

URGENSI HARMONISASI UNDANG-UNDANG DATA PRIBADI DAN HUKUM TELEMATIKA DALAM MEWUJUDKAN KEAMANAN SIBER DI INDONESIA

Ruli Vita Sari¹, Rina Arum Prastyanti²
vitaruli2@gmail.com¹, rina_arum@udb.ac.id²
Universitas Duta Bangsa Surakarta

Abstrak: Perkembangan pesat teknologi informasi dan komunikasi di Indonesia telah membawa dampak besar terhadap kehidupan sosial, ekonomi, dan hukum masyarakat. Di tengah meningkatnya penggunaan layanan digital, isu perlindungan data pribadi dan keamanan siber menjadi tantangan utama yang harus dihadapi negara. Penelitian ini bertujuan untuk menganalisis pentingnya harmonisasi antara Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dengan hukum telematika yang sudah ada, seperti UU Informasi dan Transaksi Elektronik (UU ITE) dan PP Nomor 71 Tahun 2019. Metode yang digunakan adalah yuridis normatif dengan pendekatan deskriptif analitis terhadap peraturan perundang-undangan dan dokumen hukum terkait. Hasil kajian menunjukkan bahwa tanpa harmonisasi, tumpang tindih norma dan ketidakjelasan kewenangan berpotensi melemahkan perlindungan hukum terhadap data pribadi dan menghambat upaya penanganan insiden siber. Harmonisasi bukan hanya kebutuhan teknis, tetapi juga merupakan fondasi strategis dalam memperkuat keamanan siber nasional dan membangun kepercayaan publik terhadap ekosistem digital. Oleh karena itu, harmonisasi regulasi harus menjadi prioritas lintas sektor untuk mewujudkan sistem hukum yang solid, adaptif, dan responsif terhadap tantangan era digital.

Kata Kunci: Harmonisasi, Perlindungan Data Pribadi, Hukum Telematika, Keamanan Siber, UU PDP, UU ITE.

***Abstract:** The rapid development of information and communication technology in Indonesia has had a significant impact on the social, economic, and legal aspects of society. Amid the increasing use of digital services, issues related to personal data protection and cybersecurity have become major challenges that the country must address. This study aims to analyze the importance of harmonizing Law Number 27 of 2022 on Personal Data Protection (PDP Law) with existing telematics laws, such as the Electronic Information and Transactions Law (ITE Law) and Government Regulation Number 71 of 2019. The method used is normative juridical with a descriptive-analytical approach to relevant laws and legal documents. The results of the study show that without harmonization, overlapping norms and unclear institutional authorities could weaken legal protection of personal data and hinder efforts to handle cyber incidents. Harmonization is not merely a technical necessity, but a strategic foundation for strengthening national cybersecurity and building public trust in the digital ecosystem. Therefore, regulatory harmonization must become a cross-sectoral priority to establish a legal system that is solid, adaptive, and responsive to the challenges of the digital era.*

***Keywords:** Harmonization, Personal Data Protection, Telematics Law, Cybersecurity, PDP Law, ITE Law.*

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi (TIK) telah mengubah cara manusia berinteraksi, bekerja, dan menjalani kehidupan sehari-hari. Di Indonesia, revolusi digital terjadi sangat cepat, didorong oleh tingginya penetrasi internet, penggunaan media sosial, dan adopsi teknologi digital dalam berbagai sektor, termasuk pemerintahan, layanan publik, keuangan, dan pendidikan. Fenomena ini menciptakan peluang besar untuk pertumbuhan ekonomi dan efisiensi pelayanan, namun pada saat yang sama juga menghadirkan tantangan serius, terutama terkait dengan keamanan siber dan perlindungan data pribadi.

Meningkatnya penggunaan teknologi digital di berbagai kehidupan menyebabkan data pribadi masyarakat terekspose dalam jumlah besar ke berbagai sistem elektronik. Data seperti identitas, lokasi, kebiasaan belanja, rekam medis, hingga preferensi politik, kini disimpan dan diproses oleh berbagai entitas, baik pemerintah maupun swasta. Sayangnya, perkembangan ini tidak selalu diikuti dengan sistem perlindungan data yang memadai. Kebocoran data, penyalahgunaan informasi pribadi, dan peretasan akun menjadi isu yang semakin sering terjadi dan mendapat sorotan publik.

Berikut adalah data statistik sumber <https://osnovacyber.com/blog/urgensi-perlindungan-data-pribadi-di-indonesia-butuh-aturan-ya>

Indikator / Fenomena	Statistik / Temuan
Kebocoran data (2022–2023)	113 kasus; >143 juta akun terdampak
Kebocoran data (Q2 2022)	1,04 juta akun (naik 143 % dari kuartal sebelumnya)
Anomali trafik serangan siber (2021)	1,6 miliar deteksi
Indeks Keamanan Siber (NCSI)	Peringkat 48 dari 176 negara (skor 63,64); nomor 5 di ASEAN
Literasi keamanan digital masyarakat	Skor 3,10 dari skala 5
Status harmonisasi UU PDP dan UU ITE	Transisi UU PDP hingga Oktober 2024; perguliran RPP PDP dan revisi UU ITE belum selesai

Kondisi tersebut mengindikasikan adanya kesenjangan regulasi dalam mengatur ekosistem digital secara menyeluruh. Sebelum tahun 2022, perlindungan terhadap data pribadi masih bersifat parsial dan tersebar di berbagai peraturan, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE), dan sejumlah peraturan menteri. Masing-masing aturan memiliki fokus dan cakupan yang berbeda, sehingga tidak mampu memberikan kerangka hukum yang komprehensif dalam menghadapi kompleksitas dunia digital.

Menyadari kebutuhan akan pengaturan yang lebih terstruktur dan kuat, pemerintah Indonesia mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Kehadiran UU ini merupakan tonggak penting dalam perlindungan hak privasi warga negara. UU PDP tidak hanya memberikan definisi yang lebih rinci mengenai data pribadi, tetapi juga menetapkan prinsip-prinsip pengolahan data, hak-hak subjek data, serta sanksi terhadap pelanggaran yang dilakukan oleh pengendali maupun prosesor data.

Namun demikian, lahirnya UU PDP tidak serta-merta menyelesaikan seluruh persoalan dalam ranah hukum digital. Justru, keberadaan regulasi baru ini menuntut adanya proses harmonisasi dengan regulasi sebelumnya, khususnya yang berkaitan dengan hukum telematika. Tanpa proses harmonisasi, ketentuan dalam UU PDP berpotensi bertentangan atau tumpang tindih dengan norma dalam UU ITE maupun PP PSTE, sehingga dapat menimbulkan kebingungan dalam implementasi, baik bagi aparat penegak hukum, penyelenggara sistem elektronik, maupun masyarakat.

Harmonisasi yang dimaksud adalah proses penyalarsan norma-norma hukum agar tidak terjadi pertentangan antara undang-undang satu dengan yang lain. Dalam konteks ini, harmonisasi antara

UU PDP dan hukum telematika menjadi sangat krusial, mengingat kedua payung hukum tersebut mengatur aspek yang sama, yaitu pengelolaan informasi digital dan perlindungan data pribadi. Harmonisasi diperlukan untuk membentuk satu sistem hukum yang solid, terkoordinasi, dan responsif terhadap dinamika teknologi informasi yang terus berkembang.

Lebih jauh, urgensi harmonisasi tidak hanya dilandasi oleh aspek normatif atau legal-formal semata. Harmonisasi memiliki dimensi strategis yang lebih luas, yaitu sebagai upaya mewujudkan keamanan siber nasional. Dalam era digital, keamanan siber bukan lagi hanya urusan teknis atau IT semata, melainkan telah menjadi isu geopolitik, ekonomi, dan kedaulatan negara. Tanpa perlindungan hukum yang terintegrasi, negara akan sulit melindungi infrastruktur digitalnya dari serangan siber, serta menjamin hak-hak masyarakat dalam penggunaan teknologi.

Dalam berbagai kasus, seperti kebocoran data pelanggan operator seluler, serangan ransomware terhadap institusi pemerintah, hingga peretasan sistem informasi rumah sakit, terlihat bahwa kelemahan hukum sering kali menjadi hambatan utama dalam penanganan. Ketika kewenangan tumpang tindih, definisi hukum kabur, dan tidak ada standar hukum yang seragam, maka respons terhadap insiden siber menjadi lambat dan tidak efektif. Oleh karena itu, harmonisasi hukum bukan sekadar wacana ideal, melainkan kebutuhan mendesak yang berkaitan langsung dengan perlindungan publik dan stabilitas nasional.

Selain dari aspek keamanan teknis, harmonisasi juga penting untuk membangun kepercayaan publik terhadap sistem digital. Masyarakat akan lebih percaya untuk menyerahkan data pribadinya kepada platform digital jika ada jaminan hukum yang kuat. Demikian pula, pelaku usaha, khususnya di bidang teknologi dan finansial, memerlukan kepastian hukum agar dapat menjalankan kegiatan usahanya dengan mematuhi regulasi yang jelas dan konsisten.

Harmonisasi hukum juga menjadi kunci dalam membangun kerja sama internasional, khususnya terkait arus data lintas batas (*cross-border data flow*). Negara-negara mitra akan menilai seberapa serius Indonesia melindungi data pribadi dan sistem digitalnya melalui kualitas regulasi yang dimiliki. Dengan demikian, harmonisasi akan memperkuat posisi Indonesia dalam percaturan global, serta meningkatkan daya saing nasional dalam ekonomi digital.

Oleh karena itu, tulisan ini akan mengulas lebih lanjut dua pokok bahasan utama. Pertama, mengenai apa yang dimaksud dengan harmonisasi UU Data Pribadi dan hukum telematika, termasuk urgensinya dalam konteks hukum nasional. Kedua, bagaimana harmonisasi tersebut secara konkret dapat berkontribusi terhadap terwujudnya keamanan siber di Indonesia. Pembahasan ini diharapkan dapat memberikan gambaran komprehensif mengenai pentingnya langkah harmonisasi dalam membangun ekosistem digital yang aman, terpercaya, dan berkelanjutan.

Dengan pendekatan analitis dan normatif, tulisan ini mengajak para pembaca untuk melihat harmonisasi bukan sebagai proses administratif semata, tetapi sebagai strategi hukum nasional dalam menghadapi kompleksitas era digital. Di tengah meningkatnya ketegangan geopolitik, eskalasi serangan siber, dan ketidakpastian global, Indonesia membutuhkan sistem hukum yang tangguh—dan harmonisasi adalah titik awal yang menentukan arah masa depan keamanan digital bangsa.

METODE PENELITIAN

Berdasarkan isi dan pendekatan pembahasan yang Anda paparkan, metode penelitian yang paling relevan untuk digunakan adalah metode yuridis normatif. Berikut adalah penjelasan metode penelitian yang dapat Anda cantumkan dalam karya ilmiah. Penelitian ini menggunakan metode yuridis normatif, yaitu metode penelitian hukum yang dilakukan dengan menelaah bahan-bahan hukum sekunder, seperti peraturan perundang-undangan, dokumen hukum, literatur hukum, dan putusan pengadilan. Metode ini digunakan untuk mengkaji norma-norma hukum yang berlaku, serta menganalisis kesesuaian, keterkaitan, dan harmonisasi antara peraturan yang mengatur perlindungan data pribadi dan hukum telematika dalam mewujudkan keamanan siber di Indonesia.

Pendekatan normatif dilakukan dengan mengkaji secara mendalam ketentuan dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), Undang-Undang Nomor 11 Tahun 2008 jo. UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE), serta Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE). Selain itu, juga dilakukan telaah terhadap konsep RUU Keamanan dan Ketahanan Siber serta praktik global seperti General Data Protection Regulation (GDPR) sebagai pembandingan.

Penelitian ini juga bersifat deskriptif analitis, yaitu menggambarkan keadaan hukum yang ada serta menganalisis urgensi dan tantangan dalam harmonisasi peraturan perundang-undangan. Analisis dilakukan dengan cara menilai sejauh mana peraturan-peraturan yang ada telah memenuhi kebutuhan hukum dalam menghadapi tantangan keamanan siber, serta mengidentifikasi potensi tumpang tindih, kekosongan hukum, atau konflik norma yang dapat menghambat implementasi perlindungan data secara efektif.

Dalam mendukung analisis, digunakan bahan hukum primer, yaitu peraturan perundang-undangan yang relevan, dan bahan hukum sekunder, berupa literatur ilmiah, artikel hukum, jurnal, pendapat para ahli hukum, serta data statistik terkini mengenai serangan siber dan kebocoran data di Indonesia. Selain itu, bahan hukum tersier seperti kamus hukum dan ensiklopedia hukum digunakan untuk memperkuat pemahaman terhadap konsep-konsep kunci.

Dengan metode ini, diharapkan penelitian dapat memberikan kontribusi teoritis dan praktis terhadap pengembangan sistem hukum nasional yang lebih harmonis, responsif, dan mampu menjawab tantangan digital secara komprehensif, khususnya dalam upaya mewujudkan keamanan siber yang terintegrasi dan berkelanjutan di Indonesia.

HASIL DAN PEMBAHASAN

1. Apa yang Dimaksud dengan Harmonisasi UU Data Pribadi dan Hukum Telematika

Dalam konteks hukum Indonesia, istilah harmonisasi merujuk pada upaya penyesuaian antar peraturan perundang-undangan agar tidak terjadi konflik norma, tumpang tindih kewenangan, atau kebingungan dalam penerapan hukum. Harmonisasi penting dilakukan ketika terdapat regulasi baru yang beririsan dengan regulasi sebelumnya, terutama dalam ranah hukum yang sangat dinamis seperti perlindungan data pribadi dan telematika. Seiring dengan perkembangan teknologi informasi dan komunikasi (TIK), kebutuhan akan perlindungan data pribadi menjadi semakin mendesak.

Penggunaan data pribadi oleh entitas pemerintah maupun swasta dalam berbagai platform digital menimbulkan risiko penyalahgunaan, kebocoran data, dan pelanggaran privasi. Oleh karena itu, lahirlah Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) sebagai kerangka hukum utama dalam perlindungan data pribadi di Indonesia.

Di sisi lain, sebelum hadirnya UU PDP, Indonesia telah memiliki berbagai peraturan yang secara parsial mengatur penggunaan dan perlindungan data pribadi, terutama melalui Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE), serta peraturan turunan dari Kementerian Komunikasi dan Informatika (Kominfo). Semua regulasi ini membentuk apa yang disebut sebagai hukum telematika—yakni hukum yang mengatur berbagai aspek dalam ranah teknologi komunikasi dan informasi.

Namun, karena UU ITE dan regulasi turunannya belum secara komprehensif mengatur data pribadi, lahirnya UU PDP membawa tantangan sekaligus peluang untuk melakukan harmonisasi. Harmonisasi dimaksudkan untuk menyelaraskan ketentuan-ketentuan dalam UU PDP dengan hukum telematika yang sudah ada, agar tidak terjadi ketidakpastian hukum atau tumpang tindih norma hukum yang merugikan masyarakat dan dunia usaha.

Misalnya, definisi mengenai data pribadi dalam UU ITE sebelumnya masih sangat umum dan

tidak memberikan klasifikasi yang jelas antara data pribadi umum dan data pribadi sensitif. UU PDP hadir dengan definisi yang lebih rinci dan menetapkan hak-hak subjek data secara tegas, seperti hak untuk mengakses, memperbaiki, hingga menghapus data. Harmonisasi diperlukan agar ketentuan lama dalam UU ITE dapat diperbaharui atau dicabut apabila bertentangan dengan prinsip-prinsip yang telah diatur dalam UU PDP.

Selain itu, kewenangan institusi pengawas menjadi isu penting dalam harmonisasi. UU PDP membentuk lembaga pengawas independen yang akan bertugas mengawasi pelaksanaan perlindungan data pribadi di Indonesia. Sebelumnya, pengawasan dilakukan oleh Kominfo berdasarkan UU ITE dan regulasi turunannya. Maka dari itu, perlu adanya pengaturan ulang agar tidak terjadi konflik kewenangan antara lembaga pengawas baru dengan instansi sebelumnya.

Harmonisasi juga penting untuk memberikan kepastian hukum bagi pelaku usaha digital, seperti platform e-commerce, media sosial, dan penyedia layanan cloud. Dengan aturan yang seragam dan tidak saling bertentangan, mereka dapat menjalankan kewajiban perlindungan data sesuai dengan standar nasional yang berlaku. Hal ini juga akan memperkuat posisi Indonesia dalam kerja sama lintas negara, terutama yang berkaitan dengan arus data internasional.

Selain untuk kebutuhan internal, harmonisasi UU PDP dan hukum telematika juga bertujuan untuk menyesuaikan regulasi Indonesia dengan praktik global, seperti General Data Protection Regulation (GDPR) di Uni Eropa. Hal ini penting karena saat ini arus data lintas negara menjadi bagian dari kerja sama perdagangan dan diplomasi internasional. Negara-negara mitra dagang akan lebih percaya jika Indonesia memiliki sistem hukum yang solid dan terkoordinasi dalam perlindungan data pribadi.

Secara keseluruhan, harmonisasi UU Perlindungan Data Pribadi dan hukum telematika adalah proses krusial untuk menciptakan ekosistem hukum yang kuat, konsisten, dan mampu menghadapi tantangan digital di era modern. Proses ini membutuhkan kolaborasi antara pembentuk undang-undang, pemerintah, lembaga penegak hukum, serta partisipasi aktif dari masyarakat dan pelaku industri.

2. Bagaimana Harmonisasi Dapat Mewujudkan Keamanan Siber di Indonesia?

Di era digital saat ini, hampir semua aspek kehidupan masyarakat bersinggungan dengan teknologi informasi, mulai dari transaksi keuangan, komunikasi, layanan kesehatan, pendidikan, hingga urusan pemerintahan. Ketergantungan yang tinggi terhadap teknologi ini membawa konsekuensi logis: semakin rentan pula sistem kita terhadap ancaman siber. Oleh karena itu, kebutuhan terhadap keamanan siber menjadi sangat penting dan mendesak. Dalam konteks Indonesia, salah satu pendekatan strategis untuk memperkuat keamanan siber adalah melalui harmonisasi peraturan perundang-undangan yang mengatur ruang digital.

Harmonisasi merupakan proses penyelarasan antara berbagai regulasi yang terkait agar tidak terjadi tumpang tindih, konflik norma, atau kekosongan hukum. Dalam konteks keamanan siber, harmonisasi menjadi langkah penting karena saat ini terdapat banyak aturan yang tersebar di berbagai undang-undang, seperti UU Informasi dan Transaksi Elektronik (UU ITE), UU Perlindungan Data Pribadi (UU PDP), dan rencana RUU Keamanan dan Ketahanan Siber (RUU KKS). Tanpa harmonisasi, keberadaan aturan-aturan ini justru bisa menimbulkan kebingungan dalam implementasinya.

Salah satu contoh konkrit perlunya harmonisasi adalah soal pengelolaan data pribadi. UU ITE dan PP No. 71 Tahun 2019 sudah lebih dulu memuat ketentuan tentang kewajiban menjaga data pribadi, namun secara umum dan tidak mendalam. Lalu muncul UU PDP yang memberikan pendekatan lebih rinci, seperti klasifikasi data pribadi umum dan sensitif, hak subjek data, serta mekanisme pemrosesan data. Tanpa harmonisasi, institusi yang menerapkan kebijakan berdasarkan regulasi lama dapat bertabrakan dengan ketentuan dalam UU baru.

Dari sisi keamanan siber, data pribadi merupakan aset digital yang sangat berharga. Peretas

atau pelaku kejahatan siber sering kali menargetkan data pribadi untuk disalahgunakan, dijual di pasar gelap, atau dijadikan sarana manipulasi sosial. Maka, ketika regulasi data pribadi sudah diselaraskan dengan hukum siber, pertahanan digital Indonesia menjadi lebih kuat karena sistem perlindungan tidak hanya bertumpu pada aspek teknis, tetapi juga memiliki fondasi hukum yang kokoh.

Harmonisasi juga penting dalam hal pembagian kewenangan antar lembaga. Saat ini, Badan Siber dan Sandi Negara (BSSN) menjadi aktor utama dalam pengamanan siber nasional. Namun, Kominfo, Polri, TNI, dan bahkan lembaga sektor seperti OJK atau BI juga memiliki peran dalam aspek-aspek tertentu dari keamanan siber. Tanpa pembagian peran yang jelas, koordinasi bisa melemah saat menghadapi serangan siber. Harmonisasi hukum dapat membantu memperjelas batas kewenangan antar lembaga dan menciptakan protokol kerja sama yang solid.

Tidak hanya dari sisi kelembagaan, harmonisasi juga sangat dibutuhkan untuk menyatukan standar keamanan dan prosedur teknis. Misalnya, standar mengenai pelaporan insiden siber, audit sistem elektronik, dan kebijakan pemulihan data pasca serangan perlu ditetapkan dalam satu kerangka hukum yang seragam. Dengan harmonisasi, pelaku usaha, penyelenggara sistem elektronik, dan pemerintah memiliki pedoman yang sama, sehingga tanggap darurat terhadap insiden siber bisa lebih cepat dan efektif.

Hal lain yang tak kalah penting adalah soal penegakan hukum terhadap kejahatan siber. Banyak kasus serangan digital yang sulit diusut karena belum adanya aturan yang spesifik atau tumpang tindih dengan aturan lain. Contohnya, ketika suatu data diretas, pertanyaan tentang siapa yang harus bertanggung jawab, siapa yang menangani kasusnya, dan bagaimana pelaku dihukum, menjadi tidak jelas. Harmonisasi peraturan akan memperkuat dasar hukum bagi aparat penegak hukum dalam bertindak, sekaligus menjamin kepastian hukum bagi masyarakat.

Selain mendukung penegakan hukum, harmonisasi juga berperan dalam meningkatkan literasi hukum dan kepercayaan publik. Ketika masyarakat memahami bahwa perlindungan data dan keamanan siber dijamin secara hukum dan diatur dalam kerangka yang saling mendukung, maka tingkat kepercayaan terhadap layanan digital akan meningkat. Hal ini sangat penting untuk mendukung pertumbuhan ekonomi digital di Indonesia.

Tidak hanya dalam lingkup domestik, harmonisasi juga membuka peluang untuk kerja sama internasional. Dalam banyak kasus, serangan siber melibatkan aktor lintas negara. Tanpa sistem hukum yang harmonis dan sesuai standar global seperti General Data Protection Regulation (GDPR) di Uni Eropa, Indonesia akan kesulitan menjalin kerja sama ekstradisi, investigasi bersama, atau pemulihan aset digital lintas negara.

Maka dari itu, upaya harmonisasi sebaiknya dilakukan secara menyeluruh, mulai dari penyusunan regulasi baru yang terintegrasi, revisi terhadap regulasi yang sudah tidak relevan, hingga pembentukan lembaga pengawas yang independen dan kuat. Harmonisasi juga memerlukan pelibatan semua pemangku kepentingan, mulai dari pemerintah, akademisi, sektor swasta, hingga masyarakat sipil, agar hasilnya tidak hanya sah secara hukum, tetapi juga realistis dan dapat dijalankan.

Sebagai langkah ke depan, pemerintah dapat memulai dengan merumuskan kerangka hukum keamanan siber nasional yang berbasis pada prinsip-prinsip inklusivitas, keadilan, dan perlindungan hak asasi. Kerangka ini harus memastikan bahwa semua aturan di sektor digital—termasuk perlindungan data, transaksi elektronik, dan sistem informasi publik—berjalan dalam satu garis yang selaras. Dengan adanya harmonisasi hukum dalam bidang keamanan siber, Indonesia tidak hanya lebih siap menghadapi serangan digital, tetapi juga mampu menciptakan ekosistem digital yang sehat, berdaya saing, dan menjunjung tinggi hak privasi serta keamanan warganya. Harmonisasi adalah fondasi untuk menciptakan kedaulatan digital Indonesia yang sesungguhnya.

KESIMPULAN

Harmonisasi antara Undang-Undang Perlindungan Data Pribadi (UU PDP) dan hukum telematika di Indonesia merupakan kebutuhan mendesak dalam menghadapi dinamika era digital yang penuh tantangan, terutama di bidang perlindungan data dan keamanan siber. Ketidakharmonisan antarregulasi berisiko menimbulkan tumpang tindih norma, kekosongan hukum, dan konflik kewenangan antar lembaga, yang pada akhirnya dapat melemahkan upaya negara dalam menjamin hak-hak warga serta melindungi infrastruktur digital dari serangan siber. Di sisi lain, harmonisasi memberikan kepastian hukum, memperkuat fondasi pengaturan ruang digital, serta meningkatkan kepercayaan publik terhadap sistem hukum dan layanan digital. Dalam lingkup global, harmonisasi juga memperkuat posisi Indonesia dalam kerja sama internasional, khususnya terkait arus data lintas negara. Oleh karena itu, harmonisasi tidak boleh dipandang sekadar sebagai penyesuaian administratif, melainkan sebagai strategi hukum nasional untuk membentuk ekosistem digital yang aman, terpercaya, dan berkelanjutan.

Saran

Pemerintah Indonesia perlu mengambil langkah strategis dan menyeluruh dalam melakukan harmonisasi regulasi digital, dimulai dengan membentuk gugus tugas lintas sektor yang berfokus pada sinkronisasi UU PDP dengan UU ITE, PP PSTE, serta rancangan regulasi lainnya seperti RUU Keamanan dan Ketahanan Siber. Upaya ini harus didukung oleh penyusunan regulasi turunan yang jelas, revisi terhadap aturan yang sudah tidak relevan, dan pembentukan lembaga pengawas independen yang kuat dan kredibel. Koordinasi yang solid antar lembaga seperti BSSN, Kominfo, OJK, dan aparat penegak hukum juga sangat penting untuk menghindari konflik kewenangan serta memperkuat respons terhadap insiden siber. Di samping itu, peningkatan literasi hukum masyarakat mengenai hak atas data pribadi serta pentingnya keamanan digital perlu digencarkan sebagai bagian dari pendekatan preventif. Untuk memperkuat daya saing global, Indonesia juga disarankan mengadopsi standar internasional seperti GDPR sebagai acuan dalam membangun sistem perlindungan data yang selaras dengan praktik global dan mampu mendukung ekonomi digital nasional secara berkelanjutan.

DAFTAR PUSTAKA

- FAIZIN, M. N. (2024). TINJAUAN YURIDIS PERLINDUNGAN DATA PRIBADI DI ERA DIGITAL DALAM PERSPEKTIF HUKUM POSITIF (Doctoral dissertation, Universitas Islam Sultan Agung Semarang).
- Hendri, S., SH, M., & Marlina, S. H. (2022). Pembaharuan hukum terkait kebebasan berpendapat dalam bermedia sosial di Indonesia. Deepublish.
- INDONESIA, K. H. P., & KURNIAWAN, D. PENANGGULANGAN CYBER CHILD PORNOGRAPHY DALAM.
- Luthiya, A. N., Irawan, B., & Yulia, R. (2021). Kebijakan Hukum Pidana Terhadap Pengaturan Pencurian Data Pribadi Sebagai Penyalahgunaan Teknologi Komunikasi Dan Informasi. *Jurnal Hukum Pidana dan Kriminologi*, 2(2), 14-29.
- Makarim, E. (2015). Keautentikan dokumen publik elektronik dalam administrasi pemerintahan dan pelayanan publik. *Jurnal Hukum & Pembangunan*, 45(4), 508-570.
- Melinda, S. (2022). Tinjauan Hukum Terhadap Tanggung Jawab Market Place Pada Pengembalian Dana Kepada Pembeli (Analisis Kasus Pada Pt. Shopee Internasional Indonesia) (Doctoral dissertation, Universitas Islam Riau).
- NASIONAL, D. P. D. D. HUKUM PELINDUNGAN DATA PRIBADI DAN DATA NASIONAL.
- Nisa, N. Z. (2020). Aspek Legalitas Penyimpanan Minuta Akta Notaris Secara Elektronik. *Jurnal Civic Hukum*, 5(2), 205-219.
- Nurmecca, S. C. (2020). Aspek Hukum Pemungutan Pajak Penghasilan Dari Transaksi Jual Beli Melalui Media Sosial (Bachelor's thesis, Fakultas Syariah dan Hukum Universitas Islam Negeri Syarif Hidayatullah Jakarta).

- PARDEDE, Daniel EP, et al. Urgensi Pembentukan Undang-Undang Khusus Perlindungan Data Pribadi Di Indonesia Dalam Mewujudkan Harmonisasi Hukum Perlindungan Privasi Dan Data Pribadi Dalam Era Digital (Studi Kasus: Industri Financial Technology (Fintech) Berbasis Peer To Peer Lending. *Jurnal Hukum Adigama*, 2022, 5.1: 542-558.
- PUSPA, A. E. (2024). PERAN HUKUM PIDANA TERHADAP KEJAHATAN SIBER TERKAIT PERLINDUNGAN DATA PRIBADI DI INDONESIA (Doctoral dissertation, Universitas Islam Sultan Agung Semarang).
- Ramadha, B. S. (2021). Kemampuan Hukum Pidana Terhadap Kejahatan Siber Terkait Perlindungan Data Pribadi Di Indonesia.
- Rezkia, N. U. H. P. (2020). Perlindungan Hukum Terhadap Data Pribadi Konsumen Dalam Registrasi Sim Card (Doctoral dissertation, Universitas Hasanuddin).
- Rianto, J. (2016). Kebijakan Pemblokiran Dalam Penanggulangan Kejahatan Berbasis Konten Media Elektronik (Doctoral dissertation, UNIVERSITAS ISLAM INDONESIA).
- Sabadina, U. (2021). Politik hukum pidana penanggulangan kejahatan teknologi informasi terkait kebocoran data pribadi oleh korporasi berbasis online. *Lex Renaissance*, 6(4), 799-814.
- Sandy, A. K. (2022). TINJAUAN YURIDIS TERHADAP WANPRESTASI DALAM JUAL BELI ONLINE MENURUT UNDANG-UNDANG NOMOR 8 TAHUN 1999 DAN KUHPERDATA (Doctoral dissertation, Universitas Islam Sultan Agung).
- SARI, N. E. (2011). Kebijakan Kriminal dalam Menanggulangi Kejahatan Cyber Sex (Doctoral dissertation, UNIVERSITAS ISLAM INDONESIA).
- Siburian, H. (2019). PERLINDUNGAN KONSUMEN DALAM E-COMMERCE (JUAL BELI ONLINE) MENURUT UNDANG-UNDANG NOMOR 8 TAHUN 1999 TENTANG PERLINDUNGAN KONSUMEN DAN UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK.
- Susilowati, D. E., Muhtarom, M., & Junaidi, A. (2025). Analisis yuridis keabsahan tanda tangan digital dalam transaksi e-commerce di Indonesia. *JURNAL PENELITIAN SERAMBI HUKUM*, 18(01), 17-26.
- Tarmizi, S. H., & Muhammad Ikhwan, S. H. (2021). Hak Cipta Karya Digital: Perlindungan Dan Tanggung Jawab. Merdeka Kreasi Group.
- Waspiah, W., Lies, A., Islami, T., & Setyaning Wida, N. (2023). Model Pelindungan Hukum Data Pribadi di Era Digital Guna Menjamin Hak Warga Negara Atas Pelindungan Data Pribadi. *Syntax Literate: Jurnal Ilmiah Indonesia*, 8(9), 5165-5179.