



Tinjauan Hukum terhadap Aplikasi Digital sebagai Upaya Meningkatkan Kesadaran Perlindungan Hak Privasi Data Pribadi

Berto Purnomo Sidik^{1*}, Sidi Ahyar Wiraguna²

^{1,2}Fakultas Ilmu Hukum, Hukum, Universitas Esa Unggul, Indonesia

Alamat: Jl. Arjuna Utara No.9, Kebon Jeruk, Jakarta 11510

Korespondensi penulis: bertops04@gmail.com*

Abstract. *The protection of personal data privacy rights has become a crucial issue in the digital age. This research aims to analyze the effectiveness of digital applications in increasing public awareness regarding the importance of personal data protection and its legal implications. The research method employed is a literature study with a normative juridical approach, analyzing relevant laws and regulations on personal data protection, literature studies, and an analysis of the features of digital applications that focus on privacy education and control. The results of the study indicate that digital applications have significant potential in raising public awareness through the provision of easily accessible information, visualization of risks, and consent control mechanisms for data usage. However, their effectiveness heavily relies on intuitive interface design, clear and concise information delivery, and developers' compliance with personal data protection principles. This research recommends the need for more comprehensive regulations to ensure the quality standards and accountability of digital applications in educating the public about personal data privacy rights, as well as encouraging collaboration between developers, the government, and civil society organizations to create a safer and more privacy-aware digital ecosystem.*

Keywords: Digital Applications, Legal Awareness, PDP Law, Personal Data Protection, Privacy Rights.

Abstrak. Perlindungan hak privasi data pribadi menjadi isu krusial di era digital. Penelitian ini bertujuan untuk menganalisis efektivitas aplikasi digital dalam meningkatkan kesadaran masyarakat terhadap pentingnya perlindungan data pribadi dan implikasi hukumnya. Metode penelitian yang digunakan adalah studi kepustakaan dengan pendekatan yuridis normatif, menganalisis peraturan perundang-undangan terkait perlindungan data pribadi, studi literatur, dan analisis terhadap fitur-fitur aplikasi digital yang berfokus pada edukasi dan kontrol privasi. Hasil penelitian menunjukkan bahwa aplikasi digital memiliki potensi signifikan dalam meningkatkan kesadaran masyarakat melalui penyediaan informasi yang mudah diakses, visualisasi risiko, dan mekanisme kontrol persetujuan penggunaan data. Namun, efektivitasnya sangat bergantung pada desain antarmuka yang intuitif, penyampaian informasi yang jelas dan ringkas, serta kepatuhan pengembang terhadap prinsip-prinsip perlindungan data pribadi. Penelitian ini merekomendasikan perlunya regulasi yang lebih komprehensif untuk memastikan standar kualitas dan akuntabilitas aplikasi digital dalam mengedukasi masyarakat tentang hak privasi data pribadi, serta mendorong kolaborasi antara pengembang, pemerintah, dan organisasi masyarakat sipil untuk menciptakan ekosistem digital yang lebih aman dan sadar privasi.

Kata kunci: Aplikasi Digital, Kesadaran Hukum, Hukum PDP, Perlindungan Data Pribadi, Hak Privasi.

1. LATAR BELAKANG

Era perkembangan teknologi informasi yang semakin pesat telah membawa perubahan di berbagai sektor kehidupan, mulai dari pemerintahan, pendidikan, ekonomi, hingga sosial budaya. Salah satu sektor yang mengalami transformasi besar akibat digitalisasi adalah pengelolaan dan pemanfaatan data pribadi melalui berbagai platform dan aplikasi digital. Data pribadi telah menjadi hal yang sangat berharga dalam ekosistem digital karena dapat digunakan untuk berbagai kepentingan, mulai dari pelayanan publik, pemasaran, hingga pengambilan keputusan berbasis kecerdasan buatan. Namun, di sisi lain, data pribadi juga merupakan elemen

yang sangat sensitif karena mencerminkan identitas dan eksistensi seseorang secara utuh, baik dalam aspek administratif, sosial, maupun psikologis (Kristanto, 2023).

Sensitivitas data pribadi tidak hanya terletak pada potensi penyalahgunaannya oleh pihak yang tidak bertanggung jawab, tetapi juga karena berkaitan langsung dengan hak privasi individu. Hak atas privasi adalah bagian dari hak asasi manusia yang dijamin oleh konstitusi. Di Indonesia, hak privasi telah mendapatkan pengakuan eksplisit dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD 1945), khususnya dalam Pasal 28G ayat (1) yang menyatakan bahwa *"Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi."* Dengan demikian, perlindungan data pribadi merupakan bentuk konkret dari perlindungan terhadap hak konstitusional warga negara, yang harus dijaga secara serius oleh negara, pelaku usaha, dan seluruh elemen masyarakat.

Dalam menggunakan aplikasi digital, tidak sedikit orang yang telah mengisi data pribadi secara elektronik di aplikasi yang digunakan, baik secara sadar maupun tidak. Hal ini membuat tindakan kriminal pada dunia internet, seperti peretasan meningkat. Peretasan banyak terjadi di *e-commerce* yang merupakan tempat dilakukannya kegiatan komersial secara online. Sebagai contoh adalah kasus pada tanggal 17 April 2020, yaitu peretasan aplikasi Tokopedia oleh peretas internasional sehingga terdapat 15 juta data pengguna Tokopedia diretas (Rahardjo et al., 2022). Selain itu, terdapat juga kasus kebocoran data sebanyak 1,2 juta data pengguna pada *e-commerce* Bhineka.com (Lesmana et al., 2022). Kasus-kasus tersebut mencerminkan lemahnya sistem keamanan siber dan kurangnya kesadaran pengguna, serta penyedia layanan digital terhadap urgensi perlindungan data pribadi.

Masyarakat Indonesia sendiri masih tergolong rendah dalam hal literasi digital, terutama terkait dengan kesadaran terhadap hak-hak privasi dan perlindungan data pribadi. Banyak pengguna yang masih abai dalam memberikan izin akses aplikasi terhadap informasi pribadi mereka tanpa memahami konsekuensinya. Perusahaan teknologi raksasa seperti Google, Facebook, dan Amazon juga memanfaatkan data pengguna untuk menyusun profil konsumen, menargetkan iklan, hingga mengembangkan produk berbasis prediksi algoritma. Dalam hal ini, kurangnya transparansi dari penyedia aplikasi dalam menjelaskan penggunaan data memperparah kondisi yang ada. Hal ini menunjukkan adanya kesenjangan antara perkembangan teknologi dengan kesiapan regulasi dan edukasi masyarakat (Gani, 2023).

Menanggapi permasalahan tersebut, Pemerintah Indonesia telah mengambil langkah dengan mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data

Pribadi (UU PDP). UU ini menjadi dasar hukum yang penting dalam sistem hukum nasional untuk menjamin hak atas perlindungan data pribadi. UU PDP mengatur berbagai aspek perlindungan data, mulai dari hak subjek data, kewajiban pengendali dan pemroses data, hingga sanksi administratif dan pidana bagi pelanggaran. Namun, implementasi dari UU ini membutuhkan sinergi lintas sektor, penguatan kelembagaan, dan integrasi teknologi yang akuntabel (Alfitri et al., 2024). Dalam hal ini, aplikasi digital memegang peranan ganda, yaitu di satu sisi sebagai pihak yang berpotensi mengeksploitasi data pribadi, tetapi di sisi lain dapat menjadi alat strategis dalam meningkatkan kesadaran hukum masyarakat terhadap pentingnya menjaga hak privasi. Melalui desain antarmuka yang ramah pengguna, penyampaian informasi yang transparan, dan fitur kontrol data yang terintegrasi, aplikasi digital dapat mendorong partisipasi aktif pengguna dalam mengelola informasi pribadinya. Aplikasi juga dapat menjadi sarana edukasi interaktif yang menyampaikan nilai-nilai hak asasi manusia, perlindungan hukum, serta etika digital dalam kehidupan sehari-hari.

Tantangan utama dalam mewujudkan aplikasi yang berorientasi pada perlindungan hak privasi adalah ketimpangan antara kepentingan ekonomi penyedia layanan digital dan prinsip-prinsip perlindungan data. Banyak aplikasi yang beroperasi dengan model bisnis berbasis pengumpulan dan analisis data besar (*big data*), yang cenderung mengaburkan batas antara kepentingan komersial dan hak individu (Deni et al., 2025). Oleh karena itu, dibutuhkan regulasi yang ketat dan mekanisme pengawasan independen untuk memastikan bahwa pemrosesan data pribadi dilakukan secara adil, proporsional, dan sesuai dengan prinsip hukum yang berlaku.

Di samping itu, penting untuk mengembangkan budaya hukum di masyarakat yang menempatkan hak atas privasi sebagai bagian dari kewargaan digital (*digital citizenship*). Kesadaran hukum tidak hanya lahir dari instrumen normatif seperti undang-undang, tetapi juga dari proses pembelajaran sosial yang berkelanjutan. Pendidikan digital yang menanamkan nilai-nilai tanggung jawab, kehati-hatian, dan kontrol diri dalam penggunaan teknologi akan menjadi pondasi dalam memperkuat perlindungan data pribadi (Basuki et al., 2022). Dengan demikian, tinjauan hukum terhadap aplikasi digital dalam meningkatkan kesadaran perlindungan hak privasi data pribadi menjadi sangat relevan dan mendesak untuk dilakukan. Kajian ini tidak hanya akan memperkaya wacana akademik tentang hubungan antara hukum dan teknologi, tetapi juga memberikan kontribusi praktis dalam merumuskan kebijakan publik yang inklusif dan responsif terhadap tantangan zaman digital. Dalam jangka panjang, diharapkan lahir ekosistem digital yang lebih aman, adil, dan berkeadilan sosial, dimana setiap individu merasa terlindungi dan berdaya dalam menentukan nasib informasi pribadinya.

2. METODE PENELITIAN

Metode penelitian yang digunakan dalam studi ini adalah pendekatan kualitatif dengan jenis penelitian hukum normatif. Pendekatan ini dipilih karena penelitian berfokus pada kajian mendalam terhadap norma hukum, khususnya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, serta analisis terhadap peran aplikasi digital dalam meningkatkan kesadaran masyarakat terkait hak atas privasi data pribadi. Data yang dikumpulkan bersumber dari dokumen hukum primer seperti peraturan perundang-undangan, serta sumber sekunder berupa jurnal ilmiah dan buku. Pengumpulan data dilakukan melalui studi kepustakaan, yang kemudian dianalisis secara deskriptif dan komparatif. Analisis deskriptif digunakan untuk menguraikan isi dan makna regulasi, sedangkan analisis komparatif dilakukan untuk membandingkan kerangka hukum Indonesia dengan regulasi internasional seperti *General Data Protection Regulation* (GDPR) di Uni Eropa, *Personal Data Protection Act* (PDPA) 2012 di Singapura, *Personal Data Protection Act* (PDPA) pada tahun 2010 di Malaysia, *Personal Information Protection Act* (PIPA) tahun 2011 di Korea Selatan, dan *Personal Data (Privacy) Ordinance* (PDPO) tahun 2012 di Hongkong. Penelitian ini juga menyajikan kritik terhadap efektivitas implementasi aplikasi digital dalam mengedukasi masyarakat tentang hak privasi, serta mengevaluasi sejauh mana aplikasi-aplikasi tersebut sejalan dengan prinsip perlindungan data pribadi yang ditetapkan dalam peraturan perundang-undangan. Melalui metode ini, diharapkan penelitian dapat memberikan gambaran yang komprehensif dan kritis mengenai tantangan dan peluang peningkatan kesadaran hukum di era digital.

3. HASIL DAN PEMBAHASAN

Prinsip Hak Privasi terhadap data Pribadi

Dalam era digital yang kian maju, di mana interaksi manusia dengan teknologi semakin intens dan kompleks, prinsip perlindungan hak privasi terhadap data pribadi menjadi aspek yang semakin krusial. Kehidupan modern tidak dapat dilepaskan dari penggunaan berbagai aplikasi digital, baik dalam bidang komunikasi, layanan keuangan, pendidikan, hingga kesehatan yang semuanya menuntut pengguna untuk menyerahkan sebagian data pribadinya. Data pribadi yang dimaksud mencakup berbagai informasi yang dapat digunakan untuk mengidentifikasi individu secara langsung maupun tidak langsung, seperti nama lengkap, alamat, nomor telepon, alamat email, tanggal lahir, nomor induk kependudukan, informasi rekening bank, rekam medis, hingga kebiasaan digital seperti riwayat penelusuran atau preferensi belanja online (Muin, 2023).

Fenomena ini mengindikasikan bahwa setiap kali seseorang mengakses aplikasi digital, terdapat pertukaran data yang berlangsung antara pengguna dan penyedia layanan. Di satu sisi, hal ini membawa manfaat dalam hal efisiensi, personalisasi layanan, dan kemudahan akses informasi. Namun di sisi lain, praktik ini menyisakan kekhawatiran serius tentang potensi penyalahgunaan data pribadi dan pelanggaran hak privasi. Tanpa adanya perlindungan yang memadai, individu sangat rentan terhadap risiko kebocoran data, penipuan digital, pencurian identitas, dan bentuk-bentuk kejahatan siber lainnya (Azmi et al., 2024).

Prinsip perlindungan data pribadi sebenarnya merupakan bagian tak terpisahkan dari hak asasi manusia, khususnya hak atas privasi. Perlindungan ini tidak hanya mencakup keamanan teknis terhadap data, tetapi juga mencakup hak-hak fundamental individu seperti hak untuk mengetahui data apa yang dikumpulkan, untuk tujuan apa data tersebut digunakan, siapa saja yang memiliki akses terhadap data tersebut, dan bagaimana data tersebut dikelola serta disimpan (Angraini et al., 2023). Selain itu, individu juga memiliki hak untuk memberikan persetujuan atas penggunaan data pribadinya, hak untuk menarik kembali persetujuan tersebut, serta hak untuk meminta penghapusan atau koreksi data apabila terdapat ketidaktepatan (hak untuk dilupakan atau *right to be forgotten*) (Fachmi et al., 2023). Dengan demikian, prinsip ini menuntut transparansi, akuntabilitas, serta komitmen etis dari pihak-pihak yang mengelola data pribadi, baik itu sektor privat maupun publik. Perusahaan digital, instansi pemerintah, dan lembaga non-pemerintah yang mengelola data warga negara harus tunduk pada norma-norma perlindungan data yang tidak hanya bersifat administratif, tetapi juga menjunjung tinggi prinsip moral dan hukum yang melindungi martabat manusia.

Di dalam hukum Indonesia, prinsip perlindungan terhadap data pribadi mendapatkan legitimasi konstitusional yang kuat. Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 menegaskan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda di bawah kekuasaannya, serta berhak merasa aman dan terlindungi dari ancaman ketakutan akan tindakan kriminal. Ketentuan ini menjadi landasan moral dan hukum yang memperkuat perlunya regulasi khusus dalam ranah perlindungan data pribadi. Sejalan dengan perkembangan teknologi digital, kebutuhan akan kerangka hukum yang lebih komprehensif untuk menjamin perlindungan data pribadi pun semakin mendesak. Dengan demikian, Pemerintah Indonesia telah mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) yang menjadi dasar hukum penting dalam regulasi perlindungan data di Indonesia. Undang-undang ini memberikan definisi yang jelas tentang data pribadi, menetapkan hak-hak subjek data, serta

menetapkan kewajiban para pengendali dan prosesor data, termasuk sanksi terhadap pelanggaran.

Salah satu aspek penting dari UU PDP adalah pemberian wewenang kepada subjek data untuk mengontrol bagaimana data mereka digunakan. Individu dapat menuntut penjelasan atas alasan pengumpulan data, meminta penghapusan data yang sudah tidak relevan, serta memberikan atau menolak persetujuan atas pemrosesan data. Undang-undang ini juga memperkenalkan prinsip-prinsip dasar seperti prinsip *lawful*, *fair*, dan *transparent processing*, yang mengharuskan semua pengolahan data dilakukan secara sah, adil, dan transparan. Namun, keberadaan regulasi semata tidak cukup untuk menjamin perlindungan hak privasi data pribadi. Diperlukan kesadaran dan literasi digital yang tinggi dari masyarakat sebagai pengguna layanan digital. Dalam hal ini, aplikasi digital berpotensi memainkan peran penting tidak hanya sebagai alat pengumpul data, tetapi juga sebagai sarana edukasi dan pemberdayaan pengguna. Aplikasi yang dirancang dengan prinsip *privacy by design* dan *privacy by default* dapat membantu meningkatkan pemahaman masyarakat tentang hak-haknya sebagai subjek data, serta mendorong partisipasi aktif dalam menjaga privasi mereka (Sulistianingsih et al., 2023).

Sebagai contoh adalah aplikasi dapat dilengkapi dengan fitur notifikasi yang menginformasikan pengguna setiap kali data pribadi mereka diakses atau diproses. Selain itu, penyedia layanan dapat menyertakan penjelasan singkat dan mudah dipahami mengenai kebijakan privasi dan opsi pengaturan data, sehingga pengguna tidak merasa terjebak dalam istilah-istilah hukum yang rumit. Upaya ini akan menciptakan ekosistem digital yang lebih sehat, di mana pengguna memiliki kontrol lebih besar atas data mereka sendiri. Di sisi lain, pengawasan yang ketat dan penegakan hukum yang efektif juga menjadi elemen penting dalam mewujudkan perlindungan data pribadi. Pemerintah harus membentuk lembaga pengawas independen yang memiliki kewenangan untuk menyelidiki, memberikan sanksi, dan menyelesaikan sengketa yang berkaitan dengan pelanggaran data pribadi. Tanpa mekanisme pengawasan yang jelas, keberadaan UU PDP berisiko menjadi dokumen normatif semata yang tidak memberikan dampak substantif dalam praktiknya.

Peran Undang-Undang Perlindungan Data Pribadi di Indonesia

Pemerintah Indonesia menerbitkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) sebagai langkah konkret untuk menghadirkan perlindungan hukum yang menyeluruh terhadap hak individu atas data pribadinya. UU ini merupakan regulasi *lex specialis* yang mengatur secara terperinci berbagai aspek perlindungan data pribadi, termasuk definisi, prinsip, hak-hak pemilik data, kewajiban pengendali dan

prosesor data, serta mekanisme penegakan hukum. Undang-undang ini menjadi tonggak sejarah penting karena untuk pertama kalinya Indonesia memiliki kerangka hukum tunggal yang sejalan dengan prinsip-prinsip internasional seperti *General Data Protection Regulation* (GDPR) Uni Eropa (Fuad et al., 2025).

UU PDP secara eksplisit memberikan definisi data pribadi pada Pasal 1 angka 1 yang menyatakan bahwa “*Data Pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik.*”. Definisi ini bersifat luas dan inklusif, mencakup semua bentuk data, baik digital maupun fisik, yang memungkinkan identifikasi individu secara langsung maupun tidak langsung. Hal ini memberikan payung hukum yang kuat untuk berbagai bentuk pengolahan data dalam sistem digital maupun non-digital, seperti database rumah sakit, aplikasi keuangan, sistem absensi biometrik, dan lain sebagainya.

Peran UU PDP dalam aplikasi digital sangat signifikan karena mengatur secara rinci hak-hak pemilik data, atau subjek data. Pasal 5-15 UU PDP menetapkan serangkaian hak fundamental yang dimiliki oleh subjek data, yaitu hak atas informasi, hak untuk melakukan akses dan koreksi data pribadi, hak untuk mengakhiri pemrosesan, penghapusan atau pemusnahan data pribadi, serta hak untuk menarik kembali persetujuan yang telah diberikan sebelumnya. Ketentuan ini menandai perubahan paradigma yang penting dari pendekatan sebelumnya yang cenderung memihak kepada korporasi sebagai pemilik sistem. Kini, pengguna memiliki posisi tawar yang lebih seimbang terhadap penyedia aplikasi.

Hak-hak tersebut harus diimplementasikan secara nyata oleh para pengendali data pribadi, seperti perusahaan teknologi, lembaga layanan publik, dan pengembang aplikasi digital. Dalam Pasal 20-50 UU PDP, ditegaskan bahwa pengendali data wajib memastikan keakuratan, keutuhan, dan kerahasiaan data pribadi selama pemrosesan berlangsung. Pengendali juga diwajibkan untuk menerapkan langkah-langkah keamanan teknis dan administratif guna melindungi data dari ancaman, seperti pencurian, kebocoran, atau akses ilegal. Ketentuan ini mengimplikasikan perlunya audit keamanan data, penerapan enkripsi, otentikasi berlapis, serta pelatihan berkelanjutan bagi staf teknologi informasi dalam organisasi. Kemudian, ketentuan dalam Pasal 46 ayat (1) UU PDP menyatakan bahwa jika terjadi insiden pelanggaran data pribadi, pengendali data wajib melakukan pemberitahuan kepada subjek data dan otoritas terkait paling lambat 3x24 jam sejak ditemukannya pelanggaran. Transparansi ini sangat penting dalam membangun kepercayaan publik terhadap layanan digital dan menciptakan sistem pertanggungjawaban yang tegas bagi pelaku industri

teknologi. Ketentuan ini sejalan dengan praktik internasional yang mengedepankan keterbukaan atas insiden keamanan siber sebagai bentuk akuntabilitas.

UU PDP juga mengadopsi prinsip-prinsip umum yang dikenal dalam perlindungan data global seperti *lawfulness* (keterikatan hukum), *fairness* (keadilan), dan *transparency* (transparansi), sebagaimana termuat dalam Pasal 5 ayat (1) huruf a GDPR. Ini menunjukkan bahwa regulasi Indonesia telah mulai menyesuaikan diri dengan standar global, baik untuk meningkatkan kualitas perlindungan domestik, maupun memperkuat posisi Indonesia dalam kerja sama lintas negara di bidang digital. Hal ini menjadi penting dalam konteks perdagangan internasional dan pertukaran data lintas batas negara (*cross-border data transfer*), yang menuntut adanya kerangka hukum yang kompatibel dengan mitra internasional.

Dalam rangka meningkatkan kesadaran masyarakat terhadap pentingnya hak atas data pribadi, Pasal 63 ayat (2) UU PDP memberikan mandat kepada pemerintah untuk melakukan edukasi, sosialisasi, dan advokasi perlindungan data pribadi kepada masyarakat. Upaya ini dapat diwujudkan melalui berbagai kanal, termasuk aplikasi digital. Pengembang aplikasi dapat memanfaatkan momentum ini dengan menambahkan fitur-fitur edukatif seperti tutorial interaktif kebijakan privasi, sistem peringatan otomatis saat terjadi pelanggaran, atau modul pelatihan ringkas mengenai literasi digital. Kolaborasi antara pemerintah, pengembang teknologi, dan lembaga pendidikan menjadi sangat penting dalam menciptakan budaya perlindungan data pribadi yang kuat di Indonesia.

Di sisi kelembagaan, UU PDP mengatur pembentukan Otoritas Pelindungan Data Pribadi (OPDP) sebagai lembaga independen yang memiliki wewenang untuk mengawasi pelaksanaan undang-undang ini. Berdasarkan Pasal 58 hingga Pasal 60, OPDP memiliki tugas untuk menerima laporan pelanggaran, menyelidiki kasus, menjatuhkan sanksi administratif, serta memberikan rekomendasi kebijakan kepada pemerintah. Lembaga ini berfungsi sebagai penyeimbang antara kepentingan masyarakat dan pelaku industri dalam hal perlindungan data pribadi, serta menjadi garda terdepan dalam pengawasan terhadap aplikasi digital dan platform daring yang aktif di Indonesia.

Sanksi administratif dan pidana yang diatur dalam UU PDP mencerminkan keseriusan negara dalam menegakkan perlindungan data. Pasal 57 mengatur bahwa pelanggaran dapat dikenai sanksi administratif berupa teguran tertulis, penghentian sementara aktivitas pemrosesan, penghapusan data, hingga denda administratif maksimal 2% dari pendapatan tahunan pengendali data. Sementara itu, Pasal 67 hingga Pasal 69 mengatur ketentuan pidana bagi pelanggaran berat, seperti pengumpulan data tanpa dasar hukum, penyebaran data pribadi tanpa izin, dan pelanggaran terhadap prinsip pemrosesan. Pelanggaran ini dapat dijatuhi pidana

penjara maksimal 5 tahun dan/atau denda maksimal Rp50 miliar. Pengenaan sanksi ini diharapkan mampu menimbulkan efek jera bagi pelaku industri yang mengabaikan prinsip perlindungan data.

Dalam dunia akademik, UU PDP dapat menjadi kerangka acuan untuk pengembangan studi-studi lanjut mengenai hukum siber, etika digital, dan teknologi informasi. Institusi pendidikan tinggi diharapkan dapat merespons regulasi ini dengan menyusun kurikulum yang relevan serta mendorong riset-riset interdisipliner yang mengkaji dinamika perlindungan data dalam konteks lokal maupun global. Dengan hadirnya UU PDP, Indonesia telah menampakkan langkah strategis dalam memperkuat kedaulatan data nasional. Regulasi ini tidak hanya menjadi jaminan perlindungan terhadap individu, tetapi juga menjadi bagian penting dari upaya negara dalam menjaga ketahanan digital, mengurangi risiko kejahatan siber, serta meningkatkan kepercayaan masyarakat terhadap transformasi digital. Oleh karena itu, pemanfaatan aplikasi digital sebagai sarana edukasi publik dan peningkatan kesadaran terhadap hak privasi data pribadi perlu terus ditingkatkan secara progresif dan kolaboratif.

Perbandingan Peraturan Perlindungan Data Pribadi dengan Negara Lain

Perlindungan terhadap data pribadi telah menjadi agenda hukum yang penting di banyak negara seiring dengan meningkatnya pemanfaatan teknologi digital dan internet dalam kehidupan sehari-hari. Negara-negara di kawasan Asia, termasuk Singapura, Malaysia, Korea Selatan, dan Hong Kong telah lebih dahulu menerapkan regulasi khusus yang bertujuan untuk menjamin hak-hak individu atas data pribadinya. Kebijakan-kebijakan tersebut tidak hanya memberikan kerangka hukum yang jelas, tetapi juga memperkuat kesadaran masyarakat dan tanggung jawab penyelenggara sistem elektronik terhadap pentingnya menjaga kerahasiaan serta integritas data pribadi.

Di Singapura, regulasi utama yang mengatur perlindungan data pribadi adalah *Personal Data Protection Act* (PDPA) 2012, atau Undang-Undang Perlindungan Data Pribadi No. 26 Tahun 2012. Undang-undang ini memperkenalkan prinsip-prinsip perlindungan hukum atas data pribadi yang terintegrasi dalam praktik bisnis dan layanan publik. Salah satu aspek penting dari PDPA Singapura adalah pengakuan terhadap konsep *implied consent* atau persetujuan yang dianggap telah diberikan. Hal ini berarti bahwa dalam situasi tertentu, persetujuan eksplisit tidak selalu diperlukan apabila pengguna dianggap telah menyetujuinya melalui tindakan yang masuk akal, seperti penggunaan aplikasi setelah diberikan informasi terkait. Selain itu, undang-undang ini mengatur ketentuan yang tegas mengenai pelanggaran, baik dalam bentuk sanksi perdata maupun pidana. Denda yang dapat dijatuhkan kepada pelanggar

mencapai hingga SGD 1 juta (sekitar USD 790.000), dan hukuman penjara maksimal tiga tahun, tergantung pada tingkat pelanggaran yang dilakukan. Keberadaan sanksi ini menunjukkan keseriusan pemerintah Singapura dalam menjamin pelaksanaan hukum perlindungan data pribadi yang efektif (Suari et al., 2023).

Berbeda dari Singapura, Malaysia mengesahkan *Personal Data Protection Act* (PDPA) pada tahun 2010 melalui Undang-Undang Perlindungan Data Pribadi No. 709 Tahun 2010. Regulasi ini fokus pada perlindungan data pribadi dalam konteks transaksi komersial, yang menunjukkan bahwa fokus utama perlindungan adalah pada aktivitas bisnis dan ekonomi digital. PDPA Malaysia mengharuskan para pengendali data untuk mendapatkan persetujuan dari subjek data sebelum mengumpulkan, menyimpan, atau memproses informasi pribadi mereka. Undang-undang ini juga menjamin hak individu untuk mengakses, memperbarui, dan meminta penghapusan data pribadi mereka, serta memberikan landasan hukum terhadap transfer data lintas batas. Sebagai bagian dari mekanisme pengawasan, Malaysia membentuk *Personal Data Protection Commissioner* dan juga Komite Penasihat Perlindungan Data Pribadi yang bertugas menerima laporan serta memberikan rekomendasi kebijakan berkaitan dengan pelanggaran atau potensi ancaman terhadap perlindungan data. Ini menunjukkan bahwa Malaysia menekankan pada struktur institusional yang mendukung penegakan hukum dan pengawasan terhadap data pribadi (Mutiara et al., 2020).

Sementara itu, Korea Selatan memiliki salah satu kerangka hukum paling ketat dalam hal perlindungan data pribadi melalui *Personal Information Protection Act* (PIPA) yang disahkan pada tahun 2011. Peraturan ini dirancang untuk menjawab kebutuhan perlindungan data di tengah tingginya penetrasi internet dan digitalisasi layanan publik di Korea Selatan. Pasal 3 dari PIPA 2011 menjabarkan prinsip dasar perlindungan data pribadi, seperti batasan pengumpulan data, pembatasan akses, perlunya persetujuan subjek data, serta keharusan untuk menginformasikan tujuan penggunaan data kepada pengguna. Korea Selatan juga memperkenalkan prinsip *data minimization*, yang mengharuskan pengumpulan data seminimal mungkin dan hanya untuk tujuan yang jelas. Regulasi ini menempatkan tanggung jawab besar kepada pengendali data, serta memberikan hak luas bagi individu untuk mengakses, mengoreksi, dan menghapus data mereka. Tidak hanya itu, Korea Selatan juga mengatur secara ketat transfer data ke luar negeri, serta menerapkan denda tinggi dan hukuman pidana bagi pelanggaran serius, termasuk pemrosesan data tanpa persetujuan atau penyimpanan data yang tidak aman (Palito et al., 2021).

Hong Kong telah lebih dahulu memiliki kerangka hukum melalui *Personal Data (Privacy) Ordinance* (PDPO) yang pertama kali diundangkan pada tahun 1995 dan kemudian

diperbarui pada tahun 2012. Revisi ini dilakukan karena dinilai adanya kelemahan dalam implementasi prinsip-prinsip perlindungan data pribadi dalam versi awal undang-undang tersebut. PDPO mengatur berbagai prinsip dasar perlindungan data, termasuk prinsip pengumpulan data secara adil, akurat, dan untuk tujuan yang sah. Undang-undang ini memberikan wewenang kepada *Privacy Commissioner for Personal Data* untuk menangani pengaduan dan pelanggaran, serta memastikan organisasi mematuhi prinsip-prinsip hukum terkait perlindungan data. Revisi tahun 2012 memperkuat sanksi terhadap pelanggaran dan menambahkan aturan mengenai penggunaan data untuk tujuan pemasaran langsung, dengan mengharuskan adanya persetujuan eksplisit dari subjek data. Dengan sistem ini, Hong Kong berupaya menyeimbangkan antara kebutuhan bisnis dan perlindungan hak privasi individu di era digital (Faizah et al., 2023).

Dari keempat negara yang dianalisis, terlihat bahwa meskipun masing-masing memiliki pendekatan yang berbeda, ada beberapa kesamaan dalam prinsip dasar perlindungan data pribadi, yaitu perlunya persetujuan subjek data, pembatasan penggunaan data untuk tujuan tertentu, hak akses dan koreksi data, serta penegakan hukum yang tegas melalui denda dan hukuman pidana. Perbedaan utamanya terletak pada cakupan dan pendekatan penegakan hukum. Singapura, misalnya, lebih fleksibel dengan pengakuan terhadap implied consent, sedangkan Korea Selatan lebih ketat dengan prinsip minimisasi data dan pembatasan transfer lintas batas. Malaysia menekankan pada kerangka institusional, sedangkan Hong Kong lebih fokus pada pengaturan penggunaan data dalam aktivitas komersial, terutama pemasaran langsung.

Jika dibandingkan dengan Indonesia, yang baru saja memiliki Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), maka jelas bahwa Indonesia masih berada pada tahap awal dalam proses implementasi hukum perlindungan data yang efektif. Meskipun UU PDP mengadopsi banyak prinsip serupa, seperti persetujuan eksplisit, hak akses dan koreksi, serta kewajiban perlindungan oleh pengendali data, namun tantangan terbesarnya adalah pada sisi penegakan hukum dan kesadaran publik. Negara-negara seperti Singapura dan Korea Selatan telah membuktikan bahwa keberhasilan implementasi regulasi bergantung pada konsistensi penegakan, kapasitas lembaga pengawas, serta kampanye kesadaran publik yang intensif. Oleh karena itu, penting bagi Indonesia untuk belajar dari praktik-praktik terbaik yang telah dilakukan negara-negara tersebut, baik dalam hal perumusan kebijakan, penguatan kelembagaan, maupun edukasi publik secara digital.

Dengan mengkaji dan membandingkan praktik perlindungan data pribadi di negara lain, dapat disimpulkan bahwa efektivitas suatu undang-undang tidak hanya ditentukan oleh kualitas

redaksional dan prinsip-prinsip yang diadopsi, tetapi juga oleh mekanisme implementasi dan daya dukung institusional. Dalam hal ini, aplikasi digital dapat memainkan peran signifikan untuk meningkatkan kesadaran masyarakat tentang pentingnya hak atas privasi data pribadi. Namun, aplikasi tersebut hanya akan berhasil apabila didukung oleh regulasi yang kuat dan konsisten serta pengawasan yang memadai. Perbandingan internasional ini menjadi refleksi penting bagi Indonesia dalam merumuskan strategi perlindungan data pribadi yang adaptif, komprehensif, dan berorientasi pada kepentingan masyarakat luas di era digital.

4. KESIMPULAN DAN SARAN

Perkembangan teknologi digital telah menciptakan dinamika baru dalam pengelolaan data pribadi, yang menuntut respons hukum yang cepat dan adaptif. Aplikasi digital tidak hanya menjadi alat yang berpotensi mengeksploitasi informasi pribadi, tetapi juga berpeluang menjadi instrumen strategis dalam meningkatkan kesadaran masyarakat akan pentingnya hak atas privasi. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi memberikan kerangka hukum yang penting untuk menjamin hak individu terhadap data pribadinya, dengan mengatur hak-hak subjek data, kewajiban pengendali data, serta mekanisme sanksi yang tegas. Namun, keberhasilan implementasi UU tersebut sangat bergantung pada literasi digital masyarakat, kepatuhan pelaku industri, serta kapasitas lembaga pengawas yang ditunjuk. Oleh karena itu, sinergi antara pemerintah, penyedia teknologi, dan institusi pendidikan menjadi krusial dalam menciptakan budaya hukum digital yang sehat dan partisipatif. Pendekatan multidisipliner dan kolaboratif perlu terus dikembangkan untuk memastikan bahwa transformasi digital berlangsung sejalan dengan perlindungan hak asasi manusia, khususnya hak atas privasi dan keamanan data pribadi.

DAFTAR REFERENSI

- Alfitri, N. A., et al. (2024). Perlindungan terhadap data pribadi di era digital berdasarkan Undang-Undang Nomor 27 Tahun 2022. *Journal Social Society*, 4(2), 92-111.
- Angraini, N. K., et al. (n.d.). Perlindungan hukum data pribadi dalam perspektif hak asasi manusia. *Indonesian Journal of Legality of Law*, 7(1), 46-51.
- Azmi, M. N. A., et al. (2024). Analisa kasus kebocoran data pada Bank Indonesia dalam sistem perbankan. *Jurnal Multidisiplin Ilmu Akademik*, 1(6), 448-458.
- Basuki, U., et al. (2022). Langkah strategis menangkal hoax: Suatu pendekatan kebijakan dan hukum. *Jurnal Hukum Caraka Justitia*, 2(1), 1-22.
- Deni, A., et al. (2025). *Perekonomian Indonesia 4.0 (Edisi 1)*. CV. Rey Media Grafika.

Fachmi, A., et al. (2023). Analisis bibliometrik prinsip hak untuk dilupakan (right to be forgotten) dalam penelitian kearsipan yang terindeks di Dimensions.Ai. Jurnal Imam Bonjol: Kajian Ilmu Informasi dan Perpustakaan, 7(2), 136-151.

Faizah, A. F., et al. (2023). Penguatan perlindungan data pribadi melalui otoritas pengawas di Indonesia berdasarkan perbandingan hukum Hong Kong dan Singapura. Hakim: Jurnal Ilmu Hukum dan Sosial, 1(3), 1-27.

Fuad, F., et al. (2025). Desain perlindungan hukum bagi konsumen dan data pribadi untuk kegiatan usaha menggunakan fintech di Indonesia. Jurnal Rectum, 7(1), 176-187.

Gani, T. A. (2023). Kedaulatan data digital untuk integritas bangsa (Edisi 1). Syiah Kuala University Press.

General Data Protection Regulation (GDPR)

Kristanto, A. P. (2023). Perlindungan terhadap data pribadi dalam aplikasi digital sebagai bentuk perlindungan hak asasi manusia. Unes Law Review, 5(3), 952-960.

Lesmana, C. S. A. T., et al. (2022). Urgensi Undang-Undang Perlindungan Data Pribadi dalam menjamin keamanan data pribadi sebagai pemenuhan hak atas privasi masyarakat Indonesia. In Prosiding Seminar Nasional Hukum, Kebijakan Publik, Hak Asasi Manusia dan Keadilan (Sentuhan Keadilan 2022), 1, 37-41.

Makarim, E. (2019). Cyber Law: Aspek Hukum Teknologi Informasi. Rajawali Pers.

Muin, I. (2023). Perlindungan data pribadi dalam platform e-commerce guna peningkatan pembangunan ekonomi digital Indonesia. MJP Journal Law and Justice (MJPJLJ), 1(2), 81-91.

Mutiara, U., et al. (2020). Perlindungan data pribadi sebagai bagian dari hak asasi manusia atas perlindungan diri pribadi. Indonesian Journal of Law and Policy Studies, 1(1), 43-55.

Palito, J., et al. (2021). Urgensi pembentukan pengaturan perlindungan data pribadi di Indonesia serta komparasi pengaturan di Jepang dan Korea Selatan. Supremasi Hukum, 17(1), 23-33.

Rahardjo, R. D., et al. (2022). Kesesuaian Permenkominfo Nomor 05 Tahun 2020 dengan prinsip kebebasan berpendapat dan berekspresi dalam hak asasi manusia. Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance, 2(2), 472-486.

Suari, K. R. A., et al. (2023). Menjaga privasi di era digital: Perlindungan data pribadi di Indonesia. Jurnal Analisis Hukum (JAH), 6(1), 132-146.

Sulistianingsih, D., et al. (2023). Tata kelola perlindungan data pribadi di era metaverse (telaah yuridis Undang-Undang Perlindungan Data Pribadi). Jurnal Masalah-Masalah Hukum, 52(1), 97-106.

Undang-Undang Dasar 1945

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820)

World Economic Forum. (2024). The Global Risks Report 2024.