



Analisis Peran Hukum Siber dalam Menjaga Privasi Pengguna di Indonesia pada Era Digital

Johanes Maruli Burju

Program Studi Ilmu Hukum, Universitas Pendidikan Ganesha, Indonesia

*Penulis Korespondensi: johanes@student.undiksha.ac.id

Abstract *In the ever-evolving digital era, the importance of cyber law in safeguarding user privacy cannot be overstated. As a distinct legal discipline, cyber law examines regulations that oversee activities in cyberspace, offering legal protection regarding personal data and user privacy. Referring to various credible sources, this article evaluates the role of cyber law in protecting user privacy in the Indonesian context. The article discusses regulations such as the Electronic Information and Transactions Law (UU ITE), the Government Regulation on Electronic Systems, and the Personal Data Protection Bill. The main elements analyzed include supervision, regulation, resolution, and protection of user rights when facing digital security challenges. The examination shows that cyber law plays a significant role in protecting individuals' personal information, thereby encouraging safer and more trustworthy digital services. Furthermore, the article points out the various challenges faced in enforcing cyber law, such as administrative constraints, inadequate digital literacy, and limited access to justice, especially for those without legal knowledge or support. Consequently, to improve the effectiveness of cyber law, continued efforts are needed to strengthen the digital regulatory framework and provide more comprehensive user privacy protection. This perspective seeks to enhance understanding of the significance of cyber law in safeguarding privacy and proposes recommendations for governments and relevant organizations in addressing privacy issues in the digital age.*

Keywords: *Cyber Law; Digital Era; ITE Law; Personal Data Protection; User Privacy.*

Abstrak. Di era digital yang terus berkembang, pentingnya hukum siber dalam menjaga privasi pengguna tidak dapat dilebih-lebihkan. Sebagai disiplin hukum yang berbeda, hukum siber mengkaji peraturan yang mengawasi aktivitas di dunia maya, yang menawarkan perlindungan hukum terkait data pribadi dan privasi pengguna. Mengacu pada berbagai sumber yang kredibel, artikel ini mengevaluasi peran hukum siber dalam melindungi privasi pengguna dalam konteks Indonesia. Artikel ini membahas peraturan seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Peraturan Pemerintah terkait sistem elektronik, dan RUU Perlindungan Data Pribadi. Elemen utama yang dianalisis meliputi pengawasan, regulasi, penyelesaian, dan perlindungan hak pengguna saat menghadapi tantangan keamanan digital. Pemeriksaan tersebut menunjukkan bahwa hukum siber memainkan peran penting dalam melindungi informasi pribadi individu, sehingga mendorong layanan digital yang lebih aman dan lebih tepercaya. Selain itu, artikel ini menunjukkan berbagai tantangan yang dihadapi dalam penegakan hukum siber, seperti kendala administratif, literasi digital yang tidak memadai, dan akses terbatas ke keadilan, khususnya bagi mereka yang tidak memiliki pengetahuan atau dukungan hukum. Akibatnya, untuk meningkatkan efektivitas hukum siber, upaya berkelanjutan diperlukan untuk memperkuat kerangka regulasi digital dan memberikan perlindungan privasi pengguna yang lebih menyeluruh. Perspektif ini berupaya untuk meningkatkan pemahaman tentang signifikansi hukum siber dalam menjaga privasi dan mengusulkan rekomendasi bagi pemerintah dan organisasi terkait dalam menangani masalah privasi di era digital.

Kata Kunci: *Cyber Law; Era Digital; Perlindungan Data Pribadi; Privasi Pengguna; UU ITE.*

1. LATAR BELAKANG

Manusia Era digital, yang ditandai dengan kemajuan pesat teknologi informasi dan komunikasi, telah mengubah banyak aspek kehidupan manusia secara signifikan, termasuk cara individu terhubung, berkomunikasi, dan menjalani kehidupan sehari-hari (Setiadi, 2020: 15). Meningkatnya ketergantungan masyarakat pada platform dan layanan digital merupakan salah satu dampak yang paling nyata dari pergeseran paradigma ini.

Kemajuan teknologi informasi telah memungkinkan masyarakat, bisnis, dan pemerintah untuk menggunakan perangkat digital serta internet guna mengumpulkan, menyimpan, dan mengelola data dalam jumlah besar atau *big data* (Wardani & Ghazali, 2022: 45). Namun, kemajuan ini juga menghadirkan masalah privasi, keamanan data, dan perlindungan informasi pribadi pengguna yang signifikan. Seiring meningkatnya insiden pelanggaran data, serangan siber, dan penyalahgunaan identitas yang membahayakan keamanan informasi pribadi, masalah privasi dan perlindungan data di Indonesia menjadi semakin rumit dan mendesak untuk ditangani melalui regulasi yang komprehensif (Situmeang, 2021: 88).

Potensi pelanggaran privasi meningkat secara linear seiring dengan jumlah data pribadi yang dikumpulkan, disimpan, dan diproses secara daring dalam berbagai platform digital (Barkatullah, 2019: 42). Masyarakat pada dasarnya berada dalam posisi rentan terhadap risiko pencurian data (*data theft*), penyalahgunaan informasi pribadi untuk kepentingan komersial ilegal, hingga serangan siber yang terstruktur. Oleh karena itu, di era digital ini, perlindungan privasi pengguna melalui instrumen hukum menjadi pilar utama dalam menjaga kedaulatan individu atas informasinya (Dewi, 2021: 115).

Untuk mengatur dan melindungi hak individu di ranah digital, hukum siber (*cyber law*) merupakan titik awal yang krusial. Tujuan utama dari hukum siber adalah untuk menetapkan kerangka regulasi yang berkaitan dengan penggunaan teknologi informasi dan komunikasi, dengan fokus khusus pada jaminan keamanan serta kerahasiaan data pengguna (Makarim, 2020: 78). Tanpa adanya kepastian hukum, ekosistem ekonomi digital akan kehilangan kepercayaan (*trust*) dari publik.

Inisiatif pengaturan keamanan siber dilakukan di Indonesia melalui sejumlah undang-undang, termasuk Undang-Undang Perlindungan Data Pribadi (UU PDP) yang baru disahkan dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) (Asshiddiqie, 2021: 54). Undang-undang ini diharapkan mampu mengatasi masalah pelanggaran privasi dan perlindungan data yang semakin meluas di era digital. Namun, masih terdapat sejumlah hambatan signifikan yang menghalangi penerapan hukum siber secara efektif, termasuk hambatan kelembagaan, tumpang tindih regulasi, serta budaya digital masyarakat yang masih kurang menghargai perlindungan privasi (Sinta, 2022: 129).

Kurangnya kedalaman substansi hukum siber saat ini dalam menangani berbagai jenis masalah privasi dan keamanan data menjadi salah satu isu utama. Masalah mendasar yang harus diklarifikasi adalah bagaimana perlindungan privasi pengguna di ranah digital diatur oleh aturan hukum siber Indonesia saat ini secara sinkron. Meskipun menjadi landasan hukum, UU

ITE dan UU PDP sering kali dianggap masih menyisakan celah dalam melindungi pengguna dari berbagai bahaya, termasuk peretasan, kebocoran data, dan penyalahgunaan data oleh pihak ketiga (Ramli, 2023: 88). Lebih jauh, masih terdapat ambiguitas seputar hukum siber, termasuk definisi filosofis privasi di ranah digital serta batasan yang memisahkan hak privasi individu dari kepentingan komersial maupun keamanan pihak ketiga dalam akses data (Kusumadara, 2021: 210).

Selain aspek regulasi, perlu dipertimbangkan kesulitan dan hambatan praktis terkait penerapan undang-undang siber, khususnya yang berkaitan dengan kesadaran publik, kualitas sumber daya manusia, dan kesiapan infrastruktur teknologi (Mansur & Gultom, 2022: 78). Tanpa upaya signifikan dari pemerintah, penyedia layanan digital, dan masyarakat umum untuk menginternalisasi konsep perlindungan privasi, keberadaan regulasi semata tidak akan memberikan proteksi yang cukup.

Ketidakmampuan infrastruktur keamanan siber di Indonesia dalam mengamankan data secara optimal, baik dari sisi enkripsi maupun sistem deteksi dini, menjadi kendala utama dalam efektivitas hukum siber (Widodo, 2021: 145). Di sisi lain, keterbatasan sumber daya manusia di lembaga penegak hukum yang menguasai komponen teknis keamanan siber sering kali menyebabkan ketidakefektifan dalam upaya pencegahan dan penindakan pelanggaran privasi (Sudirman, 2023: 56).

Terakhir, rendahnya literasi digital menjadi faktor krusial; banyak pengguna internet yang belum menyadari risiko inheren dalam aktivitas digital mereka, seperti membagikan data sensitif tanpa pengamanan atau mengunggah informasi pribadi secara berlebihan di media sosial (*oversharing*) yang justru membuka celah bagi pelaku kejahatan siber (Nasrullah, 2020: 112).

Analisis masalah terakhir yang diangkat adalah efektivitas hukum siber (*cyber law*) dalam melindungi data pribadi dan privasi pengguna dari ancaman pelanggaran keamanan siber yang kian kompleks. Tingkat di mana undang-undang dapat mencegah (*deterrence*) atau menuntut pelanggaran privasi daring merupakan indikator utama kemanjurannya (Raharjo, 2021: 92). Menurut penelitian, meskipun sejumlah pelanggaran privasi di Indonesia telah diselesaikan secara hukum, masih banyak kasus yang tidak terdeteksi (*dark number*) atau tidak ditangani secara optimal oleh aparat penegak hukum (Prakoso, 2022: 45).

Rasa aman pengguna secara psikologis dan teknis sebagian besar dipengaruhi oleh penegakan hukum yang efektif. Meski demikian, sistem hukum sering kali menghadapi kendala sistemik, seperti proses litigasi yang memakan waktu lama, koordinasi yang tidak memadai antar-instansi terkait (seperti Kepolisian, Kemenkominfo, dan BSSN), serta

keterbatasan teknologi forensik dalam mengidentifikasi pelaku pelanggaran privasi (Arief, 2020: 130).

Oleh karena itu, penelitian lebih lanjut sangat diperlukan untuk menentukan sejauh mana hukum siber mampu memproteksi keamanan pengguna secara daring. Berdasarkan latar belakang tersebut, fungsi undang-undang siber dalam menjaga privasi pengguna di Indonesia akan dikaji dalam studi ini. Diharapkan studi ini akan memperdalam pemahaman mengenai mekanisme hukum siber dalam menangani masalah privasi di era digital serta menawarkan saran kebijakan (*policy recommendations*) yang strategis guna meningkatkan standar perlindungan privasi nasional (Suhariyanto, 2021: 77).

2. KAJIAN TEORITIS

Kajian Konsep privasi di era digital telah berkembang dari sekadar hak untuk dibiarkan sendiri menjadi hak untuk menentukan nasib sendiri atas informasi pribadi (*informational self-determination*). Menurut (Solove, 2021: 58), privasi bukan merupakan konsep tunggal yang statis, melainkan sebuah kumpulan hak yang mencakup pengendalian atas pengumpulan, penggunaan, dan penyebaran data pribadi oleh pihak lain. Dalam konteks ini, individu harus memiliki kedaulatan penuh untuk memberikan atau menarik persetujuan terhadap akses data mereka guna menghindari eksploitasi digital yang tidak diinginkan.

Efektivitas sebuah regulasi hukum, termasuk hukum siber, sangat bergantung pada keselarasan antara substansi hukum, struktur penegakan, dan budaya hukum masyarakat. Friedman (2019: 210) menjelaskan bahwa hukum tidak akan berjalan efektif jika tidak didukung oleh kesadaran hukum masyarakat yang memahami hak dan kewajibannya di bawah undang-undang tersebut. Di Indonesia, tantangan utama hukum siber sering kali bukan terletak pada ketiadaan aturan, melainkan pada rendahnya pemahaman kolektif mengenai pentingnya melindungi integritas data pribadi dalam interaksi sosial media.

Perlindungan data pribadi kini dipandang sebagai bagian dari hak asasi manusia yang bersifat fundamental di ruang digital (Situmeang, 2021: 398) berpendapat bahwa negara memiliki kewajiban konstitusional untuk menjamin keamanan setiap warga negara dalam ruang siber melalui pembentukan otoritas pengawas yang independen. Perlindungan ini menjadi prasyarat bagi terciptanya keadilan digital, di mana setiap subjek hukum terlindungi dari penyalahgunaan identitas dan diskriminasi berbasis data yang dilakukan oleh entitas bisnis maupun pemerintah.

Hukum siber (*cyber law*) memiliki karakteristik unik karena harus menghadapi objek yang bersifat maya namun memiliki dampak nyata. (Marzuki, 2021: 147) menegaskan bahwa penelitian hukum normatif dalam bidang siber harus mampu menjangkau perkembangan teknologi yang bersifat eksponensial agar tidak terjadi kekosongan hukum (*rechtvacuum*). Oleh karena itu, pendekatan hukum tidak boleh hanya terpaku pada teks undang-undang yang kaku, melainkan harus bersifat dinamis dan adaptif terhadap inovasi teknis seperti kecerdasan buatan dan enkripsi data.

Dalam perspektif global, regulasi privasi nasional harus berharmonisasi dengan standar internasional guna memfasilitasi aliran data lintas batas yang aman. (Greenleaf, 2022: 15) mencatat bahwa keberadaan undang-undang perlindungan data pribadi yang komprehensif merupakan standar global yang harus dipenuhi oleh setiap negara untuk membangun kepercayaan dalam perdagangan digital internasional. Tanpa harmonisasi ini, penegakan hukum terhadap kejahatan siber transnasional akan terus menemui jalan buntu akibat benturan yurisdiksi antarnegara.

Efektivitas penegakan hukum siber di lapangan sangat ditentukan oleh kualitas sarana teknis dan kompetensi aparat penegak hukum. (Sujiastuti, 2022: 90) mengemukakan bahwa tanpa dukungan teknologi forensik yang memadai dan personil yang ahli dalam bidang teknologi informasi, aturan hukum siber hanya akan menjadi "macan kertas" yang tidak mampu menjerat pelaku kejahatan tingkat tinggi. Integrasi antara pengetahuan hukum dan keterampilan teknis menjadi kunci utama dalam meminimalkan angka kejahatan siber yang terus meningkat.

3. METODE PENELITIAN

Metode Penelitian yang digunakan dalam penelitian ini adalah metode yuridis normatif, yaitu penelitian yang berfokus pada norma-norma hukum sebagai objek kajian. (Adnyana, dkk, 2024: 3-4) Metode menganalisis peraturan perundang-undangan serta konsep hukum yang berkaitan dengan pelanggaran otoritas akses dan kegagalan perlindungan data dalam sengketa penguasaan data pribadi oleh penyelenggara sistem elektronik. Dalam ranah siber, fokus utama beralih pada legitimasi perolehan data, di mana penguasaan data digital oleh pihak lain tanpa dasar hukum yang sah dianggap sebagai bentuk pelanggaran terhadap kedaulatan informasi individu (Yulianto, 2022: 67). Pendekatan penelitian yang digunakan meliputi pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), Pendekatan perundang-undangan digunakan untuk menganalisis

peraturan hukum relevan (Diantha, 2016:12). Pendekatan konseptual digunakan untuk mengkaji konsep-konsep hukum yang relevan dengan penelitian ini.

4. HASIL DAN PEMBAHASAN

Peraturan *Cyber Law* di Indonesia

Hukum Indonesia telah berupaya keras menjaga privasi pengguna di ranah digital melalui serangkaian undang-undang dan peraturan yang dinamis. Landasan utama pengaturan ini bermula pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang kemudian direvisi melalui Undang-Undang Nomor 19 Tahun 2016 guna menyesuaikan dengan pesatnya kemajuan teknologi. Dalam Pasal 26 ayat (1) kemanusiaan yang harus dilindungi secara absolut oleh negara (Ramli, 2024: 89). Dengan diakuinya hak asasi manusia digital secara resmi, perlindungan informasi pribadi kini menjadi komponen dasar hak asasi manusia yang harus ditegakkan secara kolektif.

Secara keseluruhan, seluruh rangkaian regulasi ini bertujuan untuk menjamin kerahasiaan dan keamanan informasi pribadi agar tidak dieksploitasi oleh pihak ketiga tanpa izin. Prinsip persetujuan tertulis menjadi syarat mutlak dalam penggunaan data, di mana pemilik data harus diinformasikan mengenai tujuan dan potensi bahaya dari pengolahan informasi tersebut. Namun, efektivitas penerapan prinsip-prinsip ini di lapangan sangat bergantung pada kesiapan infrastruktur hukum. Sebagaimana, kepastian hukum di ruang siber hanya dapat tercapai jika terdapat sinkronisasi antara regulasi nasional dengan standar keamanan siber internasional yang berlaku secara global (Atmadja, 2023: 134). Tanpa sinergi ini, upaya menciptakan lingkungan digital yang aman melalui sanksi hukum bagi pelanggar akan sulit mencapai hasil optimal.

Penerapan hukum siber yang efektif juga menuntut adanya dukungan infrastruktur forensik dan kompetensi aparat penegak hukum. Hal ini mempunyai tantangan terbesar penegakan hukum siber saat ini adalah anonimitas pelaku dan batas yurisdiksi yang kabur, sehingga diperlukan penguatan kerja sama lintas negara dalam pertukaran data kriminal (Fakhri, 2022: 77). Di Indonesia, mekanisme pengaduan telah disusun agar masyarakat dapat mengakses jalur hukum jika hak privasinya dilanggar, namun keberhasilan ini tetap memerlukan pembaruan hukum secara berkala agar tidak terjadi kekosongan hukum akibat inovasi teknologi yang terus berubah. Transformasi digital yang cepat mengharuskan aparat penegak hukum memiliki literasi digital yang setara dengan perkembangan modus operandi kejahatan siber terbaru.

Sebagai langkah strategis, sinkronisasi antara UU ITE, UU PDP, dan peraturan pelaksanaannya diharapkan dapat menyediakan lingkungan digital yang transparan dan terjamin. Penegakan hukum yang mencakup sanksi pidana dan denda tinggi bagi pelanggar prinsip perlindungan data merupakan bagian dari upaya memberikan efek jera, bahwa pemberian sanksi administratif yang berat kepada korporasi yang membocorkan data nasabah merupakan langkah preventif yang lebih efektif dibandingkan sekadar sanksi pidana perorangan (Sinta, 2023: 56). Dengan adanya kolaborasi antara pemerintah melalui lembaga berwenang dan kepatuhan pelaku usaha, standar perlindungan privasi nasional dapat ditingkatkan sesuai dengan kebutuhan hukum di era digital guna menjaga keamanan dunia maya nasional.

Kendala dan Tantangan dalam Penerapan Cyber Law dalam upaya mengatasinya

Kejahatan Penerapan hukum siber dalam melindungi privasi pengguna saat ini menghadapi dilema akibat kecepatan inovasi teknologi yang melampaui kemampuan adaptasi regulasi. Kehadiran model bisnis berbasis *big data* dan Kecerdasan Buatan (AI) menciptakan tantangan baru dalam transparansi algoritma yang sulit dijangkau oleh aturan konvensional. fenomena *lagging behind the law* dalam ekosistem digital menyebabkan instrumen hukum sering kali kehilangan relevansinya hanya dalam hitungan bulan setelah disahkan (Siahaan, 2024: 112). Hal ini menuntut adanya regulasi yang lebih bersifat teknologis-netral agar mampu memayungi berbagai inovasi tanpa harus terus-menerus melakukan revisi pasal secara parsial.

Tantangan selanjutnya bersumber dari rendahnya tingkat literasi digital dan kesadaran hukum masyarakat dalam menjaga data pribadi mereka. Banyak pengguna internet masih secara sukarela membagikan informasi sensitif di media sosial tanpa memikirkan konsekuensi jangka panjangnya. bahwa kerentanan digital di Indonesia berbanding lurus dengan rendahnya pemahaman mengenai hak-hak subjek data, sehingga masyarakat sering kali menjadi korban eksploitasi data oleh platform digital global (Dewi, 2023: 88). Kurangnya edukasi ini menyebabkan proteksi hukum yang sudah tersedia menjadi tidak maksimal karena korban tidak menyadari bahwa hak privasinya telah dilanggar.

Secara teknis, penegakan hukum di ruang siber sering kali terbentur pada sulitnya identifikasi pelaku yang menggunakan teknik anonimitas dan enkripsi tingkat tinggi. Jejak digital yang mudah dihapus atau dimanipulasi membuat bukti digital sering kali dianggap lemah di persidangan. bahwa tingginya biaya investigasi digital forensik sering kali menjadi hambatan bagi korban untuk menuntut keadilan secara mandiri (Pratama, 2022: 54). Celah ini memberikan peluang bagi pelaku kejahatan siber untuk terus beroperasi tanpa takut akan sanksi hukum yang nyata, sehingga memperlemah wibawa hukum di ranah virtual.

Sifat internet yang tanpa batas (*borderless*) memicu konflik yurisdiksi transnasional yang rumit ketika terjadi pelanggaran data lintas negara. Perbedaan standar perlindungan privasi antarnegara sering kali menghambat proses penegakan hukum terhadap platform global yang berkantor pusat di luar negeri. Dalam kajiannya, bahwa ketiadaan perjanjian ekstradisi siber yang komprehensif membuat pelaku kejahatan dapat dengan mudah berpindah yurisdiksi secara virtual untuk menghindari jeratan hukum nasional (Pratama,2022: 54). Oleh karena itu, harmonisasi regulasi global menjadi syarat mutlak untuk menangani kejahatan siber yang semakin terorganisir.

Keterbatasan sumber daya manusia yang memiliki keahlian ganda di bidang hukum dan teknologi informasi juga menjadi penghambat utama efektivitas penegakan hukum. Banyak aparat penegak hukum yang masih kesulitan dalam menangani kerumitan kasus siber karena kurangnya pelatihan khusus dan dukungan finansial yang memadai untuk perangkat forensik. bahwa tanpa peningkatan kapasitas aparat secara berkelanjutan, lembaga penegak hukum akan selalu tertinggal dari kecanggihan modus operandi kejahatan siber yang terus berevolusi (Pratama,2022: 54). Kesenjangan kompetensi ini menyebabkan banyak laporan pelanggaran privasi tidak dapat terselesaikan hingga tuntas di tingkat penyidikan.

Untuk mengatasi berbagai kendala tersebut, diperlukan strategi holistik yang mencakup penguatan literasi digital, kolaborasi internasional, dan pembaruan regulasi secara berkala. Pendekatan *Privacy by Design* harus didorong agar setiap inovasi teknologi menyertakan perlindungan privasi sejak tahap awal pengembangan. bahwa sinergi antara pemerintah, pelaku industri, dan akademisi dalam merumuskan kebijakan siber adalah satu-satunya jalan untuk menciptakan ekosistem digital yang aman (Pratama,2022: 54). Dengan integrasi sumber daya yang kompeten dan regulasi yang dinamis, diharapkan hak privasi warga negara dapat terlindungi secara optimal di tengah pusaran kemajuan teknologi informasi.

Efektivitas Cyber Law dalam melindungi data pribadi dan privasi dari ancaman pelanggaran keamanan siber

PBB Hukum siber (*cyber law*) di Indonesia menjadi fondasi utama untuk melindungi privasi dan data pengguna di tengah dinamika era digital yang kian kompleks. Landasan hukum primer, yakni Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) beserta peraturan pelaksanaannya, memberikan definisi operasional yang krusial mengenai data pribadi dan hak-hak subjek data yang relevan (Pramono, 2020: 112). Kehadiran regulasi ini bertujuan untuk menciptakan kepastian hukum bagi setiap individu maupun badan usaha yang terlibat dalam pemrosesan data, sehingga setiap transaksi informasi dapat dikelola dengan standar keamanan yang dapat dipertanggungjawabkan.

UU ITE juga secara eksplisit mengadopsi prinsip-prinsip perlindungan data yang diakui secara global, seperti prinsip tujuan khusus dan prinsip persetujuan. Prinsip ini menegaskan bahwa data pribadi hanya boleh diproses berdasarkan persetujuan tegas dari pemilik data dan digunakan terbatas pada tujuan yang telah disepakati sejak awal (Wicaksono, 2021: 45). Selain itu, aturan mengenai penyimpanan data yang terbatas dan prinsip akuntabilitas mewajibkan setiap pengendali data untuk bertindak sah dan transparan, yang pada akhirnya berfungsi sebagai tolok ukur perlindungan privasi yang hakiki bagi masyarakat pengguna layanan digital.

Subjek data di Indonesia kini memiliki kewenangan lebih besar atas informasi pribadi mereka melalui hak-hak yang dijamin oleh undang-undang. Hak tersebut mencakup akses terhadap informasi data yang dikumpulkan, hak untuk melakukan koreksi terhadap data yang tidak akurat, hingga hak untuk menghapus data pribadi jika tidak lagi relevan atau atas permintaan pemiliknya (Siregar, 2022: 78). Pemberian hak-hak ini secara legal memungkinkan masyarakat untuk memegang kontrol penuh atas jejak digital mereka, memastikan bahwa setiap penggunaan data selaras dengan preferensi dan kepentingan pribadi mereka.

Sebagai langkah preventif, regulasi ini menetapkan sanksi yang tegas dan berat bagi pihak-pihak yang terbukti melakukan pelanggaran data pribadi. UU ITE memberikan ancaman pidana penjara serta denda administratif yang tinggi sebagai upaya menciptakan efek jera bagi para pelaku kejahatan siber (Haris, 2023: 31). Selain sanksi, negara juga menyediakan mekanisme pengaduan yang jelas melalui lembaga otoritas seperti Kementerian Komunikasi dan Informatika (Kominfo), sehingga warga negara yang merasa hak privasinya dieksploitasi memiliki jalur hukum yang nyata untuk mencari keadilan.

Peran lembaga pengawas sangat vital untuk menjamin bahwa seluruh ekosistem digital, termasuk pelaku usaha, menerapkan standar pengamanan yang mumpuni. Badan perlindungan data yang berwenang bertugas mengawasi kepatuhan terhadap regulasi dan memberikan kejelasan hukum bagi pihak yang menangani data dalam jumlah besar (Mulyadi, 2021: 156). Dengan pengawasan yang ketat, diharapkan risiko kebocoran data dapat diminimalisir secara signifikan, sekaligus mendorong budaya korporasi yang lebih menghargai hak privasi konsumen sebagai aset yang harus dilindungi secara optimal.

Namun, di balik kerangka regulasi yang kuat, implementasi hukum siber di Indonesia masih dihadapkan pada hambatan struktural yang signifikan. Kendala utama meliputi keterbatasan sumber daya manusia yang memiliki keahlian teknis-yuridis, rendahnya kesadaran hukum masyarakat terkait privasi, serta infrastruktur teknologi pengawasan yang belum memadai (Fadillah, 2022: 92). Akibatnya, upaya menciptakan lingkungan digital yang

aman dan transparan sering kali belum mencapai hasil maksimal, sehingga diperlukan sinkronisasi yang lebih baik antara kebijakan hukum dan kesiapan teknis di lapangan.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil analisis terhadap fungsi legislasi siber di Indonesia, dapat disimpulkan bahwa negara telah membangun fondasi hukum untuk melindungi privasi melalui UU ITE (UU No. 19 Tahun 2016), PP No. 71 Tahun 2019, serta amanat Pasal 28F UUD 1945. Regulasi ini menekankan pentingnya pengelolaan informasi pribadi berdasarkan persetujuan pemilik data serta penetapan sanksi bagi pelanggar. Meskipun kerangka hukum ini telah memberikan arah bagi perlindungan data, sinkronisasi antaraturan masih memerlukan pengesahan regulasi yang lebih spesifik guna memberikan proteksi menyeluruh terhadap hak-hak digital warga negara (Putra, 2022: 145).

Namun, implementasi hukum siber menghadapi tantangan serius akibat pesatnya kemajuan teknologi yang tidak diimbangi dengan literasi digital masyarakat serta kesiapan penegak hukum. Hambatan utama mencakup minimnya sumber daya manusia ahli di bidang hukum informasi dan kesulitan dalam penegakan hukum lintas batas (*borderless*). Oleh karena itu, diperlukan upaya kolektif dalam meningkatkan kapasitas petugas dan kolaborasi internasional guna memastikan bahwa hukum nasional tetap relevan dengan ancaman siber yang terus berkembang di kancah global (Mahendra, 2023: 56).

Untuk meningkatkan efektivitas implementasi hukum siber dan standar pelayanan publik, prioritas utama harus diberikan pada inisiatif edukasi digital yang berkelanjutan. Kolaborasi antara pemerintah, sektor pendidikan, dan swasta sangat diperlukan untuk memberikan pelatihan mengenai pengamanan data pribadi, pengenalan ancaman *phishing*, serta bahaya *malware*. Kesadaran publik yang tinggi merupakan garda terdepan dalam menjaga kedaulatan informasi individu dan mengurangi risiko eksploitasi data di ruang digital (Zulkarnain, 2024: 12).

Penyelesaian dan pengesahan UU Perlindungan Data Pribadi (UU PDP) yang lebih mendetail harus menjadi agenda prioritas pemerintah guna memberikan kepastian hukum terkait tata kelola pengumpulan, pemrosesan, dan penyimpanan data. Seiring dengan hal tersebut, aparat penegak hukum wajib mendapatkan pelatihan ekstensif mengenai digital forensik dan penanganan kejahatan tingkat tinggi seperti *ransomware*. Penguasaan teknologi canggih oleh personel hukum akan menjamin pengumpulan bukti digital yang sah serta proses peradilan yang lebih adil dan efisien (Budiman, 2023: 102).

Terakhir, pemerintah perlu memperkuat kerja sama internasional dalam pertukaran informasi keamanan siber dan melakukan peninjauan berkala terhadap regulasi siber agar tetap adaptif. Pembentukan komite atau badan khusus yang fokus pada pemantauan risiko teknologi baru akan membantu Indonesia dalam merespons ancaman siber secara cepat. Dengan integrasi antara regulasi yang mutakhir, penegak hukum yang kompeten, dan masyarakat yang cerdas digital, diharapkan tercipta lingkungan daring yang aman, transparan, dan terproteksi bagi seluruh warga negara

DAFTAR REFERENSI

- Adnyana, K. R., Dantes, K. F. F., & Setianto, M. J. (2024). Analisis yuridis perbuatan melawan hukum dalam sengketa kepemilikan tanah tanpa hak oleh pemerintah (Studi Putusan Nomor 83/Pdt.G/2017/PN Sgr). *Jurnal Hukum*, 7(3), 3–4.
- Arief, B. N. (2020). *Tindak pidana mayantara: Perkembangan kajian cybercrime di Indonesia*. Rajawali Pers.
- Asshiddiqie, J. (2021). *Hukum tata negara pasca perubahan UUD 1945*. Rajawali Pers.
- Atmadja, I. G. N. (2023). *Hukum digital dan transformasi yurisdiksi*. Prenada Media.
- Barkatullah, A. H. (2019). *Hukum perlindungan konsumen: Kajian teoretis dan perkembangan pemikiran*. Nusa Media.
- Dewi, S. (2021). Prinsip-prinsip perlindungan privasi dan data pribadi di Indonesia. *Jurnal Hukum & Pembangunan*, 51(1), 115–157.
- Dewi, S. (2023). Analisis literasi digital terhadap keamanan data pribadi pengguna media sosial. *Jurnal Pemikiran Hukum dan Konstitusi*, 4(2), 88.
- Diantha, M. (2016). *Metodologi penelitian hukum normatif dalam justifikasi teori hukum*. Prenada Media Group.
- Fadillah, N. (2022). Tantangan implementasi UU PDP di Indonesia. *Jurnal Ilmu Hukum*, 12(3).
- Fakhri, M. (2022). Tantangan penegakan hukum transnasional di ruang siber. *Jurnal Hukum Internasional*, 14(2), 77.
- Friedman, L. M. (2019). *Sistem hukum: Perspektif ilmu sosial*. Nusa Media.
- Greenleaf, G. (2022). Global data privacy laws 2022: 157 laws and many bills. *Privacy Laws & Business International Report*, 15.
- Haris, M. (2023). Analisis sanksi pidana dalam kejahatan siber. *Jurnal Keadilan Sosial*, 9(2), 31.
- Husin, S. (2023). *Yurisdiksi hukum siber dalam perspektif internasional*. Andalas University Press.

- Kusumadara, A. (2021). Tantangan hukum internasional dan nasional dalam melindungi data pribadi. *Jurnal Hukum & Pembangunan*, 51(3), 210.
- Makarim, E. (2020). *Pengantar hukum telematika: Suatu kompilasi kajian*. Rajawali Pers.
- Makarim, E. (2022). *Notaris dan transaksi elektronik: Kajian hukum siber di Indonesia*. RajaGrafindo Persada.
- Mansur, D. M., & Gultom, E. (2022). *Cyber law: Masalah yuridis di internet*. Refika Aditama.
- Marzuki, P. M. (2021). *Penelitian hukum* (Edisi revisi). Kencana.
- Mulyadi, L. (2021). *Teori dan praktik hukum siber*. Kencana.
- Nasrullah, R. (2020). Literasi digital dan etika privasi di media sosial. *Jurnal Komunikasi*, 12(1).
- Prakoso, G. (2022). Problematika penegakan hukum pidana siber di Indonesia. *Jurnal Hukum Nasional*, 11(2), 45–48.
- Pramono, B. (2020). *Hukum dan teknologi informasi*. Jakad Media.
- Pratama, A. B. (2022). Problematika bukti elektronik dalam persidangan pidana siber. *Jurnal Hukum Lingkungan Siber*, 9(1), 54.
- Raharjo, A. (2021). *Cybercrime: Pemahaman dan upaya pencegahan kejahatan berteknologi*. BP Undip.
- Ramli, A. M. (2023). *Cyber law dan hak privasi di Indonesia*. Alumni.
- Ramli, A. M. (2024). Perlindungan data pribadi dalam perspektif hak asasi manusia digital. *Jurnal Legislasi Indonesia*, 21(1), 89.
- Setiadi, A. (2020). *Manusia dan teknologi*. Graha Ilmu.
- Setiawan, B. (2023). *Kedaulatan data: Perlindungan privasi di era big data*. Alfabeta.
- Siahaan, N. H. T. (2024). *Hukum teknologi informasi: Tantangan global dan regulasi nasional*. Erlangga.
- Sinta, D. (2022). Urgensi legislasi perlindungan data pribadi di Indonesia. *Jurnal Hukum Lingkungan Indonesia*, 8(2), 129–131.
- Sinta, D. (2023). Analisis sanksi administratif terhadap kebocoran data oleh penyelenggara sistem elektronik. *Jurnal Hukum dan Pasar Modal*, 12(1), 56.
- Siregar, R. P. (2022). *Hak subjek data di Indonesia*. Pustaka Prima.
- Situmeang, S. M. T. (2021a). Perlindungan data pribadi di Indonesia. *Jurnal Hukum To-Ra*, 7(3), 398.
- Situmeang, S. M. T. (2021b). Penyalahgunaan data pribadi sebagai bentuk kejahatan sempalan (cyber crime). *Jurnal Hukum Lex Generalis*, 2(1), 85–92.

- Solove, D. J. (2021). *Understanding privacy*. Harvard University Press.
- Sudaryanto, A. (2023). *Kebijakan hukum siber Indonesia: Teori dan praktik*. UB Press.
- Sudirman, L. (2023). *Digital forensik dan investigasi siber dalam hukum Indonesia*. Kencana.
- Suhariyanto, B. (2021). Urgensi pembentukan otoritas pengawas perlindungan data pribadi yang independen. *Jurnal Penelitian Hukum De Jure*, 21(1), 75–77.
- Sujiastuti, T. (2022). Efektivitas penegakan hukum siber dalam perlindungan konsumen. *Jurnal Ius Kajian Hukum*, 10(1), 90.
- Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
- Wahyudi, R. (2024). Optimalisasi kapasitas aparat penegak hukum dalam menanggulangi cybercrime. *Jurnal Keamanan Digital Indonesia*, 12(1), 67.
- Wardani, A. K., & Ghozali, I. (2022). Tantangan keamanan data di era big data. *Jurnal Sistem Informasi*, 14(1), 42–47.
- Wicaksono, A. (2021). Perlindungan data pribadi dalam perspektif UU ITE. *Jurnal Hukum Digital*, 5(1), 45–47.
- Widodo, T. S. (2021). Keamanan infrastruktur digital dan tantangan penegakan hukum. *Jurnal Keamanan Nasional*, 7(2), 143–145.
- Yulianto, A. (2022). *Kedaulatan data di negara hukum*. Rajawali Pers.