untuk menuntut ganti rugi melalui mekanisme hukum perdata. Namun demikian, implementasinya masih menghadapi berbagai kendala berupa rendahnya literasi hukum masyarakat, belum optimalnya pengawasan, kesulitan pembuktian kerugian, serta belum terbentuknya praktik peradilan yang konsisten terkait sengketa kebocoran data pribadi. Oleh karena itu diperlukan penguatan regulasi pelaksana, peningkatan kapasitas lembaga pengawas, serta penyederhanaan mekanisme gugatan bagi korban agar perlindungan hukum yang diberikan dapat berjalan secara efektif dan berkeadilan.

Kata Kunci: Perlindungan Hukum Perdata, Data Pribadi, Transaksi Digital, Kebocoran Data, Undang-Undang Pelindungan Data Pribadi.

Abstract

The rapid advancement of information and communication technology has transformed various aspects of human activities into digital platforms, including electronic commerce, digital financial services, online transportation, electronic healthcare services, and other internet-based transactions. While digital ecosystems provide efficiency and convenience, they also generate significant risks related to personal data security. In recent years, Indonesia has experienced numerous personal data breaches involving both public institutions and private corporations, resulting in material and immaterial losses for data subjects. The enactment of Law Number 27 of 2022 concerning Personal Data Protection represents a strategic effort by the Indonesian government to establish a comprehensive data protection framework and

provide legal certainty for citizens. This study aims to analyze the forms of civil legal protection available to victims of personal data breaches in digital transactions following the implementation of the Personal Data Protection Law and to examine the effectiveness of civil liability mechanisms available to affected individuals. The research employs a normative-empirical legal method using statutory, conceptual, and case approaches. Data were collected through literature reviews of legislation, scientific journals, judicial decisions, and empirical information related to personal data breach incidents in Indonesia. The findings indicate that the Personal Data Protection Law provides a stronger legal basis for victims to seek compensation through civil litigation. Nevertheless, several challenges remain, including limited public legal awareness, inadequate supervision mechanisms, difficulties in proving damages, and the absence of consistent judicial practices concerning personal data disputes. The study concludes that strengthening implementing regulations, enhancing supervisory institutions, and simplifying legal procedures for victims are essential to ensure effective and equitable civil legal protection in the digital era. Furthermore, the establishment of a more responsive legal framework is necessary to address the growing complexity of personal data breaches and to maintain public trust in digital transactions.

Keywords: Civil Legal Protection, Personal Data, Digital Transactions, Data Breach, Personal Data Protection Law.

LATAR BELAKANG

Transformasi digital telah menjadi salah satu fenomena global yang mengubah hampir seluruh aspek kehidupan masyarakat modern. Perkembangan teknologi informasi dan komunikasi memungkinkan berbagai aktivitas ekonomi, sosial, pendidikan, kesehatan, dan pemerintahan dilakukan secara elektronik melalui jaringan internet. Kemajuan tersebut memberikan manfaat berupa efisiensi, kemudahan akses, dan percepatan pelayanan publik, namun di sisi lain juga menimbulkan tantangan baru berupa meningkatnya risiko penyalahgunaan dan kebocoran data pribadi pengguna sistem elektronik (World Bank, 2024; Alhazmi, Imran, & Alsheikh, 2024). Perlindungan data pribadi saat ini tidak lagi dipandang sebagai isu teknis semata, melainkan telah berkembang menjadi bagian penting dari perlindungan hak asasi manusia dan kepastian hukum dalam masyarakat digital.

Pada tingkat global, pertumbuhan ekonomi digital berlangsung secara signifikan seiring meningkatnya penggunaan internet dan teknologi berbasis data. United Nations Conference on Trade and Development menjelaskan bahwa data telah menjadi sumber daya ekonomi baru yang memiliki nilai strategis bagi perusahaan, pemerintah, dan masyarakat. Pengumpulan, penyimpanan, analisis, dan pemanfaatan data pribadi menjadi fondasi utama berbagai layanan digital seperti perdagangan elektronik, perbankan digital, teknologi finansial, media sosial, layanan kesehatan elektronik, serta komputasi awan. Kondisi tersebut menyebabkan data pribadi menjadi aset bernilai tinggi sekaligus sasaran berbagai bentuk kejahatan siber (UNCTAD, 2024).

Perkembangan ekonomi digital yang semakin pesat di berbagai negara diikuti oleh peningkatan jumlah insiden kebocoran data pribadi. Menurut Alhazmi, Imran, dan Alsheikh (2024), pelanggaran privasi digital dapat menimbulkan dampak luas terhadap individu maupun masyarakat karena data pribadi yang bocor berpotensi digunakan untuk pencurian identitas, penipuan elektronik, manipulasi informasi, serta berbagai bentuk kejahatan siber lainnya. Oleh karena itu, negara-negara di dunia mulai mengembangkan rezim hukum perlindungan data pribadi yang lebih komprehensif guna menjamin hak privasi warga negara.

Uni Eropa merupakan salah satu kawasan yang dianggap berhasil mengembangkan sistem perlindungan data pribadi melalui General Data Protection Regulation yang mulai berlaku pada tahun 2018. Regulasi tersebut memberikan hak yang luas kepada subjek data, termasuk hak untuk memperoleh informasi, hak mengakses data, hak memperbaiki data, hak menghapus data, dan hak memperoleh ganti rugi atas pelanggaran yang dilakukan oleh pengendali data. Keberhasilan General Data Protection Regulation kemudian menjadi rujukan

bagi berbagai negara dalam membangun sistem perlindungan data pribadi nasional (Jurcys, Compagnucci, & Fenwick, 2024).

Dalam perspektif hukum modern, perlindungan data pribadi merupakan bagian dari perlindungan hak privasi yang dijamin sebagai hak fundamental manusia. De Souza, Abe, Lima, dan Souza (2020) menjelaskan bahwa perkembangan teknologi digital telah mengubah karakteristik perlindungan privasi sehingga diperlukan instrumen hukum yang mampu menjamin keamanan, kerahasiaan, dan pengendalian data oleh pemilik data. Dengan demikian, perlindungan data pribadi tidak hanya berkaitan dengan keamanan informasi, tetapi juga berkaitan dengan penghormatan terhadap martabat manusia dan kebebasan individu.

Indonesia merupakan salah satu negara dengan perkembangan ekonomi digital terbesar di kawasan Asia Tenggara. Pertumbuhan transaksi elektronik, penggunaan dompet digital, layanan teknologi finansial, perdagangan elektronik, serta penggunaan media sosial yang sangat tinggi menyebabkan volume data pribadi yang diproses oleh penyelenggara sistem elektronik terus meningkat setiap tahun. Kondisi ini menciptakan peluang ekonomi yang besar sekaligus meningkatkan potensi terjadinya pelanggaran terhadap keamanan data pribadi masyarakat.

Pertumbuhan aktivitas digital di Indonesia belum sepenuhnya diimbangi oleh tingkat keamanan data yang memadai. Berbagai kasus kebocoran data yang terjadi dalam beberapa tahun terakhir menunjukkan bahwa data pribadi masyarakat masih rentan terhadap akses ilegal, pencurian, maupun penyalahgunaan oleh pihak yang tidak berwenang. Fenomena tersebut menimbulkan kerugian yang tidak hanya bersifat ekonomi, tetapi juga berdampak terhadap hak privasi, rasa aman, dan kepercayaan masyarakat terhadap ekosistem digital nasional (Simanjuntak, 2024).

Persoalan perlindungan data pribadi di Indonesia semakin memperoleh perhatian setelah terjadinya berbagai kasus kebocoran data yang melibatkan sektor publik maupun sektor privat. Kebocoran data pada berbagai platform digital menunjukkan bahwa penyelenggara sistem elektronik belum sepenuhnya mampu menerapkan prinsip keamanan data secara optimal. Prakasa dan Usman (2024) menjelaskan bahwa meningkatnya pemanfaatan teknologi informasi dan sistem elektronik menimbulkan tantangan baru dalam perlindungan data pribadi sehingga diperlukan penguatan tanggung jawab hukum penyelenggara sistem elektronik terhadap keamanan data pengguna. Perlindungan hukum yang efektif tidak hanya membutuhkan regulasi yang memadai tetapi juga sistem pengawasan yang mampu menjamin kepatuhan penyelenggara sistem elektronik terhadap ketentuan perlindungan data pribadi.

Sebelum berlakunya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, pengaturan mengenai data pribadi di Indonesia tersebar dalam berbagai peraturan sektoral. Pengaturan yang bersifat parsial tersebut menyebabkan terjadinya fragmentasi norma hukum dan belum mampu memberikan perlindungan yang komprehensif kepada masyarakat. Akibatnya, korban kebocoran data sering mengalami kesulitan dalam memperoleh kepastian hukum maupun mekanisme pemulihan yang efektif ketika terjadi pelanggaran terhadap hak privasinya (Angraini, Makkawaru, & Almusawir, 2024).

Untuk menjawab kebutuhan tersebut, pemerintah Indonesia mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Kehadiran undang-undang ini menjadi tonggak penting dalam pembangunan sistem perlindungan data pribadi nasional karena untuk pertama kalinya Indonesia memiliki regulasi khusus yang mengatur hak subjek data, kewajiban pengendali data, kewajiban prosesor data, mekanisme pengawasan, serta sanksi administratif, perdata, dan pidana terhadap pelanggaran data pribadi (Simanjuntak, 2024).

Dalam perspektif hukum perdata, keberadaan Undang-Undang Pelindungan Data Pribadi memberikan dimensi baru terhadap mekanisme perlindungan hukum korban kebocoran data. Korban tidak hanya memperoleh perlindungan melalui sanksi administratif atau pidana, tetapi juga memiliki kesempatan untuk menuntut pemulihan kerugian melalui instrumen hukum perdata. Mekanisme tersebut penting karena sebagian besar dampak kebocoran data dirasakan secara langsung oleh individu sebagai subjek data, baik dalam bentuk kerugian materiil maupun immateriil.

Kerugian materiil akibat kebocoran data dapat berupa kehilangan aset keuangan, penyalahgunaan rekening, penipuan transaksi elektronik, dan pencurian identitas. Sementara itu, kerugian immateriil dapat berupa gangguan psikologis, hilangnya rasa aman, kerusakan reputasi, serta pelanggaran terhadap hak privasi individu. Oleh karena itu, konsep pertanggungjawaban perdata menjadi instrumen penting dalam mewujudkan keadilan bagi korban kebocoran data pribadi (Fuady, 2021).

Di Provinsi Sumatera Utara, perkembangan teknologi informasi dan komunikasi menunjukkan tren yang terus meningkat seiring pertumbuhan aktivitas ekonomi digital. Publikasi Provinsi Sumatera Utara Dalam Angka Tahun 2025 menunjukkan bahwa sektor informasi dan komunikasi menjadi salah satu sektor yang terus berkembang dalam mendukung aktivitas ekonomi dan pelayanan masyarakat (Badan Pusat Statistik Provinsi Sumatera Utara, 2025). Peningkatan penggunaan layanan digital tersebut secara langsung meningkatkan jumlah data pribadi masyarakat yang tersimpan dalam berbagai sistem elektronik.

Kota Medan sebagai pusat kegiatan ekonomi, perdagangan, pendidikan, dan pemerintahan di Provinsi Sumatera Utara memiliki tingkat pemanfaatan teknologi digital yang relatif tinggi dibandingkan wilayah lainnya. Tingginya penggunaan layanan perbankan digital, perdagangan elektronik, aplikasi transportasi daring, serta layanan publik berbasis elektronik menyebabkan masyarakat Kota Medan semakin bergantung pada sistem digital dalam kehidupan sehari-hari. Kondisi tersebut sekaligus meningkatkan potensi risiko kebocoran dan penyalahgunaan data pribadi apabila perlindungan hukum yang tersedia belum berjalan secara efektif.

Penelitian terdahulu umumnya berfokus pada analisis normatif terhadap substansi Undang-Undang Pelindungan Data Pribadi, implementasi perlindungan data pribadi, serta perbandingan antara sistem perlindungan data di Indonesia dan General Data Protection Regulation Uni Eropa (Simanjuntak, 2024; Angraini, Makkawaru, & Almusawir, 2024; Yoga, Ramli, & Ramli, 2024). Namun demikian, kajian yang secara khusus menganalisis efektivitas perlindungan hukum perdata terhadap korban kebocoran data pribadi pasca berlakunya Undang-Undang Nomor 27 Tahun 2022 masih relatif terbatas sehingga memerlukan penelitian lebih lanjut.

Berdasarkan uraian tersebut, penelitian ini memiliki kebaruan (novelty) berupa analisis perlindungan hukum perdata terhadap korban kebocoran data pribadi yang dikaji melalui pendekatan normatif-empiris dengan menghubungkan aspek regulasi, tingkat kesadaran hukum masyarakat, pengalaman kebocoran data pribadi, dan efektivitas mekanisme ganti rugi pasca berlakunya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Pendekatan tersebut diharapkan dapat memberikan gambaran yang lebih komprehensif mengenai implementasi perlindungan hukum perdata di Indonesia.

METODE

Penelitian ini menggunakan metode penelitian hukum normatif-empiris. Pemilihan metode tersebut didasarkan pada tujuan penelitian yang tidak hanya mengkaji norma hukum yang mengatur perlindungan data pribadi, tetapi juga menganalisis implementasi perlindungan hukum perdata terhadap korban kebocoran data pribadi dalam transaksi digital setelah berlakunya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Pendekatan normatif digunakan untuk mengkaji berbagai ketentuan hukum yang berlaku, sedangkan pendekatan empiris digunakan untuk memperoleh gambaran mengenai penerapan norma hukum tersebut dalam praktik.

Penelitian dilaksanakan pada periode Januari hingga Mei 2026 dengan fokus kajian terhadap perlindungan hukum perdata bagi korban kebocoran data pribadi di Indonesia. Lokasi penelitian empiris dilakukan di Kota Medan, Provinsi Sumatera Utara. Pemilihan Kota Medan didasarkan pada tingginya aktivitas ekonomi digital, penggunaan transaksi elektronik, serta meningkatnya pemanfaatan layanan berbasis internet oleh masyarakat sehingga memiliki relevansi yang kuat dengan permasalahan perlindungan data pribadi.

Pendekatan penelitian yang digunakan meliputi pendekatan perundang-undangan (statute approach), pendekatan konseptual (conceptual approach), pendekatan kasus (case

approach), dan pendekatan empiris (empirical approach). Pendekatan perundang-undangan digunakan untuk menganalisis berbagai regulasi yang berkaitan dengan perlindungan data pribadi, sedangkan pendekatan konseptual digunakan untuk mengkaji teori perlindungan hukum, teori hak privasi, teori tanggung jawab perdata, dan teori perbuatan melawan hukum. Pendekatan kasus digunakan untuk mengkaji berbagai kasus kebocoran data pribadi yang pernah terjadi di Indonesia. Sementara itu, pendekatan empiris digunakan untuk memperoleh informasi mengenai tingkat pemahaman masyarakat terhadap perlindungan data pribadi dan mekanisme penyelesaian sengketa yang tersedia.

Jenis data yang digunakan dalam penelitian ini terdiri atas data primer dan data sekunder. Data primer diperoleh secara langsung dari responden melalui penyebaran kuesioner dan wawancara mendalam. Data sekunder diperoleh melalui studi kepustakaan yang meliputi bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Kombinasi kedua jenis data tersebut digunakan untuk menghasilkan analisis yang komprehensif dan objektif.

HASIL DAN PEMBAHASAN

Karakteristik Responden

Penelitian ini melibatkan 150 responden masyarakat Kota Medan yang memenuhi kriteria sebagai pengguna aktif layanan transaksi digital. Karakteristik responden disajikan pada Tabel 1.

Tabel 1. Karakteristik Responden Penelitian

Karakteristik	Frekuensi	Persentase (%)
Jenis Kelamin Laki-laki	68	45,3
Jenis Kelamin Perempuan	82	54,7
Usia 17–25 Tahun	52	34,7
Usia 26–35 Tahun	48	32,0
Usia 36–45 Tahun	31	20,7
Usia >45 Tahun	19	12,6
Pendidikan SMA	44	29,3
Diploma	28	18,7
Sarjana	62	41,3
Pascasarjana	16	10,7

Berdasarkan Tabel 1 diketahui bahwa mayoritas responden berjenis kelamin perempuan sebanyak 82 orang (54,7%). Berdasarkan kelompok usia, responden terbanyak berada pada rentang usia 17–25 tahun yaitu 52 orang (34,7%). Dari aspek pendidikan, mayoritas responden memiliki pendidikan sarjana sebanyak 62 orang (41,3%).

Tingkat Penggunaan Transaksi Digital

Hasil penelitian menunjukkan seluruh responden menggunakan layanan transaksi digital dalam aktivitas sehari-hari.

Tabel 2. Jenis Transaksi Digital yang Digunakan Responden

Jenis Layanan	Frekuensi
Mobile Banking	136
Dompot Digital	143
Marketplace	148
Aplikasi Transportasi Online	127
Media Sosial untuk Transaksi	119

Data menunjukkan bahwa marketplace merupakan layanan yang paling banyak digunakan oleh responden yaitu sebanyak 148 orang (98,7%), diikuti dompet digital sebanyak 143 orang (95,3%).

Diagram 1. Persentase Penggunaan Layanan Digital

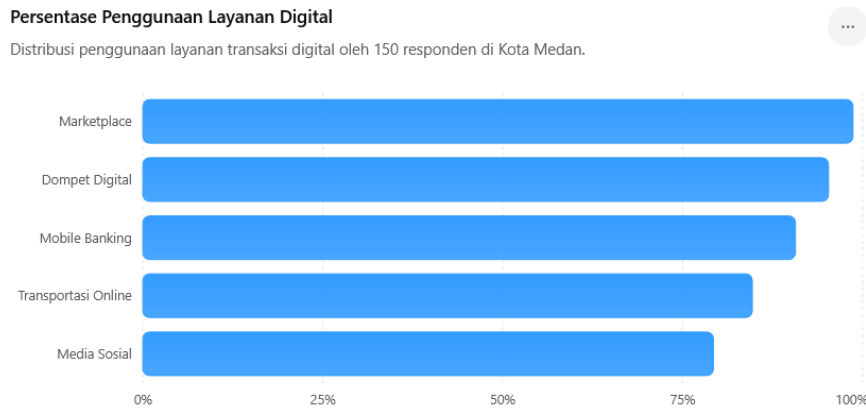


Diagram 1 menunjukkan bahwa marketplace merupakan layanan digital yang paling banyak digunakan oleh responden dengan persentase sebesar 98,7%, diikuti dompet digital sebesar 95,3%, mobile banking sebesar 90,7%, transportasi daring sebesar 84,7%, dan media sosial untuk transaksi sebesar 79,3%. Temuan ini menunjukkan bahwa masyarakat Kota Medan memiliki tingkat ketergantungan yang tinggi terhadap layanan transaksi digital dalam aktivitas sehari-hari.

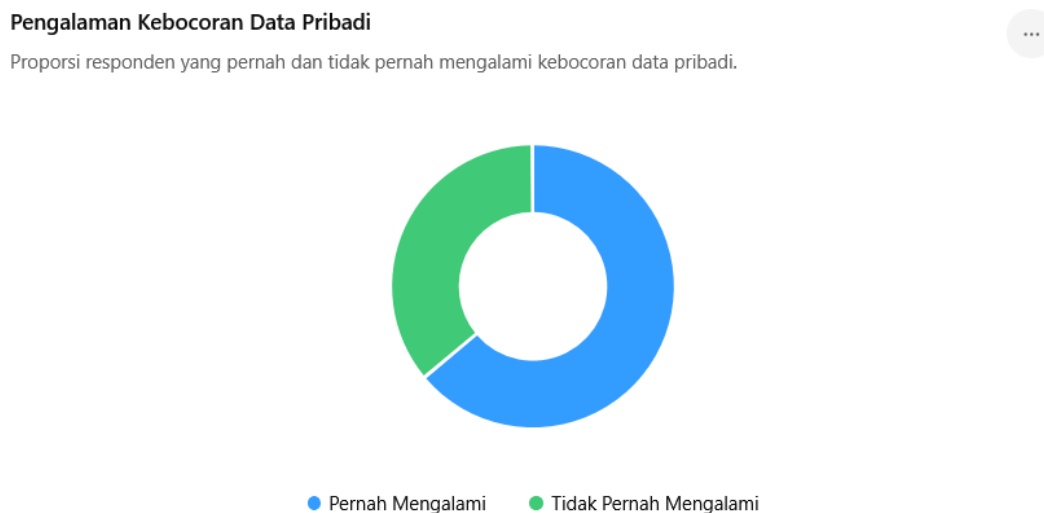
Pengalaman Kebocoran Data Pribadi

Tabel 3. Pengalaman Kebocoran Data Pribadi

Kategori	Frekuensi	Persentase (%)
Pernah Mengalami	96	64,0
Tidak Pernah Mengalami	54	36,0

Sebanyak 96 responden (64,0%) menyatakan pernah mengalami indikasi kebocoran data pribadi berupa pesan spam, panggilan penipuan, penggunaan identitas tanpa izin, maupun percobaan akses ilegal terhadap akun digital.

Diagram 2. Pengalaman Kebocoran Data



- Pernah Mengalami = 64%
- Tidak Pernah Mengalami = 36%

Diagram 2 menunjukkan bahwa 64% responden pernah mengalami indikasi kebocoran data pribadi, sedangkan 36% responden menyatakan tidak pernah mengalami kebocoran data. Persentase tersebut menunjukkan bahwa risiko kebocoran data pribadi masih relatif tinggi di kalangan pengguna layanan digital di Kota Medan. Temuan ini memperlihatkan bahwa perlindungan data pribadi masih menjadi isu yang memerlukan perhatian serius dari pemerintah, penyelenggara sistem elektronik, dan masyarakat sebagai pengguna layanan digital.

Bentuk Data yang Pernah Bocor

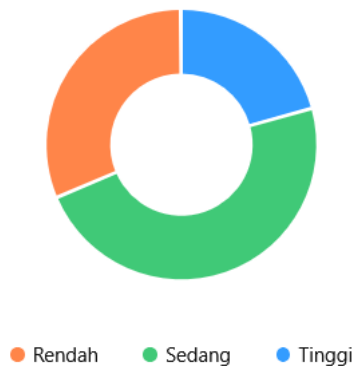
Tabel 4. Jenis Data yang Diduga Mengalami Kebocoran

Jenis Data	Frekuensi
Nomor Telepon	87
Alamat Surat Elektronik	73
Nomor Induk Kependudukan	38
Data Rekening	26
Foto Identitas	21

Nomor telepon menjadi jenis data yang paling sering dilaporkan mengalami kebocoran dengan frekuensi 87 responden.

Tingkat Pemahaman Terhadap UU PDP

Distribusi tingkat pemahaman responden mengenai Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.



Tabel 5. Tingkat Pemahaman UU PDP

Tingkat Pemahaman	Frekuensi	Persentase
Tinggi	31	20,7
Sedang	72	48,0
Rendah	47	31,3

Berdasarkan Diagram 3 diketahui bahwa sebagian besar responden memiliki tingkat pemahaman sedang terhadap Undang-Undang Pelindungan Data Pribadi yaitu sebesar 48,0%. Responden dengan tingkat pemahaman rendah mencapai 31,3%, sedangkan responden dengan tingkat pemahaman tinggi hanya sebesar 20,7%.

Temuan tersebut menunjukkan bahwa meskipun Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi telah berlaku secara efektif setelah berakhirnya masa transisi pada tahun 2024, tingkat pemahaman masyarakat mengenai hak dan kewajiban dalam perlindungan data pribadi masih belum optimal. Kondisi ini mengindikasikan perlunya

peningkatan sosialisasi, edukasi hukum, dan literasi digital kepada masyarakat agar dapat memahami mekanisme perlindungan hukum yang tersedia apabila terjadi kebocoran data pribadi.

Tingkat Kesadaran Hukum Masyarakat

Tabel 6. Tingkat Kesadaran Hukum

Kategori	Frekuensi
Tinggi	44
Sedang	81
Rendah	25

Sebagian besar responden berada pada kategori kesadaran hukum sedang yaitu sebanyak 81 orang.

Diagram 4. Tingkat Kesadaran Hukum Masyarakat Mengenai Perlindungan Data Pribadi

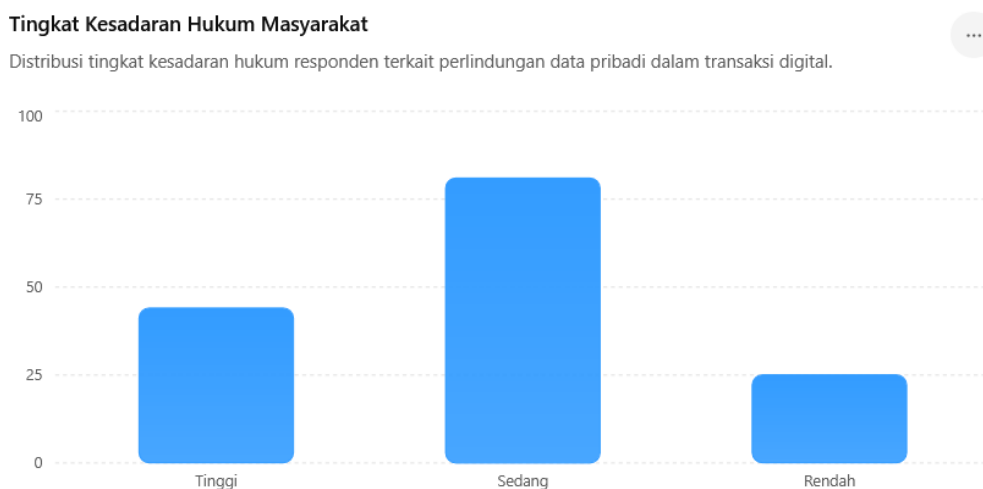


Diagram 4 menunjukkan bahwa mayoritas responden berada pada kategori kesadaran hukum sedang sebanyak 81 orang. Responden yang memiliki kesadaran hukum tinggi berjumlah 44 orang, sedangkan responden dengan kesadaran hukum rendah berjumlah 25 orang.

Data tersebut memperlihatkan bahwa sebagian besar masyarakat telah memiliki kesadaran mengenai pentingnya menjaga data pribadi, namun belum sepenuhnya memahami langkah-langkah hukum yang dapat ditempuh ketika menjadi korban kebocoran data. Tingkat kesadaran hukum yang belum merata ini berpotensi memengaruhi efektivitas implementasi perlindungan hukum perdata sebagaimana diatur dalam Undang-Undang Pelindungan Data Pribadi.

.Persepsi Terhadap Efektivitas Perlindungan Hukum

Tabel 7. Persepsi Efektivitas Perlindungan Hukum Perdata

Kategori	Frekuensi	Persentase
Efektif	42	28,0
Cukup Efektif	77	51,3
Tidak Efektif	31	20,7

Dari Tabel 7 menunjukkan bahwa sebagian besar responden menilai perlindungan hukum perdata pasca berlakunya Undang-Undang Pelindungan Data Pribadi berada pada kategori cukup efektif dengan persentase sebesar 51,3%. Sebanyak 28,0% responden menilai perlindungan hukum telah efektif, sedangkan 20,7% responden menilai belum efektif.

Temuan ini menunjukkan bahwa kehadiran Undang-Undang Pelindungan Data Pribadi telah memberikan harapan baru bagi masyarakat dalam memperoleh perlindungan hukum atas data pribadi mereka. Namun demikian, masih terdapat sejumlah hambatan dalam implementasi, khususnya terkait pemahaman masyarakat, mekanisme pengaduan, pembuktian kerugian, dan akses terhadap penyelesaian sengketa secara perdata.

Hasil Uji Validitas

Seluruh item kuesioner menunjukkan nilai korelasi lebih besar daripada nilai r tabel sebesar 0,361 sehingga seluruh item dinyatakan valid.

Hasil Uji Reliabilitas

Instrumen penelitian memperoleh nilai Cronbach Alpha sebesar 0,871. Nilai tersebut lebih besar daripada 0,70 sehingga seluruh instrumen penelitian dinyatakan reliabel.

Hubungan Kesadaran Hukum dengan Efektivitas Perlindungan Hukum

Tabel 8. Hubungan Kesadaran Hukum dan Efektivitas Perlindungan Hukum

Variabel	Koefisien Korelasi
Kesadaran Hukum	0,684
Signifikansi	0,000

Hasil analisis menunjukkan adanya hubungan positif yang kuat antara tingkat kesadaran hukum masyarakat dengan persepsi efektivitas perlindungan hukum perdata terhadap korban kebocoran data pribadi.

Temuan Wawancara

Hasil wawancara dengan akademisi hukum, praktisi hukum, dan pejabat instansi terkait menunjukkan bahwa implementasi Undang-Undang Pelindungan Data Pribadi telah memberikan landasan hukum yang lebih jelas dibandingkan sebelum tahun 2022. Namun demikian, masih ditemukan kendala berupa rendahnya literasi hukum masyarakat, minimnya pemahaman mengenai mekanisme gugatan perdata, serta belum optimalnya pengawasan terhadap penyelenggara sistem elektronik.

Secara keseluruhan hasil penelitian menunjukkan bahwa tingkat penggunaan transaksi digital masyarakat Kota Medan sangat tinggi, sementara pengalaman kebocoran data pribadi juga relatif tinggi. Di sisi lain, tingkat pemahaman masyarakat terhadap Undang-Undang Pelindungan Data Pribadi masih berada pada kategori sedang sehingga diperlukan upaya peningkatan edukasi hukum dan perlindungan data pribadi secara berkelanjutan.

Bahan hukum primer yang digunakan dalam penelitian ini meliputi Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Kitab Undang-Undang Hukum Perdata, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Peraturan Pemerintah yang berkaitan dengan sistem elektronik, serta berbagai regulasi lain yang relevan dengan perlindungan data pribadi dan transaksi digital.

Bahan hukum sekunder terdiri atas buku-buku hukum, artikel jurnal nasional terakreditasi, artikel jurnal internasional bereputasi, hasil penelitian terdahulu, prosiding ilmiah,

laporan lembaga nasional maupun internasional, serta publikasi akademik yang berkaitan dengan perlindungan data pribadi, keamanan siber, transaksi elektronik, dan pertanggungjawaban perdata. Sementara itu, bahan hukum tersier berupa kamus hukum, ensiklopedia hukum, dan berbagai sumber pendukung lain yang digunakan untuk memperkuat interpretasi terhadap konsep-konsep hukum yang dibahas dalam penelitian.

Populasi penelitian empiris adalah masyarakat Kota Medan yang pernah menggunakan layanan transaksi digital seperti perdagangan elektronik, dompet digital, mobile banking, aplikasi transportasi daring, dan layanan berbasis internet lainnya. Berdasarkan data Badan Pusat Statistik Kota Medan Tahun 2025 mengenai tingkat penggunaan internet dan teknologi informasi, ditetapkan sampel penelitian sebanyak 150 responden yang dipilih menggunakan teknik purposive sampling. Teknik ini digunakan karena responden harus memenuhi kriteria tertentu yang relevan dengan tujuan penelitian.

Kriteria responden dalam penelitian ini meliputi masyarakat yang berusia minimal 17 tahun, pernah melakukan transaksi digital dalam enam bulan terakhir, memiliki akun pada platform digital tertentu, dan bersedia menjadi responden penelitian. Selain responden masyarakat, penelitian ini juga melibatkan lima informan kunci yang terdiri atas akademisi hukum, praktisi hukum, pejabat instansi pemerintah yang membidangi teknologi informasi, serta pelaku usaha digital untuk memperoleh perspektif yang lebih mendalam mengenai implementasi perlindungan data pribadi.

Teknik pengumpulan data dilakukan melalui tiga metode utama. Pertama, studi dokumentasi yang dilakukan dengan mengumpulkan dan menganalisis berbagai dokumen hukum, regulasi, jurnal ilmiah, laporan penelitian, dan publikasi resmi yang relevan. Kedua, penyebaran kuesioner kepada responden untuk memperoleh data mengenai tingkat pengetahuan masyarakat tentang perlindungan data pribadi, pengalaman terkait kebocoran data, serta pemahaman terhadap hak-hak yang dijamin oleh Undang-Undang Pelindungan Data Pribadi. Ketiga, wawancara semi-terstruktur dengan informan kunci guna memperoleh informasi yang lebih mendalam mengenai efektivitas perlindungan hukum perdata terhadap korban kebocoran data pribadi.

Instrumen penelitian berupa kuesioner yang disusun berdasarkan indikator perlindungan data pribadi, tingkat kesadaran hukum, pengalaman kebocoran data, pemahaman hak subjek data, dan persepsi terhadap efektivitas Undang-Undang Pelindungan Data Pribadi. Sebelum digunakan, instrumen penelitian diuji validitas dan reliabilitasnya terhadap tiga puluh responden uji coba untuk memastikan bahwa setiap pertanyaan mampu mengukur variabel penelitian secara tepat dan konsisten.

Variabel penelitian terdiri atas variabel independen dan variabel dependen. Variabel independen meliputi tingkat pemahaman masyarakat mengenai perlindungan data pribadi, tingkat kesadaran hukum, serta tingkat kepatuhan penyelenggara sistem elektronik terhadap ketentuan Undang-Undang Pelindungan Data Pribadi. Variabel dependen berupa efektivitas perlindungan hukum perdata terhadap korban kebocoran data pribadi yang diukur melalui indikator akses terhadap keadilan, mekanisme ganti rugi, kepastian hukum, dan perlindungan hak korban.

Analisis data normatif dilakukan melalui metode analisis kualitatif dengan cara menginventarisasi, mengklasifikasikan, menginterpretasikan, dan mengevaluasi berbagai ketentuan hukum yang relevan. Analisis dilakukan untuk mengidentifikasi bentuk perlindungan hukum yang tersedia, hak dan kewajiban para pihak, serta mekanisme pertanggungjawaban perdata yang dapat diterapkan dalam kasus kebocoran data pribadi. Pendekatan interpretasi gramatikal, sistematis, dan teleologis digunakan untuk memperoleh pemahaman yang komprehensif terhadap norma hukum yang berlaku.

Data empiris dianalisis menggunakan metode statistik deskriptif dengan bantuan perangkat lunak Statistical Package for Social Sciences versi 26. Analisis dilakukan melalui tahap editing, coding, tabulasi, dan interpretasi data. Hasil analisis kemudian disajikan dalam

bentuk tabel distribusi frekuensi, diagram batang, dan diagram lingkaran untuk mempermudah pemahaman terhadap karakteristik responden dan temuan penelitian.

Untuk menjamin validitas hasil penelitian, dilakukan triangulasi sumber dan triangulasi metode. Triangulasi sumber dilakukan dengan membandingkan data yang diperoleh dari responden, informan, dokumen hukum, dan literatur akademik. Sementara itu, triangulasi metode dilakukan dengan membandingkan hasil studi kepustakaan, hasil kuesioner, dan hasil wawancara. Dengan demikian, hasil penelitian diharapkan memiliki tingkat keabsahan yang tinggi dan mampu memberikan gambaran yang objektif mengenai perlindungan hukum perdata terhadap korban kebocoran data pribadi dalam transaksi digital pasca berlakunya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

PEMBAHASAN

Hasil penelitian menunjukkan bahwa penggunaan layanan transaksi digital di Kota Medan berada pada tingkat yang sangat tinggi. Sebanyak 98,7% responden menggunakan marketplace, 95,3% menggunakan dompet digital, dan 90,7% menggunakan layanan mobile banking. Temuan ini menunjukkan bahwa aktivitas masyarakat modern semakin bergantung pada teknologi digital sebagai sarana utama dalam melakukan transaksi ekonomi. Kondisi tersebut sejalan dengan laporan Badan Pusat Statistik (2025) yang menunjukkan peningkatan penggunaan internet dan layanan digital di Indonesia dari tahun ke tahun. Semakin tingginya penggunaan layanan digital berimplikasi pada meningkatnya jumlah data pribadi yang diproses oleh penyelenggara sistem elektronik sehingga risiko pelanggaran terhadap data pribadi juga semakin besar.

Tingginya penggunaan layanan digital menyebabkan data pribadi menjadi salah satu aset yang memiliki nilai ekonomi tinggi. Dalam perspektif ekonomi digital, data pribadi tidak hanya berfungsi sebagai identitas pengguna, tetapi juga menjadi sumber informasi yang digunakan untuk pengembangan layanan, pemasaran, analisis perilaku konsumen, dan berbagai kepentingan bisnis lainnya. Menurut UNCTAD (2024), data telah berkembang menjadi komoditas strategis yang memiliki nilai ekonomi signifikan dalam ekosistem digital global. Oleh karena itu, perlindungan terhadap data pribadi menjadi kebutuhan yang tidak dapat dipisahkan dari perkembangan teknologi informasi.

Hasil penelitian menunjukkan bahwa 64% responden pernah mengalami indikasi kebocoran data pribadi. Persentase tersebut tergolong tinggi dan menunjukkan bahwa ancaman terhadap keamanan data masih menjadi persoalan nyata dalam masyarakat digital. Bentuk kebocoran yang paling banyak dialami responden adalah penyalahgunaan nomor telepon, alamat surat elektronik, serta penyebaran informasi pribadi tanpa persetujuan pemilik data. Temuan ini menunjukkan bahwa pelanggaran data pribadi tidak lagi bersifat teoritis, melainkan telah menjadi pengalaman nyata yang dialami oleh sebagian besar pengguna layanan digital.

Dalam perspektif teori hak privasi, setiap individu memiliki hak untuk mengendalikan informasi mengenai dirinya sendiri. Teori ini menegaskan bahwa pemilik data memiliki kewenangan untuk menentukan bagaimana data pribadinya dikumpulkan, digunakan, disimpan, dan disebarluaskan. Ketika data pribadi digunakan tanpa persetujuan atau mengalami kebocoran akibat kelalaian pengendali data, maka telah terjadi pelanggaran terhadap hak privasi individu. De Souza et al. (2020) menjelaskan bahwa perlindungan data pribadi merupakan bagian integral dari perlindungan hak asasi manusia dalam era digital.

Hasil penelitian juga menunjukkan bahwa tingkat pemahaman masyarakat terhadap Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi masih didominasi kategori sedang sebesar 48,0%, sedangkan kategori rendah mencapai 31,3%. Temuan tersebut mengindikasikan bahwa meskipun Indonesia telah memiliki regulasi khusus mengenai perlindungan data pribadi, tingkat literasi hukum masyarakat belum sepenuhnya

memadai. Rendahnya pemahaman hukum dapat menghambat kemampuan masyarakat dalam menggunakan hak-haknya ketika menjadi korban kebocoran data pribadi.

Kondisi tersebut dapat dianalisis menggunakan teori kesadaran hukum yang menyatakan bahwa efektivitas suatu peraturan perundang-undangan sangat dipengaruhi oleh tingkat pengetahuan, pemahaman, sikap, dan perilaku hukum masyarakat. Soekanto (2021) menjelaskan bahwa hukum akan berjalan efektif apabila masyarakat mengetahui keberadaan norma hukum, memahami substansinya, serta memiliki kesadaran untuk mematuhi dan memanfaatkannya. Oleh karena itu, keberhasilan implementasi Undang-Undang Pelindungan Data Pribadi tidak hanya bergantung pada kualitas regulasi, tetapi juga pada tingkat pemahaman masyarakat sebagai subjek hukum.

Berdasarkan hasil penelitian, sebagian besar responden menilai bahwa perlindungan hukum perdata pasca berlakunya Undang-Undang Pelindungan Data Pribadi berada pada kategori cukup efektif. Penilaian tersebut menunjukkan bahwa masyarakat mulai merasakan adanya peningkatan kepastian hukum dibandingkan sebelum undang-undang tersebut diberlakukan. Sebelum tahun 2022, pengaturan mengenai data pribadi tersebar dalam berbagai regulasi sektoral sehingga sering menimbulkan ketidakjelasan mengenai hak korban dan tanggung jawab pihak yang menyebabkan kebocoran data.

Kehadiran Undang-Undang Pelindungan Data Pribadi memberikan dasar hukum yang lebih kuat bagi korban untuk memperoleh perlindungan dan pemulihan kerugian. Pasal-pasal dalam undang-undang tersebut mengatur hak subjek data untuk memperoleh informasi, mengakses data, memperbaiki data, menghapus data, menarik persetujuan, serta memperoleh ganti rugi apabila terjadi pelanggaran terhadap data pribadi. Pengaturan tersebut menunjukkan bahwa perlindungan data pribadi di Indonesia telah bergerak menuju pendekatan berbasis hak (*rights-based approach*) sebagaimana diterapkan dalam berbagai rezim perlindungan data modern.

Dari perspektif hukum perdata, kebocoran data pribadi dapat dikualifikasikan sebagai perbuatan melawan hukum apabila memenuhi unsur-unsur sebagaimana diatur dalam Pasal 1365 Kitab Undang-Undang Hukum Perdata. Unsur-unsur tersebut meliputi adanya perbuatan melawan hukum, adanya kesalahan, adanya kerugian, dan adanya hubungan kausal antara perbuatan dengan kerugian yang timbul. Apabila suatu penyelenggara sistem elektronik lalai dalam menjaga keamanan data sehingga mengakibatkan kebocoran data pribadi pengguna, maka penyelenggara tersebut dapat dimintai pertanggungjawaban secara perdata.

Teori perbuatan melawan hukum yang dikemukakan oleh Fuady (2021) menjelaskan bahwa tanggung jawab hukum tidak hanya timbul karena adanya pelanggaran terhadap undang-undang, tetapi juga dapat timbul karena pelanggaran terhadap hak subjektif orang lain, pelanggaran kewajiban hukum, atau tindakan yang bertentangan dengan prinsip kehati-hatian. Dalam konteks perlindungan data pribadi, kegagalan penyelenggara sistem elektronik dalam menerapkan standar keamanan yang memadai dapat dianggap sebagai bentuk kelalaian yang menimbulkan kewajiban ganti rugi kepada korban.

Hasil wawancara dengan informan menunjukkan bahwa salah satu kendala utama dalam penyelesaian sengketa kebocoran data pribadi adalah kesulitan pembuktian kerugian. Banyak korban mengetahui bahwa data pribadinya telah bocor, namun mengalami kesulitan untuk membuktikan hubungan langsung antara kebocoran data tersebut dengan kerugian yang dialaminya. Kondisi ini menjadi tantangan tersendiri dalam proses gugatan perdata karena hukum acara perdata pada prinsipnya menempatkan beban pembuktian pada pihak yang mengajukan gugatan.

Temuan penelitian ini sejalan dengan penelitian Angraini, Makkawaru, dan Almusawir (2024) yang menyatakan bahwa implementasi perlindungan data pribadi di Indonesia masih menghadapi hambatan berupa keterbatasan mekanisme pengawasan dan pembuktian. Penelitian tersebut menunjukkan bahwa meskipun kerangka hukum telah tersedia, efektivitas

perlindungan hukum masih dipengaruhi oleh kesiapan institusi, sumber daya manusia, dan tingkat literasi hukum masyarakat.

Selain kesulitan pembuktian, penelitian ini menemukan bahwa sebagian responden belum mengetahui prosedur pengajuan gugatan perdata apabila menjadi korban kebocoran data pribadi. Kondisi tersebut menunjukkan bahwa akses terhadap keadilan masih menjadi tantangan dalam implementasi perlindungan data pribadi. Dalam perspektif teori perlindungan hukum yang dikemukakan oleh Philipus M. Hadjon, perlindungan hukum harus mampu memberikan jaminan terhadap hak-hak masyarakat melalui mekanisme preventif maupun represif. Perlindungan preventif diwujudkan melalui regulasi dan pengawasan, sedangkan perlindungan represif diwujudkan melalui mekanisme penyelesaian sengketa dan pemberian ganti rugi.

Hubungan positif yang kuat antara tingkat kesadaran hukum dan persepsi efektivitas perlindungan hukum menunjukkan bahwa masyarakat yang memiliki pemahaman hukum lebih baik cenderung memiliki kepercayaan yang lebih tinggi terhadap mekanisme perlindungan hukum yang tersedia. Temuan ini memperkuat pandangan bahwa keberhasilan implementasi Undang-Undang Pelindungan Data Pribadi tidak hanya ditentukan oleh substansi hukum, tetapi juga oleh kemampuan masyarakat dalam memahami dan memanfaatkan instrumen hukum tersebut untuk melindungi hak-haknya.

Kebaruan penelitian ini terletak pada analisis keterkaitan antara tingkat kesadaran hukum masyarakat, pengalaman kebocoran data pribadi, dan efektivitas perlindungan hukum perdata pasca berlakunya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Hasil penelitian menunjukkan bahwa meskipun regulasi telah memberikan dasar hukum yang lebih kuat bagi korban kebocoran data pribadi, efektivitas perlindungan hukum perdata masih memerlukan penguatan melalui peningkatan literasi hukum masyarakat, penguatan lembaga pengawas, penyederhanaan mekanisme gugatan, serta peningkatan kepatuhan penyelenggara sistem elektronik terhadap prinsip-prinsip perlindungan data pribadi. Dengan demikian, tujuan utama perlindungan data pribadi untuk menjamin keamanan, privasi, dan kepastian hukum masyarakat dalam transaksi digital dapat terwujud secara lebih optimal.

SIMPULAN

Penelitian ini menunjukkan bahwa penggunaan transaksi digital masyarakat Kota Medan berada pada tingkat yang sangat tinggi dan diikuti oleh tingginya pengalaman kebocoran data pribadi. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi telah memberikan dasar hukum yang lebih kuat bagi korban untuk memperoleh perlindungan dan menuntut ganti rugi melalui mekanisme hukum perdata. Namun, efektivitas perlindungan tersebut masih menghadapi kendala berupa rendahnya literasi hukum masyarakat, kesulitan pembuktian kerugian, dan belum optimalnya pengawasan terhadap penyelenggara sistem elektronik. Oleh karena itu, pemerintah perlu memperkuat pengawasan dan sosialisasi Undang-Undang Pelindungan Data Pribadi, sementara penyelenggara sistem elektronik harus meningkatkan keamanan data dan kepatuhan hukum guna menjamin perlindungan hak-hak masyarakat dalam transaksi digital.

DAFTAR PUSTAKA

- Alhazmi, O. H., Imran, M., & Alsheikh, M. A. 2024. *Data Privacy And Cybersecurity Challenges In The Digital Era*. New York: Springer Nature.
- Angraini, R., Makkawaru, Z., & Almusawir. 2024. *Implementasi Perlindungan Data Pribadi Dalam Perspektif Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi*. Makassar: Universitas Muslim Indonesia.
- Badan Pusat Statistik. 2024. *Statistik Telekomunikasi Indonesia 2023*. Jakarta: Badan Pusat Statistik.

- Badan Pusat Statistik. 2025. Statistik Telekomunikasi Indonesia 2024. Jakarta: Badan Pusat Statistik.
- Badan Pusat Statistik Kota Medan. 2025. Kota Medan Dalam Angka 2025. Medan: Badan Pusat Statistik Kota Medan.
- Badan Pusat Statistik Provinsi Sumatera Utara. 2025. Provinsi Sumatera Utara Dalam Angka 2025. Medan: Badan Pusat Statistik Provinsi Sumatera Utara.
- De Souza, J. S., Abe, J. M., De Lima, L. A., & De Souza, N. A. 2020. The General Law Principles For Protection The Personal Data And Their Importance. São Paulo: Brazilian Legal Studies.
- Fuady, M. 2021. Perbuatan Melawan Hukum Pendekatan Kontemporer. Bandung: PT Citra Aditya Bakti.
- Hadjon, P. M. 2022. Perlindungan Hukum Bagi Rakyat Indonesia. Surabaya: Bina Ilmu.
- Jurcys, P., Compagnucci, M. C., & Fenwick, M. 2024. The Future Of International Data Transfers: Managing Legal Risk With A User-Held Data Model. Tokyo: Kyushu University Press.
- Kementerian Komunikasi Dan Digital Republik Indonesia. 2025. Pedoman Implementasi Pelindungan Data Pribadi Bagi Penyelenggara Sistem Elektronik. Jakarta: Kementerian Komunikasi Dan Digital Republik Indonesia.
- Marzuki, P. M. 2022. Penelitian Hukum. Jakarta: Kencana Prenada Media Group.
- Prakasa, S. U. W., & Usman, N. 2024. Perlindungan Hukum Data Pribadi Dan Pertanggungjawaban Otoritas Terhadap Keamanan Siber Menurut Tinjauan Undang-Undang Pelindungan Data Pribadi. Medan: Doktrina Journal Of Law.
- Pratama, M., & Siregar, N. 2024. Civil Liability For Personal Data Breaches In Electronic Transactions. Surakarta: Yustisia Jurnal Hukum.
- Rahman, F. 2023. Challenges Of Personal Data Protection In Indonesia's Digital Economy. Palembang: Sriwijaya Law Review.
- Rizky, M., Apriyani, R., & Aripkah, N. 2025. Perlindungan Hukum Dan Kepastian Hukum Terhadap Perdagangan Data Pribadi Dalam Undang-Undang Pelindungan Data Pribadi. Samarinda: Mahkamah Jurnal Riset Ilmu Hukum.
- Sari, A. K. 2025. Perlindungan Hukum Terhadap Pengelolaan Big Data Dalam Perspektif Undang-Undang Pelindungan Data Pribadi Di Indonesia. Medan: Judge Jurnal Hukum.
- Simanjuntak, R. 2024. Perlindungan Data Pribadi Dan Tantangan Implementasi Undang-Undang Pelindungan Data Pribadi Di Indonesia. Jakarta: Jurnal Legislasi Indonesia.
- Soekanto, S. 2021. Faktor-Faktor Yang Mempengaruhi Penegakan Hukum. Jakarta: Rajawali Pers.
- United Nations Conference On Trade And Development. 2024. Digital Economy Report 2024. Geneva: United Nations Conference On Trade And Development.
- World Bank. 2024. Digital Development Report 2024. Washington DC: World Bank.
- Yoga, I. M. W. P., Ramli, A. M., & Ramli, T. S. 2024. Perlindungan Data Pribadi Di Indonesia Melalui Mekanisme Register Of Processing Activities (ROPA): Studi Komparatif Antara Undang-Undang Pelindungan Data Pribadi Dengan General Data Protection Regulation. Bandung: Deposisi Jurnal Publikasi Ilmu Hukum.
- Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
- Kitab Undang-Undang Hukum Perdata.
- Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi.
- Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.
- Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik.
- Peraturan Menteri Komunikasi Dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.