Ethics and Law Journal: Business and Notary (ELJBN)
Vol 3 No.2 2025 ISSN 2988-1293 (online)
http://journals.ldpb.org/index.php/eljbn

https://doi.org/10.61292/eljbn.263

Tantangan Implementasi dan Perkembangan Hukum Telematika di Indonesia

Alexander Kennedy

Universitas Pelita Harapan

Correspondence: 01053230105@student.uph.edu

Abstract

The rapid expansion of information and communications technology has inflicted drastic changes on Indonesia, from the ease of digital activities to significant challenges for legal regulation. This paper attempts to explore the development of regulation of telematics law in Indonesia, particularly focusing on Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) and Law Number 27 of 2022 concerning Personal Data Protection (UU PDP). This study also identifies significant hindrances to the use of telematics law such as the different interpretations of certain provisions, the general public low degree of digital literacy, and the inadequate capacity of police officers in handling more complex cybercrimes. Drawing from a normative juridical perspective, this study examines primary, secondary, and tertiary sources of law using a conceptual and legislative approach. The findings indicate that although legislations such as UU ITE and UU PDP have laid a positive foundation, there are still legal lacunas which should be updated, harmonized, and provided with technical elucidation. Law enforcement on telematics also requires improved human resources, infrastructure, as well as institutional and international cooperation. In order to answer these challenges, collective action is needed, like regulatory harmonization, improved digital literacy, and improved national and international cooperation. With these measures, telematics law will be able to fulfill its twofold role as a safeguarding tool and as an innovation driver in the digital age while simultaneously constructing a secure, open, and fair digital environment for all actors.

Keywords: *Cyber Law; Digital Regulation; Cybercrime.*

Abstrak

Perkembangan pesat teknologi informasi dan komunikasi telah membawa berbagai perubahan signifikan di Indonesia, baik dari segi kemudahan aktivitas digital hingga munculnya tantangan besar dalam regulasi hukum. Penelitian ini bertujuan untuk menganalisis perkembangan regulasi hukum telematika di Indonesia, dengan fokus pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Kajian ini juga mengidentifikasi tantangan utama dalam implementasi hukum telematika, seperti multitafsir dari beberapa pasal, rendahnya literasi digital masyarakat, serta kurangnya kapasitas penegak hukum dalam menangani kejahatan siber yang semakin kompleks. Menggunakan metode yuridis normatif, penelitian ini menelaah sumber hukum primer, sekunder, dan tersier, serta menerapkan pendekatan konseptual dan perundang-undangan. Hasil penelitian menunjukkan bahwa meskipun regulasi seperti UU ITE dan UU PDP telah memberikan fondasi yang signifikan, masih terdapat celah hukum yang membutuhkan pembaharuan, harmonisasi, dan kejelasan teknis. Penegakan hukum telematika juga memerlukan peningkatan kapasitas sumber daya manusia, infrastruktur, serta kerja sama lintas lembaga dan internasional. Untuk mengatasi tantangan tersebut, diperlukan strategi komprehensif, termasuk harmonisasi regulasi, peningkatan literasi digital, serta penguatan kolaborasi nasional dan global. Dengan langkah-langkah ini, hukum telematika diharapkan dapat menjalankan perannya sebagai instrumen perlindungan dan penggerak inovasi di era digital, sekaligus menciptakan ekosistem digital yang aman, inklusif, dan berkeadilan bagi semua pihak.

Kata kunci: Hukum Telematika; Regulasi Digital; Kejahatan Siber.

I. Pendahuluan

Perkembangan pesat teknologi informasi dan komunikasi di Indonesia dalam dua dekade terakhir telah membawa dampak besar di berbagai bidang kehidupan masyarakat, baik dari sisi ekonomi, sosial, budaya, hingga politik (Novita et al., 2024). Digitalisasi tidak lagi hanya sebatas alat komunikasi, tetapi juga menjadi bagian penting dalam interaksi sosial, kegiatan ekonomi, dan administrasi publik (Kennedy et al., 2024).

Transaksi jual beli daring (*online shopping*), komunikasi melalui media sosial, hingga layanan perbankan digital yang berbasis internet telah mengubah cara masyarakat menjalani keseharian mereka secara fundamental (Kennedy & Wartoyo, 2024). Di satu sisi, kemajuan teknologi informasi memberikan berbagai kemudahan dan efisiensi dalam beraktivitas, namun di sisi lain, kondisi ini juga menimbulkan beragam persoalan hukum yang semakin kompleks dan membutuhkan perhatian khusus dari para pembuat kebijakan dan aparat penegak hukum.

Hukum telematika, yang pada dasarnya merupakan penggabungan konsep teknologi telekomunikasi dan informatika, kini semakin menegaskan urgensinya sebagai payung hukum yang relevan untuk menjawab tantangan tersebut. Hukum telematika mencakup pengaturan tentang teknologi informasi dan komunikasi, termasuk regulasi mengenai transaksi elektronik, perlindungan data pribadi, keamanan siber, hingga pengaturan konten digital (Aulianisa & Indirwan, 2020). Kebutuhan terhadap hukum telematika yang adaptif sangat mendesak, karena kejahatan yang memanfaatkan celah teknologi juga semakin marak, seperti pencurian data pribadi, penipuan daring, pencemaran nama baik melalui media sosial, serta berbagai bentuk kejahatan siber lainnya yang mengancam stabilitas masyarakat (Kennedy, 2024b).

Di Indonesia, regulasi yang berkaitan dengan telematika pertama kali diperkenalkan melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang kemudian diubah melalui Undang-Undang Nomor 19 Tahun 2016. Kehadiran UU ITE menjadi landasan utama dalam mengatur berbagai aspek hukum di ruang digital, seperti legitimasi alat bukti digital, transaksi elektronik, serta pemberian sanksi terhadap pelanggaran hukum yang terjadi di dunia maya. Namun demikian, implementasi dari UU ITE ini tidak berjalan tanpa kendala. Seiring dengan berjalannya waktu, berbagai kasus menunjukkan bahwa beberapa pasal dalam UU ITE masih multitafsir dan kerap disalahgunakan, baik secara sengaja maupun akibat kurangnya pemahaman aparat penegak hukum dalam penerapannya.

Seiring semakin kompleksnya teknologi digital, Indonesia juga telah mengambil langkah penting dengan mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) (Rosadi, 2023). Undang-undang ini merupakan upaya untuk memberikan perlindungan lebih kuat terhadap hak privasi masyarakat sekaligus memaksa pelaku usaha maupun pemerintah untuk menerapkan standar keamanan data yang tinggi (Vania et al., 2023). Meski demikian, implementasi UU PDP memerlukan kesiapan seluruh elemen, khususnya terkait kesiapan teknologi, literasi masyarakat, serta kemampuan aparat penegak hukum dalam menguasai berbagai aspek teknis terkait perlindungan data.

Kebutuhan akan regulasi hukum telematika yang adaptif juga didorong oleh perkembangan teknologi canggih seperti kecerdasan buatan (*Artificial Intelligence*), komputasi awan (*cloud computing*), *Internet of Things* (IoT), hingga *blockchain* (Aulianisa & Indirwan, 2020). Teknologi-teknologi ini tidak hanya menawarkan potensi besar dalam inovasi dan pertumbuhan ekonomi, tetapi juga membawa tantangan hukum baru yang memerlukan pendekatan regulasi yang lebih fleksibel dan antisipatif. Misalnya, teknologi *blockchain*, yang banyak dimanfaatkan dalam transaksi keuangan maupun pencatatan data, menghadirkan tantangan terkait transparansi, keamanan data, dan perlindungan konsumen yang belum sepenuhnya terakomodasi dalam regulasi saat ini (Renduchintala et al., 2022).

Fenomena hoaks, ujaran kebencian, serta pencemaran nama baik melalui media sosial menjadi salah satu contoh nyata mengenai kompleksitas penerapan hukum telematika di Indonesia. Masalah ini kerap menimbulkan polemik antara kebebasan berekspresi dengan tanggung jawab hukum pengguna dan platform digital (Febriawan & Marisa, 2024). Ketidakjelasan aturan terkait tanggung jawab platform digital dalam memoderasi konten yang diunggah pengguna juga menambah kompleksitas hukum. Di sisi lain, insiden kebocoran data pribadi, terutama di sektor perbankan dan media sosial, menunjukkan bahwa regulasi hukum telematika masih harus terus dikembangkan dan disempurnakan agar mampu mengantisipasi berbagai tantangan keamanan siber yang terus berkembang.

Salah satu tantangan utama dalam penegakan hukum telematika di Indonesia adalah kurangnya kesiapan sumber daya manusia, baik dari sisi aparat penegak hukum maupun masyarakat secara umum (Febriawan & Marisa, 2024). Aparat penegak hukum sering kali menghadapi kesulitan dalam penanganan kasus siber karena kurangnya pemahaman teknis dan minimnya dukungan infrastruktur digital yang memadai. Situasi ini berdampak langsung terhadap efektivitas penegakan hukum di bidang telematika, menyebabkan kasus-kasus *cybercrime* tidak terungkap secara optimal atau bahkan terabaikan begitu saja.

Untuk menjawab tantangan tersebut, penelitian ini akan mengeksplorasi perkembangan hukum telematika di Indonesia secara mendalam, mulai dari kajian historis regulasi hingga analisis kritis terhadap implementasi UU ITE dan UU PDP beserta turunannya. Penelitian ini juga akan mengidentifikasi berbagai celah atau kelemahan dalam regulasi yang dapat dimanfaatkan oleh pelaku kejahatan digital. Melalui identifikasi tersebut, diharapkan dapat diberikan rekomendasi konkret yang mampu membantu pembuat kebijakan dan aparat penegak hukum dalam menyusun strategi yang lebih efektif dalam menangani kejahatan digital di Indonesia.

Selain itu, penelitian ini juga bertujuan untuk memetakan berbagai faktor yang menjadi hambatan utama dalam implementasi hukum telematika. Faktor-faktor tersebut mencakup aspek sumber daya manusia, infrastruktur teknologi, harmonisasi regulasi, dan kolaborasi antar lembaga yang terlibat dalam penegakan hukum. Dengan memahami berbagai kendala ini, diharapkan dapat dikembangkan langkah-langkah yang lebih terarah untuk memperkuat kemampuan kelembagaan, meningkatkan literasi digital masyarakat, dan mempersiapkan infrastruktur yang lebih tangguh dalam menghadapi ancaman siber.

Secara teoritis, penelitian ini bertujuan untuk memperkaya kajian akademik dalam disiplin hukum telematika dengan menyajikan analisis menyeluruh tentang perkembangan regulasi dan implementasinya di Indonesia. Sedangkan secara praktis, hasil penelitian ini akan memberikan manfaat nyata bagi pemerintah, legislator, aparat penegak hukum, masyarakat umum, dan pelaku industri digital dalam memahami hak dan kewajiban hukum yang berlaku di dunia maya. Dengan demikian, penelitian ini tidak hanya mengisi kekosongan dalam literatur akademik tetapi juga membantu menciptakan lingkungan digital yang aman, adil, dan kondusif bagi inovasi teknologi dan perlindungan kepentingan masyarakat secara luas.

II. Metode Penelitian

Penelitian ini menggunakan metode yuridis normatif yang bertumpu pada studi pustaka (*library research*) sebagai cara utama untuk memperoleh data (Budianto, 2022). Pendekatan yuridis normatif dipilih karena kajian hukum telematika di Indonesia memerlukan telaah mendalam terhadap peraturan perundang-undangan, putusan pengadilan, serta literatur ilmiah terkait (Soekanto & Mamudji, 2024). Metode ini memungkinkan peneliti menelaah sumber-sumber hukum primer, sekunder, dan tersier untuk mengungkap bagaimana regulasi yang berlaku dikonstruksikan, sekaligus mengidentifikasi kekurangan atau tumpang-tindih ketentuan yang relevan dengan praktik di lapangan.

Sumber hukum primer dalam penelitian ini meliputi Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (yang telah diubah dengan UU No. 19 Tahun 2016), Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, serta peraturan pelaksana atau peraturan lain yang terkait dengan ruang lingkup telematika. Adapun putusan-putusan pengadilan yang menyoroti kasus pelanggaran di dunia siber juga dikaji untuk memahami penerapan konkret dari ketentuan hukum yang berlaku. Sementara itu, sumber hukum sekunder berupa artikel ilmiah, buku teks, dan hasil-hasil penelitian sebelumnya dijadikan rujukan untuk memperoleh perspektif akademik maupun praktis mengenai isu hukum telematika. Sumber hukum tersier, seperti kamus hukum atau ensiklopedia hukum, turut berfungsi sebagai acuan untuk memperjelas istilah-istilah teknis.

Dalam pengolahan data, pendekatan konseptual (*conceptual approach*) dan pendekatan perundang-undangan (*statute approach*) dipraktikkan guna menelaah secara sistematis asas-asas, definisi, dan prinsip yang mendasari hukum telematika, serta menganalisis konsistensi antara berbagai regulasi terkait (Sunggono, 2019). Metode deskriptif-analitis diterapkan untuk memaparkan ketentuan hukum yang berlaku, diikuti oleh penilaian kritis terhadap kekuatan dan kelemahannya. Jika diperlukan, pendekatan komparatif (*comparative approach*) dilakukan dengan membandingkan praktik terbaik (*best practices*) dari negara lain sebagai upaya untuk memberikan rekomendasi yang relevan bagi perbaikan hukum telematika di Indonesia (Disemadi, 2022).

Dengan metode yuridis normatif ini, hasil penelitian diharapkan mampu memberikan gambaran rinci mengenai kerangka hukum telematika, sekaligus menawarkan solusi atas berbagai tantangan implementasinya. Pendekatan yang terstruktur tersebut juga diyakini dapat menjaga validitas kajian, sehingga kesimpulan yang diperoleh memiliki landasan ilmiah yang kuat.

III. Pembahasan

Perkembangan hukum telematika di Indonesia tidak terlepas dari sejarah panjang pemanfaatan teknologi informasi dan komunikasi yang semakin pesat sejak akhir 1990-an (Simbolon et al., 2021). Ketika internet mulai diperkenalkan secara komersial, kebutuhan akan aturan yang mampu mengakomodasi transaksi serta interaksi di dunia maya menjadi semakin mendesak. Pada mulanya, regulasi yang ada masih terbatas pada kebijakan telekomunikasi tradisional, seperti Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi, yang lebih berfokus pada pengelolaan jaringan dan infrastruktur telekomunikasi ketimbang aktivitas daring. Namun, seiring meluasnya penggunaan internet untuk keperluan bisnis, pemerintahan, dan interaksi sosial, pemerintah dan pemangku kepentingan lainnya mulai menyadari urgensi pembentukan peraturan khusus yang menata ruang digital secara lebih komprehensif. Lahirnya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (kemudian diubah melalui Undang-Undang Nomor 19 Tahun 2016) menandai tonggak penting dalam sejarah regulasi telematika di Indonesia. Undang-Undang tersebut, yang akrab disebut UU ITE, berusaha memberikan definisi dasar tentang informasi elektronik, tanda tangan elektronik, transaksi elektronik, serta mengatur hal-hal terkait tata cara penyebaran dan pemanfaatan informasi di internet (Faniyah & Maulana, 2023). Meski dalam praktiknya UU ITE tidak luput dari kritik, terutama terkait pasal-pasal yang dianggap multitafsir, regulasi ini menjadi fondasi bagi seluruh aktivitas digital yang berkembang di Indonesia.

Kehadiran UU ITE pada masa itu didorong oleh beberapa peristiwa yang memunculkan kekhawatiran akan keabsahan dokumen digital, keamanan transaksi daring, dan potensi kejahatan siber (Simbolon et al., 2021). Di satu sisi, bisnis *e-commerce* mulai tumbuh dan mendorong terjadinya transaksi lintas wilayah melalui jaringan internet (Kennedy, 2024a), sementara di sisi lain, infrastruktur hukum untuk menjamin keabsahan transaksi elektronik masih relatif minim. Dengan disahkannya UU ITE, pemerintah berupaya mengisi kekosongan hukum tersebut dengan menegaskan bahwa informasi elektronik dan atau dokumen elektronik memiliki kekuatan hukum yang sama dengan informasi atau dokumen tertulis (Rohmah, 2022). Di samping itu, UU ITE juga mengatur beberapa ketentuan pidana untuk menindak perilaku yang dianggap meresahkan, seperti penyebaran konten ilegal, penipuan daring, dan pencemaran nama baik di media sosial. Namun, tidak lama setelah pemberlakuan regulasi ini, muncul beragam kritik mengenai apakah ketentuan pidana di dalamnya justru mengekang kebebasan berekspresi (Raskasih, 2020). Kritik tersebut pun memuncak sehingga pemerintah melakukan revisi dengan keluarnya UU Nomor 19 Tahun 2016, yang antara lain mengurangi ancaman hukuman pidana dalam beberapa pasal, meski perdebatan tentang definisi pencemaran nama baik dan ujaran kebencian tetap berlanjut.

Selain UU ITE, Indonesia kemudian juga merasakan kebutuhan akan perlindungan data pribadi yang semakin mendesak, terutama setelah beberapa kasus kebocoran data besar terjadi dan menimbulkan kerugian bagi masyarakat (Kennedy, 2024b). Momen tersebut memuncak ketika banyak platform digital termasuk *e-commerce*, media sosial, dan layanan finansial teknologi menjadi sasaran peretasan yang mengekspose data pengguna. Dengan latar belakang demikian, pemerintah akhirnya mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Rosadi, 2023). Regulasi ini dimaksudkan untuk mengatur bagaimana data pribadi dikumpulkan, diolah, disimpan, dan dibagikan, serta menegaskan hak dan kewajiban berbagai pihak yang terlibat dalam pengelolaan data, termasuk pengendali dan pemroses data. UU ini juga menjelaskan prosedur penanganan pelanggaran, penjatuhan sanksi administratif maupun pidana, dan membahas pembentukan lembaga pengawas independen yang akan memastikan kepatuhan terhadap prinsip-prinsip pelindungan data. Kendati demikian, penerapan UU Pelindungan Data Pribadi masih akan menghadapi tantangan, mengingat perlu adanya harmonisasi dengan peraturan teknis lain, pemutakhiran infrastruktur keamanan siber, serta peningkatan literasi di kalangan institusi pemerintah dan swasta agar pemrosesan data sesuai standar yang ditetapkan.

Jika ditelaah lebih jauh, substansi UU ITE dan UU Pelindungan Data Pribadi menyentuh isu-isu krusial dalam hukum telematika (Rosadi, 2023). UU ITE menitikberatkan pada pengakuan keabsahan dokumen elektronik, pelindungan konsumen dalam transaksi daring, dan ketentuan pidana terkait konten ilegal, sedangkan UU Pelindungan Data Pribadi secara spesifik menyoroti hak individu atas data pribadi yang kerap disalahgunakan untuk tujuan komersial tanpa persetujuan atau pemberitahuan yang memadai. Kedua undang-undang ini memang saling melengkapi, karena berbagai aktivitas digital seperti pembuatan akun, verifikasi identitas, dan pengunggahan konten yang berkaitan erat dengan pemrosesan data pribadi (Custers, 2016). Meski demikian,

konsistensi dan keselarasan antara kedua payung hukum ini masih menjadi diskursus. Sebagian pengamat hukum mempertanyakan apakah definisi "data pribadi" dalam satu undang-undang sepenuhnya sinkron dengan definisi atau ketentuan sejenis di undang-undang lain. Ketidakselarasan dapat memicu kebingungan dalam proses penegakan hukum, terutama ketika kasus pelanggaran data melibatkan unsur tindak pidana di ranah UU ITE sekaligus melanggar prinsip pelindungan data. Dari sudut pandang standar internasional, Indonesia relatif terlambat memiliki undang-undang pelindungan data pribadi jika dibandingkan dengan Uni Eropa yang telah menerbitkan GDPR (*General Data Protection Regulation*) sejak 2016 (Li et al., 2019). Meski begitu, UU Pelindungan Data Pribadi Indonesia mencoba mengadopsi beberapa prinsip penting serupa, seperti keharusan memperoleh persetujuan subjek data dan adanya hak bagi subjek data untuk mengakses, memperbaiki, atau menghapus datanya.

Tantangan dalam implementasi hukum telematika di Indonesia mencakup beragam aspek, mulai dari penegakan hukum, kapasitas sumber daya manusia, hingga dinamika perkembangan teknologi (Laksana & Mulyani, 2024). Dari sisi penegakan hukum, aparat kerap dihadapkan pada kasus dengan karakteristik siber yang rumit, seperti penipuan lintas negara, pencurian identitas digital, atau manipulasi data terenkripsi (Kim, 2014). Pemahaman teknis, kemampuan forensik digital, serta pemanfaatan perjanjian internasional menjadi sangat vital. Sementara itu, institusi penegak hukum masih perlu meningkatkan infrastruktur teknologi dan mengembangkan kerja sama lintas lembaga, baik di level nasional antar-kementerian dan lembaga, maupun di level internasional dengan agensi penegakan hukum negara lain. Dalam beberapa kasus, proses pengungkapan *cybercrime* mandek karena terbatasnya wewenang lintas yurisdiksi yang dimiliki aparat penegak hukum Indonesia, sehingga dibutuhkan mekanisme *mutual legal assistance* yang bersifat lintas negara (Hartono & Hapsari, 2019). Selain itu, ada pula kendala kedaulatan digital yang muncul ketika perusahaan penyedia layanan internet dan platform media sosial berbasis di luar negeri, membuat proses penindakan hukum dan pencarian bukti digital semakin kompleks.

Tingkat literasi digital masyarakat yang belum merata juga menjadi persoalan pelik. Banyak pengguna internet di Indonesia belum sepenuhnya menyadari konsekuensi hukum atas perilaku mereka di ruang maya, seperti membagikan konten yang berisi ujaran kebencian, fitnah, atau mengakses layanan yang mengumpulkan data pribadi tanpa perlindungan memadai (Gomulya, 2023). Rendahnya literasi digital memperbesar risiko penipuan daring, peretasan akun, serta penyalahgunaan data, terlebih di kalangan kelompok rentan seperti anak-anak dan lansia (Novita et al., 2024). Di sisi lain, percepatan perkembangan teknologi sering kali membuat regulator dan pembuat kebijakan kelabakan. Siklus legislasi yang panjang kerap tidak sepadan dengan kecepatan munculnya inovasi baru, seperti teknologi *blockchain*, *artificial intelligence*, dan *Internet of Things*. Akibatnya, lahirnya aturan sering tertinggal jauh di belakang kebutuhan pasar, memicu situasi "*grey area*" yang rentan dimanfaatkan oleh pihak-pihak tidak bertanggung jawab (Febriawan & Marisa, 2024).

Untuk memperjelas sejauh mana efektivitas regulasi telematika di lapangan, beberapa kasus dapat dijadikan cerminan. Salah satu yang paling sering disorot adalah kasus pencemaran nama baik dan ujaran kebencian melalui media sosial, di mana sejumlah individu telah diproses pidana berdasarkan pasal karet UU ITE (Dunan & Mudjiyanto, 2022). Walaupun beberapa pelaku dinyatakan bersalah, putusan pengadilan sering menimbulkan perdebatan karena definisi pencemaran nama baik dianggap subjektif. Perbedaan tafsir tersebut menunjukkan bahwa UU ITE masih memerlukan penjelasan lebih detail, atau setidaknya panduan penerapan yang seragam, agar asas kepastian hukum dapat dijaga. Di ranah kebocoran data pribadi, sempat terjadi kasus yang menimpa platform *e-commerce* Tokopedia, di mana jutaan data pengguna diduga bocor dan dijual di forum daring. Ketika kasus tersebut diusut, muncul kendala dalam melacak sumber kebocoran serta menegosiasikan kerja sama dengan pihak internasional untuk memblokir forum jual-beli data (Raihan, 2023). Kendati pemerintah sempat mengambil langkah-langkah teknis, seperti berkoordinasi dengan kementerian dan institusi penegak hukum terkait, hasil akhirnya belum sepenuhnya menimbulkan efek jera. Hal ini mengindikasikan bahwa walaupun regulasi sudah ada, implementasi di lapangan masih memerlukan penguatan dari segi penegakan hukum dan kapabilitas teknologi.

Menilik tantangan-tantangan tersebut, diperlukan sejumlah strategi dan rekomendasi perbaikan yang komprehensif. Harmonisasi regulasi menjadi prioritas utama, dimana pemerintah perlu meninjau ulang pasal-pasal dalam UU ITE yang berpotensi multitafsir, sekaligus menyelaraskannya dengan aturan-aturan di UU Pelindungan Data Pribadi, undang-undang tentang telekomunikasi, peraturan menteri, serta peraturan sektoral lain. Harmonisasi ini tidak hanya untuk menghindari tumpang tindih aturan, melainkan juga mencegah

kebingungan di lapangan, baik bagi masyarakat, pelaku usaha, maupun aparat penegak hukum (Dunan & Mudjiyanto, 2022). Peninjauan ulang pasal yang multitafsir perlu diikuti dengan pembaharuan pedoman teknis yang dapat memberikan interpretasi lebih jelas. Dengan demikian, hakim dan penegak hukum memiliki landasan yuridis yang lebih tegas dalam menangani perkara terkait hukum telematika.

Melihat kompleksitas ruang digital yang terus berkembang dan tumpang tindihnya berbagai regulasi yang mengatur aspek telematika, pemerintah sebetulnya memiliki peluang untuk membentuk suatu undang-undang komprehensif, seperti *omnibus law* yang mana pernah dilakukan dalam konteks cipta kerja melalui Undang-Undang Nomor 6 Tahun 2023, sehingga ada panduan undang-undang yang komprehensif mengatur ekosistem hukum telematika di Indonesia. Undang-undang ini dapat mengintegrasikan substansi dari berbagai regulasi yang ada, seperti UU ITE, UU Pelindungan Data Pribadi, UU Telekomunikasi, PP PSTE, hingga peraturan sektoral lainnya yang saling berkaitan. Dengan menggabungkan berbagai instrumen hukum tersebut ke dalam satu kerangka besar, regulasi telematika tidak hanya menjadi lebih efisien dan mudah dipahami, tetapi juga mampu menjawab tantangan hukum yang bersifat lintas sektor secara lebih adaptif dan menyeluruh yang mana merupakan tujuan dibentuknya *omnibus law* seperti yang dikemukakan Anggono (2020) tentang tujuan penggunaan *omnibus law*.

Selain menyederhanakan struktur hukum, keberadaan *omnibus law* di bidang telematika juga dapat memperjelas kewenangan penegakan hukum, yang selama ini kerap terfragmentasi di antara berbagai lembaga. Ketika satu pelanggaran siber bisa mencakup aspek pelindungan data, transaksi elektronik, dan penyalahgunaan infrastruktur digital sekaligus, maka sistem hukum yang terintegrasi akan sangat membantu dalam menciptakan koordinasi penanganan yang lebih efektif. Levi & Williams (2013) mengemukakan bahwa peran kerjasama antar lembaga sangat penting dalam memberantas kejahatan siber, dimana polisi tidak akan mampu menghadapi kasus-kasus serangan siber sendiri, melainkan membutuhkan dukungan dari lembaga-lembaga terkait untuk dapat melihat secara holistik perkara siber tersebut seperti contoh Uni Eropa dengan *European Cyber Crime Centre* yang menangani segala kasus *cybercrime* di Uni Eropa (Buono, 2012). Dengan dasar hukum yang terpadu, aparat penegak hukum dapat memiliki rujukan yang lebih jelas dalam bertindak, sekaligus mendorong adanya pembentukan satuan tugas lintas sektor yang solid. Dalam konteks global, pendekatan ini juga akan memperkuat posisi Indonesia dalam kerja sama internasional terkait kejahatan siber dan perlindungan data lintas batas negara.

Peningkatan kapasitas sumber daya manusia di bidang siber wajib menjadi agenda berkelanjutan (Laksana & Mulyani, 2024). Hal ini mencakup pelatihan teknis forensik digital untuk aparat kepolisian, jaksa, hakim, serta pelatihan pemahaman hukum telematika bagi para penyidik. Kesadaran akan pentingnya bukti digital, metode pengumpulan bukti, dan penanganan data elektronik yang tepat akan meningkatkan kualitas penegakan hukum telematika. Peran pemerintah untuk menyediakan sarana dan prasarana canggih juga esensial, sehingga penyelidikan kejahatan siber dapat dilakukan dengan standar internasional (Wibowo & Hidayat, 2024). Keempat, kerja sama antar lembaga di tingkat nasional dan internasional perlu diperluas. Di level nasional, sinergi antara Kementerian Komunikasi dan Informatika, Kepolisian, Kejaksaan, Otoritas Jasa Keuangan, dan lembaga terkait lainnya harus diperkuat agar kasus-kasus siber dapat ditangani secara terpadu. Di level internasional, Indonesia dapat mempertimbangkan untuk terlibat lebih aktif dalam perjanjian atau konvensi yang relevan dengan penanggulangan kejahatan siber, sehingga jalur koordinasi lintas negara menjadi lebih efektif (Febriawan & Marisa, 2024). Hal ini akan sangat membantu dalam menyelesaikan kasus yang melibatkan pelaku dan server di luar yurisdiksi nasional.

Terakhir, pengembangan literasi digital secara masif di masyarakat tidak boleh diabaikan (Khoironi, 2020). Pemerintah dan sektor swasta dapat berkolaborasi dalam menyelenggarakan program edukasi penggunaan internet yang aman, cerdas, dan bertanggung jawab. Pendidikan tentang hak dan kewajiban digital, perlindungan data pribadi, serta etika dalam menggunakan media sosial perlu diintegrasikan ke dalam kurikulum sekolah dan kampanye publik (Parulian et al., 2021). Semakin tinggi tingkat literasi digital, semakin kecil risiko pelanggaran hukum, sekaligus semakin besar daya tahan masyarakat terhadap potensi penipuan atau manipulasi daring. Program literasi semacam ini juga memupuk pemahaman bahwa teknologi hanyalah alat, sementara perilaku manusia di baliknya yang menentukan tercipta atau tidaknya lingkungan digital yang sehat.

Berdasarkan keseluruhan analisis tersebut, pembahasan mengenai sejarah regulasi telematika di Indonesia, substansi utama UU ITE dan UU Pelindungan Data Pribadi, tantangan implementasi, contoh kasus di

lapangan, serta strategi perbaikan menegaskan bahwa hukum telematika merupakan ranah yang berkembang dinamis sesuai dengan laju teknologi. Meskipun payung hukum di Indonesia telah mengalami kemajuan signifikan dibanding beberapa dekade silam, proses adaptasi dan pembaharuan tetap diperlukan untuk menjawab tantangan-tantangan baru, mulai dari kejahatan siber yang semakin canggih hingga persoalan perlindungan privasi yang kian kompleks. Dengan pendekatan komprehensif yang melibatkan harmonisasi regulasi, peningkatan kapasitas penegak hukum, kerja sama lintas lembaga, dan program literasi digital, diharapkan ekosistem telematika di Indonesia dapat berkembang selaras dengan prinsip keadilan, keamanan, dan kemajuan teknologi. Hanya dengan langkah-langkah tersebut, hukum telematika dapat benar-benar menjalankan fungsinya sebagai instrumen perlindungan dan pendorong inovasi di era digital.

IV. Penutup

Hukum telematika di Indonesia telah berkembang seiring dengan kemajuan teknologi informasi dan komunikasi yang semakin pesat. Kehadiran UU ITE dan UU Pelindungan Data Pribadi menjadi bukti konkret bahwa pemerintah menyadari kebutuhan akan regulasi yang mampu menyeimbangkan kebebasan berinovasi dan kepentingan perlindungan publik. Meski demikian, keberadaan kedua undang-undang tersebut masih memunculkan berbagai perdebatan, terutama terkait definisi istilah yang multitafsir serta tumpang-tindih ketentuan antara satu peraturan dengan peraturan lainnya. Selain itu, tantangan penegakan hukum di ranah digital semakin kompleks karena sifat siber yang lintas yurisdiksi dan menuntut kemampuan teknis khusus dari aparat penegak hukum.

Penegakan hukum telematika di Indonesia menghadapi kendala yang meliputi kemampuan forensik digital, literasi teknologi di masyarakat yang masih rendah, serta mekanisme kerja sama lintas lembaga dan lintas negara yang belum optimal. Rendahnya literasi digital masyarakat turut memperbesar risiko penipuan dan kejahatan siber, sementara kelambanan pembaruan regulasi di tengah laju perkembangan teknologi memicu munculnya wilayah "abu-abu" yang kerap dimanfaatkan oleh pelaku kejahatan. Dalam beberapa kasus, sanksi hukum berhasil dijatuhkan kepada pelaku pelanggaran siber, tetapi efektivitasnya kerap dipertanyakan karena ketidakselarasan antara penegakan pasal pidana dan perlindungan hak-hak digital.

Untuk menjawab tantangan tersebut, diperlukan langkah komprehensif yang mencakup harmonisasi regulasi, peningkatan kapasitas aparat penegak hukum, dan pembentukan ekosistem digital yang aman serta inklusif. Pemerintah beserta pemangku kepentingan lain perlu terus memperbarui kerangka hukum telematika agar mampu mengantisipasi disrupsi teknologi dan kejahatan siber yang semakin canggih. Peningkatan literasi digital di masyarakat menjadi prioritas, diikuti peningkatan kolaborasi lintas sektor dan lintas negara untuk membangun penegakan hukum yang solid. Dengan demikian, hukum telematika dapat berfungsi optimal sebagai pelindung kepentingan publik, penyeimbang kebebasan berekspresi, dan pendorong inovasi di era digital.

Daftar Pustaka

Anggono, B. D. (2020). Omnibus Law sebagai Teknik Pembentukan Undang-Undang: Peluang Adopsi dan Tantangannya dalam Sistem Perundang-Undangan Indonesia. *Rechtsvinding*, *9*(1), 17–37. https://doi.org/10.33331/rechtsvinding.v9i1.389

Aulianisa, S. S., & Indirwan, I. (2020). Critical Review of the Urgency of Strengthening the Implementation of Cyber Security and Resilience in Indonesia. *Lex Scientia Law Review*, *4*(1), 31–45. https://doi.org/10.15294/lesrev.v4i1.38197

Budianto, A. (2022). Legal Research Methodology Reposition in Research on Social Science. *International Journal of Criminology and Sociology*, *9*, 1339–1346. https://doi.org/10.6000/1929-4409.2020.09.154

Buono, L. (2012). Gearing up the Fight against Cybercrime in the European Union: A New Set of Rules and the Establishment of the European Cybercrime Centre (Ec3). *New Journal of European Criminal Law*, *3*(3–4), 332–343. https://doi.org/10.1177/203228441200300307

Custers, B. (2016). Click Here to Consent Forever: Expiry Dates for Informed Consent. *Big Data & Society*, *3*(1), 2053951715624935. https://doi.org/10.1177/2053951715624935

Disemadi, H. S. (2022). Lensa Penelitian Hukum: Esai Deskriptif tentang Metodologi Penelitian Hukum. *Journal of Judicial Review*, *24*(2), 289–304. https://doi.org/10.37253/jjr.v24i2.7280

Dunan, A., & Mudjiyanto, B. (2022). Multitafsir Undang-Undang ITE (Perspektif Edukasi Digitalisasi dan Kebebasan Berekspresi). *Promedia*, *8*(2), 295–316. https://doi.org/10.52447/promedia.v8i2.6141

Faniyah, I., & Maulana, F. (2023). Penerapan Teknologi Informasi Elektronik Police 4.0 Untuk Merespon Secara Cepat Terjadinya Tindak Pidana Pada Wilayah Hukum Polres Payakumbuh. *Unes Journal of Swara Justisia*, *7*(1), 30–41.

Febriawan, D., & Marisa, H. (2024). Understanding Indonesia's Cyber Security Policies: Opportunities and Challenges In The Digitalization Transformation Era. *JOELS: Journal of Election and Leadership*, *5*(1 SE-Articles), 13–21. https://doi.org/10.31849/joels.v5i1.15908

Gomulya, A. M. (2023). Efektivitas Peran Literasi Digital dalam Pembangunan Ekonomi Digital, Studi Kasus pada Korban Kejahatan Pinjaman Online Ilegal. *Jurnal Kritis*, *32*(2), 117–136. https://doi.org/10.24246/kritis.v32i2p117-136

Hartono, B., & Hapsari, R. A. (2019). Mutual Legal Assistance Pada pemberantasan Cyber Crime Lintas Yurisdiksi di Indonesia. *SASI*, *25*(1), 59–71. https://doi.org/10.47268/sasi.v25i1.136

Kennedy, A. (2024a). Analisis Hukum Persaingan Usaha Platform Marketplace Online Pada Era Ekonomi Digital. *Ethics and Law Journal: Business and Notary*, *2*(4), 1–16. https://doi.org/10.61292/eljbn.243

Kennedy, A. (2024b). Perlindungan Data Pribadi Dalam Dunia Siber Di Indonesia Ditinjau Berdasarkan Hukum Tata Negara. *Hukum Dinamika Ekselensia*, *6*(2), 82–98.

Kennedy, A., Surya, W. H., & Wartoyo, F. X. (2024). Tantangan dan Solusi Penerapan E-Government di Indonesia. *Jurnal Terapan Pemerintahan Minangkabau*, *4*(2), 134–147. https://doi.org/10.33701/jtpm.v4i2.4459

Kennedy, A., & Wartoyo, F. X. (2024). Perlindungan Merek Dagang pada Platform E-Commerce di Indonesia Ditinjau dari Perspektif HAM. *JIPRO: Journal of Intellectual Property*, *7*(2), 94–119. https://doi.org/10.20885/jipro.vol7.iss2.art1

Khoironi, S. C. (2020). Pengaruh Analisis Kebutuhan Pelatihan Budaya Keamanan Siber Sebagai Upaya Pengembangan Kompetensi bagi Aparatur Sipil Negara di Era Digital. *Jurnal Studi Komunikasi dan Media*, *24*(1), 37–56. https://doi.org/10.31445/jskm.2020.2945

Kim, S. (2014). Cyber Security and Middle Power Diplomacy: A Network Perspective. *The Korean Journal of International Studies*, *12*(2), 323–352. https://doi.org/10.14731/kjis.2014.12.12.2.323

Laksana, T. G., & Mulyani, S. (2024). Pengetahuan Dasar Identifikasi Dini Deteksi Serangan Kejahatan Siber untuk Mencegah Pembobolan Data Perusahaan. *Jurnal Ilmiah Multidisiplin*, *3*(1), 109–122. https://doi.org/10.56127/jukim.v3i01.1143

Levi, M., & Williams, M. L. (2013). Multi-agency partnerships in cybercrime reduction. *Information Management & Computer Security*, *21*(5), 420–443. https://doi.org/10.1108/IMCS-04-2013-0027

Li, H., Lu, Y., & and He, W. (2019). The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management*, *22*(1), 1–6. https://doi.org/10.1080/1097198X.2019.1569186

Novita, D., Mulyono, M., & Retnowati, A. (2024). Perkembangan Hukum Siber di Indonesia: Studi Literatur tentang Tantangan dan Solusi Keamanan Nasional. *Innovative: Journal Of Social Science Research*, *4*(6), 1179–1186. https://doi.org/10.31004/innovative.v4i6.16144

Parulian, S., Pratiwi, D. A., & Yustina, M. C. (2021). Studi Tentang Ancaman dan Solusi Serangan Siber di Indonesia. *Elnect*, *1*(2), 85–92. https://doi.org/10.17509/telnect.v1i2.40866

Raihan, M. (2023). Perlindungan Data Diri Konsumen dan Tanggungjawab Marketplace Terhadap Data Diri Konsumen (Studi Kasus: Kebocoran Data 91 Juta Akun Tokopedia). *Jurnal Inovasi Penelitian*, *3*(10), 7847–7856. https://doi.org/10.47492/jip.v3i10.2513

Raskasih, F. (2020). Batasan Kebebasan Berpendapat Melalui Media Elektronik dalam Perspektif HAM Dikaitkan dengan Tingak Pidana Menurut UU ITE. *Journal Equitable*, *5*(2), 147–167. https://doi.org/10.37859/jeq.v5i2.2462

Renduchintala, T., Alfauri, H., Yang, Z., Pietro, R. Di, & Jain, R. (2022). A Survey of Blockchain Applications in the FinTech Sector. *Journal of Open Innovation: Technology, Market and Complexity*, *8*(4), 185. https://doi.org/10.3390/joitmc8040185

Rohmah, R. N. (2022). Upaya Membangun Kesadaran Keamanan Siber pada Konsumen E-commerce di Indonesia. *Journal of Trade Development and Studies*, *6*(1), 1–11. https://doi.org/10.52391/jcn.v6i1.629

Rosadi, S. D. (2023). *Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022)* (Tarmizi (ed.)). Sinar Grafika.

Simbolon, M. M., Kesuma, I. G. K. W., & Wibowo, A. E. (2021). Kejahatan Siber pada Penyelenggaraan Perdagangan Berbasis Sistem Elektronik Dalam langkah Pengamanan Pertumbuhan Ekonomi Digital Indonesia. *Junral DEFENDONESIA*, *5*(1), 1–12. https://doi.org/10.54755/defendonesia.v5i1.98

Soekanto, S., & Mamudji, S. (2024). *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Rajawali Pers.

Sunggono, B. (2019). *Metodologi Penelitian Hukum*. Rajawali Pers.

Vania, C., Markoni, M., Saragih, H., & Widarto, J. (2023). Tinjauan Yuridis terhadap Perlindungan Data Pribadi dari Aspek Pengamanan Data dan Keamanan Siber. *2023*, *2*(3), 654–666. https://doi.org/10.58344/jmi.v2i3.157

Wibowo, B., & Hidayat, T. (2024). Strategi Efektif dalam Meningkatkan Kesadaran Keamanan Siber terhadap Ancaman Phishing di Lingkungan Perusahaan PT. XYZ. *Jurnal Pengabdian Masyarakat Sultan Indonesia*, *2*(1), 1–9. https://doi.org/10.58291/abdisultan.v2i1.294