

Legal Analysis of the Use and Circulation of Virtex or Digital Bugs as a Means of Disrupting Electronic Systems in Indonesian Criminal Law

[Analisis Yuridis Penggunaan dan Peredaran Virtex atau Bug Digital sebagai Sarana Gangguan Sistem Elektronik dalam Hukum Pidana Indonesia]

Ranina Bill Ma'fu¹⁾, Mochamad Tanzil Multazam^{*2)}

¹⁾Program Studi Ilmu Hukum, Universitas Muhammadiyah Sidoarjo, Indonesia

²⁾Program Studi Ilmu Hukum, Universitas Muhammadiyah Sidoarjo, Indonesia

*Email Penulis Korespondensi: Tanzilmultazam@umsida.ac.id

Abstract. *The development of digital technology has given rise to new forms of cybercrime, one of which is the use and distribution of virtex (virtual text bugs) as a means of disrupting electronic systems. This study aims to analyze the legal qualifications of this practice in Indonesian criminal law and determine its position in the construction of criminal liability. The research method uses a normative legal approach with a statutory and conceptual approach and deductive analysis through systematic interpretation. The results show that virtex is not a crime, but rather a relevant means (instrumentum sceleris) in the structure of the crime. Its use is punishable if it meets the elements of unlawfulness and causes disruption to electronic systems, while its distribution is only punishable if it meets the element of participation. Data damage or personal data breaches are not a direct result of virtex, but rather a subsequent consequence that depends on the perpetrator's additional actions.*

Keywords- *Virtex, Cyber Crime, System Intrusion*

Abstrak. *Perkembangan teknologi digital melahirkan bentuk kejahatan siber baru, salah satunya praktik penggunaan dan peredaran virtex (virtual text bug) sebagai sarana gangguan sistem elektronik. Penelitian ini bertujuan menganalisis kualifikasi yuridis praktik tersebut dalam hukum pidana Indonesia serta menentukan kedudukannya dalam konstruksi pertanggungjawaban pidana. Metode penelitian menggunakan pendekatan hukum normatif dengan pendekatan perundang-undangan dan konseptual serta analisis deduktif melalui penafsiran sistematis. Hasil penelitian menunjukkan bahwa virtex bukan merupakan tindak pidana, melainkan sarana (instrumentum sceleris) yang relevan dalam struktur delik. Penggunaannya dapat dipidana apabila memenuhi unsur melawan hukum dan menimbulkan gangguan sistem elektronik, sedangkan peredarannya hanya dapat dipidana apabila memenuhi unsur penyertaan. Kerusakan data atau pelanggaran data pribadi bukan akibat langsung virtex, melainkan akibat lanjutan yang bergantung pada perbuatan tambahan pelaku.*

Kata Kunci- *Virtex, Kejahatan Siber, Gangguan Sistem*

I. PENDAHULUAN

Perkembangan teknologi informasi telah mengubah perangkat digital dari sekadar alat komunikasi menjadi pusat penyimpanan data dan identitas elektronik seseorang. Transformasi ini diikuti oleh munculnya berbagai bentuk kejahatan siber dengan karakteristik teknis yang semakin kompleks, salah satunya adalah penggunaan virtual text (virtex) atau bug digital. Virtex merupakan rangkaian teks digital yang dirancang untuk membebani sistem pemrosesan perangkat sehingga sistem tidak bekerja sebagaimana mestinya.[1] Dalam konteks teknis, virtex tidak secara langsung merusak data, melainkan berfungsi sebagai sarana gangguan sistem yang berpotensi membuka peluang terjadinya perbuatan melawan hukum lanjutan seperti manipulasi atau penghapusan data. Kondisi ini menimbulkan persoalan hukum karena penilaian yuridis terhadap perbuatan tersebut harus didasarkan pada hubungan kausalitas antara alat, perbuatan, dan akibat yang ditimbulkan.[2]

Dalam sistem hukum Indonesia, pengaturan mengenai perbuatan yang mengganggu sistem elektronik maupun yang berkaitan dengan data digital tersebar dalam berbagai instrumen peraturan perundang-undangan, baik dalam hukum pidana umum maupun hukum pidana khusus. Meskipun istilah virtex tidak disebut secara eksplisit dalam peraturan perundang-undangan, karakteristik perbuatannya memiliki kesesuaian dengan unsur-unsur delik yang mengatur gangguan sistem elektronik, penggunaan sarana

kejahatan, serta pelanggaran terhadap data elektronik. Seiring dengan berlakunya Kitab Undang-Undang Hukum Pidana yang baru, sebagian ketentuan mengenai kejahatan terhadap sistem elektronik telah diintegrasikan ke dalam kodifikasi hukum pidana nasional. Namun demikian, pengaturan yang berkaitan dengan penyediaan atau fasilitasi sarana kejahatan siber belum seluruhnya dirumuskan secara eksplisit, sehingga masih memerlukan penafsiran sistematis terhadap ketentuan yang tersebar dalam berbagai peraturan hukum.[3]

Permasalahan hukum terkait *virtex* pada dasarnya tidak terletak pada ketiadaan norma, melainkan pada konstruksi penafsiran hukum dalam menentukan kualifikasi perbuatan, hubungan kausalitas antara penggunaan sarana dengan akibat yang ditimbulkan, serta bentuk pertanggungjawaban pidana baik terhadap pelaku utama maupun pihak yang memfasilitasi. Oleh karena itu, analisis terhadap praktik *virtex* perlu ditempatkan dalam kerangka hukum pidana yang berlapis dan tidak semata-mata didasarkan pada dampak teknis yang terlihat.

Berbagai penelitian terdahulu telah mengkaji isu keamanan data pribadi pada perangkat seluler akibat penggunaan dan penyalahgunaan perangkat lunak berbahaya seperti *virtex* dan bug, meskipun masing-masing memiliki fokus yang berbeda. Pertama penelitian yang dilakukan oleh Ririn Silvana Silalahi et al dengan judul “Analisis Hukum Tindak Pidana Cyber Data Breach di Era Digital Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik” Hasil penelitian ini menunjukkan bahwa regulasi yang ada, seperti UU ITE dan UU PDP, masih mengalami tantangan implementatif, terutama dalam keterpaduan antara satu dengan yang lain untuk penanganan kasus nyata di persidangan pidana. Studi kasus putusan pengadilan terhadap pelaku pelanggaran data juga menunjukkan perlunya integrasi dua rezim hukum tersebut agar penanganan pelanggaran data dapat efektif secara preventif dan represif.[4]

Penelitian terdahulu kedua oleh Seri Mughni Sulubara dengan judul “Perlindungan Data Pribadi dalam Kasus Ransomware: Apa Kata Hukum?” Hasil penelitian ini menunjukkan bahwa serangan seperti ransomware memperlihatkan ancaman tersebut secara teknis berbeda dari praktik *virtex*, fenomena ransomware juga berdampak terhadap data pribadi dan menunjukkan bahwa kerangka hukum pidana siber di Indonesia harus mampu menjangkau tindakan yang mengakibatkan gangguan atau kehilangan data sebagai objek hukum yang dilindungi. Penelitian ini mengkaji respons hukum terhadap ransomware berdasarkan UU ITE dan UU PDP, sehingga relevan untuk memahami bagaimana hukum pidana siber menangani ancaman data digital yang destruktif.[5] Penelitian terdahulu ketiga yang dilakukan oleh Devi Anjheli dengan judul “Privasi Digital dan Kejahatan Phishing di Indonesia: Evaluasi Kritis terhadap Efektivitas UU ITE dan UU PDP” Hasil penelitian ini menunjukkan bahwa bentuk-bentuk kejahatan siber seperti phishing atau kebocoran data pribadi menegaskan mengenai tantangan hukum tidak hanya berada pada regulasi substantif, tetapi juga pada aspek teknis pembuktian digital dan konsistensi pemidanaan terhadap pelaku kejahatan berbasis teknologi, sehingga kajian normatif perlu dilengkapi dengan pendekatan pembuktian digital yang mutakhir di dalam hukum pidana siber Indonesia.[6]

Penelitian ini memiliki kebaharuan (*novelty*) yang terletak pada fokus analisis terhadap *virtex* bukan sekadar sebagai fenomena teknis, melainkan sebagai sarana yang dapat digunakan dalam konstruksi tindak pidana siber. Berbeda dengan penelitian sebelumnya yang umumnya membahas kejahatan siber secara umum seperti peretasan, kebocoran data, atau ransomware, penelitian ini secara khusus menelaah kualifikasi yuridis penggunaan dan peredaran *virtex* serta hubungannya dengan unsur delik pidana. Dengan demikian, penelitian ini menempatkan *virtex* dalam kerangka analisis hukum pidana sebagai alat (*instrumentum sceleris*) yang relevan untuk dinilai dalam struktur pertanggungjawaban pidana.

Berbeda dari penelitian sebelumnya, penelitian yang sedang dilakukan saat ini dengan judul “Analisis Yuridis Penggunaan dan Peredaran *Virtex* atau Bug Digital sebagai Sarana Gangguan Sistem Elektronik dalam Hukum Pidana Indonesia” secara khusus mengkaji praktik jual beli *virtex* atau bug sebagai sarana tindak pidana yang digunakan untuk merusak sistem elektronik dan menghapus data pribadi. Penelitian ini tidak hanya menempatkan *virtex* sebagai fenomena teknis, tetapi sebagai objek dan alat kejahatan dalam kerangka hukum pidana. Selain itu, penelitian ini mengintegrasikan dua peraturan hukum, yaitu hukum pidana siber (UU ITE) dan perlindungan data pribadi (UU PDP), secara terpadu untuk menganalisis pertanggungjawaban pidana pelaku, unsur-unsur delik yang terpenuhi, serta implikasi hukum terhadap korban.

Penelitian ini bertujuan untuk menganalisis secara yuridis kualifikasi praktik penggunaan dan peredaran *virtex* (*virtual text bug*) sebagai sarana gangguan sistem elektronik dalam hukum pidana Indonesia melalui penafsiran sistematis terhadap norma-norma pidana yang relevan guna menilai apakah perbuatan tersebut memenuhi unsur tindak pidana, bagaimana hubungan kausalitas antara penggunaan *virtex* sebagai alat dengan akibat yang ditimbulkan, serta sejauh mana konstruksi pertanggungjawaban pidana dapat dibebankan kepada pelaku baik sebagai pelaku langsung maupun sebagai pihak yang memfasilitasi, sehingga diperoleh

argumentasi hukum yang konsisten dan dapat dipertanggungjawabkan secara doktrinal.

Rumusan Masalah

1. Kualifikasi yuridis praktik penggunaan dan peredaran virtex sebagai sarana gangguan sistem elektronik dalam hukum pidana Indonesia.

Kategori SDGs: Sesuai ketentuan indikator Sustainable Development Goals (SDGs) ke-16 yaitu *Peace, Justice, and Strong Institutions*.

II. METODE

Penelitian ini menggunakan metode penelitian hukum normatif (normative legal research) dengan menerapkan Pendekatan Perundang-undangan (Statute Approach), Pendekatan Konseptual (Conceptual Approach). Bahan hukum primer meliputi, KUHP, Undang-Undang No. 11 Tahun 2008 jo. Undang-Undang No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Bahan hukum sekunder seperti literatur, artikel jurnal, buku hukum, dan pendapat ahli yang mendukung penelitian ini. Analisis bahan hukum menggunakan analisa deduktif dengan penafsiran sistematis terhadap norma hukum.

III. HASIL DAN PEMBAHASAN

A. Kerangka Regulasi Tindak Pidana Berbasis Teknologi Informasi di Indonesia

Sebelum membahas kerangka regulasi tindak pidana berbasis teknologi informasi di Indonesia, penting untuk menegaskan terlebih dahulu kedudukan konseptual virtex (*virtual text*) dalam perspektif hukum pidana siber. Rangkaian huruf digital terstruktur yang dikenal sebagai "virtex" dimaksudkan untuk membebani daya pemrosesan perangkat dan mengganggu fungsinya. Secara teknis, virtex mengganggu sistem dan bukan menghancurkan data secara langsung. Kerusakan data hanya terjadi jika kondisi sistem yang telah terganggu tersebut kemudian digunakan untuk melakukan tindakan tambahan seperti manipulasi, penghapusan, atau akses tanpa izin. Oleh karena itu, dalam analisis hukum pidana virtex harus diposisikan sebagai alat atau metode yang relevan dalam penciptaan kejahatan dan pertanggungjawaban pidana, bukan sebagai tindakan utama dalam analisis hukum pidana.

Dalam sistem hukum Indonesia, pengaturan mengenai perbuatan yang berkaitan dengan gangguan sistem elektronik dan data digital tidak hanya terdapat dalam peraturan khusus, tetapi juga dalam hukum pidana umum. Seiring berlakunya Kitab Undang-Undang Hukum Pidana yang baru, sebagian norma mengenai perbuatan terhadap sistem elektronik telah terintegrasi dalam kodifikasi pidana nasional, meskipun ketentuan khusus mengenai aspek teknis tertentu masih tersebar dalam peraturan sektoral. Kondisi ini memerlukan interpretasi komprehensif dari kerangka hukum pidana secara keseluruhan agar dapat menentukan secara tepat kualifikasi perbuatan penggunaan maupun fasilitasi virtex sebagai bentuk perbuatan yang berpotensi melanggar hukum.

Dengan demikian, analisis terhadap praktik virtex tidak cukup hanya menilai akibat yang timbul, tetapi harus dilakukan melalui pengujian unsur delik secara berlapis yang mencakup identifikasi perbuatan, sifat melawan hukum, hubungan kausalitas, serta bentuk keterlibatan pelaku. Pendekatan ini penting karena penggunaan virtex dapat berdiri sebagai perbuatan tersendiri berupa gangguan sistem, namun juga dapat menjadi bagian dari rangkaian perbuatan lain yang menimbulkan akibat hukum berbeda. Oleh sebab itu, konstruksi hukum terhadap virtex harus dibangun melalui penafsiran normatif yang komprehensif dan tidak semata-mata didasarkan pada dampak teknis yang terlihat.

Untuk menilai kualifikasi yuridis praktik penggunaan dan peredaran virtex sebagai sarana gangguan sistem elektronik, diperlukan pemetaan komprehensif terhadap kerangka regulasi yang relevan dalam hukum positif Indonesia. Pemetaan ini penting karena pengaturan mengenai perbuatan terhadap sistem elektronik, data digital, serta penggunaan sarana kejahatan tidak hanya terdapat dalam satu peraturan perundang-undangan, melainkan tersebar dalam beberapa instrumen hukum yang memiliki karakteristik pengaturan berbeda. Oleh karena itu, tabel 1 menyajikan perbandingan sistematis antara ketentuan dalam KUHP, Undang-Undang Informasi dan Transaksi Elektronik, dan Undang-Undang Perlindungan Data Pribadi untuk menunjukkan ruang lingkup pengaturan serta relevansinya terhadap praktik virtex.

Tabel 1. Kerangka Regulasi Tindak Pidana Terkait Sistem Elektronik dan Data Digital

No.	Komponen Regulasi	KUHP (Baru)	UU ITE	UU PDP	Karakter Pengaturan
1.	Objek Perlindungan	Sistem elektronik, data, dan keamanan informasi digital.	Sistem elektronik dan informasi elektronik (Pasal 1 angka 5, 6, 15)	Data pribadi sebagai hak subjek data (Pasal 1 angka 1, 4, 5)	KUHP bersifat umum, UU ITE teknis sistem, UU PDP berbasis hak privasi
2.	Jenis Delik	Gangguan sistem, akses ilegal, manipulasi data (ketentuan kejahatan teknologi informasi dalam KUHP).	Akses ilegal (Pasal 30), Intersepsi ilegal (Pasal 31), Manipulasi/Perusakan Data (Pasal 32), Gangguan Sistem (Pasal 33)	Perolehan Data tanpa hak (Pasal 35), Pengungkapan Data (Pasal 36), Penggunaan Data (Pasal 37)	KUHP delik umum, UU ITE delik siber teknis, UU PDP delik perlindungan data
3.	Unsur Melawan Hukum	Melawan hukum dan kesengajaan sebagai unsur umum delik.	“Tanpa hak” dan “melawan hukum” (Pasal 30–33)	“Secara melawan hukum” (Pasal 35–37)	Unsur melawan hukum menjadi dasar pertanggungjawaban pidana
4.	Subjek Hukum	Setiap orang.	Setiap orang (Pasal 52 ayat 1)	Setiap orang dan korporasi (Pasal 70–71)	Memungkinkan pertanggungjawaban individu maupun badan hukum
5.	Penyertaan/Fasilitasi	Diatur dalam ketentuan penyertaan KUHP	Tidak diatur spesifik	Tidak diatur spesifik	KUHP menjadi dasar menjerat penjual/penyedia alat
6.	Sistem Sanksi	Pidana pokok dan tambahan	Penjara dan/atau denda (Pasal 46–48)	Penjara dan/atau denda (Pasal 67–69)	Semua peraturan memungkinkan sanksi kumulatif-alternatif
7.	Sifat Delik	Delik umum	Delik khusus siber	Delik khusus data pribadi	Berlaku berlapis sesuai konteks perbuatan
8.	Hubungan Antar Regulasi	Hukum pidana umum	Lex specialis terhadap kejahatan siber	Lex specialis terhadap perlindungan data	Berlaku komplementer dan saling melengkapi

Berdasarkan tabel 1, terlihat bahwa praktik virtex berada dalam irisan pengaturan antara KUHP sebagai hukum pidana umum, Undang-Undang Informasi dan Transaksi Elektronik sebagai peraturan khusus yang mengatur perbuatan terhadap sistem elektronik, serta Undang-Undang Perlindungan Data Pribadi sebagai instrumen perlindungan hak atas data pribadi. Struktur pengaturan yang berlapis ini

ght © Universitas Muhammadiyah Sidoarjo. This preprint is protected by copyright held by Universitas Muhammadiyah Sidoarjo and is distributed under the Creative Commons Attribution License (CC BY). Users may share, distribute, or reproduce the work as long as the original author(s) and copyright holder are credited, and the preprint server is cited per academic standards.

rs retain the right to publish their work in academic journals where copyright remains with them. Any use, distribution, or reproduction that does not comply with these terms is not permitted.

menunjukkan bahwa penilaian yuridis terhadap praktik virtex harus dilakukan melalui pendekatan interpretasi sistematis dengan menempatkan masing-masing undang-undang sesuai fungsi normatifnya. Dalam konteks perbuatan utama berupa penggunaan virtex, ketentuan yang paling relevan terdapat dalam UU ITE, khususnya Pasal 33 yang melarang setiap perbuatan yang secara melawan hukum mengakibatkan terganggunya sistem elektronik sehingga tidak bekerja sebagaimana mestinya. Selain itu, Pasal 30 dan Pasal 32 UU ITE dapat menjadi relevan apabila penggunaan virtex diikuti oleh perbuatan lanjutan seperti akses tanpa hak atau manipulasi informasi elektronik. Sementara itu, KUHP berfungsi sebagai dasar umum untuk menilai konstruksi pertanggungjawaban pidana, terutama dalam hal keterlibatan pihak lain yang menyediakan, menjual, atau memfasilitasi sarana virtex melalui doktrin penyertaan.[7]

Di sisi lain, UU PDP berperan apabila gangguan sistem yang ditimbulkan berdampak pada data pribadi, misalnya apabila setelah sistem terganggu terjadi perolehan, pengungkapan, atau penggunaan data secara melawan hukum sebagaimana diatur dalam Pasal 35, Pasal 36, dan Pasal 37 beserta ketentuan sanksinya. Dengan demikian, praktik virtex tidak secara otomatis merupakan pelanggaran terhadap data pribadi, melainkan harus dinilai berdasarkan ada atau tidaknya perbuatan lanjutan yang memenuhi unsur delik dalam UU PDP. Keterkaitan antara UU ITE dan UU PDP menunjukkan bahwa kedudukan hukum virtex dalam sistem hukum Indonesia harus dipahami sebagai sarana atau alat yang relevan dalam konstruksi tindak pidana, bukan sebagai delik yang berdiri sendiri, sehingga analisis hukumnya harus mempertimbangkan jenis perbuatan, posisi pelaku, serta akibat yang ditimbulkan dalam suatu rangkaian peristiwa hukum.[8]

Selain pemetaan regulasi normatif, analisis yuridis terhadap virtex juga memerlukan pemahaman mengenai karakteristik teknis sarana yang digunakan. Hal ini penting karena dalam hukum pidana siber, bentuk alat dan cara kerja teknisnya berpengaruh terhadap penilaian unsur perbuatan, kesengajaan, serta hubungan kausalitas antara tindakan dan akibat yang ditimbulkan. Oleh karena itu, berikut disajikan klasifikasi bentuk sarana digital yang secara teknis dapat digunakan sebagaimana disajikan dalam Tabel 2.

Tabel 2. Klasifikasi Sarana Teknis Virtex dan Potensi Dampak Hukumnya

No.	Jenis Sarana	Karakteristik Teknis	Mekanisme Kerja	Dampak Sistem	Potensi Konsekuensi Hukum
1.	Text overload	String teks sangat panjang	Membebani memori	Aplikasi freeze	Gangguan sistem elektronik
2.	Unicode crash text	Karakter kompleks	Error parsing	Sistem crash	Delik gangguan sistem
3.	Loop text	Teks berulang	Infinite process	Device hang	Unsur menghambat fungsi sistem
4.	Structured payload text	Teks berstruktur kode	Trigger bug	Sistem tidak responsif	Potensi sarana kejahatan
5.	Dual text bug	Kombinasi karakter	Overload rendering	Aplikasi keluar paksa	Relevan sebagai alat kejahatan
6.	Text exploit chain	Teks berlapis	Trigger vulnerability	Sistem terbuka	Potensi akses ilegal lanjutan

Berdasarkan tabel 2 menunjukkan bahwa secara teknis virtex bukanlah program perusak data, melainkan sarana yang dirancang untuk mengganggu kinerja sistem melalui pembebanan proses atau eksploitasi kerentanan perangkat lunak. Oleh karena itu, akibat hukum yang timbul tidak selalu berupa

kerusakan data, melainkan dapat berupa gangguan fungsi sistem. Dalam konteks hukum pidana, perbedaan ini sangat penting karena menentukan jenis delik yang dapat dikenakan. Gangguan sistem merupakan perbuatan yang berdiri sendiri sebagai delik, sedangkan kerusakan data baru dapat dipertanggungjawabkan apabila terdapat perbuatan lanjutan setelah sistem mengalami gangguan.[1]

Secara doktrinal, kedudukan virtex lebih tepat dipahami sebagai alat (*instrumentum sceleris*) daripada sebagai perbuatan pidana itu sendiri. Dengan demikian, penggunaan virtex hanya dapat dikualifikasikan sebagai tindak pidana apabila memenuhi unsur-unsur delik yang diatur dalam undang-undang, seperti unsur tanpa hak, kesengajaan, dan akibat yang dilarang. Sebaliknya, apabila tidak terdapat unsur tersebut, penggunaan virtex tidak dapat secara otomatis dianggap sebagai perbuatan pidana. Pendekatan ini mencerminkan prinsip legalitas dalam hukum pidana yang menegaskan bahwa tidak ada perbuatan yang dapat dipidana tanpa ketentuan hukum yang mengaturnya secara jelas.[2]

B. Kedudukan Hukum Virtex dalam Sistem Hukum Indonesia

Virtex (*virtual text*) merupakan rangkaian teks digital terstruktur yang dirancang untuk membebani sistem pemrosesan perangkat sehingga menyebabkan sistem tidak bekerja sebagaimana mestinya. Virtex juga salah satu bentuk manipulasi kode digital yang dalam praktik dapat menyebabkan gangguan terhadap sistem elektronik maupun penghapusan data dalam perangkat korban. Namun, dalam perspektif teknis virtex bukanlah program perusak data, melainkan sarana yang menimbulkan gangguan fungsi sistem melalui eksploitasi keterbatasan pemrosesan atau kerentanan perangkat lunak. Meskipun istilah *virtex* tidak disebut secara eksplisit dalam undang-undang, secara substansial virtex berpotensi menimbulkan dampak yang sama dengan kejahatan siber lain seperti ransomware atau serangan malware yang mengakibatkan terganggunya integritas serta ketersediaan data dan sistem elektronik.[9] Oleh karena itu, virtex tidak secara langsung mengakibatkan kerusakan data, melainkan hanya menciptakan kondisi sistem yang tidak stabil. Kerusakan data baru dapat terjadi apabila kondisi tersebut kemudian dimanfaatkan untuk melakukan perbuatan lanjutan seperti manipulasi, penghapusan, atau akses tanpa hak terhadap sistem elektronik.[10]

Dalam kerangka hukum pidana, virtex tidak dapat diposisikan sebagai tindak pidana itu sendiri, melainkan sebagai alat atau sarana (*instrumentum sceleris*) yang relevan dalam konstruksi delik. Hal ini sejalan dengan prinsip dasar hukum pidana yang menilai pertanggungjawaban bukan pada alat yang digunakan, melainkan pada perbuatan melawan hukum yang dilakukan dengan alat tersebut.[11] Dengan demikian, penggunaan virtex hanya dapat dikualifikasikan sebagai tindak pidana apabila memenuhi unsur delik yang diatur dalam peraturan perundang-undangan, seperti adanya perbuatan tanpa hak, kesengajaan, serta akibat yang dilarang oleh hukum.[12] Dalam sistem hukum Indonesia, penilaian terhadap praktik virtex harus dilakukan melalui pendekatan normatif yang mempertimbangkan hubungan antara berbagai ketentuan pengaturan. Ketentuan dalam UU ITE relevan untuk menilai perbuatan yang secara langsung menyebabkan gangguan sistem elektronik, sedangkan KUHP berfungsi sebagai dasar umum dalam menilai bentuk pertanggungjawaban pidana dan keterlibatan pihak lain, termasuk dalam hal fasilitasi atau penyediaan sarana. Sementara itu, UU PDP menjadi relevan apabila gangguan sistem yang ditimbulkan berdampak pada data pribadi, misalnya ketika setelah sistem terganggu terjadi perolehan, pengungkapan, atau penggunaan data tanpa hak. Struktur pengaturan yang berlapis ini menunjukkan bahwa praktik virtex tidak dapat dinilai secara tunggal, melainkan harus dianalisis berdasarkan konteks perbuatan dan akibat yang timbul.[13]

Dengan demikian, kedudukan hukum virtex harus dipahami melalui konstruksi delik berlapis yang mencakup identifikasi perbuatan utama, perbuatan lanjutan, dan hubungan kausalitas di antara keduanya. Penggunaan virtex dapat berdiri sebagai perbuatan yang menimbulkan gangguan sistem apabila memenuhi unsur delik yang relevan, namun dapat pula menjadi bagian dari rangkaian perbuatan yang lebih kompleks apabila diikuti tindakan lain seperti manipulasi data atau akses ilegal. Oleh karena itu, analisis hukum terhadap praktik virtex harus dilakukan secara sistematis dengan menilai posisi alat, jenis perbuatan, dan akibat yang ditimbulkan dalam satu rangkaian peristiwa hukum, sehingga kualifikasi pidana yang ditetapkan tetap sejalan dengan asas legalitas dan prinsip pertanggungjawaban pidana yang proporsional.

C. Kualifikasi Hukum Praktik Jual Beli Virtex

Praktik jual beli virtex atau bug digital tidak dapat dipahami semata-mata sebagai aktivitas transaksi biasa dalam ruang digital, melainkan harus dinilai berdasarkan potensi penggunaannya sebagai sarana untuk melakukan perbuatan melawan hukum. Secara konseptual, virtex merupakan alat digital yang

secara teknis berfungsi mengganggu kinerja sistem elektronik, sehingga nilai hukumnya tidak ditentukan oleh bentuk objeknya, melainkan oleh tujuan penggunaan dan konteks perbuatannya. Oleh karena itu, transaksi yang melibatkan peredaran virtex hanya dapat dikualifikasikan sebagai tindak pidana apabila terdapat keterkaitan antara penyediaan sarana tersebut dengan perbuatan melawan hukum yang dilakukan atau direncanakan.[10]

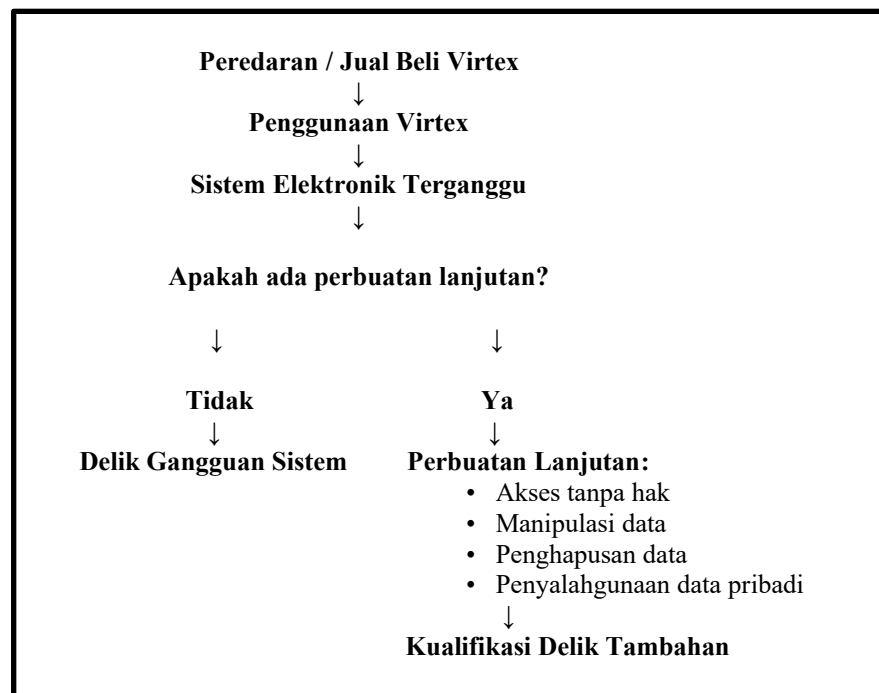
Dalam perspektif hukum pidana, pihak yang menjual, menyediakan, atau mendistribusikan virtex dapat dimintai pertanggungjawaban pidana apabila perbuatannya memenuhi unsur penyertaan atau pembantuan dalam tindak pidana. Doktrin penyertaan dalam hukum pidana menegaskan bahwa seseorang tidak harus menjadi pelaku utama untuk dapat dipidana, melainkan cukup terbukti memberikan kontribusi yang secara sadar membantu terjadinya tindak pidana. Dengan demikian, peredaran virtex dapat dikualifikasikan sebagai perbuatan yang relevan secara pidana apabila penjual mengetahui atau patut mengetahui bahwa sarana tersebut akan digunakan untuk mengganggu sistem elektronik atau melakukan perbuatan melawan hukum lainnya.[15]

Dalam kaitannya dengan ketentuan hukum positif, penggunaan virtex untuk mengganggu sistem elektronik dapat memenuhi unsur delik sebagaimana diatur dalam ketentuan yang melarang perbuatan yang mengakibatkan sistem elektronik tidak bekerja sebagaimana mestinya. Apabila penggunaan tersebut diikuti dengan perbuatan lanjutan seperti akses tanpa hak atau manipulasi informasi elektronik, maka ketentuan lain yang mengatur akses ilegal maupun perubahan data dapat diterapkan secara kumulatif. Hal ini menunjukkan bahwa penggunaan virtex dapat berfungsi sebagai perbuatan awal yang membuka kemungkinan terjadinya tindak pidana lain dalam satu rangkaian peristiwa hukum.[4]

Dari perspektif perlindungan data pribadi, praktik virtex hanya menjadi relevan secara hukum apabila gangguan sistem yang ditimbulkan berimplikasi pada data pribadi. Dengan kata lain, penggunaan virtex tidak serta-merta merupakan pelanggaran terhadap data pribadi, melainkan baru dapat dikualifikasikan sebagai delik apabila setelah sistem terganggu terjadi perolehan, pengungkapan, atau penggunaan data pribadi tanpa hak. Pendekatan ini penting untuk menegaskan bahwa tidak setiap gangguan sistem otomatis menjadi pelanggaran privasi, melainkan harus dibuktikan adanya hubungan kausal antara perbuatan dan akibat terhadap data. [10]

Berdasarkan konstruksi tersebut, praktik jual beli virtex harus dipahami sebagai perbuatan yang bersifat kondisional dalam hukum pidana, yaitu hanya dapat dipidana apabila memenuhi unsur-unsur delik yang ditentukan undang-undang. Virtex tidak memiliki sifat melawan hukum secara inheren, melainkan memperoleh relevansi pidana ketika digunakan atau disediakan sebagai sarana untuk melakukan perbuatan yang dilarang. Oleh karena itu, penilaian yuridis terhadap praktik peredaran virtex harus mempertimbangkan secara cermat unsur kesengajaan, hubungan kausalitas, serta bentuk keterlibatan pelaku dalam suatu rangkaian peristiwa pidana.[16]

Dengan demikian, kualifikasi hukum terhadap praktik penggunaan dan peredaran virtex tidak dapat ditentukan secara abstrak, melainkan harus dianalisis secara konkret berdasarkan struktur perbuatan yang terjadi. Pendekatan ini sejalan dengan asas legalitas dan prinsip pertanggungjawaban pidana yang menuntut pembuktian unsur delik secara spesifik sebelum seseorang dapat dipidana. Oleh sebab itu, virtex dalam sistem hukum pidana Indonesia lebih tepat dipahami sebagai sarana yang dapat menjadi relevan secara hukum apabila digunakan dalam konteks perbuatan melawan hukum, bukan sebagai objek delik yang berdiri sendiri. Sebagaimana tergambar dalam Gambar 1, praktik virtex tidak dapat dianalisis secara linear, melainkan harus dipahami melalui konstruksi delik berlapis yang memisahkan antara peredaran, penggunaan, akibat gangguan sistem, dan kemungkinan timbulnya delik lanjutan.



Gambar 1. Struktur Berlapis Kualifikasi Hukum Praktik Virtex

Gambar 1 menunjukkan bahwa kualifikasi hukum terhadap praktik virtex harus dianalisis melalui struktur berlapis yang dimulai dari identifikasi bentuk perbuatan, dilanjutkan dengan penilaian akibat langsung, dan kemudian diuji kemungkinan adanya perbuatan lanjutan.[17] Tahap pertama adalah peredaran atau penyediaan virtex yang secara hukum baru relevan apabila terbukti memiliki hubungan dengan penggunaan untuk tujuan melawan hukum. Tahap kedua adalah penggunaan virtex yang dapat menimbulkan gangguan sistem elektronik sebagai akibat langsung. Gangguan sistem ini merupakan akibat teknis utama yang secara yuridis dapat berdiri sebagai delik tersendiri apabila memenuhi unsur melawan hukum.[18] Tahap ketiga bersifat kondisional, yaitu menilai apakah setelah sistem terganggu terdapat perbuatan lanjutan seperti akses tanpa hak, manipulasi data, atau penggunaan data pribadi secara ilegal. Apabila perbuatan lanjutan tersebut terjadi, maka kualifikasi pidana dapat berkembang menjadi beberapa delik tambahan yang berdiri sendiri namun tetap memiliki hubungan kausal dengan perbuatan awal. Struktur analisis berlapis ini menunjukkan bahwa virtex bukan merupakan tindak pidana itu sendiri, melainkan sarana yang dapat menimbulkan konsekuensi hukum apabila digunakan dalam rangkaian perbuatan yang memenuhi unsur delik.[19]

Model analisis berlapis tersebut sejalan dengan teori struktur delik dalam hukum pidana yang menekankan pentingnya pemisahan antara alat, perbuatan, dan akibat. Dalam konteks ini, virtex harus ditempatkan sebagai alat yang secara yuridis netral, sedangkan relevansi pidananya ditentukan oleh penggunaan alat tersebut dalam perbuatan melawan hukum. Pendekatan ini penting untuk menjaga konsistensi dengan asas legalitas yang melarang kriminalisasi objek tanpa dasar normatif yang jelas. Oleh karena itu, penilaian terhadap praktik virtex harus dilakukan secara sistematis dengan menilai setiap tahap peristiwa hukum secara terpisah namun tetap mempertimbangkan hubungan kausal di antaranya.

D. Implikasi Hukum dan Rekomendasi Penguatan Pengaturan

Praktik virtex yang digunakan untuk merusak sistem elektronik atau menghapus data pribadi secara tanpa hak memiliki implikasi hukum yang penting bagi pelaku, korban, dan sistem hukum secara keseluruhan. Secara yuridis, penggunaan virtex dapat memenuhi unsur tindak pidana berdasarkan ketentuan dalam UU ITE maupun UU Perlindungan Data Pribadi (UU PDP), sehingga pelakunya berpotensi dikenai sanksi pidana apabila unsur perbuatan melawan hukum, tanpa hak, dan akibat kerugian terpenuhi. Penelitian terbaru menunjukkan bahwa ancaman terhadap integritas data pribadi berdampak tidak hanya

pada kerugian material tetapi juga pada hak privasi dan kepercayaan masyarakat terhadap penggunaan teknologi digital secara umum.[20]

Selain itu, terdapat implikasi hukum yang signifikan terhadap korban, karena pelanggaran terhadap data pribadi yang diakibatkan oleh virtex tidak hanya menyebabkan hilangnya data, tetapi juga mempengaruhi reputasi serta rasa aman individu dalam beraktivitas di dunia digital. Hal ini sesuai dengan temuan penelitian yang menunjukkan bagaimana pelanggaran data menimbulkan dampak psikologis dan sosial yang mendalam bagi korban, terutama ketika data sensitif terekspos atau dihapus secara tidak sah.[21]

Agar penegakan hukum terhadap praktik virtex lebih efektif, diperlukan penguatan regulasi dan mekanisme penegakan hukum. Pertama, perlu disusun pedoman penafsiran hukum yang lebih jelas bagi aparat penegak hukum dalam menerapkan pasal-pasal dalam UU ITE dan UU PDP, terutama yang berkaitan dengan akses tanpa hak, perusakan sistem, dan penghilangan informasi elektronik. Penelitian lain menunjukkan bahwa ketidakjelasan interpretasi norma merupakan salah satu hambatan utama dalam konsistensi putusan kasus siber di tingkat peradilan. [22]

Kedua, penguatan koordinasi antarlembaga penegak hukum menjadi bagian penting dalam strategi penanganan kasus yang kompleks. Koordinasi antara kepolisian, kejaksaan, dan Komisi Perlindungan Data Pribadi perlu ditingkatkan agar proses investigasi dan penindakan berjalan lebih cepat dan tidak terfragmentasi. Penelitian juga menunjukkan bahwa mekanisme kerja sama yang kuat dapat mempercepat penyidikan dan memperbaiki kualitas pengumpulan bukti digital.[23]

Selain itu, perlu adanya peningkatan kapasitas teknis aparat hukum, khususnya dalam forensik digital yang terkait dengan bukti siber. Teknologi terus berkembang dengan cepat, sehingga kemampuan aparat dalam memahami dan mengolah bukti digital sangat menentukan keberhasilan proses hukum di pengadilan. Peningkatan kemampuan ini dapat dilakukan melalui pelatihan dan kolaborasi dengan pakar teknologi informasi.[24]

Terakhir, peningkatan literasi digital masyarakat juga menjadi bagian dari strategi perlindungan hukum yang berkelanjutan. Ketika masyarakat memiliki pemahaman yang baik mengenai hak atas data pribadi serta risiko siber, mereka akan lebih proaktif dalam melaporkan pelanggaran dan bekerja sama dalam proses hukum. Studi menunjukkan bahwa literasi digital yang rendah menjadi salah satu faktor yang menghambat proses penanganan kasus siber karena korban tidak memahami hak mereka atau tidak dapat menyediakan bukti yang relevan.

Dengan demikian, penguatan pengaturan hukum terhadap praktik virtex tidak hanya ditujukan pada pengetatan norma pidana, tetapi juga mencakup pembentukan pedoman hukum yang jelas, peningkatan capacity building aparat penegak hukum, koordinasi antarlembaga yang efektif, dan peningkatan literasi digital masyarakat, sehingga penegakan hukum terhadap praktik siber destruktif seperti virtex dapat terlaksana secara optimal.

IV. KESIMPULAN

Praktik penggunaan dan peredaran virtex dalam sistem hukum Indonesia tidak dapat dikualifikasikan sebagai tindak pidana secara otomatis, melainkan harus dinilai berdasarkan pemenuhan unsur delik yang diatur dalam hukum positif. Virtex secara konseptual merupakan sarana digital yang berfungsi mengganggu kinerja sistem elektronik, sehingga kedudukannya dalam hukum pidana lebih tepat dipahami sebagai alat (*instrumentum sceleris*) daripada sebagai perbuatan pidana itu sendiri. Penggunaan virtex dapat dikualifikasikan sebagai tindak pidana apabila terbukti dilakukan tanpa hak dan menimbulkan akibat berupa terganggunya sistem elektronik sebagaimana diatur dalam ketentuan hukum yang relevan, sedangkan peredaran atau penyediaannya hanya dapat dipidana apabila memenuhi unsur penyertaan atau pembantuan dalam tindak pidana. Kerusakan data atau pelanggaran data pribadi bukan merupakan akibat langsung dari virtex, melainkan konsekuensi lanjutan yang baru memiliki relevansi pidana apabila terdapat perbuatan tambahan seperti akses ilegal, manipulasi, atau penggunaan data tanpa hak. Dengan demikian, penilaian yuridis terhadap praktik virtex harus dilakukan melalui konstruksi delik berlapis yang mempertimbangkan jenis perbuatan, hubungan kausalitas, dan posisi pelaku dalam rangkaian peristiwa hukum. Pendekatan ini menegaskan bahwa pengaturan hukum terhadap praktik virtex dalam sistem hukum Indonesia pada dasarnya telah tersedia melalui kombinasi norma hukum pidana umum dan khusus, sehingga yang diperlukan bukan pembentukan delik baru, melainkan penafsiran hukum yang sistematis, konsisten, dan selaras dengan asas legalitas serta prinsip pertanggungjawaban pidana. Hal ini menunjukkan bahwa perkembangan teknologi digital menuntut pendekatan interpretasi hukum pidana yang adaptif namun tetap berlandaskan asas legalitas.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada kedua orang tua tercinta atas doa, kasih sayang, dukungan, pengorbanan, serta motivasi yang tiada henti selama proses penyusunan tugas akhir ini. Ucapan terima kasih juga penulis sampaikan kepada dosen pembimbing, keluarga, sahabat, serta semua pihak yang telah memberikan arahan, bantuan, dan dukungan sehingga tugas akhir ini dapat diselesaikan dengan baik. Penulis menyadari bahwa tugas akhir ini masih memiliki keterbatasan. Oleh karena itu, kritik dan saran yang membangun sangat diharapkan demi penyempurnaan di masa mendatang. Semoga tugas akhir ini dapat memberikan manfaat bagi pengembangan ilmu pengetahuan dan menjadi referensi bagi penelitian selanjutnya.

REFERENSI

- [1] M. Alazab, S. Venkatraman, P. Watters, M. Alazab, dan A. Alazab, "Cybercrime: The Case of Obfuscated Malware," dalam *Global Security, Safety and Sustainability & e-Democracy*, vol. 99, C. K. Georgiadis, H. Jahankhani, E. Pimenidis, R. Bashroush, dan A. Al-Nemrat, Ed., dalam *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, vol. 99., Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, hlm. 204–211. doi: https://doi.org/10.1007/978-3-642-33448-1_28.
- [2] Maksudul Shadat Akash, "The end of phone numbers: A future without traditional communication identifiers," *World J. Adv. Eng. Technol. Sci.*, vol. 14, no. 1, hlm. 060–068, Jan 2025, doi: <https://doi.org/10.30574/wjaets.2025.14.1.0660>.
- [3] C. Reed, "Information Ownership in the Cloud (Second Edition)," *SSRN Electronic Journal*, Sep. 2021, doi: <https://doi.org/10.2139/SSRN.420491>
- [4] R. S. Silalahi, M. Mulyadi, dan W. Trisna, "Analisis Hukuk Tindak Pidana Cyber Data Breach di Era Digital Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik (Studi Putusan Nomor 2447/PID.SUS/2024/PN MDN)," vol. 4, 2025, doi: <https://doi.org/10.54443/sibatik.v4i9.3249>
- [5] Seri Mughni Sulubara, "Perlindungan Data Pribadi dalam Kasus Ransomware: Apa Kata Hukum?," *Eksekusi J. Ilmu Huk. Dan Adm. Negara*, vol. 2, no. 4, hlm. 426–434, Nov 2024, doi: <https://doi.org/10.55606/eksekusi.v2i4.1823>.
- [6] K. F. Steinmetz, B. P. Schaefer, A. L. McCarthy, C. G. Brewer, dan D. L. Kurtz, "Exploring Cybercrime Capabilities: Variations Among Cybercrime Investigative Units," *Crim. Justice Policy Rev.*, vol. 35, no. 4, hlm. 194–215, Agu 2024, doi: <https://doi.org/10.1177/08874034241265106>.
- [7] R. Rencang, "Analisis Kritis Terhadap Penegakan Hukum Dalam Penanganan Kejahatan Siber Pada Kasus Data Breach Dalam Perspektif Hukum Pidana Indonesia," Vol. 6, No. 7, 2025, doi: <https://doi.org/10.56370/jhlg.v6i7.1002>
- [8] L. Judijanto, A. F. Lubis, D. E. Sam Karauwan, S. S. Bungin, dan H. A. Mau, "Efektivitas Kebijakan Perlindungan Data Pribadi dalam Menjaga Hak Asasi Manusia di Era Teknologi di Indonesia," *Sanskara Huk. Dan HAM*, vol. 3, no. 01, hlm. 34–42, Agu 2024, doi: <https://doi.org/10.58812/shh.v3i01.445>.
- [9] I. G. A. S. K. Singgi, I. G. B. Suryawan, dan I. N. G. Sugiarta, "Penegakan Hukum terhadap Tindak Pidana Peretasan sebagai Bentuk Kejahatan Mayantara (Cyber Crime)," *J. Konstr. Huk.*, vol. 1, no. 2, hlm. 334–339, Okt 2020, doi: <https://doi.org/10.22225/jkh.2.1.2553.334-339>.
- [10] Deva Inggria, Wayne Gladys, Octatiana Bella, Asmak Ul Hosnah, "Penegakan Hukum Terhadap Tindak Pidana Cybercrime Dalam Kasus Peretasan dan Pelanggaran Data Pribadi oleh Hacker Bjorka", Vol. 8 No. 4, 2025, doi: <https://doi.org/P-2655-710X> e-ISSN 2655-6022
- [11] Saptaning Ruju Paminto, Ahdi Hidayat, Bilkis Nabila, M. Raihan Husaeni, dan Siti Jenar Maharani, "Perlindungan Hukum Bagi Korban Pencurian Data Dan Informasi Pribadi Di Era Kejahatan Siber," *J. Dunia Ilmu Huk. JURDIKUM*, vol. 2, no. 2, hlm. 54–61, Des 2024, doi: <https://doi.org/10.59435/jurdikum.v2i2.453>.
- [12] D. Tendeand dan W. Susanto, "Tinjauan Yuridis Terhadap Kejahatan Siber dan Perlindungan Data Pribadi," vol. 1, no. 1, 2025, url: <https://ejournal.kalibra.or.id/index.php/legalnote/article/view/24>
- [13] I. M. Kholis, "Perlindungan Data Pribadi dan Keamanan Siber di Sektor Perbankan: Studi Kritis atas Penerapan UU PDP dan UU ITE di Indonesia," vol. 4, no. 2, 2024, doi: <https://doi.org/10.14421/t5sfe747>
- [14] H. Akbar dan P. B. Wicaksana, "Perlindungan Hukum Terhadap Kebocoran Data Pribadi Akibat Tindak Pidana Siber: Perspektif Undang-Undang Nomor 27 Tahun 2022," vol. 18, no. 02, 2025, doi: <https://doi.org/10.59582/sh.v18i02.1333>
- [15] Ahmad Sauki Warouw, "Peran Hukum Pidana dalam Perlindungan Data Pribadi dan Pencegahan

ght © Universitas Muhammadiyah Sidoarjo. This preprint is protected by copyright held by Universitas Muhammadiyah Sidoarjo and is distributed under the Creative Commons Attribution License (CC BY). Users may share, distribute, or reproduce the work as long as the original author(s) and copyright holder are credited, and the preprint server is cited per academic standards.

rs retain the right to publish their work in academic journals where copyright remains with them. Any use, distribution, or reproduction that does not comply with these terms is not permitted.

- Kejahatan Siber di Indonesia,” *Aliansi J. Huk. Pendidik. Dan Sos. Hum.*, vol. 2, no. 6, hlm. 65–71, Okt 2025, doi: <https://doi.org/10.62383/aliansi.v2i6.1310>.
- [16] M. A. P. Indradjaja, S. Suseno, dan B. A. Atmaja, “Implementasi Penyidikan Terhadap Tindak Pidana Siber Dalam Perspektif Perbandingan Hukum: Indonesia dan Inggris Raya,” *J. Ilm. Penegakan Huk.*, vol. 11, no. 2, hlm. 162–172, Des 2024, doi: <https://doi.org/10.31289/jiph.v11i2.12931>.
- [17] Z. Arifin, Z. J. Fernando, dan E. P. Handayani, “Implikasi Hukum Perubahan Kedua Undang-Undang Informasi dan Transaksi Elektronik: Menyeimbangkan Kebebasan Berpendapat dan Partisipasi Publik dalam Demokrasi Digital: Legal Implications of The Second Amendment to The Electronic Information and Transactions Law: Balancing Freedom of Expression and Public Participation in Digital Democracy,” *LITIGASI*, vol. 26, no. 1, hlm. 165–200, Apr 2025, doi: <https://doi.org/10.23969/litigasi.v26i1.21555>.
- [18] N. Aini dan F. Lubis, “Tantangan Pembuktian dalam Kasus kejahatan Siber”, Vol. 5 No. 02 (2024) doi: <https://doi.org/10.54209/judge.v5i02.566>
- [19] D. E. K. Wardani, A. Rahman, dan M. Irwan, “Perlindungan Hukum di Ruang Siber: Telaah Yuridis atas Rancangan Undang-Undang Keamanan dan Ketahanan Siber,” vol. 18, no. 2, 2025, doi: <https://doi.org/10.59582/sh.v18i02.1333>
- [20] S. A. Hardiansyah dan T. Sutabri, “Analisis Pelanggaran Etika Teknologi Informasi Di Indonesia: Studi Kasus Kebocoran Data,” *JIPM*, vol. 4, no. 1, 2026, doi: <https://doi.org/10.61722/jipm.v4i1.1951>
- [21] I. Nurjanah, “Tantangan Penegakan Hukum terhadap kejahatan Siber di Era Digital,” *SENPISHUM*, Vol. 1, No. 1, 2025, url: <https://journal.unj.ac.id/unj/index.php/senpishum/article/view/62679>
- [22] F. Febrian, I. Y. Saputra, dan D. R. W. Napitupulu, “Implikasi Hukum terhadap Perlindungan Data Pribadi dalam Transaksi Fintech,” *Rechtsnormen J. Komun. Dan Inf. Huk.*, vol. 4, no. 1, hlm. 21–30, Agu 2025, doi: <https://doi.org/10.56211/rechtsnormen.v4i1.1153>.
- [23] Ahmad Sauki Warouw, “Peran Hukum Pidana dalam Perlindungan Data Pribadi dan Pencegahan Kejahatan Siber di Indonesia,” *Aliansi J. Huk. Pendidik. Dan Sos. Hum.*, vol. 2, no. 6, hlm. 65–71, Okt 2025, doi: <https://doi.org/10.62383/aliansi.v2i6.1310>.
- [24] D. Tendeand dan W. Susanto, “Tinjauan Yuridis Terhadap Kejahatan Siber dan Perlindungan Data Pribadi,” vol. 1, no. 1, 2025, url: <https://ejournal.kalibra.or.id/index.php/legalnote/article/view/24>

Conflict of Interest Statement:

The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.