JURNAL HUKUM PELITA, Vol. 7 No. 1 (Mei 2026) : Hal 15-28
ISSN 2809-2082 (online)
Available online at: https://jurnal.pelitabangsa.ac.id/index.php/JH

Pemenuhan Perlindungan Data Pribadi dalam Proses Sistem Peradilan Pidana di Indonesia

Sarman[1*], Husein Manalu[2], Yudha Adi Nugraha[3]

[123] Universitas Pelita Bangsa, Jawa Barat
[*]Korespondensi: sarman@pelitabangsa.ac.id

Info Artikel

Diterima : 3-12-2024	Direvisi : 19-2-2026	Disetujui : 20-3-2026	Diterbitkan : 25-5-2026

DOI : https://doi.org/10.37366/jhp.v7i1.5231

Keywords : *Electronic Evidence, Personal Data Protection, Law Enforcement*

Abstract : *The advancement of digital technology has heightened the role of electronic evidence in law enforcement, particularly in cybercrime cases. However, the seizure of electronic evidence often triggers conflicts between the needs of law enforcement and the protection of personal data. This study aims to analyze the harmonization of Law No. 27 of 2022 on Personal Data Protection (PDP Law) and Law No. 1 of 2024 on Electronic Information and Transactions (ITE Law) in the context of electronic evidence seizure. Using a normative juridical method and a statutory approach, the study finds that the principles of minimality, transparency, and accountability in the PDP Law can complement the seizure procedures outlined in the ITE Law. Nonetheless, regulatory gaps, including the lack of technical guidelines and oversight mechanisms, remain and must be addressed to balance privacy rights and law enforcement.*

Kata kunci : Barang Bukti Elektronik, Perlindungan Data Pribadi, Penegakan Hukum

Abstrak : Perkembangan teknologi digital telah meningkatkan peran barang bukti elektronik dalam penegakan hukum, terutama dalam kasus kejahatan siber. Namun, penyitaan barang bukti elektronik sering kali menimbulkan konflik antara kebutuhan penegakan hukum dan perlindungan data pribadi. Penelitian ini bertujuan untuk menganalisis harmonisasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dan Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE) dalam konteks penyitaan barang bukti elektronik. Dengan menggunakan metode normatif yuridis dan pendekatan perundang-undangan, penelitian ini menemukan bahwa prinsip minimalitas, transparansi, dan akuntabilitas dalam UU PDP dapat diterapkan untuk melengkapi prosedur penyitaan yang diatur dalam UU ITE. Meski demikian, masih terdapat celah regulasi, termasuk kurangnya pedoman teknis dan mekanisme pengawasan, yang perlu diatasi untuk memastikan keseimbangan antara hak privasi dan penegakan hukum.

I. PENDAHULUAN

Kemajuan teknologi informasi dan komunikasi telah memberikan dampak besar pada berbagai aspek kehidupan manusia. Teknologi digital kini menjadi bagian integral dari aktivitas sehari-hari, mulai dari komunikasi, pendidikan, hingga transaksi ekonomi. Perangkat digital seperti ponsel pintar, komputer, hingga layanan penyimpanan berbasis cloud memudahkan pengelolaan data dan informasi. Namun, kemajuan ini juga menghadirkan tantangan baru, terutama meningkatnya ancaman kejahatan siber (*cybercrime*). Kejahatan siber sering kali melibatkan tindakan melanggar hukum yang menggunakan teknologi informasi, termasuk pencurian data pribadi, peretasan, penipuan online, hingga penyebaran ujaran kebencian. Dalam konteks hukum, data pribadi dan barang bukti elektronik memainkan peran penting dalam penanganan kasus-kasus ini.

Isu perlindungan data pribadi menjadi semakin krusial mengingat risiko penyalahgunaan data yang terus meningkat. Dalam konteks Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) telah memberikan landasan hukum untuk melindungi hak privasi individu. UU ini mengatur pengelolaan data pribadi dengan prinsip kehati-hatian, transparansi, dan akuntabilitas. Di sisi lain, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) memberikan pedoman tentang validitas dan pengelolaan data elektronik sebagai alat bukti hukum. Kedua regulasi ini menunjukkan komitmen pemerintah dalam melindungi privasi individu sekaligus mendukung proses penegakan hukum. Meskipun regulasi tersebut telah ada, implementasi di lapangan masih menghadapi berbagai tantangan. Salah satu persoalan utama adalah konflik antara kebutuhan penegakan hukum dengan perlindungan privasi individu, khususnya dalam proses penyitaan barang bukti elektronik. Penyitaan barang bukti elektronik sering kali mencakup data sensitif yang melibatkan terdakwa maupun pihak ketiga yang tidak terlibat langsung dalam perkara[1]. Risiko penyalahgunaan atau kebocoran data pribadi menjadi isu yang tidak dapat diabaikan, terutama jika prosedur penyitaan tidak dijalankan sesuai dengan prinsip-prinsip yang diatur dalam UU PDP dan UU ITE.

Contoh konkret dari kompleksitas ini dapat dilihat pada kasus I Gede Aryastina alias Jerinx yang tercantum dalam Putusan No. 72/PID.SUS/2020/PT.DPS. Dalam kasus ini, Jerinx, seorang musisi dan aktivis, didakwa berdasarkan Pasal 28 ayat (2) UU ITE karena

[1] Niko Darmawan, "Kekuatan Alat Bukti Elektronik Dalam Pembuktian Tindak Pidana Ujaran Kebencian Di Media Sosial (Studi Putusan Nomor: 374/Pid. Sus/2024/PT. SMG)" (Fakultas Syariah dan Hukum UIN Syarif Hidayatullah Jakarta, 2024).

unggahannya di media sosial dianggap menimbulkan kebencian atau permusuhan terhadap Ikatan Dokter Indonesia (IDI). Barang bukti elektronik yang digunakan dalam perkara ini meliputi tangkapan layar unggahan di media sosial, komentar dari pengikutnya, dan perangkat elektronik yang digunakan untuk membuat unggahan tersebut. Barang bukti ini menjadi dasar dakwaan, tetapi proses penyitaannya menimbulkan kekhawatiran terkait privasi terdakwa dan pihak lain yang mungkin terlibat dalam interaksi digital tersebut. Kasus Jerinx mencerminkan tantangan besar dalam pengelolaan barang bukti elektronik di era digital. Penyitaan barang bukti elektronik tidak hanya menjadi alat untuk mendukung pembuktian di pengadilan tetapi juga memunculkan risiko terhadap privasi[2]. Dalam kasus ini, barang bukti seperti tangkapan layar komentar dari pengikut Jerinx dapat melibatkan data pribadi pihak ketiga yang tidak terkait langsung dengan perkara. Situasi ini menunjukkan pentingnya prosedur penyitaan yang sah dan sesuai dengan peraturan yang berlaku, baik untuk melindungi data pribadi maupun untuk memastikan validitas barang bukti.

Selain itu, penyitaan barang bukti elektronik memerlukan kepatuhan terhadap prosedur hukum yang ketat. Dalam kasus Jerinx, barang bukti seperti ponsel, tangkapan layar unggahan media sosial, dan perangkat penyimpanan digital digunakan sebagai dasar untuk mendukung dakwaan. Namun, terdakwa mengajukan banding dengan alasan bahwa proses penyitaan tersebut tidak memenuhi prinsip-prinsip perlindungan data pribadi sebagaimana diatur dalam UU PDP. Kasus ini menggarisbawahi pentingnya kehati-hatian dalam penyitaan barang bukti elektronik agar tidak melanggar hak privasi individu. Regulasi yang ada, seperti UU PDP dan UU ITE, telah memberikan pedoman tentang bagaimana data pribadi dan barang bukti elektronik seharusnya dikelola. UU PDP, misalnya, menetapkan bahwa data pribadi yang disita harus diproses dengan prinsip minimalitas, yaitu hanya data yang relevan dan diperlukan yang boleh diakses. Sementara itu, UU ITE memberikan kerangka hukum mengenai validitas data elektronik sebagai alat bukti, termasuk persyaratan teknis yang harus dipenuhi agar data tersebut dapat diterima di pengadilan. Namun, implementasi kedua undang-undang ini sering kali menghadapi tantangan dalam harmonisasi, terutama dalam menjawab persoalan-persoalan praktis yang muncul di lapangan.

Tantangan serupa juga terlihat dalam kasus-kasus lain yang melibatkan barang bukti elektronik, seperti penyidikan kejahatan pencucian uang atau pelanggaran hak cipta digital. Barang bukti elektronik sering kali menjadi kunci untuk mengungkap jaringan kejahatan,

[2] Henny Saida Flora et al., *Hukum Pidana Di Era Digital* (CV Rey Media Grafika, 2024).

tetapi di sisi lain, proses penyitaan dapat membuka akses terhadap data pribadi yang seharusnya dilindungi. Sebagai contoh, dalam kasus pencucian uang, data yang disita mencakup informasi finansial individu yang sangat sensitif[3]. Jika tidak dikelola dengan baik, data tersebut dapat disalahgunakan oleh pihak yang tidak bertanggung jawab. Kasus Jerinx dan regulasi terkait menunjukkan bahwa perlindungan data pribadi dalam konteks penyitaan barang bukti elektronik masih membutuhkan perhatian serius. Harmonisasi antara UU PDP dan UU ITE perlu diperkuat untuk memastikan bahwa proses penyitaan tidak hanya sah secara hukum tetapi juga menghormati hak privasi individu. Selain itu, prinsip-prinsip seperti transparansi, akuntabilitas, dan minimalitas harus diterapkan secara konsisten dalam setiap tahap penyitaan barang bukti elektronik.

Melalui pendekatan yang lebih adaptif terhadap tantangan era digital, perlindungan data pribadi dan penegakan hukum dapat berjalan seiring. Dengan demikian, sistem hukum di Indonesia dapat memastikan bahwa keseimbangan antara kebutuhan hukum dan hak privasi individu dapat tercapai secara berkelanjutan. Hal ini penting untuk menjaga kepercayaan masyarakat terhadap sistem peradilan, sekaligus memastikan bahwa hak-hak fundamental individu tetap dihormati di tengah kemajuan teknologi yang terus berkembang.

II. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian normatif yuridis, yang berfokus pada analisis terhadap peraturan perundang-undangan, doktrin hukum, dan putusan pengadilan yang relevan[4]. Pendekatan ini bertujuan untuk memahami dan mengevaluasi aspek hukum terkait perlindungan data pribadi dalam konteks penyitaan barang bukti elektronik. Pendekatan yang digunakan meliputi pendekatan perundang-undangan (statute approach) untuk menganalisis UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dan UU Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), pendekatan konseptual (conceptual approach) untuk memahami konsep perlindungan data pribadi dan barang bukti elektronik, serta pendekatan kasus (case approach) dengan mengkaji Putusan No. 72/PID.SUS/2020/PT.DPS terkait kasus I Gede Aryastina alias Jerinx.

[3] Ahmad Nur Setiawan Rosalia Dika Agustanti, "Tindak Pidana Penipuan Pada Transaksi ," no. 2016 (2019): 183–202.

[4] Saputra, Trias, Sarman Sarman, and Ickbal Hofifi Bairuroh. 2024. "Quo Vadis Mahkamah Agung Sebagai Judex Juris Atau Judex Factie ? : Telaah Perubahan Sanksi Pidana Terhadap Ferdy Sambo". *JURNAL HUKUM PELITA* 5 (2):344-56. https://doi.org/10.37366/jh.v5i2.5224

Sumber data penelitian ini meliputi bahan hukum primer seperti UU PDP, UU ITE, dan Kitab Undang-Undang Hukum Acara Pidana (KUHAP), bahan hukum sekunder berupa buku, jurnal, dan artikel ilmiah yang relevan, serta bahan hukum tersier seperti dokumen resmi, laporan penelitian, dan putusan pengadilan lainnya. Teknik pengumpulan data dilakukan melalui studi kepustakaan dan analisis dokumen untuk memperoleh informasi yang valid dan relevan. Data yang terkumpul dianalisis menggunakan metode deskriptif-analitis, yang bertujuan untuk menggambarkan dan mengevaluasi penerapan prinsip-prinsip perlindungan data pribadi dalam prosedur penyitaan barang bukti elektronik. Analisis ini difokuskan pada harmonisasi antara UU PDP dan UU ITE dalam menjawab tantangan hukum di era digital.

III. PEMBAHASAN

A. Ruang Lingkup Data Elektronik dan Data Pribadi Berdasarkan Peraturan Perundang undangan di Indonesia

Kemajuan teknologi informasi telah membawa perubahan besar dalam pengelolaan data, di mana data elektronik dan data pribadi menjadi dua elemen penting yang sering menjadi pusat perhatian, terutama dalam penegakan hukum. Data elektronik, sebagaimana didefinisikan dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), adalah informasi atau dokumen yang dibuat, dikirim, diterima, disimpan, atau diproses melalui perangkat elektronik. Data ini mencakup berbagai format seperti teks, gambar, suara, video, atau kombinasi dari elemen-elemen tersebut. UU ITE menetapkan bahwa data elektronik dapat digunakan sebagai alat bukti yang sah di pengadilan asalkan memenuhi syarat integritas, autentisitas, dan akurasi sebagaimana diatur dalam Pasal 5 dan Pasal 6. Dalam konteks penegakan hukum, data elektronik menjadi sangat penting untuk mengungkap fakta, terutama dalam kasus-kasus yang melibatkan teknologi digital.

Di sisi lain, data pribadi sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) adalah informasi yang dapat diidentifikasi secara langsung atau tidak langsung dengan seseorang, baik secara mandiri maupun dalam kombinasi dengan informasi lainnya. Data pribadi mencakup informasi dasar seperti nama, alamat, dan nomor identitas, serta informasi sensitif seperti data kesehatan, biometrik, atau informasi keuangan. UU PDP membagi data pribadi menjadi dua jenis: data pribadi umum dan data pribadi spesifik, dengan perlindungan yang lebih ketat untuk data spesifik karena potensi dampaknya terhadap privasi individu. Undang-undang ini juga mengatur prinsip-prinsip pengelolaan data pribadi, seperti persetujuan

pemilik data, transparansi, akuntabilitas, dan minimalitas dalam pengumpulan dan penggunaan data. Dalam konteks penegakan hukum, data elektronik dan data pribadi memiliki hubungan yang erat karena data pribadi sering kali menjadi bagian dari data elektronik yang dikelola melalui perangkat digital[5]. Sebagai contoh, dalam kasus kejahatan siber, data elektronik berupa log aktivitas pengguna aplikasi dapat memuat data pribadi seperti nama, alamat IP, atau detail transaksi[6]. Data pribadi ini sering kali menjadi kunci dalam mengidentifikasi pelaku atau mengungkap motif kejahatan. Namun, hubungan ini juga menimbulkan tantangan besar, terutama terkait perlindungan privasi. Dalam penyitaan barang bukti elektronik seperti ponsel atau komputer, data yang terkandung di dalamnya sering kali mencakup informasi yang tidak relevan dengan kasus. Hal ini menimbulkan risiko pelanggaran privasi jika data tersebut tidak dikelola sesuai prinsip-prinsip yang diatur dalam UU PDP.

UU PDP dan UU ITE memberikan pedoman yang saling melengkapi untuk mengatur penggunaan data pribadi dalam konteks penegakan hukum. UU PDP, misalnya, mengatur bahwa data pribadi yang diambil untuk keperluan hukum hanya boleh digunakan sesuai tujuan pengambilan data tersebut. Sementara itu, UU ITE menetapkan standar teknis untuk memastikan integritas dan autentisitas data elektronik yang akan digunakan sebagai alat bukti. Dengan demikian, kedua undang-undang ini berupaya menyeimbangkan antara kebutuhan penegakan hukum dan perlindungan hak privasi individu. Contoh nyata dari hubungan ini dapat dilihat dalam kasus penyitaan barang bukti elektronik dalam investigasi kejahatan siber, di mana data pribadi yang relevan sering kali menjadi bukti penting[7]. Namun, tanpa prosedur yang jelas untuk memisahkan data yang relevan dari data yang tidak relevan, risiko pelanggaran privasi tetap ada. Hubungan antara data elektronik dan data pribadi dalam konteks penegakan hukum mencerminkan tantangan besar di era digital. Di satu sisi, data elektronik menyediakan bukti yang sangat penting untuk mendukung proses hukum. Di sisi lain, pengelolaan data tersebut harus dilakukan dengan hati-hati agar tidak melanggar hak-hak privasi individu. Oleh karena itu, penerapan prinsip seperti transparansi, akuntabilitas, dan minimalitas dalam pengumpulan

[5] Sakti Nugraha, Dwi Andayani, and M S Tumanggor, "Pertanggungjawaban Hukum Pelaku Usaha E-Commerce Atas Terjadinya Pencurian Data Konsumen Melalui Aplikasi Tokopedia Berdasarkan Pasal 19 Dan Pasal 62 Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen," *UNES Law Review* 6, no. 2 (2023): 4896–4909.

[6] Adinda Evita Puspa, "Peran Hukum Pidana Terhadap Kejahatan Siber Terkait Perlindungan Data Pribadi Di Indonesia" (Universitas Islam Sultan Agung Semarang, 2024).

[7] Suryani Alawiyah and Handar Subhandi Bakhtiar, "Peranan Bukti Digital Forensik Dalam Pembuktian Penganiayaan Berat Berencana Kasus Terdakwa Mario Dandy Satriyo Dkk Terhadap David Ozora," *Journal of Multidisciplinary Inquiry in Science, Technology and Educational Research* 2, no. 1 (2025): 234–249.

dan penggunaan data menjadi sangat penting untuk memastikan bahwa hak-hak individu tetap dihormati, sekaligus memungkinkan penegakan hukum berjalan secara efektif dan adil. Dengan kerangka hukum yang kuat, tantangan ini dapat diatasi, menciptakan keseimbangan yang diperlukan antara perlindungan privasi dan kebutuhan penegakan hukum di era digital. Terdapat beberapa hak atas privasi yang diatur dalam UU PDP yakni, hak akses, hak koreksi dan hak keberatan serta hak untuk dilupakan.

Selain memberikan perlindungan terhadap data pribadi, UU ITE juga menetapkan ketentuan mengenai validitas data elektronik sebagai alat bukti hukum. Pasal 5 ayat (1) UU ITE menyatakan bahwa informasi elektronik dan dokumen elektronik merupakan alat bukti hukum yang sah, setara dengan alat bukti lainnya yang diatur dalam Kitab Undang-Undang Hukum Acara Pidana (KUHAP). Ketentuan ini memberikan dasar hukum yang kuat untuk menggunakan data elektronik dalam proses persidangan, terutama dalam kasus-kasus yang melibatkan kejahatan siber, pelanggaran kontrak elektronik, atau tindak pidana lainnya yang terkait dengan teknologi informasi. Namun, agar data elektronik dapat diterima di pengadilan, Pasal 6 UU ITE menetapkan beberapa persyaratan yang harus dipenuhi, yaitu keaslian, integritas, dan keandalan data. Keaslian mengacu pada kemampuan untuk memastikan bahwa data tersebut belum mengalami perubahan sejak pertama kali dibuat atau diterima. Integritas mengacu pada kondisi data yang lengkap, tidak rusak, dan tidak diubah. Sementara itu, keandalan mengacu pada kredibilitas sistem elektronik yang digunakan untuk menghasilkan, menyimpan, atau memproses data tersebut[8].

Persyaratan ini menjadi penting untuk mencegah penyalahgunaan atau manipulasi data elektronik dalam proses hukum. Misalnya, dalam kasus pencemaran nama baik melalui media sosial, tangkapan layar percakapan atau unggahan sering kali diajukan sebagai barang bukti. Agar bukti ini dapat diterima, pihak yang mengajukan bukti harus memastikan bahwa data tersebut memenuhi standar keaslian dan integritas yang diatur oleh UU ITE. Ketentuan dalam UU ITE juga memberikan landasan hukum bagi penyitaan barang bukti elektronik oleh aparat penegak hukum. Namun, penyitaan ini harus dilakukan sesuai dengan prosedur yang ditetapkan dalam KUHAP dan dengan memperhatikan prinsip perlindungan data pribadi yang diatur dalam UU PDP[9]. Dengan demikian, ada keseimbangan antara kebutuhan penegakan hukum dan perlindungan privasi individu.

[8] Riris Katharina, *Pelayanan Publik & Pemerintahan Digital Indonesia* (Yayasan Pustaka Obor Indonesia, 2021).
[9] Ahmad Ihsan Amri and Y A Triana Ohoiwutun, "Analisis Perlindungan Data Pribadi Ditinjau Dari Aspek Sistem Peradilan Pidana," *Opinia de Journal* 4, no. 1 (2024): 13–26.

Hak-hak yang dijamin dalam UU PDP dan UU ITE memberikan perlindungan menyeluruh bagi individu dalam menghadapi tantangan era digital. UU PDP menegaskan pentingnya hak atas privasi dan perlindungan data pribadi, serta memberikan hak-hak digital seperti akses, koreksi, keberatan, dan hak untuk dilupakan. Di sisi lain, UU ITE memastikan bahwa data elektronik dapat digunakan sebagai alat bukti hukum yang sah, dengan syarat memenuhi standar keaslian, integritas, dan keandalan. Kedua undang-undang ini mencerminkan upaya pemerintah dalam menciptakan sistem hukum yang responsif terhadap perkembangan teknologi, sekaligus memastikan bahwa hak-hak individu tetap terlindungi. Namun, implementasi hak-hak ini membutuhkan pengawasan dan kesadaran hukum yang lebih baik untuk menjamin pelaksanaannya secara efektif.

B. Prosedur Penyitaan Barang Bukti Elektronik dalam Hukum Acara Pidana

Penyitaan barang bukti elektronik dalam penegakan hukum di Indonesia merupakan langkah yang sangat penting untuk mengungkap kejahatan, terutama di era digital. Dalam hukum acara pidana, prosedur penyitaan diatur oleh Kitab Undang-Undang Hukum Acara Pidana (KUHAP), yang menjadi pedoman bagi aparat penegak hukum untuk melakukan tindakan penyitaan dengan sah dan sesuai hukum. Dengan berkembangnya teknologi, relevansi dan tantangan dalam penyitaan barang bukti elektronik semakin menjadi perhatian, khususnya dalam menangani kasus kejahatan siber[10]. Di sisi lain, kompleksitas teknis dan hukum yang terkait dengan penyitaan barang bukti elektronik membutuhkan pendekatan yang lebih modern dan terintegrasi dengan peraturan terkait, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Perlindungan Data Pribadi (UU PDP).

Syarat yang perlu dipenuhi untuk dapat dilakukan penyitaan berdasarkan pasal 1 angka 35 Undang-undang nomor 25 tahun 2025 tentang Kitab undang undang hukum acara pidana (KUHAP) Penyitaan adalah tindakan Penyidik untuk mengambil alih dan/atau menyimpan di bawah penguasaannya atas benda bergerak atau tidak bergerak, berwujud atau tidak berwujud, untuk kepentingan pembuktian dalam Penyidikan, Penuntutan, dan/atau pemeriksaan di sidang pengadilan.

Adapun relevansi prosedur penyitaan barang bukti elektronik dalam konteks kejahatan siber Di era digital, barang bukti elektronik menjadi elemen penting dalam pengungkapan berbagai kasus kejahatan siber, seperti peretasan, pencurian identitas, penipuan online, atau penyebaran ujaran kebencian. Barang bukti elektronik mencakup data yang tersimpan dalam perangkat seperti ponsel, komputer, server, atau sistem cloud,

[10] Eddy Army, *Bukti Elektronik Dalam Praktik Peradilan* (Sinar Grafika, 2020).

termasuk dokumen digital, email, riwayat percakapan, atau metadata lainnya. Dalam konteks ini, penyitaan barang bukti elektronik memiliki peranan strategis untuk membuktikan keterlibatan pelaku dalam tindakan kriminal. Namun, prosedur penyitaan barang bukti elektronik memerlukan penyesuaian dengan karakteristik data elektronik. Tidak seperti barang bukti fisik, data elektronik bersifat tidak berwujud, mudah dimodifikasi, dan dapat disalin atau dipindahkan dengan cepat. Oleh karena itu, penyitaan data elektronik harus memperhatikan aspek keaslian, integritas, dan keamanan data agar dapat digunakan sebagai alat bukti yang sah di pengadilan[11]. Selain itu, prosedur ini harus mematuhi peraturan yang diatur dalam UU ITE terkait validitas data elektronik sebagai alat bukti hukum. Dalam penanganan kejahatan siber, relevansi penyitaan barang bukti elektronik juga melibatkan perlindungan hak-hak digital individu yang diatur dalam UU PDP. Misalnya, data pribadi yang disita dari perangkat elektronik pelaku atau saksi harus diproses sesuai dengan prinsip-prinsip perlindungan data pribadi, seperti minimalitas dan transparansi. Hal ini penting untuk mencegah penyalahgunaan data yang dapat merugikan individu yang tidak terkait langsung dengan kasus.

C. Konflik antara Perlindungan Data Pribadi dan Penegakan Hukum

Dalam era digital, data elektronik menjadi alat bukti yang penting dalam penegakan hukum, khususnya untuk kasus kejahatan siber dan tindak pidana berbasis teknologi. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU ITE menetapkan bahwa data elektronik, termasuk informasi digital seperti teks, gambar, suara, dan video, dapat digunakan sebagai barang bukti hukum yang sah jika memenuhi persyaratan tertentu. Persyaratan ini meliputi keaslian, integritas, keandalan, relevansi, dan kepatuhan terhadap prosedur hukum.

Keaslian (*Authenticity*) memastikan data berasal dari sumber sah dan tidak berubah sejak dibuat. Hal ini dapat dibuktikan melalui tanda tangan elektronik atau mekanisme otentikasi lainnya. Integritas (*Integrity*) memastikan data tidak rusak atau diubah secara ilegal, yang dapat diverifikasi menggunakan teknologi seperti hashing. Keandalan (*Reliability*) mengacu pada sistem elektronik yang digunakan untuk menghasilkan data, yang harus dioperasikan secara aman dan sesuai standar[12], sebagaimana diatur dalam UU ITE. Selain itu, data harus relevan dengan perkara hukum dan diperoleh melalui penyitaan

[11] Hasanudin1 Soerya Respationo2 Erniyanti3 Bachtiar Simatupang and Ramon Nofrial, "Analisis Yuridis Penggunaan Informasi/Dokumen Elektronik Sebagai Alat Bukti Dalam Penegakan Hukum Pidana (Studi Perkara Putusan Nomor: 192/Pid. B/2023/PN Btm)" (n.d.).

[12] Achmad Syaiful Hidayat Anwar, "Peran Auditor Teknologi Informasi Dalam Mengurangi Kejahatan Komputer," *Journal of Innovation in Business and Economics* 1, no. 02 (2010).

yang sah, sesuai Pasal 38-46 KUHAP, yang mensyaratkan izin pengadilan, dokumentasi, dan pemberitahuan kepada pemilik barang.

Tantangan teknis, seperti keamanan data, volume data besar, serta kurangnya keahlian teknis pada penegak hukum, sering kali menghambat pemenuhan persyaratan ini. Data elektronik juga kerap melibatkan data pribadi, yang memunculkan konflik dengan hak privasi yang dilindungi UU Perlindungan Data Pribadi (UU PDP). Oleh karena itu, penting untuk memastikan bahwa data pribadi yang tidak relevan tidak terekspos selama proses hukum. Keabsahan data elektronik sebagai barang bukti memerlukan pengelolaan yang hati-hati, teknologi yang andal, dan pemahaman hukum yang memadai. Dengan memenuhi persyaratan tersebut, data elektronik dapat mendukung proses peradilan yang adil, transparan, dan sesuai dengan prinsip hukum acara pidana. Hal ini mendukung penegakan hukum yang adaptif terhadap tantangan era digital.

D. Harmonisasi UU PDP dan UU ITE dalam Penyitaan Barang Bukti Elektronik

Penyitaan barang bukti elektronik menjadi salah satu elemen penting dalam penegakan hukum di era digital. Namun, proses ini memunculkan tantangan besar terkait perlindungan data pribadi. Data elektronik yang disita sering kali mencakup informasi sensitif, baik milik pelaku, korban, maupun pihak ketiga yang tidak terlibat langsung dalam kasus hukum. Untuk mengelola tantangan ini, diperlukan harmonisasi antara Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Harmonisasi ini bertujuan untuk menciptakan keseimbangan antara kebutuhan penegakan hukum dan perlindungan hak privasi individu.

Terdapat Prinsip-Prinsip Perlindungan Data Pribadi yang Relevan untuk Penyitaan UU PDP menetapkan sejumlah prinsip yang harus dipatuhi dalam pengelolaan data pribadi, termasuk saat data tersebut menjadi barang bukti dalam proses hukum. Tiga prinsip utama yang relevan dalam konteks penyitaan barang bukti elektronik adalah minimalitas, transparansi, dan akuntabilitas :

1. Prinsip Minimalitas

   Prinsip ini menekankan bahwa pengumpulan dan penggunaan data pribadi harus dibatasi pada hal-hal yang benar-benar relevan dengan tujuan hukum yang sah. Dalam penyitaan barang bukti elektronik, prinsip minimalitas berarti bahwa data yang disita harus selektif, hanya mencakup informasi yang diperlukan untuk pembuktian perkara. Misalnya, jika penyitaan terkait kasus penipuan online, data yang disita seharusnya

terbatas pada riwayat transaksi atau komunikasi terkait, tanpa mengakses informasi pribadi lainnya yang tidak relevan. Prinsip ini bertujuan untuk melindungi data pribadi individu dari eksposur yang tidak diperlukan.

2. Prinsip Transparansi

   Prinsip transparansi mengharuskan aparat penegak hukum untuk memberikan informasi kepada pemilik data mengenai alasan penyitaan, data apa saja yang akan diambil, dan bagaimana data tersebut akan digunakan. Dalam konteks penyitaan barang bukti elektronik, transparansi juga mencakup pemberitahuan resmi kepada pemilik barang dan pihak terkait, seperti yang diatur dalam Pasal 43 KUHAP. Prinsip ini penting untuk membangun kepercayaan masyarakat terhadap proses hukum.

3. Prinsip Akuntabilitas

   Akuntabilitas berarti bahwa pihak yang melakukan penyitaan bertanggung jawab penuh atas pengelolaan data pribadi yang disita. Data harus disimpan dengan aman, diproses sesuai hukum, dan tidak boleh disalahgunakan untuk kepentingan lain di luar proses hukum. Jika terjadi pelanggaran terhadap perlindungan data pribadi selama proses penyitaan, pihak yang bertanggung jawab harus dapat dimintai pertanggungjawaban.

Harmonisasi antara UU PDP dan UU ITE maupun KUHAP dalam penyitaan barang bukti elektronik merupakan langkah penting untuk menciptakan keseimbangan antara perlindungan data pribadi dan kebutuhan penegakan hukum. Prinsip minimalitas, transparansi, dan akuntabilitas harus menjadi landasan dalam setiap proses penyitaan. Selain itu, pengintegrasian ketentuan kedua undang-undang ini memerlukan standarisasi prosedur, penggunaan teknologi yang tepat, pelatihan penegak hukum, dan penyusunan pedoman teknis yang komprehensif[13]. Meski demikian, terdapat celah hukum yang perlu diperbaiki, seperti kurangnya panduan khusus, pengawasan yang lemah, dan sanksi yang belum memadai. Dengan perbaikan ini, sistem hukum Indonesia dapat lebih responsif terhadap tantangan era digital, menjaga hak privasi individu, sekaligus mendukung proses penegakan hukum yang adil dan transparan.

IV. KESIMPULAN

Penyitaan barang bukti elektronik merupakan elemen penting dalam penegakan hukum di era digital. Namun, proses ini sering memunculkan tantangan, terutama dalam menjaga keseimbangan antara penegakan hukum dan perlindungan data pribadi. Harmonisasi antara UU PDP dan UU ITE serta KUHAP menjadi kunci untuk memastikan penyitaan dilakukan secara sah dan adil, dengan menerapkan prinsip

[13] Flora et al., *Hukum Pidana Di Era Digital.*

minimalitas, transparansi, dan akuntabilitas. Meskipun kedua undang-undang tersebut telah memberikan kerangka hukum yang jelas, masih terdapat celah regulasi, seperti kurangnya pedoman teknis khusus, lemahnya pengawasan, dan ketiadaan sanksi spesifik untuk pelanggaran. Oleh karena itu, diperlukan langkah perbaikan melalui penyusunan pedoman teknis, peningkatan kapasitas penegak hukum, dan penguatan pengawasan untuk mendukung penegakan hukum yang efektif sekaligus melindungi hak privasi individu di era teknologi.

V. SARAN

1. Pemerintah perlu menyusun pedoman teknis yang terperinci untuk mengintegrasikan prinsip perlindungan data pribadi dalam prosedur penyitaan barang bukti elektronik. Pedoman ini harus mencakup langkah-langkah praktis untuk memastikan prinsip minimalitas, transparansi, dan akuntabilitas diterapkan secara konsisten.
2. Aparat penegak hukum perlu mendapatkan pelatihan khusus terkait pengelolaan data elektronik, penggunaan teknologi forensik digital, dan penerapan prinsip perlindungan data pribadi. Pelatihan ini penting untuk memastikan penyitaan dilakukan secara profesional, sah, dan sesuai dengan ketentuan hukum.
3. Diperlukan mekanisme pengawasan yang lebih kuat untuk memastikan bahwa proses penyitaan barang bukti elektronik sesuai dengan aturan yang berlaku. Pengawasan ini dapat dilakukan oleh lembaga independen atau internal melalui audit berkala atas praktik penyitaan yang dilakukan oleh penegak hukum.
4. Regulasi perlu diperkuat dengan ketentuan sanksi khusus bagi pelanggaran dalam proses penyitaan barang bukti elektronik, terutama jika melibatkan penyalahgunaan atau kebocoran data pribadi. Sanksi ini bertujuan untuk meningkatkan akuntabilitas dan mencegah pelanggaran.
5. Edukasi kepada masyarakat tentang hak-hak digital dan perlindungan data pribadi perlu ditingkatkan. Dengan pemahaman yang lebih baik, masyarakat dapat berperan aktif dalam mengawasi pelaksanaan hukum terkait barang bukti elektronik dan melindungi privasi mereka.

DAFTAR PUSTAKA

Army, Eddy. *Bukti Elektronik Dalam Praktik Peradilan*. Sinar Grafika, 2020.

Flora, Henny Saida, M SH, M Kn, M H Kes, S H Kasmanto Rinaldi, M SI, S H Jusri Mudjrimin, et al. *Hukum Pidana Di Era Digital*. CV Rey Media Grafika, 2024.

Katharina, Riris. *Pelayanan Publik & Pemerintahan Digital Indonesia*. Yayasan Pustaka Obor

Indonesia, 2021.

Alawiyah, Suryani, and Handar Subhandi Bakhtiar. "Peranan Bukti Digital Forensik Dalam Pembuktian Penganiayaan Berat Berencana Kasus Terdakwa Mario Dandy Satriyo Dkk Terhadap David Ozora." *Journal of Multidisciplinary Inquiry in Science, Technology and Educational Research* 2, no. 1 (2025): 234–249.

Amri, Ahmad Ihsan, and Y A Triana Ohoiwutun. "Analisis Perlindungan Data Pribadi Ditinjau Dari Aspek Sistem Peradilan Pidana." *Opinia de Journal* 4, no. 1 (2024): 13–26.

Anwar, Achmad Syaiful Hidayat. "Peran Auditor Teknologi Informasi Dalam Mengurangi Kejahatan Komputer." *Journal of Innovation in Business and Economics* 1, no. 02 (2010).

Darmawan, Niko. "Kekuatan Alat Bukti Elektronik Dalam Pembuktian Tindak Pidana Ujaran Kebencian Di Media Sosial (Studi Putusan Nomor: 374/Pid. Sus/2024/PT. SMG)." Fakultas Syariah dan Hukum UIN Syarif Hidayatullah Jakarta, 2024.

Nugraha, Sakti, Dwi Andayani, and M S Tumanggor. "Pertanggungjawaban Hukum Pelaku Usaha E-Commerce Atas Terjadinya Pencurian Data Konsumen Melalui Aplikasi Tokopedia Berdasarkan Pasal 19 Dan Pasal 62 Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen." *UNES Law Review* 6, no. 2 (2023): 4896–4909.

Nugraha, Yudha Adi, and Trias Saputra. "Penerapan Hukum Terhadap Tindak Pidana Doxing Di Indonesia." *JURNAL HUKUM PELITA* 5, no. 1 (2024): 1–12.

Puspa, Adinda Evita. "Peran Hukum Pidana Terhadap Kejahatan Siber Terkait Perlindungan Data Pribadi Di Indonesia." Universitas Islam Sultan Agung Semarang, 2024.

Rosalia Dika Agustanti, Ahmad Nur Setiawan. "Tindak Pidana Penipuan Pada Transaksi ," no. 2016 (2019): 183–202.

Simatupang, Hasanudin1 Soerya Respationo2 Erniyanti3 Bachtiar, and Ramon Nofrial. "Analisis Yuridis Penggunaan Informasi/Dokumen Elektronik Sebagai Alat Bukti Dalam Penegakan Hukum Pidana (Studi Perkara Putusan Nomor: 192/Pid. B/2023/PN Btm)" (n.d.).

Saputra, Trias, Sarman Sarman, and Ickbal Hofifi Bairuroh. 2024. "Quo Vadis Mahkamah Agung Sebagai Judex Juris Atau Judex Factie ? : Telaah Perubahan Sanksi Pidana Terhadap Ferdy Sambo". *JURNAL HUKUM PELITA* 5 (2):344-56. https://doi.org/10.37366/jh.v5i2.5224

Saputra, Trias, Ali Masyhar, Anis Widyawati, and Rahmiati Rahmiati. 2024. "Application

of Restitution for Criminal Acts Victims: Between Rules and Reality". *IJCLS (Indonesian Journal of Criminal Law Studies)* 9 (2): 333-56. https://doi.org/10.15294/ijcls.v9i2.36635.

Kitab Undang-Undang Hukum Acara Pidana

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP)

Putusan Pengadilan Negeri Denpasar No. 72/PID.SUS/2020/PT.DPS