JERUMI: Journal of Education Religion Humanities and Multidiciplinary
E-ISSN: 3025-7980 P-ISSN: 3025-7999
Vol. 2 No. 2 Desember 2024

Peran Hukum Pidana Dalam Menangani Kejahatan Siber pada Masa Sekarang: Tinjauan Terhadap Undang Undang Informasi Transaksi Elektronik

Azra Salsabilla[1] Jennifer Angelina[2]
Magister Ilmu Hukum, Universitas Trisakti, Kota Jakarta Barat, Provinsi DKI Jakarta, Indonesia[1,2]
Email: azra.caca21@gmail.com[1] jenniferaangelina@gmail.com[2]

Abstrak

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia merupakan instrumen hukum yang dirancang untuk mengatasi kejahatan siber yang terus berkembang. Meskipun UU ini bertujuan untuk memberikan perlindungan hukum bagi masyarakat digital, efektivitasnya dalam menanggulangi berbagai bentuk kejahatan siber masih menjadi sorotan. Penelitian ini bertujuan untuk menganalisis efektivitas UU ITE dalam menanggulangi kejahatan siber dengan mempertimbangkan beberapa faktor penting, termasuk ketepatan pasal, penerapan hukum yang konsisten, dan dukungan terhadap penegakan hukum. Hasil analisis menunjukkan bahwa multitafsirnya pasal-pasal dalam UU ITE, keterbatasan pemahaman teknis oleh aparat penegak hukum, dan kurangnya koordinasi antar lembaga menjadi tantangan signifikan dalam implementasi undang-undang ini. Oleh karena itu, disarankan perlunya revisi terhadap pasal-pasal yang multitafsir, peningkatan kapasitas aparat melalui pelatihan yang relevan, dan pembangunan infrastruktur yang mendukung penegakan hukum siber yang lebih efektif. Penelitian ini diharapkan dapat memberikan kontribusi bagi pengembangan kebijakan dan penegakan hukum di bidang kejahatan siber di Indonesia.
Kata Kunci: UU ITE, Kejahatan Siber, Efektivitas, Penegakan Hukum, Kebijakan

Abstract

The Law on Electronic Information and Transactions (UU ITE) in Indonesia is a legal instrument designed to address the ever-evolving issue of cybercrime. Although this law aims to provide legal protection for the digital community, its effectiveness in combating various forms of cybercrime remains a subject of scrutiny. This study aims to analyze the effectiveness of UU ITE in tackling cybercrime by considering several key factors, including the precision of its articles, the consistency of legal application, and support for law enforcement. The analysis reveals that the ambiguous interpretation of certain articles, the limited technical understanding among law enforcement officers, and insufficient inter-agency coordination pose significant challenges to the implementation of this law. Therefore, this study recommends revising ambiguous articles, enhancing the capacity of law enforcement through relevant training, and developing infrastructure that supports more effective cyber law enforcement. This research is expected to contribute to the development of policies and legal enforcement concerning cybercrime in Indonesia.
Keywords: *UU ITE, Cybercrime, Effectiveness, Law Enforcement, Policy*

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

PENDAHULUAN

Kejahatan siber atau *cybercrime* telah menjadi ancaman serius di era digital ini. Berkembangnya teknologi informasi membawa kemudahan dan kecepatan dalam berbagai aspek kehidupan, tetapi di sisi lain, juga memunculkan peluang bagi tindakan kriminal berbasis teknologi. Di Indonesia, perkembangan teknologi dan internet telah berdampak besar pada masyarakat, mulai dari bisnis, pendidikan, hingga kehidupan sehari-hari. Namun, seiring dengan kemajuan ini, kejahatan siber juga semakin marak dan kompleks, mencakup berbagai bentuk, mulai dari pencurian data, penipuan online, peretasan, hingga penyebaran hoaks

(Susanto, 2020). Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) No. 11 Tahun 2008, yang kemudian direvisi menjadi UU No. 19 Tahun 2016, disahkan untuk menghadapi tantangan hukum dalam dunia maya. UU ITE bertujuan untuk melindungi masyarakat dari tindakan-tindakan yang melanggar hukum di ranah digital, baik dalam bentuk pencemaran nama baik, penyebaran informasi palsu, hingga pencurian data (Hendro, 2019). Meski telah ada kerangka hukum ini, penerapan UU ITE sering kali menuai kritik dan kontroversi, terutama dalam hal penafsiran pasal-pasal yang dianggap rawan disalahgunakan atau terlalu luas cakupannya (Putra, 2021). Masalah ini menjadi tantangan serius dalam menangani kejahatan siber di Indonesia.

Kejahatan siber semakin meningkat tidak hanya dalam hal frekuensi, tetapi juga dalam hal kompleksitasnya. Menurut Supriyadi (2022), kejahatan siber kini melibatkan jaringan internasional yang terorganisir, sehingga membutuhkan kerja sama lintas negara untuk dapat ditangani secara efektif. Selain itu, pelaku kejahatan siber seringkali memanfaatkan kecanggihan teknologi untuk menyembunyikan identitas mereka, yang membuat proses penegakan hukum menjadi semakin sulit. Hal ini menunjukkan bahwa hukum pidana konvensional mungkin tidak cukup untuk menangani kejahatan siber yang bersifat lintas batas (Supriyadi, 2022). UU ITE sendiri mencakup berbagai ketentuan yang dimaksudkan untuk mengatasi kejahatan siber, seperti penetapan sanksi terhadap tindakan yang mengancam keamanan data, penyalahgunaan teknologi informasi, dan pelanggaran privasi individu. Namun, dalam praktiknya, penerapan UU ITE sering kali mengalami kendala, terutama terkait dengan masalah interpretasi hukum dan kurangnya pemahaman aparat penegak hukum tentang teknologi informasi (Fajrin, 2020). Di sisi lain, menurut Rachman (2021), meskipun UU ITE telah mengalami revisi, beberapa pasal di dalamnya masih dianggap terlalu multitafsir dan memiliki potensi untuk disalahgunakan, terutama dalam kasus yang melibatkan kebebasan berekspresi di ranah digital.

Salah satu tantangan utama dalam penerapan UU ITE adalah bagaimana hukum pidana dapat menyeimbangkan antara perlindungan terhadap korban dan hak-hak individu, termasuk hak atas kebebasan berekspresi. Menurut Sari (2021), meskipun UU ITE bertujuan untuk melindungi masyarakat, dalam beberapa kasus, undang-undang ini telah digunakan untuk menekan kebebasan berekspresi, khususnya di media sosial. Hal ini menjadi perdebatan yang memerlukan perhatian serius, karena kebebasan berekspresi adalah salah satu pilar penting dalam masyarakat demokratis (Sari, 2021). Pentingnya pengembangan regulasi yang lebih adaptif terhadap perkembangan teknologi juga menjadi sorotan dalam banyak studi. Menurut Setiawan (2020), UU ITE sebagai produk hukum masih memiliki beberapa kelemahan dalam hal fleksibilitas menghadapi perubahan cepat di dunia teknologi. Sifat statis dari undang-undang ini dianggap kurang mampu untuk menghadapi sifat dinamis kejahatan siber yang terus berevolusi, terutama dengan munculnya jenis-jenis kejahatan baru seperti serangan siber berbasis kecerdasan buatan (AI) dan pembajakan data melalui ransomware (Setiawan, 2020). Selain itu, pelaksanaan UU ITE dalam menghadapi kejahatan siber sering kali terhambat oleh keterbatasan infrastruktur teknologi penegak hukum di Indonesia. Supriyadi (2022) mencatat bahwa aparat penegak hukum, terutama di wilayah-wilayah tertentu, masih memiliki keterbatasan dalam hal fasilitas pendukung dan pengetahuan terkait teknologi informasi. Keterbatasan ini menyebabkan proses investigasi dan penegakan hukum menjadi kurang optimal dalam menangani kasus-kasus siber yang memerlukan keahlian khusus (Supriyadi, 2022).

Terdapat pula pandangan bahwa peran hukum pidana dalam menangani kejahatan siber di Indonesia tidak hanya bergantung pada UU ITE saja, tetapi juga memerlukan kolaborasi dengan regulasi internasional. Menurut Hendro (2019), sifat lintas batas dari kejahatan siber

memerlukan kerja sama antarnegara dalam hal penyelidikan, pertukaran informasi, dan penegakan hukum. Dalam konteks ini, Indonesia telah bekerja sama dengan beberapa negara untuk memperkuat upaya melawan kejahatan siber, meskipun masih ada tantangan besar terkait harmonisasi hukum dan perbedaan sistem peradilan antarnegara (Hendro, 2019). Dengan demikian, kajian ini akan menyoroti peran hukum pidana dalam menangani kejahatan siber, khususnya melalui penerapan UU ITE di Indonesia. Penelitian ini akan memaparkan bagaimana UU ITE dalam konteks hukum pidana diterapkan dalam menangani berbagai bentuk kejahatan siber, serta mengevaluasi efektivitas dan tantangan yang dihadapi dalam praktiknya. Selain itu, penelitian ini juga akan melihat peran hukum pidana dalam melindungi masyarakat dari dampak negatif teknologi informasi sekaligus menjaga hak-hak individu dalam masyarakat demokratis. Harapannya, penelitian ini dapat memberikan wawasan yang lebih mendalam mengenai kebutuhan untuk menyusun regulasi yang lebih adaptif dan efektif dalam menghadapi perkembangan teknologi dan kejahatan siber di masa mendatang.

METODE PENELITIAN

Penelitian ini menggunakan metode kajian pustaka yang bertujuan untuk menganalisis peran hukum pidana dalam menangani kejahatan siber di Indonesia, dengan fokus pada penerapan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Kajian pustaka dilakukan dengan mengumpulkan, menelaah, dan mensintesis berbagai literatur yang relevan, termasuk buku, jurnal, artikel ilmiah, dan dokumen hukum yang membahas UU ITE serta penerapannya dalam konteks kejahatan siber. Metode ini dipilih karena dapat memberikan gambaran menyeluruh mengenai berbagai pandangan dan hasil penelitian sebelumnya terkait efektivitas serta tantangan UU ITE. Proses pengumpulan data dilakukan dengan memilih literatur yang memuat pembahasan tentang kejahatan siber dan hukum pidana, khususnya yang mengulas isu-isu yang muncul dari penerapan UU ITE di Indonesia. Literatur yang digunakan mencakup studi hukum, hasil penelitian empiris, analisis yuridis, serta artikel yang mengevaluasi permasalahan penegakan hukum terkait kejahatan siber. Data yang dikumpulkan dianalisis secara kualitatif melalui teknik analisis tematik, di mana informasi yang serupa atau relevan dikelompokkan ke dalam tema-tema tertentu, seperti tantangan hukum, implikasi pasal dalam UU ITE, dan pendekatan internasional dalam menanggulangi kejahatan siber. Untuk menjaga kualitas kajian, penelitian ini menerapkan validasi melalui triangulasi sumber, yakni dengan membandingkan kesimpulan dari berbagai literatur guna mengurangi bias dan memperkuat keakuratan interpretasi. Hasil analisis ini diharapkan dapat menjawab pertanyaan penelitian mengenai sejauh mana UU ITE efektif dalam menanggulangi kejahatan siber, serta memberikan rekomendasi untuk pengembangan hukum pidana yang lebih adaptif dalam menghadapi tantangan kejahatan siber di masa depan.

HASIL PENELITIAN DAN PEMBAHASAN

Tantangan Penerapan UU ITE dalam Menangani Kejahatan Siber

Penerapan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia menjadi salah satu upaya negara dalam menanggulangi kejahatan siber yang semakin kompleks. UU ini telah menjadi landasan hukum yang digunakan untuk mengatur berbagai aktivitas digital, terutama yang melibatkan informasi elektronik, privasi, dan transaksi digital. Meski demikian, implementasinya masih menghadapi berbagai tantangan. Beberapa hambatan yang ditemui dalam penerapan UU ITE antara lain adalah isu multitafsir pada beberapa pasalnya, keterbatasan kapasitas teknis aparat penegak hukum, dan kurangnya adaptasi terhadap perkembangan teknologi siber yang pesat. Salah satu isu paling mendasar dalam penerapan UU ITE adalah multitafsirnya beberapa pasal, khususnya yang berkaitan dengan

pencemaran nama baik dan penyebaran informasi yang dianggap palsu atau menyesatkan. Menurut Arifin (2020), pasal-pasal terkait pencemaran nama baik dalam UU ITE, seperti Pasal 27 ayat (3), sering dianggap bias karena dapat ditafsirkan secara subjektif oleh aparat penegak hukum. Pasal tersebut memuat ketentuan yang memungkinkan pelaporan pencemaran nama baik di media sosial atau platform digital lainnya, namun rentan digunakan untuk membatasi kebebasan berekspresi. Hal ini sering menjadi kritik dari masyarakat dan aktivis hak asasi manusia, yang melihat bahwa undang-undang ini dapat digunakan sebagai alat untuk mengkriminalisasi kritik atau opini yang berbeda (Susanto, 2021).

Selain itu, pasal-pasal dalam UU ITE yang multitafsir ini juga kerap menimbulkan perbedaan pandangan di antara penegak hukum sendiri. Dalam beberapa kasus, perbedaan interpretasi pasal oleh jaksa dan hakim menyebabkan hasil putusan yang tidak konsisten. Hal ini menimbulkan ketidakpastian hukum yang berdampak pada publik, karena masyarakat menjadi khawatir bahwa aktivitas mereka di ruang digital dapat dianggap sebagai pelanggaran hukum hanya karena interpretasi yang berbeda (Putra & Rahman, 2019). Menurut studi dari Supriyadi (2022), kerancuan ini berdampak negatif pada efektivitas UU ITE dalam menangani kejahatan siber, karena undang-undang yang multitafsir justru menimbulkan ketakutan pada masyarakat yang menggunakan media digital sebagai ruang berekspresi. Di samping itu, kejahatan siber seringkali memerlukan penanganan khusus dengan keterampilan teknis yang mendalam, seperti investigasi digital, pengumpulan bukti elektronik, serta pelacakan aktivitas daring. Dalam penerapannya, aparat penegak hukum di Indonesia kerap menghadapi keterbatasan teknis dalam menanggulangi kejahatan siber, terutama dalam hal pemahaman teknologi yang terus berkembang pesat. Menurut Fajrin (2020), banyak aparat penegak hukum yang belum memiliki pengetahuan memadai mengenai teknik penyelidikan forensik digital, sehingga proses pengumpulan bukti sering kali terkendala dan menyebabkan kasus-kasus kejahatan siber tidak dapat diselesaikan dengan optimal. Keterbatasan teknis ini juga diperparah oleh kurangnya pelatihan khusus yang tersedia bagi aparat penegak hukum. Sementara negara-negara maju memiliki tim penegak hukum khusus yang menangani kejahatan siber, di Indonesia, sumber daya dan pelatihan untuk keahlian tersebut masih minim (Rachman, 2021). Hal ini menghambat efektivitas UU ITE dalam memberantas kejahatan siber yang memerlukan keahlian khusus, terutama ketika kasus tersebut melibatkan jaringan internasional atau menggunakan teknologi yang sulit dilacak. Menurut Rachman (2021), untuk mengatasi hal ini, Indonesia perlu meningkatkan kapasitas penegakan hukum siber melalui pelatihan khusus, pengadaan perangkat lunak yang mendukung penyelidikan digital, serta kerja sama internasional dengan negara-negara lain.

Perkembangan teknologi digital sangat cepat, sehingga metode kejahatan siber terus berevolusi, menciptakan tantangan baru bagi penegakan hukum. UU ITE, meski telah direvisi pada tahun 2016, belum mampu sepenuhnya mengakomodasi jenis-jenis kejahatan siber yang lebih canggih, seperti penggunaan kecerdasan buatan untuk serangan siber atau penyebaran malware dalam bentuk baru (Hendro, 2019). Menurut studi Setiawan (2020), UU ITE dirancang sebagai undang-undang yang berlaku umum dan belum secara spesifik mengatur metode-metode kejahatan siber yang terus berkembang. Ini menyebabkan UU ITE sering kali tidak dapat menanggapi kejahatan siber yang sifatnya dinamis dan semakin kompleks. Kejahatan siber memiliki sifat lintas batas negara yang memerlukan kerangka hukum yang bersifat global. Namun, UU ITE saat ini belum memiliki peraturan yang memadai untuk mengatasi kejahatan siber lintas batas (Fajrin, 2020). Sebagai contoh, jika pelaku berada di luar negeri, Indonesia sering kali kesulitan untuk membawa kasus kejahatan siber ke pengadilan karena perbedaan yurisdiksi. Dalam hal ini, Supriyadi (2022) menyarankan agar UU ITE dilengkapi dengan ketentuan yang mendukung kerja sama internasional dalam menangani kejahatan siber, seperti

yang diterapkan di negara-negara Eropa melalui *Budapest Convention on Cybercrime*. Ketiga tantangan ini menunjukkan bahwa meskipun UU ITE bertujuan untuk melindungi masyarakat dari kejahatan siber, efektivitasnya masih terbatas karena berbagai faktor. Multitafsir pasal, keterbatasan teknis aparat, serta kurangnya adaptasi terhadap perkembangan teknologi menjadi kendala serius yang menghambat penegakan hukum di dunia siber. Kondisi ini menimbulkan implikasi penting terhadap keamanan siber di Indonesia dan perlindungan terhadap masyarakat digital. Menurut Susanto (2021), untuk mengatasi tantangan ini, perlu ada pembaruan undang-undang yang lebih adaptif terhadap perkembangan teknologi dan upaya untuk memperkuat kapasitas penegak hukum melalui pelatihan khusus dan kolaborasi internasional. Dengan adanya perubahan dan adaptasi terhadap UU ITE, diharapkan undang-undang ini dapat lebih efektif dalam menangani berbagai jenis kejahatan siber yang semakin kompleks. Selain itu, upaya edukasi publik tentang etika dan hukum di ruang digital juga menjadi penting agar masyarakat dapat berpartisipasi secara aktif dalam menciptakan lingkungan siber yang aman dan bertanggung jawab.

Efektivitas UU ITE dalam Menanggulangi Berbagai Bentuk Kejahatan Siber

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia, yang diundangkan pada tahun 2008 dan direvisi pada tahun 2016, bertujuan untuk mengatur penyelenggaraan informasi dan transaksi elektronik. UU ini juga menjadi payung hukum untuk menanggulangi kejahatan siber yang semakin berkembang, termasuk penipuan daring, pencemaran nama baik, dan peretasan. Meskipun UU ITE telah memberikan kerangka hukum yang jelas, efektivitasnya dalam menanggulangi kejahatan siber masih menjadi perdebatan. Beberapa faktor yang memengaruhi efektivitas UU ITE termasuk ketepatan pasal yang diatur, penerapan hukum yang konsisten, serta dukungan terhadap penegakan hukum yang memadai.

Ketepatan Pasal dalam UU ITE

Salah satu aspek penting yang menentukan efektivitas UU ITE adalah ketepatan dan kejelasan pasal-pasal yang diatur dalam undang-undang tersebut. Beberapa pasal dalam UU ITE, terutama yang berkaitan dengan pencemaran nama baik dan penipuan siber, telah banyak dipakai dalam praktik penegakan hukum. Pasal 27 hingga Pasal 32 mengatur berbagai bentuk kejahatan siber, namun kritik muncul terkait multitafsirnya pasal-pasal ini. Menurut Amri (2021), pasal-pasal tersebut seringkali terlalu luas dan dapat disalahgunakan untuk mengekang kebebasan berekspresi. Misalnya, Pasal 27 ayat (3) yang mengatur tentang pencemaran nama baik dapat diterapkan secara subjektif oleh aparat penegak hukum, yang berpotensi menimbulkan ketidakpastian hukum dan ketakutan di kalangan masyarakat untuk berkomentar di ruang digital. Sebuah studi oleh Setiawan dan Siregar (2020) menunjukkan bahwa banyak kasus yang melibatkan pelanggaran pasal UU ITE berakhir dengan putusan yang tidak konsisten. Penegakan hukum yang tidak seragam ini menciptakan kesan bahwa UU ITE tidak hanya berfungsi untuk melindungi masyarakat, tetapi juga dapat menjadi alat untuk mengontrol suara-suara yang kritis terhadap pemerintah. Ini menciptakan tantangan bagi efektivitas UU ITE sebagai instrumen hukum dalam menanggulangi kejahatan siber yang semakin marak.

Penerapan Hukum yang Konsisten

Efektivitas UU ITE juga sangat dipengaruhi oleh konsistensi dalam penerapannya. Penerapan hukum yang konsisten memerlukan pemahaman yang mendalam oleh aparat penegak hukum terhadap teknologi dan kejahatan siber. Keterbatasan pemahaman ini menjadi salah satu penghambat dalam menegakkan UU ITE. Menurut Rachman (2021), banyak aparat

penegak hukum yang kurang mendapatkan pelatihan mengenai teknologi informasi dan cara penegakan hukum dalam konteks digital. Hal ini menyebabkan mereka kesulitan dalam menyelidiki dan membuktikan kasus-kasus kejahatan siber yang kompleks. Studi oleh Hanif (2022) menunjukkan bahwa ada banyak kasus penipuan daring yang tidak terdeteksi dan tidak dilaporkan karena ketidakmampuan aparat dalam menangani bukti digital dan kejahatan siber. Kurangnya pelatihan dan pemahaman ini berakibat pada rendahnya angka penyelesaian kasus yang melibatkan UU ITE. Tanpa dukungan yang memadai untuk peningkatan kapasitas aparat penegak hukum, efektivitas UU ITE dalam menanggulangi kejahatan siber akan terus terhambat. Dukungan terhadap penegakan hukum yang memadai juga menjadi faktor kunci dalam efektivitas UU ITE. Penegakan hukum yang baik memerlukan kerjasama antara berbagai lembaga, seperti kepolisian, kejaksaan, dan pengadilan. Sayangnya, koordinasi antar lembaga seringkali tidak berjalan dengan baik. Menurut Irawan (2020), keterbatasan anggaran dan sumber daya manusia menjadi hambatan serius dalam penegakan hukum siber di Indonesia. Ini berpengaruh pada kemampuan lembaga-lembaga ini untuk merespons dan menyelesaikan kasus kejahatan siber dengan cepat dan efektif. Dukungan teknologi dan infrastruktur yang memadai juga sangat penting. Banyak negara maju telah membangun sistem hukum yang mendukung penyelidikan dan penegakan hukum siber yang lebih efektif. Dalam konteks Indonesia, menurut Fajrin (2021), pengembangan infrastruktur digital dan peningkatan teknologi informasi dalam penegakan hukum sangat diperlukan untuk meningkatkan responsivitas dan efektivitas UU ITE. Negara harus berinvestasi dalam pelatihan aparat penegak hukum serta menyediakan alat dan teknologi yang diperlukan untuk mendeteksi dan menangani kejahatan siber.

KESIMPULAN

Berdasarkan analisis di atas, dapat disimpulkan bahwa meskipun UU ITE telah memberikan kerangka hukum untuk menanggulangi kejahatan siber, efektivitasnya masih menghadapi berbagai tantangan. Ketepatan pasal yang diatur, penerapan hukum yang konsisten, serta dukungan terhadap penegakan hukum yang memadai adalah faktor-faktor penting yang mempengaruhi efektivitas UU ITE. Untuk meningkatkan efektivitas UU ITE dalam menanggulangi berbagai bentuk kejahatan siber, disarankan agar pemerintah dan lembaga terkait:

1. Melakukan revisi terhadap pasal-pasal yang multitafsir dalam UU ITE untuk menghindari penyalahgunaan dan memberikan kepastian hukum bagi masyarakat.
2. Meningkatkan kapasitas aparat penegak hukum melalui pelatihan dan pendidikan yang berfokus pada teknologi informasi dan penyelidikan kejahatan siber.
3. Membangun infrastruktur dan sistem yang mendukung penegakan hukum, serta meningkatkan kerja sama antar lembaga dalam menangani kejahatan siber secara lebih efektif.

Dengan langkah-langkah tersebut, diharapkan UU ITE dapat berfungsi dengan lebih baik dalam menanggulangi kejahatan siber dan melindungi masyarakat digital di Indonesia.

DAFTAR. PUSTAKA

Amri, S. (2021). *Kritik terhadap UU ITE: Pasal pencemaran nama baik dan kebebasan berekspresi*. Jurnal Hukum dan Masyarakat, 12(1), 27-40.

Arifin, Z. (2020). *Analisis pasal pencemaran nama baik dalam UU ITE*. Jurnal Hukum Siber, 5(2), 45-58.

Fajrin, R. (2020). *Kendala penerapan UU ITE dalam penegakan hukum terhadap kejahatan siber di Indonesia*. Jurnal Hukum dan Kebijakan, 10(1), 23-34.

Hanif, A. (2022). *Tantangan penegakan hukum terhadap kejahatan siber di Indonesia: Kasus penipuan daring*. Jurnal Kriminologi, 13(2), 88-102.

Hendro, S. (2019). *Kerja sama internasional dalam penegakan hukum siber*. Jurnal Kejahatan Siber Internasional, 3(4), 101-115.

Nurrohman, R., Nugroho, F. R., Tiastiwi, U. N., & Nurgiansah, T. H. (2024). Analisis Permasalahan Penerapan Demokrasi dan Prospek Perbaikannya di Indonesia. HELIUM: Journal of Health Education Law Information and Humanities, 1(1), 9-20.

Putra, D. A. (2021). *Kontroversi pasal-pasal dalam UU ITE: Analisis dampak terhadap kebebasan berekspresi*. Jurnal Hak Asasi, 15(2), 87-98.

Rachman, B. (2021). *Penafsiran multitafsir dalam UU ITE dan implikasinya pada kebebasan berekspresi*. Jurnal Hukum dan Masyarakat, 6(1), 45-58.

Robiansyah, A., Al Fahlevi, A., Jauhari, F. A., & Nurgiansah, T. H. (2024). Studi Pelanggaran HAM di Indonesia. REAL: Journal of Religion Education Accounting and Law, 1(1), 6-12.

Sari, N. P. (2021). *UU ITE dalam perspektif kebebasan berekspresi di media sosial*. Jurnal Komunikasi dan Hukum, 8(3), 59-72.

Setiaji, Y., Zhafir, M. A., Anjani, R., & Nurgiansah, T. H. (2024). Penerimaan Hak dan Kewajiban Terhadap Akses Pendidikan yang Merata di Indonesia. SMASH: Journal of Social Management Sains and Health, 1(1), 7-11.

Setiawan, T. (2020). *Evolusi kejahatan siber: Tantangan bagi sistem hukum pidana Indonesia*. Jurnal Teknologi dan Hukum, 12(2), 30-42.

Supriyadi, A. (2022). *Dinamika kejahatan siber dan tantangan hukum lintas batas*. Jurnal Keamanan Siber, 14(1), 15-29.

Susanto, E. (2020). *Fenomena cybercrime dan peran hukum dalam menanganinya di era digital*. Jurnal Kriminologi dan Hukum, 11(2), 22-38.