E-NISN : 2614-2643
P-NISN : 2541-7037
Journal Equitable
Vol 11 No 1
2026

PERLINDUNGAN HUKUM TERHADAP DATA PRIBADI PENGGUNA PLATFORM DIGITAL DALAM PERSFEKTIF KEPASTIAN HUKUM

Ahmad Ardaful Abror Jauhari
Universitas 17 Agustus 1945 Surabaya, Indonesia, 1322300013@surel.untag-sby.ac.id

Frans Simangunsong
Universitas 17 Agustus 1945 Surabaya, Indonesia, frans@untag-sby.ac.id

Abstract

The ongoing digital transformation demands collective awareness of privacy as a fundamental right. Referring to the thoughts of Warren and Brandeis, privacy is an essential right for personal freedom and protection from external interference, making its regulation within a legal framework a necessity of our time. Confidentiality in personal data protection is crucial. However, evidence shows that personal data protection in Indonesia has not been effectively implemented despite having adequate legal foundations. Starting from this situation, this research focuses on examining the effectiveness of cyber law using a normative juridical method that combines analysis of legislation and conceptual approaches. Through normative analysis and descriptive reasoning, the findings of this study indicate that existing cyber law regulations, including the Consumer Protection Law, the Electronic Information and Transactions Law, the Personal Data Protection Law, and Kominfo Regulation No. 5 of 2020 on Private Electronic System Operators, have provided a sufficiently comprehensive legal basis for protecting users' digital personal data. However, its effectiveness still faces several challenges, particularly in law enforcement and the strength of sanctions, which require further evaluation. Furthermore, the implementation of cyber law in Indonesia continues to face fundamental challenges. Analysis reveals that systemic weaknesses lie not only in the execution of established regulations but also in the substantive content of the legislation itself. Critical analysis uncovers substantive inconsistencies between Article 67 of the Personal Data Protection Law and Article 48 of the Electronic Information and Transactions Law regarding provisions on personal data violations. This situation creates legal ambiguity that significantly reduces the effectiveness of law enforcement. Such regulatory overlaps risk producing inconsistent legal decisions.

Keywords: *Personal data protection, cyberlaw, digital privacy*

Abstrak

Transformasi digital yang terus bergulir menuntut kesadaran kolektif akan nilai privasi sebagai hak dasar. Merujuk pada pemikiran Warren dan Brandeis, privasi merupakan hak esensial untuk kebebasan personal dan perlindungan dari gangguan eksternal, yang pengaturannya dalam kerangka hukum menjadi suatu keharusan zaman. Kerahasiaan atas perlindungan data pribadi sangat diperlukan. Fakta menunjukkan bahwa perlindungan data pribadi di Indonesia belum berjalan efektif walau telah memiliki dasar hukum yang memadai. Berangkat dari kondisi ini, penelitian difokuskan pada pengkajian efektivitas cyber law melalui metode yuridis normatif yang mengombinasikan analisis peraturan perundang-undangan dan pendekatan konseptual. Melalui analisis normatif serta penalaran deskriptif , hasil dari penelitian ini menunjukkan bahwa Regulasi cyber law yang ada saat ini, termasuk Undang-Undang Perlindungan Konsumen, Undang-Undang Informasi Dan Transaksi Eletronik, Undang-Undang Perlindungan Data

E-NISN : 2614-2643
P-NISN : 2541-7037
Journal Equitable
Vol 11 No 1 2026

Pribadi,Dan Permenkominfo Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat, telah memberikan dasar hukum yang cukup komprehensif dalam melindungi data pribadi pengguna digital. Namun, efektivitasnya masih menghadapi beberapa tantangan, hal ini perlu sedikit dievaluasi dalam penegakkan hukum dan kekuatan sanksi. Kemudian Implementasi hukum siber di Indonesia masih menghadapi berbagai tantangan mendasar. Analisis menunjukkan bahwa kelemahan sistem tidak hanya terletak pada pelaksanaan regulasi yang sudah ditetapkan, tetapi juga pada muatan substansial peraturan perundang-undangan itu sendiri. Analisis kritis mengungkap adanya inkonsistensi substantif antara ketentuan Pasal 67 UU Perlindungan Data Pribadi dengan Pasal 48 UU ITE dalam pengaturan delik terkait pelanggaran data pribadi. Kondisi ini memunculkan ambiguitas yuridis yang secara nyata menurunkan tingkat efektivitas penindakan hukum. Tumpang tindih dari pengaturan semacam ini berisiko menghasilkan putusan hukum yang inkonsisten.
Kata kunci: Perlindungan data pribadi, *cyber law*, privasi digital

A. Pendahuluan

Aktivitas masyarakat merambah ke dunia maya (*cyberspace*). Menurut data dari Internet World Stats 2019, bahwa 58,78% dari total populasi dunia pengguna internet aktif, atau setara dengan 4.536.248.808 orang. Dari jumlah tersebut, benua Asia menyumbang 50,7% pengguna internet global, dengan total 2.300.469.859 pengguna. Maka dengan hasil analisis data, masyarakat dunia sedang menghadapi tantangan untuk beradaptasi dan beralih ke platform digital. Platform digital dapat diartikan sebagai ruang, fasilitas, atau wadah yang memungkinkan interaksi antara berbagai pihak untuk bertukar informasi, melakukan transaksi perdagangan, atau menawarkan barang dan jasa. Keberadaan platform digital memudahkan semua aktivitas tersebut dilakukan dalam satu tempat, karena menghubungkan penjual dengan pembeli, penyedia informasi dengan penerima, serta penyedia layanan dengan pengguna. [1]

Resiko yang terkait dengan penggunaan teknologi digital dapat

[1] Astir Rumondang Banjarnahor, dkk. *Resonansi Kualitas Layanan Perdagangan Sosial: Strategi Peningkatan Kinerja Penjualan UMKM Di Indonesia.* (Universitas Jendral Soedirman, 2024).

menimbulkan berbagai dampak negatif, termasuk dalam hal tindakan kriminal terutama pada aset digital pribadi yang dimiliki oleh masyarakat. Transformasi besar dalam ruang hidup manusia yang dimungkinkan berkat penggunaan ponsel pintar dan koneksi internet. Data APJII 2018 mengungkapkan bahwa lebih dari 171 juta warga Indonesia telah terhubung ke internet, mencakup hampir 65% populasi. Jumlah ini melonjak dibanding tahun 2017 yang baru menyentuh angka 143 juta pengguna. Adopsi penggunaan internet di Indonesia mengaksesnya melalui ponsel, dengan persentase pengguna telepon seluler mencapai 59,59%. Lebih dari separuh lapisan masyarakat Indonesia berpotensi menjadi korban kejahatan di dunia maya. Dan data tersebut berangsur menaik hingga 221 juta pengguna ditahun 2024.[2]

Dampak utamanya adalah semua hal yang mencakup hilangnya aset data dan bahkan kerusakan data pribadi. Ketika perangkat digital diretas, maka informasi sensitif seperti data keuangan, foto pribadi, dan dokumen penting secara tidak langsung dapat berpindah kepemilikan dan bisa jatuh ke tangan yang salah. Ini tidak hanya mengakibatkan kerugian finansial . Dalam praktiknya, pelaku memerlukan berbagai data sensitif seperti nomor kartu kredit, kode PIN, ID pengguna, nomor gawai, nomor rekening bank, serta informasi pribadi yang lainnya. Melalui tindakan ini, pelaku dapat memperoleh keuntungan dari kejahatan yang dilakukan, sementara korban yang datanya

[2] Asosiasi Penelenggara Jasa Internet Indonesia (APJII) , *APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang,* (Jakarta, 2024).

dicuri akan menanggung beban berat, baik secara finansial maupun psikologis.

Fenomena kejahatan dunia maya ini biasanya dikenal sebagai cybercrime. Cyber crime menjadi sorotan utama dalam era digital ini. [3] Hal tersebut mempengaruhi berbagai sektor dari kehidupan sehari-hari masyarakat khususnya bagi kalangan yang baru saja mengenal teknologi. Kajahatan cyber mencakup berbagai aktivitas jahat seperti pencurian identitas, penipuan online, serta berbagai penyebaran informasi palsu. Dan sebagian besar targetnya adalah masyarakat minim pengetahuan karena yang pertama kekurangan kesadaran akan risiko kemudian kurangnya langkah-langkah perlindungan yang memadai.

Kecemasan yang dialami oleh masyarakat sering kali mendorong pemerintah untuk membentuk atau mengamandemen Undang-undang guna memberikan perlindungan secara efektif. Untuk menanggulangi kejahatan siber yang semakin kompleks, diperlukan adanya regulasi siber sebagai landasan hukum yang memberikan keamanan atas aktivitas di dunia maya. Hukum ini tidak hanya mencakup perlindungan terhadap individu dan perusahaan dari serangan cyber seperti pencurian data dan serangan malware, tetapi juga mengatur hak dan kewajiban dalam penggunaan teknologi informasi. UU ITE (Undang-Undang Nomor 11 Tahun 2008) telah menjadi pilar utama sistem hukum Indonesia dalam memerangi kejahatan dunia maya. Regulasi ini tidak hanya menjadi landasan hukum, tetapi juga menciptakan paradigma baru dalam penanganan tindak

[3] Mohammad Labib dan Abdul Wahid , "*Kejahatan Mayantara", (Cyber Crime)* (Bandung : PT. Refika Aditama, 2005).

pidana di era digital yang terus mengalami transformasi. Pemanfaatan teknologi informasi dan transaksi elektronik mencakup berbagai aspek penting, mulai dari perlindungan data pribadi, keamanan siber, hingga transaksi digital yang aman, sekaligus memberikan kerangka hukum yang jelas untuk melindungi masyarakat dari ancaman dunia maya seperti penipuan online, peretasan, dan penyalahgunaan informasi. [4]

Regulasi transaksi elektronik mengalami beberapa kali amendemen dan terakhir kali ditinjau adalah melalui Undang-undang Nomor 1 Tahun 2024.[5] Pembaruan undang-undang ini memiliki tiga tujuan utama: (1) mempertegas jaminan perlindungan privasi digital warga, (2) menyempurnakan sistem deteksi dini dan pencegahan kejahatan maya, serta (3) melakukan penyesuaian hukum terhadap inovasi teknologi yang terus berubah dengan cepat. Salah satu perubahan penting dalam amendemen ini adalah penambahan ketentuan mengenai keamanan data pribadi dan sanksi yang lebih tegas terhadap pelanggaran di bidang cyber crime. Adanya regulasi yang jelas, masyarakat dapat merasa lebih aman dalam beraktivitas online. [6] Prioritas utama dari amandemen yang dilakukan merupakan wujud tanggap cepat dari pemerintah dalam memvalidasi beberapa tindakan kejahatan yang mengkhawatirkan dapat terjadi.

Berbicara mengenai istilah data pribadi, menurut pengertian secara terminologi "data" merupakan kumpulan

[4] Ersya. "Permasalahan Hukum dalam Menanggulangi Cyber Crime di Indonesia". Jurnal of Moral and Civic Education 1 No. 1, (2017).

[5] Rodia. "Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara(Cybercrime)". Jurisprudentie 6 no.2. (2019): 230-239

[6] Situmeang., S. M. *CYBER LAW* (Bandung : CV.Cakra, 2020.).

fakta, informasi, atau nilai yang dapat dikumpulkan, dianalisis, dan digunakan untuk berbagai tujuan. Maka secara garis besar, data pribadi dapat diartikan sebagai informasi pribadi pengguna yang dapat digunakan untuk dilakukannya identifikasi.[7] Kebijakan e-KTP sebagai transformasi digital data kependudukan justru menimbulkan tantangan baru dalam perlindungan data pribadi. Sentralisasi informasi warga negara dalam sistem elektronik pemerintah meningkatkan kerentanan terhadap potensi penyalahgunaan yang memerlukan pengawasan ketat. Salah satu komponen penting dalam e-KTP adalah Nomor Induk Kependudukan (NIK) yang digunakan untuk mengidentifikasi setiap individu dalam sistem administrasi kependudukan. Bentuk dari e-KTP berisikan berbagai informasi pribadi terekam, data sensistif yang berpotensi penyalahgunaan data pribadi menjadi kekhawatiran, terutama jika sistem keamanan yang ada tidak cukup kuat. Mengingat pada beberapa dekade yang lalu menurut yang ditulis pada *medcom.id* yang menyatakan bahwa terjadi beberapa kebocoran data pribadi yang jumlahnya tidak sedikit. Pada tahun 2019, Indonesia dikejutkan oleh insiden kebocoran data masif yang mengekspos informasi sensitif seluruh 279 juta peserta BPJS Kesehatan. Data yang terekspos meliputi identitas lengkap (nama, alamat, kontak) hingga riwayat medis pribadi, yang kemudian beredar di pasar gelap digital. Kasus ini tidak hanya mengungkap kerapuhan sistem proteksi data kesehatan nasional, tetapi juga memunculkan ancaman riil terhadap privasi dan keamanan warga dalam skala epidemik.

[7] https://kbbi.web.id/data, diakses pada 08 Agustus 2024, 13:04 WIB.

Kelalaian dalam mengelola kebocoran data dapat menimbulkan dampak negatif yang signifikan sementara legalitas dari hukum atas kejahatan pencurian data pribadi telah diamandemenkan. *Proteksi* data pribadi menjadi suatu kebutuhan yang mendesak. Penulis memiliki ketertarikan akademik untuk melakukan kajian teoritis mendalam mengenai regulasi perlindungan data pribadi di platform digital Indonesia, dengan pendekatan analisis kepastian hukum sebagai perspektif utama. Secara yuridis, Indonesia sebenarnya telah membangun kerangka hukum yang komprehensif melalui:

1. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) sebagai payung hukum utama
2. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) sebagai dasar hukum siber
3. Berbagai peraturan turunan sebagai implementasi teknis.

Dari uraian diatas, penelitian ini menitikberatkan permasalahan cyberlaw khususnya pada platform digital. Mengingat eksistensi hukum cyberlaw saat ini tidak dapat dilepaskan dalam kehidupan sehari-hari.

B. Rumusan Masalah

1. Bagaimana pengaturan perlindungan data pribadi pada platform digital di Indonesia?
2. Bagaimana perlindungan hukum data pribadi pada platform digital dalam persfektif kepastian hukum?

C. Tujuan Penelitian

Adapun tujuan dari penelitian untuk mengetahui dan menganalisis tentangpengaturan perlindungan data pribadi pada platform digital di Indonesia dan perlindungan hukum data pribadi pada

platform digital dalam persfektif kepastian hukum

D. Metode Penelitian

Jenis penelitian ini bersifat yuridis normatif dan mengadopsi metode kuantitatif untuk mengeksplorasi permasalahan hukum. Terdapat dua pendekatan yang digunakan: *pertama*, pendekatan *statute approach* (perundang-undangan) untuk memahami norma-norma hukum yang berlaku, *kedua,* pendekatan *conceptual approach* (konseptual) yang bertujuan untuk membedah konsep-konsep hukum. Teknik pengumpulan data penelitian dilakukan dengan *library research* yakni penelitian kepustakaan dengan cara mengumpulkan data kemudian menganalisis berbagai sumber literature. Bahan hukum primer yang dikaji meliputi peraturan perundang-undangan terkait, sedangkan bahan hukum sekunder mencakup jurnal akademik, buku referensi, serta hasil-hasil penelitian sebelumnya yang relevan dengan topik penelitian.[8]

E. Hasil Penelitian dan Pembahasan

1. Perspektif Perlindungan Data Pribadi Pada Platform Digital di Indonesia

Landasan hukum perlindungan data tercantum dalam konstitusi, Pasal 28G Ayat (1) UUD 1945, mengakui hak seluruh warga negara atas perlindungan individu, keluarga, kehormatan, harta benda, serta jaminan keamanan dari segala bentuk ancaman dalam pelaksanaan hak-hak dasar pengguna. Pemerintah mengimplementasikan regulasi khusus yang mengatur penyimpanan dan penggunaan data pribadi. Penanggulangan kejahatan melalui hukum pidana merupakan bagian integral dari penegakan hukum, khususnya dalam ranah pidana, di mana politik hukum pidana berperan sebagai

[8] Peter Mahmud Marzuki, *Penelitian Hukum* (Bandung: Prenada Media, 2020).

komponen kebijakan dalam law enforcement policy untuk mengatasi tindak kriminal secara efektif. Penggunaan alat hukum termasuk hukum pidana secara langsung menjadi sarana untuk mengatasi masalah sosial. Mengacu dalam situasi perkembangan era globalisasi, penegakan hukum tidak hanya didasarkan oleh tindak kejahatan kontak fisik melainkan juga berdasarkan kejahatan *cybercrime*. Maka muncul istilah cyber law sebagai wujud landasan atas tindak kejahatan tersebut.

Menurut Widodo, *Cyber Law* adalah hukum yang mengatur tindak kejahatan di ruang digital yang dilakukan melalui jaringan internet. Konsep cyber law telah menciptakan perspektif hukum yang berbeda di Indonesia, terutama terkait penggunaan teknologi dan informasi. Di Indonesia, keberadaan cyber law diwujudkan melalui penerbitan Undang-Undang yang berfungsi sebagai dasar hukum dalam proses peradilan.[9] Bila ditelaah jauh sebelum adanya cyberlaw seperti sekarang, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen sebagai dasar dalam penaggulangan atas hak konsumen mencakup juga mengenai ha katas perlindungan data pribadi. Maka sepenuhnya isi landasan ini memberikan pandangan luas maupun landasan atas hak konsumen maupun perlindungan data pribadi, namun sebab perkembangan era digitalisasi yang meningkat perundang-undangan tentang perlindungan konsumen perlu ada penyempurna landasan hukum lain untuk dilakukannya perlindungan secara kompleks.

Peranan hukum cyber menjadi sangat penting dan strategis, terutama untuk melindungi masyarakat yang berperan.

[9] Widodo." *Hukum Pidana Di Bidang Teknologi Informasi (Cybercrime Law) : Telaah Teoritik Dan Bedah Kampus".* (Yogyakarta: Aswaja Pressindo, 2013).

Dengan munculnya regulasi penyempurna sebagai landasan utama dalam menanggulangi kejahatan cybercrime tidak terkecuali mengenai kasus-kasus pencurian data pribadi pada platform digital. Tingginya kasus pencurian data pribadi di platform digital telah menjadi ancaman keamanan siber yang kritis. Berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), data pribadi dibedakan menjadi dua jenis: data pribadi biasa dan data sensitif. Data pribadi biasa meliputi informasi identitas dasar seperti nama, alamat, tanggal lahir, nomor telepon, email, dan nomor identitas (KTP, SIM, paspor). Sementara itu, data sensitif—seperti informasi kesehatan, keuangan, biometrik, dan keyakinan agama memerlukan perlindungan ekstra karena dampak buruknya jika mengalami kebocoran. Kejahatan pencurian data pribadi di dunia maya atau yang sering disebut phishing, merupakan tindakan kriminal yang bertujuan mengambil informasi pribadi atau rahasia secara ilegal. Pelaku biasanya meminta korban untuk memberikan detail sensitif seperti nomor kartu kredit, kode PIN, ID pengguna, nomor telepon, nomor rekening bank, dan informasi pribadi lainnya.[10] Pelaku mendapatkan keuntungan finansial atau lainnya, sementara korban mengalami kerugian besar akibat penyalahgunaan data yang dicuri.

Tanpa pemahaman yang cukup tentang risiko dan tanggung jawab dalam menggunakan teknologi digital, masyarakat rentan terjerumus ke dalam aktivitas yang melanggar hukum ataupun sebagai korban daripada kehajatan yang dialami. Umumnya kejahatan pada platform digital mengenai

[10] Muhammad Fikri and Abdurrakhman Alhakim, "Urgensi Pengaturan Hukum Terhadap Pelaku Tindak Pidana Pencurian Data Pribadi Di Indonesia," YUSTISI 9, no. 1 (2022).

pencurian data pribadi dikenal dengan *phishing*. Phishing dapat difahami sebagai bentuk kejahatan digital yang dilakukan secara online dengan tujuan mencuri informasi pribadi korban, seperti kata sandi, data pribadi yang berkenaan langsung dengan identitas platform digital dan lainnya. Tindakan ini seringkali bertujuan untuk mencuri identitas dengan mengambil dana secara illegal. Phishing merupakan salah satu ancaman serius yang perlu mendapatkan perhatian khusus karena tidak hanya membahayakan keamanan data pribadi, tetapi juga mengganggu kenyamanan bertransaksi online dan mengancam stabilitas ekonomi suatu negara.[11]

Oknum pelaku phishing biasanya berkamuflase sebagai pihak ataupun institusi yang terpercaya, seperti perusahaan ternama, bank, atau lembaga keuangan, untuk mengelabui korban agar mau memberikan informasi sensitif mereka. Mereka menggunakan berbagai teknik mulai dari manipulasi psikologis (social engineering) hingga pemanfaatan teknologi canggih untuk membuat korban percaya bahwa permintaan informasi tersebut adalah sah. [12]Modus operandi ini sangat berbahaya karena tidak hanya merugikan individu. Keberadaan modus operandi sem acam ini menimbulkan ancaman serius, baik bagi individu maupun stabilitas keamanan dunia digital. Secara esensial, modus operandi merujuk pada teknik terstruktur yang sengaja dirancang pelaku kejahatan siber untuk melakukan eksploitasi. Metode penipuan digital dengan mengelabui korban untuk membagikan data sensitif tidak hanya menimbulkan kerugian

[11] Sunarso Siswanto, "*Hukum Informasi Dan Transaksi Elektronik*". (Jakarta: PT Rineka Cipta. 2009).

[12] Raharjo Agus, "*Cybercrime , Pemahaman Dan Upaya Pencegaha Kejahatan Berteknologi*".(Yogyakarta : PT.Citra Aditya Bakti,2002).

finansial bagi individu, tetapi juga berpotensi membahayakan stabilitas keamanan nasional. Modus ini semakin canggih dengan penggunaan teknik rekayasa sosial (social engineering) dan pemalsuan identitas yang sulit terdeteksiKetika pelaku berhasil mencuri data penting seperti kata sandi akun bank atau informasi pribadi, dampaknya bisa meluas hingga merusak ekonomi dan stabilitas sosial. Banyak kasus menunjukkan bagaimana data hasil phishing digunakan untuk penipuan besar-besaran, pencucian uang, bahkan spionase terhadap institusi penting negara.

Teknik phishing terus berkembang, pelaku sering memanfaatkan AI untuk membuat email atau website palsu yang nyaris sempurna sulit dibedakan dengan aslinya. Mereka juga memanfaatkan momen-momen tertentu seperti pembaruan sistem atau bencana alam, ketika kewaspadaan korban cenderung menurun. Tanpa edukasi yang memadai, masyarakat awam sangat rentan terjebak dalam skema ini. Salah satu bentuk kejahatan siber yang diatur secara eksplisit dalam Pasal 30 Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) merupakan tindakan kriminal di mana pelaku menyusup ke dalam jaringan atau sistem komputer tanpa hak akses legal atau persetujuan pemilik. Modus ini tidak hanya mengancam privasi, tetapi juga berpotensi melumpuhkan infrastruktur digital, baik milik korporasi maupun negara. Para peretas umumnya melakukan tindakan ini dengan tujuan merusak sistem atau mencuri data sensitif dan rahasia.[13]

Dampak dari praktik ini sangat merusak. Banyak korban yang baru menyadari menjadi sasaran kejahatan setelah

[13] Windi, dkk, "Konstruksi Hukum dalam Cybercrime Pelaku Kejahatan Teknologi Informasi" Siyasah: Jurnal Hukum Tata Negara 3, No. 2, (Desember, 2023), 220-239.

mengalami kerugian material atau kerusakan reputasi. Undang-undang Informasi dan Transaksi Elektronik terbaru yakni Pasal 27A dan Pasal 27B, yang dirancang untuk mengatasi kekosongan hukum dan memberikan perlindungan yang lebih komprehensif terkait aktivitas didunia maya. Pada pasal 27A, mengenai perlindungan terhadap hak privasi individu. Secara tegas melarang penyebaran informasi elektronik yang memuat data pribadi tanpa izin pemilik, kecuali diatur lain oleh undang-undang. Aturan ini dirancang untuk melindungi privasi individu dari penyalahgunaan data, namun implementasinya di lapangan menghadapi sejumlah tantangan kompleks.

Sementara itu, Pasal 27B mengatur tentang perlindungan terhadap reputasi dan kehormatan seseorang. Pasal ini melarang penyebaran konten elektronik yang mengandung penghinaan, pencemaran nama baik, atau fitnah. Meskipun mirip dengan Pasal 27 Ayat (3) yang dihapus, Pasal 27B dirumuskan dengan lebih spesifik untuk menghindari multitafsir dan penyalahgunaan pasal tersebut. Perubahan tersebut dilakukan sebagai respons terhadap perkembangan masalah dan situasi nyata yang terjadi di masyarakat. Dinamika dunia digital yang terus berubah menuntut adanya penyesuaian regulasi agar tetap relevan dan efektif dalam menangani berbagai tantangan baru, seperti kejahatan siber, penyebaran hoaks, serta pelanggaran privasi dan data pribadi. Ketetapan yang disahkan memiliki kekuatan hukum yang konkret sebagai alur dalam penanggulangan aktivitas tindak kejahatan di dunia maya.[14]

Pengaturan mengenai pencurian data pribadi secara jelas diatur dalam Pasal 30

[14] Rahmat Syah "Strategi Kepolisian Dalam Pencegahan Kejahatan Phising Melalui Media Sosial Di Ruang Siber". Jurnal Impresi Indonesia, 2, No. 9(2023), 864–870.

mengenai larangan terhadap akses ilega (*unauthorized access*) ke sistem elektronik. landasan hukum tersebut menjadi langkah awal dalam menangani kasus pencurian data pribadi. Menurut Ayat (1), "*siapa pun yang dengan sengaja dan tanpa izin mengakses komputer atau sistem elektronik milik orang lain dapat dipidana*". Sementara itu, Ayat (3) "*menetapkan sanksi yang lebih berat jika akses ilegal tersebut mengakibatkan terekspos nya data pribadi. Pelaku dapat dihukum penjara maksimal 8 tahun dan/atau didenda hingga Rp2 miliar*".

Beberapa kasus yang terjadi pada pengguna platform digital, sebagai contoh media sosial instagram maupun whatsapp rentan mengalami penyadapan. Kejadian tersebut marak dilakukan oleh oknum kejahatan. Penyadapan dalam konteks ini merujuk pada tindakan mengambil atau mengakses informasi elektronik secara tidak sah, baik melalui cara teknis maupun non-teknis. Penyadapan data pribadi, seperti mengintip atau mencuri informasi sensitif milik orang lain, termasuk dalam tindakan yang dilarang oleh Pasal 32. Bila mana pelaku yang terbukti melakukan penyadapan dapat dikenakan sanksi pidana yang serius. Ditambah dengan penguatan pada Pasal 36 yang mengatur tentang perusakan data. Perusakan data mencakup tindakan menghapus, merusak, atau mengubah data elektronik milik orang lain tanpa izin. Dalam kasus pencurian data, pelaku sering kali tidak hanya mencuri data tetapi juga merusak atau memanipulasi data tersebut untuk menyembunyikan jejak atau untuk tujuan tertentu. Konsikuensinya pun Pelaku tindak perusakan data dapat dikenakan sanksi pidana.

Latar belakang diamandemenkannya regulasi mengenai informasi dan transaksi elektronik kerap menuai kontroversi, terutama terkait pasal-pasal yang dianggap

ambigu dan multitafsir. [15]Beberapa pasal pemberdayaan dan perlindungan pada platform digital khususnya data pribadi, seperti Pasal 26 dan Pasal 40, menjadi sorotan utama. Pasal 26 UU ITE secara tegas menjamin hak warga atas keamanan data pribadi dalam sistem elektronik, dengan menetapkan syarat mutlak: persetujuan pemilik data sebagai landasan legal pengolahan informasi, kecuali ada pengecualian hukum.[16] Pasal 40 kemudian memperkuat ini dengan mewajibkan penyelenggara sistem untuk menjamin tiga aspek vital: kerahasiaan, keutuhan, dan ketersediaan data pengguna. Namun, fakta di lapangan berbicara lain. Maraknya kasus peretasan, jual-beli data, hingga kebocoran massal menguak paradoks pahit regulasi yang terlihat komprehensif justru gagal menjadi tameng nyata bagi privasi digital masyarakat.

Dalam konteks perlindungan data, Undang-undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menetapkan mekanisme penegakan hukum yang bersifat gradual (progressive enforcement). Regulasi terbaru tersebut mengadopsi mekanisme penegakan hukum berbasis struktur sanksi berjenjang (tiered sanctions), yang dirancang untuk memberikan efek jera secara progresif. Penerapan sanksi terhadap pelanggaran dirancang secara bertahap, dimulai dari tindakan persuasif berupa teguran tertulis sebagai bentuk sanksi administratif. Namun, jika pelaku tetap tidak mematuhi aturan,

[15] Fikri Irfan Adristi, Erika Ramadhani "Analisis Dampak Kebocoran Data Pusat Data NasionalSementara2 (PDNS 2)Surabaya: Pendekatan Matriks Budaya Keamanan Siber dan Dimensi Budaya Nasional Hofstede"Selekta Manajemen: Jurnal Mahasiswa Bisnis & Manajemen 2, No. 06, (2024), 196-212.

[16] Sumiaty Adelina Hutabarat, dkk," *CYBER-LAW: Quo Vadis Regulasi UU ITE dalam Revolusi Industri 4.0 Menuju Era Society 5.0*" (PT. Sonpedia Publishing Indonesia, 2023).

otoritas berwenang akan memberlakukan eskalasi hukuman, mulai dari denda finansial hingga sanksi hukum yang lebih represif—mencerminkan pendekatan progresif dalam penegakan aturan. Pelanggaran yang bersifat berat (egregious violations), UU PDP menerapkan sanksi pidana dengan ancaman hukuman penjara maksimal 5 (lima) tahun dan/atau denda pidana mencapai Rp5.000.000.000,00 (lima miliar rupiah), sebagaimana diatur dalam Pasal 67. Salah satu kewajiban penting yang diatur dalam Pasal 21, adalah pelaporan kebocoran data kepada Otoritas Perlindungan Data Pribadi (OPDP) dan subjek data yang terkena dampak dalam waktu 72 jam setelah kebocoran terdeteksi. Regulasi ini secara tegas melarang pelapor tanpa pengecualian untuk melewati batas waktu yang telah ditetapkan, bahkan dalam situasi darurat sekalipun. Kebijakan ini dirancang untuk memaksa respons yang cepat dan akuntabel dalam menangani kasus kebocoran data, dengan tujuan utama membatasi kerugian bagi pemilik data yang terdampak.

Namun, ketentuan ini juga menimbulkan sejumlah tantangan dan kritik. *Pertama*, dalam praktiknya, mendeteksi dan mengidentifikasi kebocoran data seringkali memerlukan waktu yang tidak sedikit, terutama jika kebocoran terjadi dalam sistem yang kompleks atau melibatkan serangan siber yang canggih. *Kedua*, keterbatasan sumber daya yang dimiliki oleh pengontrol data, terutama perusahaan kecil atau menengah, dapat menghambat kemampuan mereka untuk memenuhi tenggat waktu 72 jam. *Ketiga*, ada kekhawatiran bahwa tekanan untuk melapor dalam waktu singkat dapat menyebabkan laporan yang kurang akurat atau tidak lengkap, yang justru dapat mengurangi efektivitas penanganan insiden.

Permenkominfo Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik

Lingkup Privat. Mekanisme pengujian peraturan di Indonesia berjalan secara optimal. Fakta ini terlihat banyaknya regulasi yang tegas dalam perlindungan data pribadi. Sebagai contoh *Pertama,* Pasal 9 secara imperatif mewajibkan seluruh penyelenggara sistem elektronik sektor privat, baik yang berkedudukan hukum di dalam yurisdiksi Indonesia maupun yang beroperasi secara lintas batas negara (*cross border*) untuk melakukan pendaftaran kepada Kementerian Komunikasi dan Informatika sebagai otoritas yang berwenang. Pendaftaran ini mencakup penyediaan informasi mengenai identitas, jenis layanan, dan mekanisme operasional . Pengguna yang tidak mematuhi kewajiban ini dapat dikenai sanksi, termasuk pemblokiran akses. Tujuannya adalah untuk memastikan akuntabilitas dan transparansi.

Kedua, Pasal 13 tentang kewajiban membuka data untuk kepentingan penegakan hukum. Pada pasal ini, mewajibkan penyelenggara sistem elektronik memberikan akses data pengguna kepada aparat penegak hukum jika diminta untuk kepentingan investigasi kasus pidana. Pengawasan yang ketat mendorong akuntabilitas dalam pengelolaan data. Yang mana secara tidak langsung membantu membangun kepercayaan publik terhadap institusi atau organisasi yang mengelola data tersebut. Pengawasan ketat memang diperlukan, akan tetapi mengingat penting juga untuk menyeimbangkannya dengan kebebasan individu. Regulasi harus dirancang sedemikian rupa sehingga tidak menghambat inovasi atau kebebasan berekspresi.

Secara keseluruhan, Permenkominfo Nomor 5 Tahun 2020 memiliki tujuan tegas yaitu menciptakan platform digital yang aman. Mengingat undang-undang adalah kebutuhan dan juga jawaban atas keluhan yang diterima berdasarkan tindakan yang

terjadi pada masyarakat. Konsenkuensinya diterima atau bahkan ditolak mentah-mentah karena ketidakefisiensinya ketentuan yang berlaku. Maka asas pertimbang hukum perlu dituguhkan dalam pembentukan satu ketentuan. Beberapa ketentuan yang tertera memiliki kontrofersi. Meskipun demikian, menurut data pembanding lain dari National Cyber Security Index (NCSI), keamanan siber (cybersecurity) Indonesia berada di peringkat ke-6 di Asia Tenggara. NSCI memuat data tersebut berdasarkan indikator siber, yang salah satunya adalah produk hukum terkait keamanan siber. Meskipun Indonesia telah memiliki beberapa regulasi dan upaya dalam meningkatkan keamanan siber, masih ada ruang untuk perbaikan dan peningkatan, terutama jika dibandingkan dengan negara-negara lain di kawasan Asia Tenggara.

Salah satu faktor penyebabnya adalah kurangnya pengawasan dan penegakan hukum yang ketat terhadap penyelenggara sistem elektronik. tantangan ini semakin kompleks karena negara ini belum sepenuhnya memiliki tim siber (*cyber team*) yang khusus dan terintegrasi untuk menanggulangi kesenjangan hukum tersebut. Sejumlah instansi, seperti Kepolisian Republik Indonesia (Polri) melalui Direktorat Tindak Pidana Siber dan Badan Siber dan Sandi Negara (BSSN), telah berupaya menangani kejahatan siber. Namun, cakupan penanganannya masih terbatas. Akibatnya, proses penyelesaian kasus seperti pencurian data pribadi seringkali lambat. Kondisi ini membuat korban—khususnya pengguna yang datanya dicuri merasa sangat dirugikan. Aset pribadi mereka kerap dimanfaatkan oleh oknum tidak bertanggung jawab tanpa tindakan hukum yang cepat dan tegas.

2. Perlindungan Hukum Data Pribadi Pada Platform Digital dalam Perspektif Kepastian Hukum

Adopsi digitalisasi media dunia maya yang meluas secara global telah membawa dampak signifikan.[17] Transisi menuju era digital ini turut mendorong percepatan pertumbuhan ekonomi dalam beberapa tahun terakhir. Di era serba teknologi seperti sekarang, pelanggaran terhadap kerahasiaan informasi personal telah berkembang menjadi persoalan krusial yang membahayakan privasi warga. Dampak kejahatan siber di seluruh dunia sangat signifikan, dengan kerugian ekonomi yang diproyeksikan mencapai 8 triliun USD per tahun pada tahun 2023 dan berpotensi meningkat menjadi $10,5 triliun pada tahun 2025. Angka tersebut menunjukkan betapa besar beban finansial yang ditanggung oleh masyarakat global akibat kejahatan siber. Ditengah pesatnya transformasi digital, kerentanan data pribadi terhadap eksploitasi dan pelanggaran privasi semakin mengkhawatirkan. Perlindungan informasi individu bukan sekadar kebutuhan teknis, melainkan hak fundamental yang harus dijamin oleh negaraIndonesia sebagai negara berkembang dengan tingkat adopsi teknologi digital yang masif (*digital massive adoption*) menghadapi tantangan serius dalam aspek pengamanan data pribadi warga negara (*data privacy protection*). Hak atas privasi termasuk keamanan data pribadi harus menjadi prioritas kebijakan mengingat maraknya kasus kebocoran dan penyalahgunaan informasi. Jika tidak segera ditangani, dampaknya bisa merugikan masyarakat secara sistemik.

[17] Aris Basuki, dkk. "Pengaruh Perkembangan Teknologi Informasi Dan Komunikasi Terhadap Pelaksanaan Tugas Tni"Jurnal Mahatvavirya 11. No. 2. (2024).

Masalah-masalah yang ditimbulkan berkaitan dengan efisiensi atas perlindungan hukum. Menurut Jimly Asshiddqie, perlindungan hukum memiliki prinsip dipatuhi oleh semua pihak, termasuk para pemegang kekuasaan. Tidak ada individu atau kelompok yang boleh berada di atas hukum, karena kedaulatan hukum menjamin keadilan dan kesetaraan bagi seluruh masyarakat. Prinsip kesetaraan dalam penegakan hukum menjadi pilar utama yang justru memperkuat efektivitas perlindungan hukum. Tanpa perlakuan yang adil dan non-diskriminatif, upaya penegakan aturan berisiko kehilangan legitimasi dan partisipasi publik. Menurut R. La Porte dalam Journal of Financial Economics, upaya perlindungan hukum yang memanfaatkan instrumen dan mekanisme penegakan hukum dari negara memiliki dua ciri utama, yaitu bersifat preventif dan bersifat represif. Tindakan represif diwujudkan melalui penerapan regulasi dan sanksi, yang menjadi salah satu bentuk jaminan perlindungan hukum paling kuat. Langkah preventif bertujuan untuk menghindari terjadinya konflik, di mana subjek hukum diberi hak untuk menyampaikan sanggahan atau pandangan sebelum keputusan pemerintah. [18]

Berbicara mengenai jaminan perlindungan, sesuai dengan perundang-undangan khususnya persyaratan mengenai tingkat keamanan platform digital tertera pada pasal 34 ayat (2) Undang-undang perlindungan data pribadi. Adanya petunjuk yang jelas mengenai standarisasi efisiesi platform digital yang aman memunjang keamanan perangkat sekaligus data pribadi

[18] Muhammad Raditya Vijayaputro, Perlindungan Hukum Mengenai Investasi Digital dalam Bentuk Non-Fungible Token Berdasarkan Undang-Undang Nomor 25 Tahun 2007" UNES LAW REVIEW Vol. 6, No. 2, (2023)

pengguna. Persyaratan tersebut menjadi dasar hukum bagi penyelenggaraan platform digital yang memenuhi prinsip security by design dan security by default. Alur perlindungan data pribadi memiliki beberapa perundang-undangan yang melatar belakangi keadilan tersebut. Meski sejumlah aturan hukum telah memberikan payung perlindungan bagi data pribadi, implementasinya masih menyisakan berbagai celah yang belum diatur secara komprehensif. Definisi mengenai kategori data yang termasuk dalam ranah privasi individu, khususnya ketika terjadi penggabungan berbagai jenis informasi, masih belum dijelaskan secara rinci dalam produk hukum yang ada. Kondisi ini pada akhirnya menciptakan multitafsir dan ketidakjelasan regulasi dalam upaya safeguard informasi personal para pengguna.

Regulasi mengenai perlindungan data pengguna ini menetapkan sejumlah prinsip kunci, mulai dari pengumpulan data yang transparan, batasan pemrosesan, hingga sanksi tegas bagi pelanggar. Adanya landasan hukum tersebut, terbentuk kerangka hukum yang lebih komprehensif untuk melindungi hak konsumen. Setiap entitas yang mengelola data pribadi wajib mematuhi ketentuan penyimpanan, penggunaan, dan pelaporan, mengurangi risiko penyalahgunaan oleh pihak tak bertanggung jawab.. Regulasi ini secara rinci mengklasifikasikan berbagai kategori data sensitif, mekanisme pengolahan informasi, serta mendefinisikan secara jelas peran masing-masing pihak yang terlibat seperti Pemilik Data, Pengelola Data, dan Penyedia Pemrosesan Data. dalam Bab IX tentang Struktur Kelembagaan (Pasal 58-61), Undang-Undang Perlindungan Data Pribadi menegaskan peran aktif pemerintah dalam menjaga kerahasiaan data konsumen melalui

pembentukan badan khusus. Lembaga ini memiliki wewenang untuk:

1. Merumuskan kebijakan dan rencana aksi perlindungan data.
2. Melakukan pengawasan terhadap penerapan aturan perlindungan data.
3. Memberikan sanksi administratif atas pelanggaran terhadap ketentuan Undang-Undang Perlindungan Data Pribadi.

Analisis perspektif teori kepastian hukum, yang menekankan bahwa keberlakuan suatu undang-undang harus dinilai berdasarkan tingkat keadilan yang dirasakan masyarakat, regulasi ini sangat menunjang dalam hal sinkronisasi perlindungan hukum. [19]Terlihat dalam Pasal 56, yang mengizinkan Pengendali Data Pribadi untuk melakukan transfer data ke pihak luar negeri mencantumkan persyaratan persetujuan dari subjek data. Teori kepastian hukum menekankan bahwa suatu peraturan harus memberikan jaminan keadilan bagi masyarakat. Sehingga regulasi ini hadir untuk melindungi privasi individu. Adanya frasa *"persetujuan subjek data"* dalam transfer data lintas batas mengurangi resiko kontrol individu atas data pribadi mereka. Prinsip consent atau persetujuan pihak pengguna merupakan fondasi utama dalam perlindungan data.

Persetujuan atas pengguna platform digital menunjang keamanan digital. Undang-undang tersebut secara tegas mewajibkan melakukan proteksi tersebut guna penunjang daripada perlindungan maupun penegakkan hukum. Mekanisme penegakan hukum merupakan pilar sentral dalam mewujudkan kepastian hukum, khususnya dalam konteks perlindungan data

[19] *Ibid.*

pribadi. Tanpa penegakan yang tegas, undang-undang seperti Undang-Undang Perlindungan Data Pribadi hanya akan menjadi norma normatif tanpa dampak nyata bagi masyarakat. Kepastian hukum mensyaratkan bahwa setiap pelanggaran harus diikuti dengan konsekuensi hukum yang jelas, sehingga menciptakan deterrent effect atau efek jera sekaligus melindungi hak-hak subjek data.

Sistem hukum Indonesia dalam melakukan penegakan hukum atas pelanggaran data pribadi dapat dilakukan melalui tiga jalur utama: *sanksi administratif, gugatan perdata, dan tindakan pidana*. [20]Ketiga mekanisme ini saling melengkapi untuk memastikan bahwa pelanggaran tidak hanya dihentikan, tetapi juga memberikan kompensasi bagi korban dan menghukum pelaku sesuai tingkat kesalahannya. Sebagaimana diatur dalam Pasal 12 Ayat (1), pemilik data pribadi berhak mengajukan gugatan dan memperoleh kompensasi jika terjadi pelanggaran dalam pengolahan data pribadi mereka, sesuai dengan ketentuan hukum yang berlaku. Hal ini memperkuat posisi individu dalam menjaga kerahasiaan dan keamanan data mereka. Dalam perspektif hukum, ruang siber (cyber space) tidak lagi dapat diukur dengan parameter hukum tradisional jika digunakan sebagai dasar untuk menentukan objek atau subjek tindak pidana. Pendekatan konvensional justru akan menimbulkan banyak kelemahan, mengakibatkan berbagai pelanggaran hukum terlepas dari penegakan hukum.

Meskipun transformasi digital yang terus bergerak maju menuntut adanya pembaruan sistem keamanan yang lebih komprehensif, Undang-Undang Informasi

[20] Winda Agustina1 dan Sidi Ahyar Wiraguna, "Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi dari Kejahatan Peretasan"Media Hukum Indonesia 2, No. 6 (2025), 117-127.

dan Transaksi Elektronik dan Undang-Undang Perlindungan Data Pribadi menjadi dasar hukum dalam penanganan kejahatan siber, termasuk kasus kebocoran data pribadi pada platform digital, kedua regulasi ini dinilai masih memiliki sejumlah kelemahan. Keterbatasan utamanya terletak pada kurangnya cakupan yang menyeluruh dalam pengaturan teknis. Pertama, dalam regulasi mengenai saknsi atas tindak kejahatan pencurian data pribadi. Pasal 67 Ayat 1 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) memberikan dasar hukum tegas bagi penindakan pelaku kejahatan data. Setiap pihak yang secara sengaja dan melawan hukum mengumpulkan atau menggunakan data pribadi orang lain tanpa izin, dengan maksud menguntungkan diri sendiri atau orang lain, dapat dijerat dengan:

1. Pidana penjara maksimal 5 tahun, dan/atau.
2. Denda hingga Rp5 miliar.

Artinya efiensi kedua undang-undang ini perlu dipertanyakan secara yuridis. Overlapping antara Pasal 67 Undang-Undang Perlindungan Data Pribadi dan Pasal 48 Undang-Undang tentang Informasi dan Transaksi Elektronik terlihat jelas dalam pengaturan kejahatan data pribadi. Undang-Undang Perlindungan Data Pribadi fokus pada perlindungan subjek data (hak habeas data), sementara Undang-Undang tentang Informasi dan Transaksi Elektronik lebih menekankan aspek transaksi elektronik dan keamanan sistem.[21] Perbedaan ini terlihat jelas dari sanksi yang diatur. Pasal 48 Ayat 1 UU ITE menjatuhkan hukuman lebih berat pidana penjara hingga 8 tahun dan/atau denda Rp2 miliaruntuk pelanggaran akses ilegal

[21] *Ibid.*

sebagaimana dimaksud dalam Pasal 32. Namun, ketentuan ini bersifat umum dan tidak secara spesifik mengatur perlindungan data pribadi.

Meskipun kedua aspek pada topik utama berbeda akan tetapi secara kharfiah keduanya adalah penegakan atas tindak keamanan data pribadi pengguna. Maka Keberadaan dua pasal ini menciptakan dualisme ancaman hukuman yang justru dapat melemahkan efek jera. Landasan hukum informasi dan transaksi elektronik (Pasal 48) memberikan ancaman hukuman lebih berat—pidana penjara hingga 8 tahun dibandingkan maksimal 5 tahun dalam landasan hukum Perlindungan Data Pribadi (Pasal 67)ketentuan ini tidak secara khusus mengatur perlindungan data pribadi. Kasus seperti kebocoran data pada platform digital seringkali dijerat dengan Undang-undang Informasi Dan Transaksi Elektronik karena pertimbangan pembuktian yang lebih mudah, meskipun sebenarnya Undang-Undang Perlindungan Data Pribadi lebih relevan untuk melindungi hak korban.

Sinkronisasi atas tumpang tindih menimbulkan pertanyaan atas pengujian undang-undang yang terapkan. Menurut Guru Besar Hukum Pidana Eddy O.S. Hiariej, penanganan kasus pelanggaran data pribadi harus mengedepankan prinsip *lex specialis derogat legi generali* hukum khusus mengesampingkan hukum umum.[22] Dalam konteks ini, Undang-Undang Perlindungan Data Pribadi (UU PDP) yang secara spesifik mengatur perlindungan data pribadi seharusnya menjadi landasan utama, mengesampingkan Undang-Undang

[22] Wisnu Indaryanto, "Bestandeel Percobaan Dan Permufakatan Jahat Pada Undang-Undang Tentang Narkotika Dalam Surat Dakwaan (Perspektif Tujuan Hukum)", Jurnal Legal Reasoning 4, No.2, (2022), 136-167.

Informasi dan Transaksi Elektronik (UU ITE) yang hanya mengatur "*akses ilegal*" secara umum dalam Pasal 32. Konsekuensi logisnya, aparat penegak hukum harus menyesuaikan proses penanganan kasus dengan ketentuan Undang-Undang Perlindungan Data Pribadi sebagai regulasi khusus.

Hakim perlu menelaah dengan cermat mana yang tepat landasan hukum atas kasus cybercrime data pribadi. Penelaahan mendalam (judicial consideration) untuk menentukan landasan hukum bagi kasus yang sedang diperiksa. Analisis dari sudut pandang kedua undang-undang tersebut memiliki perbedaan signifikan. Undang-undang data pribadi secara khusus mengadili perkara yang berkaitan pencurian data pribadi dan undang-undang infromasi dan transaksi elektronik lebih kompleks tentang transaksi elektronik. bila ditemukan kasus semisal pencurian data pribadi pada platfrom digital e-commers maka perlindungan hukum atas kejahatan seluruhnya harus berlandaskan Undang-undang Informasi Dan Transaksi Elektronik sebagai aturan dari hukuman yang dikenakan.

Dalam konteks kasus pencurian data pribadi pada platform *e-commerce*, meskipun unsur pelanggaran berkaitan dengan perlindungan data, sanksi pidana tetap merujuk pada Undang-undang Informasi Dan Transaksi Elektronik sebagai *lex specialis* yang secara khusus mengatur tindak pidana diranah digital. Hal ini didasarkan Pasal 32 mengenai akses tanpa hak (*unauthorized access*) dan Pasal 36 tentang pemalsuan data elektronik (*data falsification*), sementara Undang-Undang Perlindungan Data Pribadi lebih berfokus pada sanksi administratif (administrative sanctions) dan mekanisme ganti rugi.Pertimbangan ini juga didasarkan pada asas hierarki peraturan perundang-undangan. Ketika terjadi tumpang tindih,

hakim seyogianya mengutamakan Undang-undang Informasi Dan Transaksi Elektronik sebagai dasar penuntutan pidana, mengingat sifatnya yang lebih khusus dalam mengatur sanksi tindak pidana elektronik.

Keduanya berfokus mengenai hukuman bagi pihak yang melakukan pelangaran atau kejahatan data pribadi yakni berkaitan dengan informasi pribadi. Pelangaran berupa pencurian, perentasan, ataupun sejenisnya yang sifatnya merugikan bagi pihak pengguna. Namun, Undang-Undang Perlindungan Data Pribadi tetap dapat digunakan sebagai dasar gugatan perdata atau administratif bagi subjek data yang dirugikan, sehingga kedua peraturan ini dapat berfungsi secara komplementer. Akan tetapi sekali lagi bila titik focus atas kasus ini secara luas adalah e-commers maka pasal 48 ayat 1 Undang-Undang Informasi dan Transaksi Elektronik yang menjadi prioritas hukuman bagi pelaku.

Secara keseluruhan cyberlaw di Indonesia sepenuhnya mengatur standarisasi kewajiban pengguna dalam mengamankan data pada platform digital. Mengetahui bahwa keamanan data sangat penting, standarisasi yang diamandemenkan oleh undang-undang khususnya pada platform digital. Platform digital menunjang kinerja maupun aktivitas digital memiliki keterangan terperinci atas pemberlakuan. Beberapa diataranya seperti bank digital, pinjaman online perlu data pribadi sebagai jaminan. Namun dalam implimentasinya masih menuai berbagai hambatan khususnya pada faktor dari pengguna atau masyarakat. Menurut teori efektifitas, salah satu cara efektif dari keberhasilan peraturan adalah faktor dari masyarakat itu sendiri. Maka konsep ini dapat dianalisis bahwa kesadaran atas keamanan data pribadi dimulai dari pemahaman masyarakat atau pentingnya mengerti mengenai hukum atas perlindungan

data pribadi. Memang seutuhnya negara mampu mengintegrasikan inovasi ini dalam sistem pertahanannya akan memiliki keunggulan strategis, namun tantangan regulasi juga harus diperhatikan dari pengguna pribadi. Undang-undang lahir sebagai respons terhadap dinamika hukum dalam masyarakat, termasuk peningkatan kasus pelanggaran dan kebutuhan akan pengaturan yang lebih jelas. Keberadaan undang-undang seperti Undang-Undang Perlindungan Data Pribadi bukan muncul secara tiba-tiba melainkan didorong oleh tuntutan sosial akibat maraknya kejahatan siber. Maka disini literasi digitalisasi atas keamanan data pribadi dari pengguna sangat penting. Sebab membangun sistem keamanan siber nasional yang kuat membutuhkan struktur kelembagaan terkoordinasi.

Tantangan besar masih menghadang upaya memperkuat pertahanan siber di Tanah Air, dengan tingkat literasi digital masyarakat yang belum optimal sebagai salah satu kendala utamanya. Minimnya pemahaman publik terhadap risiko dunia maya membuat banyak pengguna internet Indonesia rentan terhadap berbagai ancaman siber. Kondisi ini diperparah oleh pesatnya pertumbuhan pengguna internet yang tidak diimbangi edukasi memadai. Banyak masyarakat terutama kelompok usia produktif dan pelajar, aktif bersosial media di dunia digital tanpa memahami dasar-dasar keamanan seperti membuat password kuat atau mengenali tautan mencurigakan. Akibatnya kasus penipuan online, peretasan akun, dan penyalahgunaan data pribadi semakin marak terjadi.

Pendekatan keamanan siber di Indonesia saat ini masih cenderung terfokus pada aspek pertahanan negara, sementara perlindungan terhadap hak-hak digital warga negara sebagai individu belum mendapatkan porsi yang memadai. Kesenjangan

konseptual inilah yang menyebabkan strategi keamanan siber nasional belum benar-benar holistik. Padahal di era digital dimana aktivitas masyarakat semakin terkoneksi, jaminan perlindungan privasi dan keamanan data pribadi justru menjadi kebutuhan mendasar yang tidak bisa diabaikan.

F. Penutup/Kesimpulan

Penegakan *cyber law* sangatlah penting, terutama terkait dengan data pribadi atau privasi. Pengaturan perlindungan data pribadi pada platform digital di Indonesia sebenarnya telah memiliki kerangka hukum yang cukup kuat, khususnya setelah disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Regulasi ini menunjukkan komitmen negara dalam memberikan payung hukum terhadap pengelolaan dan pemrosesan data pribadi oleh penyelenggara sistem elektronik. Namun demikian, efektivitas implementasi *cyber law* tersebut masih menghadapi sejumlah tantangan, baik dari sisi penegakan hukum maupun kesiapan infrastruktur dan sumber daya manusia. Oleh karena itu, evaluasi menyeluruh terhadap pelaksanaan hukum yang berlaku menjadi langkah penting agar perlindungan data pribadi di ruang digital dapat terlaksana secara optimal.

Pelaksanaan *cyber law* di Indonesia masih menunjukkan kelemahan yang cukup signifikan, terutama dalam aspek penegakan sanksi terhadap pelanggar. Penjatuhan hukuman atau denda sering kali belum memberikan efek jera yang memadai, yang menunjukkan bahwa masih terdapat celah antara norma hukum yang ideal dengan praktik di lapangan. Oleh karena itu, perbaikan pada sistem penegakan hukum dan penguatan kelembagaan menjadi kunci untuk mewujudkan perlindungan hukum yang efektif dan berkeadilan dalam ekosistem digital.

Daftar Pustaka

1. Buku

Achmad Zubaidi dan Kaelan, *Pendidikan Kewarganegaraan***,** Cetakan Pertama, Paradigma, Yogyakarta, 2012.

Aris Basuki, dkk. "Pengaruh Perkembangan Teknologi Informasi Dan Komunikasi Terhadap Pelaksanaan Tugas Tni"Jurnal Mahatvavirya 11. No. 2. (2024).

Asosiasi Penelenggara Jasa Internet Indonesia (APJII) *, APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang,* (Jakarta, 2024).

Astir Rumondang Banjarnahor, dkk. *Resonansi Kualitas Layanan Perdagangan Sosial: Strategi Peningkatan Kinerja Penjualan UMKM Di Indonesia.* (Universitas Jendral Soedirman, 2024).

Mohammad Labib dan Abdul Wahid , "*Kejahatan Mayantara", (Cyber Crime)* (Bandung : PT. Refika Aditama, 2005).

Peter Mahmud Marzuki, *Penelitian Hukum* (Bandung: Prenada Media, 2020).

Raharjo Agus, "*Cybercrime , Pemahaman Dan Upaya Pencegaha Kejahatan Berteknologi*".(Yogyakarta : PT.Citra Aditya Bakti,2002).

Rodia. "Pengaruh Perkembangan()Teknologi Terhadap Terjadinya Kejahatan()Mayantara(Cybercrime) ". Jurisprudentie 6 no.2. (2019): 230-239

Situmeang., S. M. *CYBER LAW* (Bandung : CV.Cakra, 2020.).

Sumiaty Adelina Hutabarat, dkk," *CYBER-LAW: Quo Vadis Regulasi UU ITE dalam Revolusi Industri 4.0 Menuju Era Society 5.0*" (PT. Sonpedia Publishing Indonesia, 2023).

Sunarso Siswanto, "*Hukum Informasi Dan Transaksi Elektronik*". (Jakarta: PT Rineka Cipta. 2009).

Widodo." *Hukum Pidana Di Bidang Teknologi Informasi (Cybercrime Law) : Telaah Teoritik Dan Bedah Kampus".* (Yogyakarta: Aswaja Pressindo, 2013).

2. Artikel Jurnal

Ersya. "Permasalahan Hukum()dalam Menanggulangi Cyber Crime di Indonesia". Jurnal of Moral and Civic Education 1 No. 1, (2017).

Fikri Irfan Adristi, Erika Ramadhani "Analisis Dampak Kebocoran Data Pusat Data NasionalSementara2 (PDNS 2)Surabaya: Pendekatan Matriks Budaya Keamanan Siber dan Dimensi Budaya Nasional Hofstede"Selekta Manajemen: Jurnal Mahasiswa Bisnis & Manajemen 2, No. 06, (2024), 196-212.

Winda Agustina1 dan Sidi Ahyar Wiraguna, "Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi dari

Kejahatan Peretasan"Media Hukum Indonesia 2, No. 6 (2025), 117-127.

Windi, dkk, "Konstruksi Hukum dalam Cybercrime Pelaku Kejahatan Teknologi Informasi" Siyasah: Jurnal Hukum Tata Negara 3, No. 2, (Desember, 2023), 220-239.

Wisnu Indaryanto, "Bestandeel Percobaan Dan Permufakatan Jahat Pada Undang-Undang Tentang Narkotika Dalam Surat Dakwaan (Perspektif Tujuan Hukum)", Jurnal Legal Reasoning 4, No.2, (2022), 136-167.

Muhammad Fikri and Abdurrakhman Alhakim, "Urgensi Pengaturan Hukum Terhadap Pelaku Tindak Pidana Pencurian Data Pribadi Di Indonesia," YUSTISI 9, no. 1 (2022).

Muhammad Raditya Vijayaputro, Perlindungan Hukum Mengenai Investasi Digital dalam Bentuk Non-Fungible Token Berdasarkan Undang-Undang Nomor 25 Tahun 2007" UNES LAW REVIEW Vol. 6, No. 2, (2023)

Rahmat Syah "Strategi Kepolisian Dalam Pencegahan Kejahatan Phising Melalui Media Sosial Di Ruang Siber". Jurnal Impresi Indonesia, 2, No. 9(2023), 864–870.

3. Makalah/Pidato

Warassih, Esmi, " Mengapa Harus Legal Hermeneutic?" *Makalah* pada Seminar Nasional "Legal Hermeneutics sebagai Alternatif Kajian Hukum", Semarang, 24 November 2007.

Ismail, Maqdir, " Menyongsong Masa Depan Bangsa", Pidato Sambutan Alumni yang dibacakan di hadapan wisudawan/wisudawati UII Periode VI Tahun Akademik 2009-2010, di Yogyakarta, 24 Juli 2010.

4. Internet

https://kbbi.web.id/data, diakses pada 08 Agustus 2024, 13:04 WIB.\

5. Peraturan Perundang-Undangan

Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. Tambahan Lembar Negara No. 3821

Undang-Undang Nomor 11 Tahun 20008 tentang Informasi Dan Transaksi Eletronik. Tambahan Lembar Negara No. 5952

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Tambahan Lembar Negara No. 6843

Permenkominfo Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik