
IMPLEMENTASI PRINSIP *CONSENT* DALAM PELINDUNGAN DATA PRIBADI PADA APLIKASI DIGITAL

Oleh

Yireh Gamaliel¹, Deli Bunga Saravistha², Kadek Mery Herawati³

^{1,2,3}Fakultas Hukum, Universitas Mahendradatta, Denpasar, Indonesia

E-mail: ¹jirehgamaliel@gmail.com, ²delisaravistha@gmail.com,

³kadekmeryherawati@gmail.com

Article History:

Received: 09-06-2026

Revised: 29-06-2026

Accepted: 12-07-2026

Keywords:

Consent, Data Pribadi,
Aplikasi Digital,
Pelindungan Data
Pribadi, Hak Privasi.

Abstract: Pesatnya perkembangan aplikasi digital di Indonesia diikuti oleh meningkatnya pengumpulan dan pemrosesan data pribadi, namun juga memunculkan berbagai kasus kebocoran data, seperti pada Tokopedia, Bukalapak, dan BRI Life, yang menunjukkan masih lemahnya pelindungan data pribadi. Fenomena tersebut mencerminkan adanya kesenjangan antara law in the books dan law in practice dalam implementasi prinsip consent sebagai dasar legitimasi pemrosesan data pribadi. Secara normatif, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi telah mewajibkan adanya persetujuan yang sah dari subjek data, tetapi belum memberikan pengaturan yang komprehensif mengenai standar, mekanisme, dan batasan consent yang valid dalam ekosistem digital. Kondisi ini mengakibatkan praktik persetujuan masih didominasi mekanisme click-wrap agreement yang sering kali tidak disertai transparansi informasi dan pilihan yang bermakna bagi pengguna. Penelitian ini bertujuan menganalisis implementasi prinsip consent dalam pemrosesan data pribadi pada aplikasi digital serta mengidentifikasi faktor penyebab kesenjangan antara pengaturan normatif dan praktik pelaksanaannya. Penelitian menggunakan metode hukum normatif dengan pendekatan peraturan perundang-undangan dan pendekatan konseptual, serta dianalisis menggunakan Teori Pelindungan Data Pribadi, Teori Efektivitas Hukum, dan Teori Data Governance. Hasil penelitian menunjukkan bahwa implementasi prinsip consent belum berjalan optimal akibat belum adanya standar teknis yang jelas, rendahnya transparansi penyelenggara sistem elektronik, serta lemahnya mekanisme pengawasan. Oleh karena itu, diperlukan penguatan regulasi pelaksana dan sistem pengawasan yang efektif guna menjamin pelindungan data pribadi yang berorientasi pada hak subjek data di era digital.

PENDAHULUAN

Perkembangan teknologi informasi telah mendorong transformasi digital dalam berbagai aspek kehidupan masyarakat, termasuk pelayanan publik, perdagangan elektronik, media sosial, layanan keuangan digital, hingga pelayanan kesehatan berbasis elektronik.

Kondisi tersebut menyebabkan aktivitas pengumpulan dan pemrosesan data pribadi menjadi bagian yang tidak terpisahkan dari penggunaan aplikasi digital (Akbar, 2026). Data pribadi tidak lagi dipandang hanya sebagai identitas individu, tetapi telah berkembang menjadi aset yang memiliki nilai ekonomi, sosial, maupun strategis sehingga membutuhkan perlindungan hukum yang memadai (Fuad, 2025).

Pengakuan terhadap data pribadi sebagai bagian dari hak privasi juga telah berkembang dalam berbagai instrumen hukum internasional, termasuk *Universal Declaration of Human Rights*, *International Covenant on Civil and Political Rights*, serta *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)*. Di Indonesia, perlindungan tersebut diperkuat melalui Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi yang menempatkan persetujuan (*consent*) sebagai salah satu dasar sah pemrosesan data pribadi (Hadisuprpto, 2025).

Transformasi digital telah mengubah cara masyarakat berinteraksi, bertransaksi, dan mengakses berbagai layanan publik maupun privat. Perkembangan teknologi informasi dan komunikasi mendorong lahirnya berbagai aplikasi digital yang menawarkan kemudahan, efisiensi, dan konektivitas tanpa batas. Di balik berbagai manfaat tersebut, aktivitas digital pada dasarnya bergantung pada pengumpulan, penyimpanan, dan pemrosesan data pribadi pengguna sebagai fondasi utama penyelenggaraan layanan. Data pribadi tidak lagi dipandang sekadar sebagai informasi identitas seseorang, melainkan telah berkembang menjadi aset strategis yang memiliki nilai ekonomi tinggi dan menjadi komoditas dalam ekosistem ekonomi digital. Oleh karena itu, perlindungan data pribadi merupakan prasyarat fundamental dalam mewujudkan ruang digital yang aman, terpercaya, dan menghormati hak asasi manusia.

Dalam rezim perlindungan data pribadi modern, prinsip *consent* (persetujuan) merupakan salah satu dasar legitimasi pemrosesan data pribadi. Persetujuan tidak hanya dipahami sebagai formalitas administratif, tetapi merupakan manifestasi hak otonomi individu (*informational self-determination*) untuk menentukan apakah data pribadinya dapat dikumpulkan, digunakan, disimpan, atau dibagikan kepada pihak lain. Dengan demikian, *consent* yang sah harus diberikan secara bebas, spesifik, berdasarkan informasi yang memadai (*informed consent*), serta dapat ditarik kembali sewaktu-waktu. Prinsip tersebut menjadi instrumen penting dalam menjaga keseimbangan antara kepentingan penyelenggara sistem elektronik dalam memanfaatkan data dan hak pengguna untuk mempertahankan kontrol atas informasi pribadinya.

Namun demikian, perkembangan ekonomi digital juga diikuti oleh meningkatnya ancaman terhadap keamanan data pribadi. Indonesia dalam beberapa tahun terakhir menghadapi berbagai insiden kebocoran data berskala besar yang menunjukkan bahwa perlindungan data pribadi masih menghadapi tantangan serius. Kebocoran sekitar 91 juta data pengguna Tokopedia pada tahun 2020, sekitar 13 juta akun pengguna Bukalapak pada tahun 2021, serta sekitar 2 juta data nasabah BRI Life pada tahun 2022 memperlihatkan bahwa penyelenggara sistem elektronik belum sepenuhnya mampu menjamin keamanan data yang dipercayakan oleh pengguna (Indonesia, 2020). Kebocoran tersebut tidak hanya menimbulkan kerugian ekonomi, tetapi juga meningkatkan risiko pencurian identitas, penyalahgunaan data, penipuan digital, hingga pelanggaran hak atas privasi (Indonesia,

2022). Fenomena sosial ini menunjukkan bahwa meningkatnya digitalisasi belum diimbangi dengan tata kelola pemrosesan data pribadi yang akuntabel (Mutiara, 2025).

Permasalahan tersebut memperlihatkan adanya kesenjangan antara *law in the books* dan *law in practice*. Secara normatif, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi telah menempatkan persetujuan sebagai salah satu dasar yang sah dalam pemrosesan data pribadi serta memberikan berbagai hak kepada subjek data untuk mengendalikan informasi mengenai dirinya. Akan tetapi, dalam praktiknya, persetujuan pengguna masih didominasi oleh mekanisme *click-wrap agreement*, yaitu persetujuan melalui tombol "setuju" terhadap syarat dan ketentuan yang panjang, kompleks, dan sulit dipahami. Kondisi tersebut menyebabkan pengguna pada umumnya memberikan persetujuan tanpa memperoleh informasi yang memadai mengenai tujuan pemrosesan, ruang lingkup penggunaan data, jangka waktu penyimpanan, maupun kemungkinan distribusi data kepada pihak ketiga. Akibatnya, persetujuan yang diberikan lebih bersifat formal daripada substantif.

Fenomena tersebut dikenal sebagai *illusory consent*, yaitu keadaan ketika persetujuan secara yuridis dianggap telah diberikan, tetapi secara substansial tidak mencerminkan kehendak yang bebas, spesifik, dan terinformasi dari subjek data. Dalam praktik aplikasi digital, *illusory consent* mengakibatkan penyelenggara sistem elektronik memperoleh legitimasi formal untuk memproses data pribadi dalam cakupan yang sangat luas, sementara pengguna kehilangan kendali terhadap data yang telah diserahkannya (Haley, 2025). Kondisi ini memperlihatkan bahwa keberadaan persetujuan secara administratif belum tentu menjamin terpenuhinya prinsip pelindungan data pribadi maupun perlindungan hak atas privasi secara efektif (Mutiara, 2025).

Selain kesenjangan implementasi, penelitian ini juga menemukan adanya kesenjangan normatif (*normative gap*) dalam pengaturan hukum positif Indonesia. Pasal 20 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi memang mewajibkan adanya dasar yang sah dalam pemrosesan data pribadi, termasuk persetujuan dari subjek data. Namun, ketentuan tersebut belum memberikan parameter yang jelas mengenai bentuk, mekanisme, standar transparansi, maupun indikator persetujuan yang benar-benar memenuhi prinsip *freely given*, *specific*, *informed*, dan *unambiguous consent* sebagaimana berkembang dalam rezim pelindungan data pribadi internasional. Sebelum berlakunya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, pengaturan mengenai persetujuan juga masih tersebar dalam berbagai peraturan sektoral, seperti Pasal 26 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya, yang hanya mengatur persetujuan secara umum tanpa memberikan standar operasional yang komprehensif. Fragmentasi pengaturan tersebut menimbulkan ketidakseragaman dalam praktik pemrosesan data pribadi oleh penyelenggara sistem elektronik (Fuad, 2025).

Permasalahan tersebut menunjukkan bahwa tantangan utama pelindungan data pribadi di Indonesia tidak lagi terletak pada ketiadaan regulasi, melainkan pada efektivitas implementasi norma hukum dalam menjawab kompleksitas ekosistem digital. Oleh karena itu, penelitian ini menggunakan Teori Pelindungan Data Pribadi untuk menganalisis hak kontrol individu atas data pribadinya, Teori Efektivitas Hukum untuk mengkaji kesesuaian antara norma hukum dan implementasinya dalam masyarakat, serta Teori *Data Governance* untuk menilai tata kelola pemrosesan data oleh penyelenggara sistem elektronik

berdasarkan prinsip transparansi, akuntabilitas, dan keamanan informasi (Akbar, 2026). Berdasarkan uraian tersebut, penelitian ini menjadi penting untuk menganalisis implementasi prinsip *consent* dalam pengumpulan dan pemrosesan data pribadi pada aplikasi digital berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, sekaligus mengidentifikasi faktor-faktor yang menyebabkan terjadinya kesenjangan antara pengaturan normatif dan praktik pelaksanaannya. Hasil penelitian diharapkan dapat memberikan rekomendasi bagi penyempurnaan regulasi pelaksana, penguatan mekanisme pengawasan, serta pembentukan standar *consent* yang lebih transparan, akuntabel, dan berorientasi pada perlindungan hak subjek data dalam ekosistem digital Indonesia.

METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif dengan menggunakan pendekatan peraturan perundang-undangan (*statutory approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan perbandingan (*comparative approach*). Bahan hukum primer terdiri atas Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, serta instrumen hukum internasional yang berkaitan dengan pelindungan data pribadi. Bahan hukum sekunder diperoleh melalui buku, jurnal ilmiah, hasil penelitian, dan dokumen kebijakan. Seluruh bahan hukum dianalisis secara kualitatif menggunakan metode deskriptif-analitis dengan menitikberatkan pada sinkronisasi norma, penerapan prinsip *consent*, serta kesesuaiannya dengan teori hukum dan standar internasional.

HASIL DAN PEMBAHASAN

A. Implementasi Prinsip *Consent* Berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

Prinsip *consent* merupakan salah satu pilar utama dalam rezim pelindungan data pribadi karena menjadi dasar legitimasi hukum bagi setiap kegiatan pengumpulan dan pemrosesan data pribadi. Dalam paradigma modern pelindungan data pribadi, persetujuan tidak lagi dipandang sebagai formalitas administratif semata, melainkan sebagai perwujudan hak otonomi individu (*informational self-determination*) untuk menentukan bagaimana data pribadinya dikumpulkan, digunakan, disimpan, diungkapkan, maupun dihapus. Dengan demikian, implementasi prinsip *consent* harus dipahami sebagai mekanisme perlindungan hak subjek data, bukan sekadar instrumen yang memberikan kewenangan kepada pengendali data untuk memproses informasi pribadi.

Pengaturan mengenai persetujuan dalam hukum Indonesia memperoleh dasar hukum yang lebih komprehensif melalui Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Sebelumnya, pengaturan mengenai persetujuan hanya tersebar dalam berbagai peraturan sektoral, terutama Pasal 26 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang pada prinsipnya mensyaratkan adanya persetujuan atas penggunaan data pribadi seseorang. Namun, ketentuan tersebut belum mengatur secara rinci mengenai standar persetujuan, hak subjek

data, maupun kewajiban pengendali data. Kehadiran Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menjadi tonggak penting karena membangun rezim pelindungan data pribadi yang lebih sistematis dengan menempatkan persetujuan sebagai salah satu dasar sah pemrosesan data pribadi.

Secara normatif, Pasal 20 ayat (1) Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menentukan bahwa pemrosesan data pribadi hanya dapat dilakukan apabila memiliki dasar pemrosesan yang sah, salah satunya adalah persetujuan yang diberikan secara eksplisit oleh subjek data pribadi. Ketentuan ini menunjukkan bahwa persetujuan bukan satu-satunya dasar hukum pemrosesan data, namun merupakan dasar yang paling dominan dalam penyelenggaraan aplikasi digital, terutama pada platform e-commerce, media sosial, financial technology, layanan kesehatan digital, maupun penyelenggara sistem elektronik lainnya. Secara legal reasoning, ketentuan tersebut memberikan keseimbangan antara kepentingan pengendali data dalam menjalankan kegiatan usaha dan hak subjek data untuk mempertahankan kontrol atas informasi mengenai dirinya.

Lebih lanjut, implementasi prinsip consent tidak dapat dilepaskan dari pengaturan mengenai hak subjek data pribadi sebagaimana diatur dalam Pasal 5 sampai dengan Pasal 15 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Ketentuan tersebut memberikan hak kepada setiap individu untuk memperoleh informasi mengenai identitas pengendali data, tujuan pemrosesan, dasar hukum pemrosesan, akses terhadap data pribadi, perbaikan data, penghapusan data, pembatasan pemrosesan, hingga hak untuk menarik kembali persetujuan. Dengan demikian, persetujuan dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi tidak berdiri sendiri, tetapi merupakan bagian dari sistem pelindungan data pribadi yang menempatkan individu sebagai pemegang kendali (*data subject control*) atas data pribadinya.

Dari perspektif doktrin, implementasi consent harus memenuhi prinsip autonomi individu sebagaimana dikembangkan oleh Alan F. Westin dalam teori *privacy as control*. Menurut teori ini, hak atas privasi memberikan kewenangan kepada individu untuk menentukan kapan, bagaimana, dan sejauh mana informasi mengenai dirinya dapat dikomunikasikan kepada pihak lain. Persetujuan yang diberikan tanpa informasi yang memadai atau tanpa adanya pilihan yang nyata tidak memenuhi esensi perlindungan privasi karena individu kehilangan kendali atas penggunaan data pribadinya. Oleh karena itu, validitas persetujuan tidak hanya diukur dari adanya tindakan menekan tombol "setuju", tetapi juga dari terpenuhinya unsur kebebasan, pemahaman, dan kesadaran subjek data terhadap konsekuensi hukum dari persetujuan tersebut.

Dalam praktik penyelenggaraan aplikasi digital di Indonesia, implementasi prinsip consent masih menghadapi berbagai permasalahan. Sebagian besar penyelenggara sistem elektronik menggunakan mekanisme *click-wrap agreement*, yaitu persetujuan yang diberikan melalui satu klik terhadap syarat dan ketentuan penggunaan layanan. Secara formal mekanisme tersebut memenuhi unsur adanya persetujuan, namun secara substantif belum tentu mencerminkan persetujuan yang sah. Dokumen kebijakan privasi umumnya disusun dalam bahasa hukum yang kompleks, memuat klausula yang panjang, serta memberikan ruang yang sangat luas kepada penyelenggara sistem elektronik untuk mengumpulkan, menggunakan, menganalisis, bahkan membagikan data kepada pihak ketiga. Dalam kondisi demikian, pengguna cenderung memberikan persetujuan semata-mata agar

dapat mengakses layanan tanpa benar-benar memahami konsekuensi hukum dari persetujuan yang diberikan.

Fenomena tersebut menunjukkan bahwa implementasi prinsip consent di Indonesia masih didominasi oleh pendekatan formalistik, bukan substantif. Persetujuan diperlakukan sebagai syarat administratif untuk memenuhi ketentuan peraturan perundang-undangan, sementara esensi perlindungan hak subjek data belum sepenuhnya terwujud. Kondisi ini melahirkan praktik yang dalam berbagai kajian dikenal sebagai *illusory consent*, yaitu persetujuan yang secara formal dianggap sah tetapi secara substantif tidak mencerminkan kehendak bebas, spesifik, dan berdasarkan informasi yang memadai. Persetujuan yang demikian pada hakikatnya hanya memberikan legitimasi hukum kepada pengendali data tanpa benar-benar memberikan perlindungan kepada subjek data.

Permasalahan tersebut semakin terlihat apabila dikaitkan dengan prinsip transparansi yang diatur dalam Pasal 16 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, yang mewajibkan pemrosesan data dilakukan secara terbatas, spesifik, sah, transparan, akurat, bertanggung jawab, serta menjamin keamanan data pribadi. Dalam praktiknya, banyak aplikasi digital belum memberikan informasi yang mudah dipahami mengenai kategori data yang dikumpulkan, tujuan pemrosesan, jangka waktu penyimpanan, maupun identitas pihak ketiga yang menerima data. Akibatnya, pengguna kehilangan kesempatan untuk memberikan persetujuan secara sadar (*informed consent*), sehingga hak kontrol terhadap data pribadinya menjadi sangat terbatas.

Apabila dibandingkan dengan perkembangan rezim pelindungan data pribadi internasional, pengaturan dalam *General Data Protection Regulation* (GDPR) telah menetapkan standar yang lebih rinci mengenai persetujuan. Persetujuan harus diberikan secara bebas (*freely given*), spesifik (*specific*), berdasarkan informasi (*informed*), dan melalui tindakan yang tegas (*unambiguous indication*). Selain itu, subjek data berhak menarik kembali persetujuan dengan cara yang sama mudahnya ketika persetujuan diberikan. Meskipun Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi telah mengadopsi sebagian prinsip tersebut, pengaturan mengenai parameter teknis persetujuan masih relatif umum sehingga implementasinya sangat bergantung pada kebijakan masing-masing penyelenggara sistem elektronik.

Dalam praktik penegakan hukum internasional, beberapa putusan otoritas pelindungan data juga memperlihatkan bahwa persetujuan tidak dapat dianggap sah apabila diperoleh melalui klausula yang tidak transparan atau memaksa pengguna untuk menerima seluruh pemrosesan data sebagai syarat penggunaan layanan. Pendekatan tersebut menegaskan bahwa prinsip consent harus selalu dikaitkan dengan perlindungan hak individu, bukan semata-mata kepentingan ekonomi pengendali data. Pendekatan serupa relevan diterapkan dalam konteks Indonesia sebagai bentuk penguatan implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, terutama dalam menghadapi model bisnis digital yang semakin bergantung pada eksploitasi data pribadi.

Berdasarkan analisis tersebut, implementasi prinsip consent berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi pada dasarnya telah memiliki landasan normatif yang memadai. Namun, efektivitasnya masih menghadapi kendala berupa belum adanya standar teknis yang seragam mengenai persetujuan yang sah, dominannya penggunaan *click-wrap agreement*, rendahnya transparansi pemrosesan data,

serta lemahnya mekanisme pengawasan terhadap kepatuhan penyelenggara sistem elektronik. Oleh karena itu, penguatan implementasi prinsip consent memerlukan pembentukan regulasi pelaksana yang lebih operasional, pengawasan yang efektif oleh otoritas perlindungan data pribadi, serta penerapan prinsip *privacy by design* dan *privacy by default* agar persetujuan benar-benar menjadi instrumen perlindungan hak subjek data, bukan sekadar formalitas dalam pemrosesan data pribadi.

B. Kesenjangan antara *Law in the Books* dan *Law in Practice*

Salah satu persoalan utama dalam perlindungan data pribadi di Indonesia adalah masih lebarnya kesenjangan antara pengaturan hukum (*law in the books*) dan implementasi di lapangan (*law in practice*). Dalam perspektif Lawrence M. Friedman, efektivitas suatu sistem hukum tidak hanya ditentukan oleh substansi hukum (*legal substance*), tetapi juga oleh struktur hukum (*legal structure*) dan budaya hukum (*legal culture*) (Friedman, 2026). Dengan demikian, keberhasilan implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi tidak hanya bergantung pada keberadaan norma yang mengatur prinsip consent, tetapi juga pada efektivitas lembaga pengawas, kepatuhan penyelenggara sistem elektronik, serta tingkat kesadaran hukum masyarakat sebagai subjek data pribadi. Apabila ketiga komponen tersebut tidak berjalan secara seimbang, maka norma hukum akan kehilangan daya guna dalam praktik (Shalmont, 2026).

Secara normatif, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi telah mengatur bahwa pemrosesan data pribadi harus didasarkan pada dasar pemrosesan yang sah sebagaimana diatur dalam Pasal 20, disertai dengan kewajiban pengendali data untuk menerapkan prinsip transparansi, akuntabilitas, pembatasan tujuan, dan keamanan pemrosesan sebagaimana diatur dalam Pasal 16. Selain itu, Pasal 5 sampai dengan Pasal 15 memberikan berbagai hak kepada subjek data, termasuk hak memperoleh informasi, hak mengakses data, hak memperbaiki data, hak menghapus data, serta hak menarik kembali persetujuan. Secara konseptual, pengaturan tersebut telah mencerminkan prinsip-prinsip utama perlindungan data pribadi yang berkembang dalam rezim hukum internasional (Haley, 2025).

Namun demikian, implementasi norma tersebut masih menghadapi berbagai kendala. Praktik penyelenggaraan aplikasi digital menunjukkan bahwa mekanisme consent lebih banyak diposisikan sebagai syarat administratif agar pengguna dapat mengakses suatu layanan, bukan sebagai bentuk penghormatan terhadap hak otonomi subjek data. Sebagian besar aplikasi digital masih menggunakan mekanisme *click-wrap agreement* yang mengharuskan pengguna menyetujui seluruh syarat dan ketentuan tanpa diberikan alternatif yang proporsional. Persetujuan diberikan dalam waktu yang sangat singkat terhadap dokumen kebijakan privasi yang panjang, menggunakan istilah teknis yang sulit dipahami, dan sering kali tidak menjelaskan secara rinci tujuan pemrosesan, kategori data yang dikumpulkan, jangka waktu penyimpanan, maupun identitas pihak ketiga yang menerima data. Kondisi tersebut menyebabkan persetujuan kehilangan makna substantif sebagai bentuk kehendak bebas (*free will*) dari subjek data.

Fenomena tersebut memperlihatkan bahwa praktik consent di Indonesia masih didominasi oleh pendekatan *compliance-oriented*, yaitu sekadar memenuhi kewajiban administratif agar penyelenggara sistem elektronik dianggap telah memperoleh dasar hukum pemrosesan data. Padahal, secara filosofis, prinsip consent bertujuan memberikan kendali kepada individu terhadap data pribadinya. Ketika pengguna dipaksa memilih antara

menerima seluruh syarat atau tidak dapat menggunakan layanan (take it or leave it), maka persetujuan tersebut sesungguhnya tidak lagi diberikan secara bebas (freely given). Dalam doktrin perlindungan data pribadi, kondisi tersebut dikenal sebagai *illusory consent*, yaitu persetujuan yang secara formal memenuhi syarat hukum tetapi secara substansial tidak mencerminkan kehendak yang bebas, spesifik, dan berdasarkan informasi yang memadai.

Kesenjangan tersebut semakin nyata apabila dikaitkan dengan berbagai kasus kebocoran data pribadi yang terjadi dalam beberapa tahun terakhir. Kebocoran data pada platform Tokopedia, Bukalapak, maupun BRI Life menunjukkan bahwa keberadaan persetujuan pengguna tidak secara otomatis menjamin keamanan data pribadi setelah data tersebut berada dalam penguasaan pengendali data. Dalam praktiknya, pengguna telah memberikan persetujuan untuk pemrosesan data, tetapi tidak memperoleh jaminan bahwa data tersebut akan diproses sesuai prinsip keamanan informasi dan pembatasan tujuan. Dengan kata lain, persetujuan lebih banyak berfungsi sebagai dasar legal bagi pengumpulan data daripada sebagai instrumen perlindungan terhadap hak subjek data.

Apabila dianalisis menggunakan Teori Efektivitas Hukum yang dikemukakan oleh Soerjono Soekanto, rendahnya efektivitas implementasi prinsip *consent* dipengaruhi oleh beberapa faktor. Pertama, faktor hukum, yaitu masih adanya norma yang bersifat umum sehingga memerlukan pengaturan teknis lebih lanjut mengenai standar persetujuan yang sah dalam ekosistem digital. Kedua, faktor penegak hukum, yaitu belum optimalnya mekanisme pengawasan terhadap kepatuhan penyelenggara sistem elektronik serta belum efektifnya penerapan sanksi administratif maupun pidana. Ketiga, faktor sarana dan prasarana, yang berkaitan dengan kesiapan infrastruktur keamanan informasi dan tata kelola data pribadi. Keempat, faktor masyarakat, yaitu masih rendahnya literasi digital dan kesadaran pengguna mengenai hak-haknya sebagai subjek data. Kelima, faktor budaya hukum, yang menunjukkan bahwa praktik penggunaan aplikasi digital lebih didominasi oleh orientasi kemudahan akses daripada perlindungan hak privasi.

Dari perspektif Teori Data Governance, kesenjangan tersebut juga disebabkan oleh belum optimalnya penerapan prinsip tata kelola data yang baik (*good data governance*). Tata kelola data yang efektif mensyaratkan adanya transparansi, akuntabilitas, pembatasan tujuan (*purpose limitation*), minimalisasi data (*data minimization*), keamanan pemrosesan (*security safeguards*), dan mekanisme audit yang berkelanjutan. Dalam praktiknya, masih ditemukan kecenderungan penyelenggara sistem elektronik mengumpulkan data pribadi secara berlebihan (*excessive data collection*), meskipun tidak seluruh data tersebut relevan dengan layanan yang diberikan. Pengumpulan data yang tidak proporsional tersebut meningkatkan risiko penyalahgunaan maupun kebocoran data pribadi apabila terjadi kegagalan sistem keamanan.

Kesenjangan antara *law in the books* dan *law in practice* juga terlihat dari belum optimalnya pelaksanaan prinsip akuntabilitas (*accountability principle*). Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi telah mewajibkan pengendali data bertanggung jawab atas seluruh aktivitas pemrosesan data pribadi. Akan tetapi, dalam praktik, mekanisme pertanggungjawaban sering kali baru dilakukan setelah terjadi insiden kebocoran data. Pendekatan yang bersifat reaktif tersebut menunjukkan bahwa kepatuhan terhadap perlindungan data pribadi masih berorientasi pada penanganan akibat (*reactive compliance*), bukan pada pencegahan risiko (*preventive compliance*). Akibatnya,

perlindungan terhadap hak subjek data belum terlaksana secara optimal.

Apabila dibandingkan dengan perkembangan hukum perlindungan data pribadi internasional, *General Data Protection Regulation* menerapkan pendekatan yang lebih komprehensif melalui prinsip *accountability*, *privacy by design*, dan *privacy by default*. Pengendali data tidak hanya diwajibkan memperoleh persetujuan yang sah, tetapi juga harus mampu membuktikan bahwa seluruh proses pemrosesan data telah memenuhi prinsip perlindungan data sejak tahap perancangan sistem. Selain itu, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)* menekankan bahwa setiap negara wajib menjamin pemrosesan data dilakukan secara adil, sah, dan proporsional sebagai bentuk perlindungan terhadap hak privasi individu. Pendekatan tersebut menunjukkan bahwa efektivitas perlindungan data pribadi tidak cukup hanya mengandalkan keberadaan norma hukum, melainkan juga memerlukan tata kelola kelembagaan dan mekanisme pengawasan yang kuat.

Berdasarkan uraian tersebut, dapat disimpulkan bahwa kesenjangan antara *law in the books* dan *law in practice* dalam implementasi prinsip *consent* tidak disebabkan oleh ketiadaan pengaturan hukum, melainkan oleh belum optimalnya penerapan norma dalam praktik penyelenggaraan sistem elektronik. Norma dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi pada dasarnya telah memberikan dasar hukum yang memadai, namun efektivitasnya masih terkendala oleh belum adanya standar teknis *consent* yang seragam, lemahnya pengawasan, rendahnya kepatuhan penyelenggara sistem elektronik, serta minimnya literasi masyarakat mengenai hak atas data pribadi. Oleh karena itu, diperlukan penguatan regulasi pelaksana, pembentukan mekanisme pengawasan yang independen dan efektif, peningkatan kepatuhan melalui penerapan prinsip *privacy by design* dan *privacy by default*, serta penguatan literasi digital agar prinsip *consent* benar-benar berfungsi sebagai instrumen perlindungan hak subjek data, bukan sekadar formalitas administratif dalam pemrosesan data pribadi.

C. Analisis Berdasarkan Teori Hukum dan Instrumen Internasional

Implementasi prinsip *consent* dalam pemrosesan data pribadi perlu dianalisis tidak hanya berdasarkan ketentuan hukum positif Indonesia, tetapi juga melalui pendekatan teoritis dan standar hukum internasional yang berkembang dalam rezim perlindungan data pribadi. Analisis tersebut memberikan gambaran mengenai sejauh mana pengaturan dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi telah mampu mewujudkan perlindungan hak subjek data secara efektif sekaligus menjawab dinamika pemrosesan data dalam ekosistem digital. Pendekatan ini menggunakan Teori Pelindungan Data Pribadi, Teori Efektivitas Hukum, dan Teori *Data Governance* sebagai kerangka analisis terhadap implementasi prinsip *consent*.

Teori Pelindungan Data Pribadi menempatkan data pribadi sebagai bagian dari hak privasi yang memberikan kewenangan kepada setiap individu untuk mengendalikan informasi mengenai dirinya. Alan F. Westin menjelaskan bahwa hak atas privasi merupakan hak seseorang untuk menentukan kapan, bagaimana, dan sejauh mana informasi pribadi dikomunikasikan kepada pihak lain. Perspektif tersebut menunjukkan bahwa persetujuan bukan sekadar persyaratan administratif, melainkan instrumen hukum yang menjamin kendali individu terhadap seluruh proses pemrosesan data pribadi. Pengaturan dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi telah mengakomodasi prinsip tersebut melalui pengakuan terhadap hak subjek data untuk

memperoleh informasi, mengakses, memperbaiki, menghapus, serta menarik kembali persetujuan atas pemrosesan data pribadinya. Realitas implementasi menunjukkan bahwa hak tersebut belum sepenuhnya terlaksana karena mekanisme persetujuan masih didominasi oleh dokumen kebijakan privasi yang kompleks dan sulit dipahami (Samin, 2025). Kondisi tersebut mengurangi kemampuan subjek data untuk mengambil keputusan secara bebas dan terinformasi sehingga hak kontrol atas data pribadi menjadi terbatas.

Teori Efektivitas Hukum yang dikemukakan oleh Soerjono Soekanto menjelaskan bahwa keberhasilan penerapan suatu norma hukum dipengaruhi oleh lima faktor, yaitu substansi hukum, aparat penegak hukum, sarana atau fasilitas, masyarakat, dan budaya hukum. Analisis terhadap implementasi prinsip *consent* menunjukkan bahwa kelima faktor tersebut belum bekerja secara optimal. Substansi hukum dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi telah memberikan dasar hukum mengenai persetujuan sebagai salah satu dasar sah pemrosesan data pribadi, tetapi belum disertai parameter teknis yang rinci mengenai bentuk, mekanisme, dan standar persetujuan yang sah dalam layanan digital. Struktur hukum juga masih menghadapi tantangan berupa belum optimalnya pengawasan terhadap kepatuhan penyelenggara sistem elektronik. Faktor masyarakat memperlihatkan rendahnya literasi digital yang menyebabkan pengguna cenderung memberikan persetujuan tanpa memahami konsekuensi hukumnya. Budaya hukum dalam penyelenggaraan layanan digital masih berorientasi pada kemudahan akses layanan dibandingkan dengan perlindungan hak atas data pribadi. Kondisi tersebut menjelaskan bahwa keberadaan norma hukum belum secara otomatis menghasilkan kepatuhan dalam praktik.

Teori *Data Governance* memandang bahwa pengelolaan data pribadi harus dilakukan berdasarkan prinsip transparansi, akuntabilitas, keamanan, pembatasan tujuan, serta pengendalian risiko. Tata kelola data yang baik tidak hanya berorientasi pada kepatuhan terhadap regulasi, tetapi juga memastikan seluruh siklus pemrosesan data dilaksanakan secara bertanggung jawab. Implementasi prinsip tersebut dalam praktik masih menghadapi berbagai kelemahan, terutama berupa pengumpulan data secara berlebihan, penggunaan data di luar tujuan awal pemrosesan, kurangnya transparansi mengenai distribusi data kepada pihak ketiga, serta lemahnya mekanisme audit dan pengawasan internal. Persetujuan yang diberikan pengguna akhirnya hanya menjadi legitimasi formal bagi pengendali data tanpa diikuti tata kelola yang mampu menjamin keamanan dan integritas data pribadi. Praktik demikian menunjukkan bahwa prinsip *good data governance* belum sepenuhnya menjadi budaya kepatuhan dalam penyelenggaraan sistem elektronik.

Perspektif hukum internasional menunjukkan bahwa perlindungan data pribadi telah berkembang sebagai bagian dari perlindungan hak asasi manusia. Universal Declaration of Human Rights melalui Pasal 12 menegaskan bahwa tidak seorang pun boleh menjadi sasaran campur tangan sewenang-wenang terhadap kehidupan pribadi, keluarga, tempat tinggal, maupun korespondensinya. Prinsip tersebut diperkuat dalam International Covenant on Civil and Political Rights melalui Pasal 17 yang mewajibkan negara memberikan perlindungan hukum terhadap setiap bentuk intervensi yang melanggar privasi individu. Pengakuan tersebut menempatkan perlindungan data pribadi sebagai konsekuensi dari penghormatan terhadap martabat manusia dan hak atas kehidupan pribadi (Yokotani, 2025).

Standar internasional mengenai pemrosesan data pribadi berkembang lebih

komprehensif melalui Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (*Convention 108*). Instrumen ini mengatur bahwa setiap pemrosesan data pribadi harus dilakukan secara sah, adil, proporsional, dan hanya untuk tujuan yang jelas serta terbatas. Pengendali data juga diwajibkan menerapkan langkah-langkah keamanan yang memadai untuk mencegah akses, penggunaan, perubahan, maupun pengungkapan data secara tidak sah. Prinsip tersebut menunjukkan bahwa persetujuan bukan satu-satunya unsur perlindungan data pribadi, melainkan harus didukung oleh tata kelola data yang akuntabel dan sistem keamanan informasi yang efektif.

Pendekatan yang lebih rinci terdapat dalam General Data Protection Regulation yang menetapkan bahwa persetujuan harus diberikan secara bebas (*freely given*), spesifik (*specific*), berdasarkan informasi (*informed*), dan melalui tindakan yang tegas (*unambiguous*). Pengendali data wajib membuktikan bahwa persetujuan telah diperoleh secara sah serta memberikan kemudahan bagi subjek data untuk menarik kembali persetujuannya setiap saat. Pengaturan tersebut juga menerapkan prinsip *privacy by design* dan *privacy by default*, yaitu kewajiban membangun sistem pemrosesan data yang sejak awal dirancang untuk melindungi hak subjek data. Pendekatan tersebut memperlihatkan bahwa perlindungan data pribadi tidak hanya bergantung pada adanya persetujuan, tetapi juga pada desain sistem dan tata kelola yang menjamin keamanan data secara berkelanjutan.

Analisis terhadap Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menunjukkan bahwa substansi pengaturannya telah mengadopsi sebagian besar prinsip yang berkembang dalam instrumen internasional, terutama mengenai dasar sah pemrosesan data, pengakuan terhadap hak subjek data, serta kewajiban pengendali data untuk menerapkan prinsip keamanan dan akuntabilitas. Pengaturan tersebut masih memerlukan penguatan pada aspek implementasi melalui pembentukan regulasi pelaksana yang memberikan standar teknis mengenai mekanisme *consent*, kewajiban transparansi, tata kelola data, dan pengawasan terhadap penyelenggara sistem elektronik. Penguatan tersebut diperlukan agar prinsip *consent* tidak berhenti sebagai legitimasi formal dalam pemrosesan data pribadi, melainkan menjadi instrumen yang secara efektif menjamin penghormatan terhadap hak privasi dan perlindungan data pribadi sesuai dengan perkembangan hukum nasional maupun standar hukum internasional.

PENUTUP

A. Kesimpulan

Implementasi prinsip *consent* dalam pengumpulan dan pemrosesan data pribadi berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi telah memberikan landasan hukum yang lebih komprehensif dibandingkan pengaturan sebelumnya dengan menempatkan persetujuan sebagai salah satu dasar yang sah dalam pemrosesan data pribadi serta memberikan pengakuan terhadap hak-hak subjek data. Meskipun demikian, implementasi prinsip tersebut belum sepenuhnya mewujudkan perlindungan data pribadi secara efektif. Praktik penggunaan mekanisme *click-wrap agreement*, rendahnya transparansi informasi, pengumpulan data yang berlebihan, serta lemahnya pengawasan menunjukkan masih adanya kesenjangan antara *law in the books* dan *law in practice*, sehingga persetujuan yang diberikan pengguna sering kali hanya memenuhi aspek formal tanpa mencerminkan kehendak yang bebas, spesifik, dan berdasarkan informasi yang memadai.

Analisis berdasarkan Teori Pelindungan Data Pribadi menunjukkan bahwa hak kontrol individu terhadap data pribadinya belum terlindungi secara optimal karena mekanisme *consent* belum memberikan ruang yang memadai bagi subjek data untuk mengambil keputusan secara sadar dan independen. Teori Efektivitas Hukum membuktikan bahwa keberadaan norma dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi belum diikuti oleh efektivitas implementasi akibat belum optimalnya substansi pengaturan teknis, kelembagaan pengawasan, kepatuhan penyelenggara sistem elektronik, serta budaya hukum masyarakat. Sementara itu, Teori *Data Governance* memperlihatkan bahwa tata kelola data pribadi masih belum sepenuhnya menerapkan prinsip transparansi, akuntabilitas, pembatasan tujuan, minimalisasi data, dan keamanan informasi sebagaimana menjadi standar pengelolaan data yang baik.

Perspektif instrumen hukum internasional, khususnya *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, *General Data Protection Regulation*, *Universal Declaration of Human Rights*, dan *International Covenant on Civil and Political Rights*, menunjukkan bahwa pelindungan data pribadi merupakan bagian dari perlindungan hak asasi manusia yang menuntut persetujuan diberikan secara bebas, spesifik, berdasarkan informasi, serta didukung oleh sistem tata kelola data yang akuntabel. Oleh karena itu, penguatan implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi memerlukan regulasi pelaksana yang lebih operasional, pengawasan yang efektif, penerapan prinsip *privacy by design* dan *privacy by default*, serta peningkatan literasi digital masyarakat agar prinsip *consent* tidak hanya menjadi legitimasi formal pemrosesan data, tetapi benar-benar berfungsi sebagai instrumen perlindungan hak subjek data dalam ekosistem digital Indonesia.

B. Saran

Penguatan implementasi prinsip *consent* dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi memerlukan penyempurnaan regulasi pelaksana yang mengatur secara lebih jelas mengenai standar persetujuan yang sah, mekanisme pemberian dan pencabutan persetujuan, kewajiban transparansi informasi, serta pembatasan tujuan pemrosesan data pribadi. Efektivitas pengaturan tersebut perlu didukung oleh penguatan fungsi pengawasan melalui audit kepatuhan, evaluasi berkala terhadap penyelenggara sistem elektronik, dan penerapan sanksi yang proporsional untuk mendorong kepatuhan terhadap prinsip pelindungan data pribadi.

Penyelenggara sistem elektronik perlu mengintegrasikan prinsip *privacy by design*, *privacy by default*, dan *data minimization* dalam setiap tahapan pemrosesan data, disertai penyusunan kebijakan privasi yang sederhana, transparan, dan mudah dipahami oleh pengguna. Peningkatan literasi digital masyarakat mengenai hak-hak subjek data juga perlu dilakukan secara berkelanjutan agar pengguna mampu memberikan persetujuan secara sadar dan terinformasi. Sinergi antara pemerintah, penyelenggara sistem elektronik, dan masyarakat diharapkan dapat mewujudkan tata kelola data pribadi yang akuntabel, meningkatkan efektivitas pelindungan data pribadi, serta memperkecil kesenjangan antara *law in the books* dan *law in practice*.

DAFTAR PUSTAKA

- [1] Akbar, B., Rahim, N., Sinaga, C. and Niko, F., 2026. *Hukum Teknologi Digital: Regulasi, Tata Kelola dan Tantangan Masa Depan*. Serasi Media Teknologi.
- [2] Efendi, J., Ibrahim, J. and Rijadi, P., 2016. Metode penelitian hukum: Normatif dan empiris
- [3] Friedman, L.M. and Hayden, G.M., 2026. *American law: An introduction*. Oxford University Press.
- [4] Rahayu, D.P., SH, M. and Ke, S., 2020. Metode Penelitian Hukum. *Yogyakarta: Thafa Media*, pp.1-25.
- [5] Apriana, M. and Nugroho, A., 2025. Perlindungan Hukum bagi Perempuan Korban Tindak Pidana Kejahatan Artificial Intelligence (AI) Deepfake Berdasarkan Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual. *Journal of Social and Economics Research*, 7(1), pp.57-75.
- [6] Fuad, F., Baskara, R.R. and Urbaningrum, A., 2025. Desain perlindungan hukum bagi konsumen dan data pribadi untuk kegiatan usaha menggunakan fintech di Indonesia. *Jurnal Rectum: Tinjauan Yuridis Penanganan Tindak Pidana*, 7(1), pp.176-187.
- [7] Hadisuprpto, P. (2010). Ilmu Hukum (Pendekatan Kajiannya). *Inovatif: Jurnal Ilmu Hukum*, 2(4), 43180.
- [8] Hartati, A.Y. and Wahyuni, Y., 2021. Oligopoli di Negara Demokrasi: Praktek dan Kepentingan Ekonomi Politik Media Massa di Australia. *Spektrum*, 18(1).
- [9] Henakin, A.S.P., Kantikha, I.M., Helvis, H., Saragih, H. and Elawati, T., 2025. Pelindungan Hukum terhadap Kebocoran Data Pribadi Peserta Badan Penyelenggara Jaminan Sosial Ketenagakerjaan. *Almufi Jurnal Sosial Dan Humaniora*, 2(2), pp.117-128.
- [10] Haley, T., 2022. Illusory privacy. *Indiana Law Journal*, 98(75).
- [11] Mutiara, U. and Maulana, R., 2020. Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi. *Indonesian Journal of Law and Policy Studies*, 1(1).
- [12] Nabilla, R.Q., 2026. Perlindungan Hukum Bagi Konsumen dalam Transaksi Uang Elektronik Berdasarkan Peraturan Bank Indonesia No. 23/6/PBI/2021 dan Undang-Undang PDP No. 22 Tahun 2022 Tentang Perlindungan Data Pribadi. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, 4(2), pp.2474-2483.
- [13] Najib, A., 2023. Perlindungan Hukum Keamanan Data Cyber Notary Berdasarkan Undang-Undang Perlindungan Data Pribadi. *ACTA DIURNAL Jurnal Ilmu Hukum Kenotariatan*, 7(1), pp.43-59.
- [14] Niffari, H., 2020. Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain). *Jurnal Yuridis*, 7(1), pp.105-119.
- [15] Rahmawati¹, E.P., Nurhandayani, P. and Dwipayana, D.P., 2026. Ilusi Persetujuan (Consent Illusion) dalam Kebijakan Privasi Digital: Tinjauan Hukum terhadap Validitas Persetujuan Pengguna. *Jurnal Cendekia Hukum Indonesia (JCHI)*, 2(2).
- [16] Ramadhani, S.A., 2022. Komparasi Perlindungan Data Pribadi di Indonesia dan Uni Eropa. *Jurnal Hukum Lex Generalis*, 3(1), pp.73-84.
- [17] Rahman, F., 2021. Kerangka hukum perlindungan data pribadi dalam penerapan sistem pemerintahan berbasis elektronik di Indonesia. *Jurnal Legislasi Indonesia*, 18(1), pp.81-

102.

- [18] Rosadi, S.D., 2017. Prinsip-prinsip perlindungan data pribadi nasabah kartu kredit menurut ketentuan nasional dan implementasinya. *Sosiohumaniora*, 19(3), pp.206-212.
- [19] Shalmont, J., Chow, J.V. and Chen, N.E., 2026. Analisis Implementasi Pengelolaan Persampahan di Kota Medan Berdasarkan Teori Sistem Hukum Lawrence M. Friedman. *Begawan Abioso*, 17(1), pp.127-146.
- [20] Samin, H.H., 2024. Perlindungan hukum terhadap kebocoran data pribadi oleh pengendali data melalui pendekatan hukum progresif. *Jurnal Ilmiah Research Student*, 1(3), pp.1-15.
- [21] Suari, K.R.A. and Sarjana, I.M., 2023. Menjaga privasi di era digital: Perlindungan data pribadi di Indonesia. *Jurnal Analisis Hukum*, 6(1), pp.132-142.
- [22] Yokotani, Y., Kurnia, A.C., Wirazilmustaan, W. and Salfutra, R.D., 2025. Pengendalian Data Pribadi Dan Ruang Siber Oleh Platform Digital Big Data Global Terkait Kedaulatan Digital Indonesia. *PROGRESIF: Jurnal Hukum*, 19(1), pp.70-80.
- [23] CNN Indonesia, 2020, Kronologi Lengkap 91 Juta Akun Tokopedia Bocor dan Dijual, diakses pada laman: <https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual>
- [24] CNN Indonesia, 2022, Pada tahun 2021, kasus serupa terjadi pada platform Bukalapak, diakses pada laman: Pada tahun 2021, <https://www.cnnindonesia.com/ekonomi/20220222171416-92-762563/alasan-tokopedia-bukalapak-dan-shopee-masuk-daftar-pengawasan-as>
- [25] Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi
- [26] Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
- [27] Universal Declaration of Human Rights
- [28] International Covenant on Civil and Political Rights
- [29] General Data Protection Regulation
- [30] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)