



## Peran Teknologi Informasi Dalam Pencegahan Dan Pengungkapan Tindak Pidana Ekonomi Khusus: Studi Tentang Kejahatan Keuangan Berbasis Digital

### *The Role of Information Technology in the Prevention and Disclosure of Special Economic Crimes: A Study of Digital-Based Financial Crimes*

Andi Ahmad Munajat<sup>1</sup>, Hudi Yusuf<sup>2</sup>

Fakultas Hukum Universitas Bung Karno

E-mail: [aamunajat@me.com](mailto:aamunajat@me.com)<sup>1</sup>, [hoedyjoesoef@gmail.com](mailto:hoedyjoesoef@gmail.com)<sup>2</sup>

#### Article Info

##### Article history :

Received : 02-11-2024

Revised : 04-11-2024

Accepted : 06-11-2024

Published : 08-11-2024

#### Abstract

*The development of information technology has made a significant contribution to the prevention and disclosure of specific economic crimes, especially in cases of digital-based financial crimes. Although information technology can facilitate efficiency and accessibility in the financial system, the risk of economic crimes such as online fraud, data theft, and money laundering is also increasing. This study reviews the role of technology such as artificial intelligence (AI), big data analysis, and blockchain in detecting suspicious activities in the financial sector. In addition, this study discusses the legal framework in Indonesia, including the Electronic Information and Transactions Law (ITE) and regulations related to money laundering crimes that regulate the use of technology in law enforcement. Through a literature study, this study aims to provide guidance for policy makers and law enforcement in adopting technology to minimize digital economic crimes.*

**Keywords:** *Information Technology, Digital Economic Crime, Law Enforcement*

#### Abstrak

*Perkembangan teknologi informasi telah memberikan kontribusi signifikan terhadap pencegahan dan pengungkapan tindak pidana ekonomi khusus, terutama dalam kasus kejahatan keuangan berbasis digital. Meskipun teknologi informasi dapat memfasilitasi efisiensi dan aksesibilitas dalam sistem keuangan, risiko kejahatan ekonomi seperti penipuan online, pencurian data, dan pencucian uang juga meningkat. Penelitian ini mengulas peran teknologi seperti kecerdasan buatan (AI), analisis big data, dan blockchain dalam mendeteksi aktivitas mencurigakan di sektor keuangan. Selain itu, penelitian ini membahas kerangka hukum di Indonesia, termasuk Undang-Undang Informasi dan Transaksi Elektronik (ITE) serta peraturan terkait tindak pidana pencucian uang yang mengatur penggunaan teknologi dalam penegakan hukum. Melalui studi literatur, penelitian ini bertujuan untuk memberikan panduan bagi pembuat kebijakan dan aparat hukum dalam mengadopsi teknologi guna meminimalisasi kejahatan ekonomi digital.*

**Kata Kunci:** *Teknologi Informasi, Kejahatan Ekonomi Digital, Penegakan Hukum*

#### PENDAHULUAN

Perkembangan teknologi informasi telah membawa dampak positif dalam berbagai aspek kehidupan, tetapi juga memicu peningkatan kejahatan ekonomi berbasis digital. Kejahatan ini meliputi berbagai bentuk pelanggaran, seperti penipuan online, pencurian data pribadi, dan pencucian uang melalui jaringan internet, yang semakin meningkat sejalan dengan semakin



besarnya peran internet dalam kehidupan sehari-hari. Jenis kejahatan ini memiliki konsekuensi yang serius, baik bagi individu yang kehilangan data atau dana, perusahaan yang mengalami kerugian akibat serangan siber, maupun negara yang dirugikan oleh hilangnya potensi pendapatan. Berdasarkan hukum di Indonesia, beberapa tindak kejahatan ini melanggar Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) Nomor 19 Tahun 2016 Pasal 28 ayat (1), yang mengatur tentang larangan penyebaran informasi yang menyesatkan atau penipuan melalui media elektronik (UU No. 19 Tahun 2016). Selain itu, pencurian data pribadi dapat dianggap melanggar Pasal 30 dan Pasal 32 UU ITE, yang mengatur larangan mengakses atau mengambil informasi elektronik tanpa izin. Sementara itu, tindak pidana pencucian uang diatur dalam Undang-Undang Tindak Pidana Pencucian Uang (TPPU) Nomor 8 Tahun 2010, terutama pada Pasal 3 dan Pasal 4, yang melarang konversi atau penggunaan harta yang diperoleh dari kejahatan untuk menyembunyikan asal-usul aset tersebut (UU No. 8 Tahun 2010).

Meskipun sistem keuangan digital telah memberikan banyak keuntungan seperti kemudahan akses, efisiensi waktu, dan biaya yang lebih rendah, kerentanan terhadap ancaman keamanan masih menjadi isu besar yang perlu diperhatikan. Sistem ini, yang mengandalkan teknologi mutakhir seperti internet dan aplikasi digital, sering kali menghadapi risiko dari serangan siber yang dilakukan oleh pelaku kejahatan yang memanfaatkan celah keamanan (Seldal, dkk., 2022). Faktor-faktor seperti teknologi yang belum sepenuhnya aman dan lemahnya infrastruktur keamanan siber turut memperbesar risiko tersebut, membuka peluang bagi para peretas untuk mengakses data pribadi atau bahkan melakukan transaksi ilegal. Kondisi ini diperparah dengan perkembangan teknologi yang lebih cepat dibandingkan kemampuan sistem keamanan untuk mengantisipasi berbagai ancaman baru. Oleh karena itu, ada kebutuhan mendesak untuk memperkuat sistem keamanan dan membangun infrastruktur yang lebih andal, sehingga dapat melindungi konsumen dan integritas keuangan digital secara keseluruhan (Akbar, dkk., 2024).

Teknologi informasi memainkan peran penting dalam pencegahan kejahatan ekonomi, terutama dalam era digital yang semakin kompleks. Teknologi canggih seperti kecerdasan buatan (AI) untuk deteksi penipuan, analisis data besar (big data analytics), dan blockchain memberikan pendekatan baru untuk mengenali serta menindak aktivitas mencurigakan dalam sistem keuangan. AI mampu mendeteksi pola yang tidak biasa dan memprediksi kemungkinan tindakan ilegal dengan menganalisis sejumlah besar data secara real-time (Martinus, dkk., 2023). Sementara itu, big data analytics memungkinkan lembaga keuangan mengidentifikasi tren dan anomali yang mungkin mengindikasikan penipuan atau praktik curang lainnya. Blockchain, dengan sifatnya yang transparan dan sulit diubah, membantu menjaga integritas data transaksi serta meminimalkan risiko manipulasi. Kombinasi berbagai teknologi ini menciptakan sistem yang adaptif dan responsif, memungkinkan deteksi dini yang efektif serta meningkatkan keamanan, baik bagi pelaku industri keuangan maupun konsumen. Dengan implementasi yang tepat, teknologi informasi tidak hanya berfungsi sebagai alat pendeteksi, tetapi juga sebagai tameng yang mencegah timbulnya kejahatan ekonomi digital sejak dini, yang pada akhirnya membantu mengurangi dampak negatif pada perekonomian global (Baza, dkk., 2023).

Dalam konteks hukum, penggunaan teknologi informasi dalam pengungkapan tindak pidana ekonomi diatur dalam beberapa ketentuan perundang-undangan di Indonesia. Salah satu pasal yang relevan adalah Pasal 45 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), yang mengatur bahwa setiap orang yang dengan sengaja dan tanpa hak melakukan akses terhadap sistem elektronik orang lain yang dapat merugikan, dikenai sanksi pidana (UU No. 11 Tahun 2008). Selain itu, dalam Pasal 74 ayat (2) Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (TPPU), disebutkan bahwa pihak berwenang dapat memanfaatkan teknologi informasi untuk menganalisis transaksi keuangan yang mencurigakan sebagai bagian dari upaya pengungkapan tindak pidana ekonomi. Pemanfaatan teknologi dalam bentuk digital forensik, pelacakan transaksi digital, serta



analisis pola ini penting dalam mendukung proses penegakan hukum dan meningkatkan efektivitas pemberantasan tindak pidana ekonomi (UU No. 8 Tahun 2010).

Urgensi penelitian ini tidak dapat diabaikan, mengingat perkembangan pesat dalam dunia digital yang telah membawa dampak signifikan terhadap keamanan ekonomi global. Dalam konteks ini, kejahatan ekonomi berbasis digital, seperti penipuan online, pencucian uang, dan pencurian identitas, semakin beragam dan canggih, mengancam integritas sistem keuangan dan stabilitas ekonomi. Oleh karena itu, studi ini berfokus pada pengembangan dan penerapan teknologi informasi yang dapat berfungsi sebagai alat pencegahan dan pengungkapan dalam menghadapi tindak pidana ekonomi yang terus berevolusi. Selain itu, kebaruan dalam pendekatan yang ditawarkan oleh penelitian ini juga berfungsi untuk menanggapi tantangan yang belum sepenuhnya dijawab oleh teknologi dan kebijakan yang ada saat ini. Dengan menggunakan teknik seperti analisis data besar, kecerdasan buatan, dan teknologi blockchain, penelitian ini bertujuan untuk memberikan solusi yang inovatif dan efektif dalam mendeteksi serta mencegah kejahatan ekonomi. Hal ini menjadikan penelitian ini sangat relevan, tidak hanya untuk memberikan kontribusi akademis, tetapi juga untuk membantu para praktisi dan pembuat kebijakan dalam merancang strategi yang lebih tangguh dalam melindungi masyarakat dari ancaman kejahatan ekonomi digital, serta menjaga kepercayaan publik terhadap sistem keuangan yang ada.

## **METODE PENELITIAN**

Metode penelitian yang digunakan dalam studi ini adalah studi literatur, yang merupakan pendekatan sistematis dalam mengumpulkan, menganalisis, dan menginterpretasi informasi yang telah dipublikasikan terkait peran teknologi informasi dalam pencegahan dan pengungkapan tindak pidana ekonomi berbasis digital. Studi literatur ini mencakup pengumpulan sumber-sumber dari jurnal akademik, buku, artikel, dan laporan yang relevan untuk memahami konteks teoretis dan praktis mengenai kejahatan ekonomi digital. Dengan memanfaatkan basis data online dan perpustakaan digital, penelitian ini akan menganalisis literatur yang ada untuk mengevaluasi kerangka hukum yang berlaku, efektivitas teknologi informasi dalam penegakan hukum, serta tantangan dan kendala yang dihadapi dalam implementasinya. Proses ini akan mencakup pemilihan sumber yang kredibel dan terkini, serta pengorganisasian informasi untuk mendapatkan gambaran menyeluruh mengenai masalah yang diteliti.

Selain itu, studi literatur ini juga akan mencakup analisis komparatif antara berbagai pendekatan yang diambil oleh negara-negara lain dalam menangani kejahatan ekonomi berbasis digital. Dengan membandingkan kebijakan dan praktik terbaik yang diterapkan di berbagai negara, penelitian ini berupaya untuk mengidentifikasi elemen-elemen yang dapat diadaptasi atau diterapkan di Indonesia untuk meningkatkan efektivitas pencegahan dan pengungkapan kejahatan ekonomi. Temuan dari studi literatur ini diharapkan dapat memberikan dasar yang kuat bagi pengembangan rekomendasi kebijakan yang lebih baik dan penerapan teknologi informasi yang lebih efisien dalam konteks hukum dan ekonomi. Dengan demikian, studi ini tidak hanya akan memberikan kontribusi bagi pengembangan ilmu pengetahuan, tetapi juga bagi praktik penegakan hukum di era digital yang terus berkembang.

## **HASIL DAN PEMBAHASAN**

### **Landasan Hukum dalam Penanganan Kejahatan Ekonomi Berbasis Digital**

Penanganan tindak pidana ekonomi berbasis digital di Indonesia diatur oleh berbagai peraturan perundang-undangan yang saling berkaitan dan membentuk kerangka hukum yang diharapkan dapat melindungi masyarakat dari tindakan kriminal yang memanfaatkan teknologi. Salah satu regulasi utama adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Undang-undang ini mencakup ketentuan mengenai berbagai bentuk



penyalahgunaan teknologi informasi, termasuk penipuan elektronik dan pencucian uang yang menggunakan sarana digital. Dalam konteks ini, Pasal 27 hingga Pasal 37 mengatur larangan-larangan yang ditujukan untuk mencegah tindakan yang merugikan pihak lain melalui media elektronik. Dengan landasan hukum ini, diharapkan penegak hukum dapat menindak pelaku kejahatan ekonomi digital secara lebih efektif dan memberikan perlindungan kepada konsumen yang menjadi korban (Undang-Undang Nomor 11 Tahun 2008).

Selain Undang-Undang ITE, terdapat juga Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang, yang berfungsi sebagai payung hukum untuk mencegah praktik pencucian uang yang sering kali melibatkan transaksi digital (Undang-Undang Nomor 8 Tahun 2010). Dalam undang-undang ini, Pasal 2 hingga Pasal 4 menjelaskan tindakan pencegahan dan penindakan terhadap praktik yang berkaitan dengan pencucian uang, yang relevan dengan kejahatan ekonomi berbasis digital. Di samping itu, Peraturan Bank Indonesia Nomor 19/12/PBI/2017 tentang Penyelenggaraan Teknologi Finansial juga menjadi regulasi penting yang memberikan kerangka hukum bagi perusahaan teknologi finansial untuk beroperasi dengan aman dan transparan. Melalui regulasi ini, pemerintah berupaya menciptakan ekosistem yang sehat bagi inovasi di bidang teknologi finansial, sekaligus memberikan perlindungan hukum bagi konsumen dan mencegah tindakan kriminal (Peraturan Bank Indonesia Nomor 19/12/PBI/2017).

Meskipun kerangka hukum yang ada sudah cukup komprehensif, terdapat sejumlah kekuatan dan kelemahan yang perlu dicermati untuk meningkatkan efektivitas penegakan hukum. Kekuatan dari regulasi yang ada terletak pada adanya definisi yang jelas mengenai tindak pidana ekonomi berbasis digital, serta pengaturan sanksi yang tegas bagi pelanggar. Namun, kelemahan utama terletak pada kurangnya penyesuaian terhadap perkembangan teknologi yang cepat, seperti penggunaan blockchain dan cryptocurrency, yang sering kali tidak tercover dalam peraturan yang ada. Hal ini menyebabkan kesulitan dalam penegakan hukum dan perlindungan konsumen di era digital, di mana modus operandi kejahatan terus berkembang. Tanpa adanya penyesuaian yang tepat, regulasi yang ada akan semakin sulit untuk diterapkan dan memberikan efek jera bagi pelaku kejahatan (Yoserwan, and Nani Mulyati, 2021).

Kesesuaian antara regulasi dan perkembangan teknologi merupakan hal yang krusial dalam penanganan kejahatan ekonomi berbasis digital. Saat ini, banyak modus operandi baru yang muncul dalam kejahatan ekonomi digital, seperti penipuan melalui aplikasi e-commerce, pemalsuan identitas di dunia maya, dan serangan siber yang semakin canggih. Oleh karena itu, perlu adanya revisi dan pembaruan regulasi untuk mencakup teknologi baru ini agar tidak ketinggalan zaman. Contohnya, Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang ITE telah mencakup beberapa aspek terkait dengan pengaturan media sosial dan konten digital, tetapi masih belum sepenuhnya menjawab tantangan yang dihadapi oleh penegak hukum. Penegakan hukum yang efektif menuntut adanya respons cepat terhadap perkembangan teknologi, sehingga peraturan yang ada harus dirancang untuk adaptif dan responsif terhadap situasi yang terus berubah (Undang-Undang Nomor 19 Tahun 2016).

Ketika membandingkan kerangka hukum Indonesia dengan negara lain, terlihat bahwa banyak negara telah mengembangkan regulasi yang lebih adaptif terhadap perkembangan teknologi. Misalnya, di Uni Eropa, Direktif 2013/40/EU tentang Serangan Siber memberikan landasan hukum yang kuat dalam penanganan kejahatan siber, termasuk pencurian data dan penipuan online. Negara-negara seperti Australia dan Singapura juga telah menerapkan regulasi yang inovatif untuk mengatasi kejahatan ekonomi berbasis digital. Singapura, misalnya, memiliki undang-undang yang mengatur perlindungan data pribadi dan transaksi elektronik yang sangat ketat, sehingga memberikan contoh baik dalam hal pengaturan yang komprehensif dan responsif. Dengan membandingkan praktik ini, Indonesia dapat belajar dari pengalaman negara lain dan mengadopsi elemen-elemen yang terbukti efektif untuk memperbaiki kerangka hukum yang ada.



Hukum di negara lain menangani kejahatan ekonomi digital dengan pendekatan yang lebih komprehensif dan sering kali melibatkan kolaborasi antara pemerintah, industri, dan lembaga penegak hukum. Di Amerika Serikat, misalnya, Computer Fraud and Abuse Act (CFAA) memberikan dasar hukum untuk menangani berbagai bentuk penipuan dan penyalahgunaan teknologi informasi. Selain itu, undang-undang di negara-negara maju sering kali mencakup elemen-elemen seperti perlindungan privasi data dan respons insiden yang lebih terstruktur, sehingga dapat menjadi model bagi Indonesia dalam menyusun regulasi yang lebih baik. Dengan mempelajari berbagai pendekatan yang diterapkan di negara lain, Indonesia dapat memahami tantangan yang ada dan menemukan solusi yang sesuai untuk situasi lokal yang dihadapi.

Identifikasi praktik terbaik dari negara-negara tersebut dapat memberikan pelajaran berharga bagi Indonesia dalam meningkatkan kerangka hukum dan penegakan hukum terhadap kejahatan ekonomi berbasis digital. Misalnya, penerapan sistem peringatan dini terhadap aktivitas mencurigakan dalam transaksi keuangan yang diterapkan di Singapura dapat meningkatkan kemampuan penegakan hukum dalam mencegah kejahatan. Selain itu, penggunaan teknologi seperti kecerdasan buatan untuk mendeteksi pola perilaku yang mencurigakan telah berhasil diterapkan di beberapa negara dan dapat diadopsi oleh Indonesia untuk meningkatkan efektivitas pencegahan kejahatan ekonomi berbasis digital. Dengan memanfaatkan teknologi dan praktik terbaik yang ada, Indonesia dapat memperkuat upaya pencegahan dan penegakan hukum dalam menghadapi tantangan di era digital.

Dalam rangka meningkatkan kerangka hukum yang ada, disarankan agar pemerintah Indonesia melakukan revisi terhadap undang-undang yang ada dengan mempertimbangkan perkembangan teknologi yang cepat. Revisi ini harus mencakup pengaturan yang lebih spesifik mengenai teknologi baru seperti cryptocurrency dan blockchain. Selain itu, penting untuk mengembangkan kolaborasi antara pemerintah, sektor swasta, dan lembaga internasional dalam rangka berbagi informasi dan praktik terbaik dalam penanganan kejahatan ekonomi berbasis digital. Dengan menciptakan ruang diskusi dan kerja sama yang baik antar pihak terkait, diharapkan regulasi yang dihasilkan akan lebih relevan dan efektif dalam menghadapi tantangan yang ada.

Penegakan hukum yang efektif memerlukan dukungan sumber daya manusia yang terlatih dan memiliki pemahaman yang mendalam tentang teknologi. Oleh karena itu, pelatihan dan pendidikan bagi penegak hukum perlu ditingkatkan untuk memastikan mereka dapat menghadapi tantangan yang muncul dalam kejahatan ekonomi digital. Selain itu, peningkatan infrastruktur teknologi informasi di lembaga penegak hukum juga menjadi hal yang penting untuk dilakukan. Keterlibatan akademisi dan praktisi dalam merumuskan kebijakan dan regulasi dapat meningkatkan relevansi dan efektivitas hukum yang diterapkan. Dengan dukungan yang tepat, penegakan hukum di bidang ini dapat dilakukan secara lebih optimal dan responsif.

Secara keseluruhan, meskipun Indonesia telah memiliki kerangka hukum yang mengatur tindak pidana ekonomi berbasis digital, masih banyak pekerjaan yang perlu dilakukan untuk menyesuaikan regulasi dengan perkembangan teknologi yang cepat. Dengan mempelajari praktik terbaik dari negara lain dan melakukan perbaikan kebijakan yang komprehensif, Indonesia dapat meningkatkan efektivitas penanganan kejahatan ekonomi berbasis digital, sekaligus melindungi masyarakat dari risiko yang ditimbulkan oleh tindakan kriminal di dunia maya. Melalui upaya yang terkoordinasi dan kolaboratif, diharapkan Indonesia dapat menjadi lebih siap dalam menghadapi tantangan kejahatan ekonomi di era digital, menciptakan lingkungan yang aman dan kondusif bagi perkembangan ekonomi dan teknologi informasi.

### **Penerapan Teknologi Informasi dalam Proses Investigasi**

Dalam era digital yang terus berkembang, penerapan teknologi informasi dalam proses investigasi kejahatan, khususnya tindak pidana ekonomi, menjadi hal yang krusial bagi aparat



penegak hukum. Teknologi informasi tidak hanya mempercepat proses pengumpulan bukti, tetapi juga meningkatkan akurasi dan efektivitas investigasi. Di Indonesia, berbagai peraturan memberikan dasar hukum bagi penggunaan teknologi dalam investigasi. Salah satu pasal yang relevan adalah Pasal 45 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang mengatur sanksi bagi pihak yang mengakses sistem elektronik tanpa izin (Undang-Undang Nomor 11 Tahun 2008). Pasal ini sangat penting karena memberikan perlindungan hukum bagi proses pengumpulan bukti yang dilakukan oleh pihak berwenang, serta menegaskan pentingnya menjaga integritas data yang digunakan dalam investigasi. Dalam konteks ini, teknologi informasi berperan tidak hanya sebagai alat bantu, tetapi juga sebagai landasan dalam memastikan bahwa semua langkah investigasi berjalan sesuai dengan ketentuan hukum yang berlaku, yang pada akhirnya dapat mendukung proses penegakan hukum yang lebih transparan dan akuntabel.

Salah satu metode yang digunakan oleh aparat penegak hukum adalah digital forensik, yang mencakup pengumpulan, analisis, dan pelaporan informasi yang diperoleh dari perangkat elektronik. Digital forensik memungkinkan penyelidik untuk menyelidiki berbagai sumber data, seperti komputer, ponsel, dan jaringan internet, untuk mengidentifikasi dan menelusuri jejak kejahatan yang sulit terdeteksi oleh metode konvensional. Dalam konteks ini, Pasal 4 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 juga memberikan kerangka hukum terkait perlindungan data dan informasi, yang sangat relevan untuk menjaga integritas bukti yang diperoleh selama investigasi. Dengan demikian, penerapan teknologi informasi dalam digital forensik memberikan banyak keuntungan, termasuk kemampuan untuk mengumpulkan bukti yang lebih komprehensif dan relevan (Undang-Undang Nomor 19 Tahun 2016). Hal ini tidak hanya mendukung upaya penegakan hukum, tetapi juga dapat memperkuat posisi hukum dalam persidangan, di mana keabsahan bukti sangat penting untuk menentukan hasil akhir dari suatu kasus (Ilham Jeryawan, 2024).

Penggunaan teknologi informasi juga mencakup sistem pemantauan dan pelacakan transaksi keuangan yang mencurigakan. Melalui analisis big data dan algoritma canggih, aparat penegak hukum dapat mendeteksi pola transaksi yang tidak wajar, yang mungkin menunjukkan adanya tindak pidana pencucian uang atau korupsi. Sebagai contoh, Pasal 74 ayat (2) Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang memberikan wewenang kepada instansi tertentu untuk melakukan pemantauan terhadap transaksi yang berpotensi melanggar hukum (Undang-Undang Nomor 8 Tahun 2010). Penggunaan teknologi dalam pengawasan transaksi keuangan memungkinkan penegak hukum untuk lebih proaktif dalam mengidentifikasi dan mencegah kejahatan ekonomi, serta merespons lebih cepat terhadap potensi ancaman. Namun, penting untuk dicatat bahwa penerapan teknologi ini harus diimbangi dengan kebijakan dan prosedur yang ketat untuk melindungi privasi individu dan mencegah penyalahgunaan data, sehingga kepercayaan publik terhadap penegakan hukum tetap terjaga.

Meskipun terdapat banyak keuntungan, penerapan teknologi informasi dalam investigasi tidak selalu berjalan mulus. Beberapa studi kasus menunjukkan keberhasilan dan kegagalan dalam penggunaan teknologi ini. Misalnya, dalam kasus pengungkapan korupsi di sektor publik, penggunaan sistem pelaporan elektronik berhasil mengidentifikasi sejumlah transaksi mencurigakan, memberikan informasi berharga bagi penegakan hukum. Namun, terdapat juga kasus di mana kurangnya pelatihan bagi petugas menyebabkan pemanfaatan alat teknologi menjadi kurang efektif, sehingga hasil yang diharapkan tidak tercapai. Hal ini menunjukkan bahwa meskipun teknologi memiliki potensi besar untuk mendukung investigasi, faktor manusia dan kebijakan dalam penggunaannya juga harus diperhatikan secara serius. Keberhasilan implementasi teknologi dalam investigasi sangat bergantung pada kesiapan sumber daya manusia yang terlibat,



termasuk pelatihan dan pengembangan keterampilan yang sesuai agar mereka dapat memanfaatkan teknologi dengan maksimal (Rayhan, dkk., 2024).

Lebih jauh, teknologi informasi dapat digunakan untuk membangun basis data yang terintegrasi, sehingga memungkinkan berbagi informasi antar lembaga penegak hukum dengan lebih efektif. Pasal 17 Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan menekankan pentingnya pengelolaan arsip yang baik, termasuk arsip digital yang dapat diakses oleh berbagai instansi (Undang-Undang Nomor 43 Tahun 2009). Dengan adanya basis data yang terintegrasi, proses investigasi akan menjadi lebih efisien, karena informasi yang relevan dapat diakses dengan cepat oleh berbagai pihak yang terlibat. Hal ini juga berpotensi mengurangi tumpang tindih dalam investigasi dan mempercepat penanganan kasus. Dengan memanfaatkan teknologi informasi secara optimal, proses pengumpulan bukti dan analisis data dapat dilakukan secara lebih komprehensif, sehingga menghasilkan informasi yang lebih akurat dan dapat dipertanggungjawabkan. Ini adalah langkah penting untuk memastikan bahwa penegakan hukum dalam kasus-kasus tindak pidana ekonomi berlangsung dengan transparansi dan keadilan.

Keberhasilan penerapan teknologi dalam proses investigasi juga bergantung pada dukungan infrastruktur yang memadai. Ketersediaan perangkat keras dan perangkat lunak yang sesuai sangat penting untuk menjalankan aplikasi teknologi informasi yang digunakan dalam investigasi. Dalam konteks ini, Pasal 5 ayat (1) Undang-Undang Nomor 11 Tahun 2008 menekankan perlunya sistem yang dapat menjamin keamanan dan kehandalan data elektronik, yang merupakan prasyarat untuk membangun kepercayaan publik terhadap proses penegakan hukum. Jika infrastruktur yang dibangun tidak memadai, maka efektivitas teknologi dalam pengumpulan dan analisis bukti dapat terhambat. Oleh karena itu, investasi dalam pengembangan teknologi dan infrastruktur menjadi sangat penting untuk memastikan bahwa aparat penegak hukum dapat bekerja dengan optimal. Peningkatan infrastruktur yang berkelanjutan akan mendukung kemampuan lembaga dalam menggunakan teknologi informasi dan memperkuat upaya mereka dalam menanggulangi tindak pidana ekonomi.

Dalam menganalisis efektivitas teknologi informasi dalam investigasi, perlu dilakukan evaluasi secara berkala untuk mengetahui dampaknya terhadap proses penegakan hukum. Pemanfaatan metode analisis yang tepat, seperti analisis kualitatif dan kuantitatif, dapat memberikan gambaran yang lebih jelas mengenai seberapa jauh teknologi informasi dapat membantu aparat penegak hukum dalam mengungkap tindak pidana. Pasal 71 Undang-Undang Nomor 8 Tahun 2010 mengatur tentang evaluasi dan pengawasan dalam implementasi kebijakan anti-korupsi, sehingga memberikan ruang bagi perbaikan berkelanjutan dalam penggunaan teknologi. Proses evaluasi ini penting dilakukan untuk memastikan bahwa teknologi yang digunakan selalu relevan dengan perkembangan zaman dan kebutuhan penegakan hukum yang dinamis. Selain itu, hasil evaluasi juga dapat digunakan sebagai dasar untuk pengembangan kebijakan yang lebih baik, sehingga penerapan teknologi informasi dalam investigasi dapat semakin efektif dan efisien (Asaad, dkk., 2023).

Penerapan teknologi informasi dalam proses investigasi tindak pidana ekonomi menunjukkan potensi yang signifikan untuk meningkatkan efektivitas penegakan hukum. Namun, hal ini memerlukan sinergi antara teknologi, kebijakan, dan sumber daya manusia yang terlatih. Hasil dari penelitian dan analisis ini diharapkan dapat memberikan rekomendasi yang konstruktif untuk perbaikan kebijakan dan praktik penegakan hukum di masa mendatang. Dengan memperkuat infrastruktur, meningkatkan keterampilan sumber daya manusia, dan melakukan evaluasi secara berkala, pengungkapan tindak pidana ekonomi dapat dilakukan dengan lebih baik dan akuntabel. Melalui pendekatan yang komprehensif dan kolaboratif, diharapkan bahwa teknologi informasi dapat menjadi alat yang efektif dalam memberantas kejahatan ekonomi dan meningkatkan kepercayaan publik terhadap sistem hukum di Indonesia.



Penerapan teknologi informasi dalam proses investigasi telah membawa dampak signifikan terhadap efisiensi dan efektivitas penegakan hukum. Dengan memanfaatkan berbagai alat dan sistem digital, aparat penegak hukum kini dapat mengumpulkan, menganalisis, dan mengelola data dengan lebih baik daripada sebelumnya. Teknologi seperti perangkat lunak analisis data, sistem pemantauan elektronik, dan digital forensik telah menjadi bagian integral dari investigasi modern. Misalnya, penggunaan big data analytics memungkinkan penyidik untuk menganalisis pola dan tren dari sejumlah besar informasi yang dihasilkan dari aktivitas kriminal, yang sebelumnya sulit untuk diidentifikasi. Dengan demikian, penerapan teknologi informasi tidak hanya meningkatkan kecepatan pengumpulan bukti, tetapi juga memberikan peluang lebih besar untuk mengungkap kejahatan secara lebih mendalam dan menyeluruh (Indriani, Safitri, 2020).

Namun, meskipun teknologi informasi memiliki potensi besar, ada juga tantangan yang dapat menghambat efektivitasnya dalam proses penegakan hukum. Salah satu isu yang sering dihadapi adalah kurangnya pelatihan yang memadai bagi aparat penegak hukum dalam menggunakan alat dan sistem digital. Tanpa pemahaman yang baik tentang bagaimana teknologi ini berfungsi dan cara memanfaatkannya secara optimal, hasil dari investigasi bisa jadi kurang akurat atau tidak efektif. Selain itu, ketergantungan yang tinggi pada teknologi juga dapat menjadi kendala ketika sistem mengalami gangguan atau ketika data yang diperlukan tidak tersedia. Oleh karena itu, penting bagi lembaga penegak hukum untuk tidak hanya berinvestasi dalam teknologi, tetapi juga dalam pengembangan sumber daya manusia agar mampu memaksimalkan penggunaan teknologi tersebut dalam proses investigasi.

Di sisi lain, penerapan teknologi informasi dalam investigasi juga dapat menghadirkan masalah terkait privasi dan perlindungan data. Penggunaan sistem pemantauan elektronik dan alat pengumpulan data digital sering kali menimbulkan pertanyaan mengenai sejauh mana hak-hak individu dilindungi dalam proses penegakan hukum. Ketika aparat penegak hukum menggunakan teknologi untuk mengumpulkan informasi, ada risiko bahwa data pribadi dapat disalahgunakan atau diakses tanpa izin. Dalam konteks ini, regulasi dan kebijakan yang jelas sangat diperlukan untuk menjaga keseimbangan antara kebutuhan penegakan hukum dan perlindungan hak asasi manusia. Pasal 4 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, misalnya, mengatur tentang perlindungan data dan informasi, yang menjadi landasan penting bagi penggunaan teknologi dalam investigasi.

Lebih jauh lagi, kolaborasi antara lembaga penegak hukum dan penyedia teknologi juga sangat penting untuk meningkatkan efektivitas penerapan teknologi informasi. Melalui kemitraan ini, penegak hukum dapat memperoleh akses ke alat yang lebih canggih dan mendapatkan dukungan teknis dalam penggunaannya. Selain itu, penyedia teknologi dapat lebih memahami kebutuhan praktis di lapangan, sehingga dapat mengembangkan solusi yang lebih sesuai untuk tantangan yang dihadapi oleh aparat penegak hukum. Sinergi antara teknologi dan penegakan hukum ini juga dapat menciptakan inovasi baru yang dapat meningkatkan cara investigasi dilakukan, serta mempercepat proses penanganan kasus-kasus kriminal. Kolaborasi ini akan memberikan manfaat ganda, baik bagi penegak hukum maupun masyarakat, dengan menghasilkan sistem hukum yang lebih responsif dan efektif (Ningrum, dkk., 2022).

Secara keseluruhan, penerapan teknologi informasi dalam proses investigasi memberikan dampak yang signifikan terhadap penegakan hukum. Meskipun ada tantangan yang perlu diatasi, potensi yang ditawarkan oleh teknologi modern sangat besar dalam meningkatkan efisiensi dan akurasi proses investigasi (Salim, Agus dan Bima, Elfran, 2020). Oleh karena itu, diperlukan pendekatan holistik yang mencakup pelatihan bagi sumber daya manusia, pengembangan kebijakan yang melindungi privasi individu, dan kolaborasi yang kuat antara lembaga penegak hukum dan penyedia teknologi. Dengan langkah-langkah ini, diharapkan bahwa teknologi informasi dapat digunakan secara optimal untuk mendukung penegakan hukum yang lebih baik dan lebih adil, serta membangun kepercayaan masyarakat terhadap sistem hukum yang ada.



## **Tantangan Hukum dalam Implementasi Teknologi Informasi**

Dalam era digital yang berkembang pesat, implementasi teknologi informasi (TI) telah membawa perubahan besar dalam berbagai aspek kehidupan, termasuk pemerintahan, sektor bisnis, dan pendidikan. Namun, di balik kemudahan yang ditawarkan oleh teknologi ini, terdapat berbagai tantangan hukum yang perlu dihadapi, yang meliputi isu-isu penting seperti perlindungan privasi data, yurisdiksi, dan pengelolaan sumber daya manusia. Sebagai contoh, semakin meningkatnya penggunaan TI dalam mengelola data dan informasi membuat perlindungan terhadap data pribadi menjadi prioritas utama. Masyarakat dihadapkan pada risiko kebocoran data dan penyalahgunaan informasi pribadi, sehingga penting bagi setiap individu untuk menyadari hak-hak mereka. Untuk itu, penting untuk melakukan identifikasi terhadap tantangan yang dihadapi dalam implementasi TI, sehingga kebijakan yang ada dapat diperkuat dan disesuaikan dengan kebutuhan dan dinamika perkembangan teknologi yang terus berubah.

Salah satu tantangan utama yang signifikan dalam implementasi teknologi informasi adalah masalah privasi data. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP) memberikan kerangka hukum yang mengatur pengelolaan dan perlindungan data pribadi di Indonesia. Dalam Pasal 5 undang-undang tersebut, ditegaskan bahwa pengumpulan, penyimpanan, dan pemrosesan data pribadi harus dilakukan dengan persetujuan dari subjek data. Meskipun sudah ada regulasi yang jelas, dalam praktiknya masih banyak organisasi yang kesulitan untuk mematuhi ketentuan ini. Sebagian besar masyarakat belum sepenuhnya memahami hak-hak mereka terkait perlindungan data pribadi, sehingga kesadaran tentang pentingnya privasi data masih rendah. Hal ini menunjukkan bahwa diperlukan upaya lebih lanjut dalam meningkatkan literasi hukum di masyarakat agar mereka bisa lebih memahami dan mengawal pengelolaan data pribadi mereka.

Di samping isu privasi, masalah yurisdiksi juga menjadi tantangan penting yang harus dihadapi dalam implementasi TI. Ketika data dan informasi berpindah lintas batas, sering kali muncul pertanyaan mengenai hukum mana yang seharusnya diterapkan. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) memberikan dasar hukum untuk transaksi elektronik, namun tidak secara eksplisit mengatur masalah yurisdiksi lintas negara. Pasal 26 dari Undang-Undang ITE menyebutkan bahwa transaksi elektronik yang dilakukan di wilayah hukum Indonesia tunduk pada hukum Indonesia (Undang-Undang Nomor 11 Tahun 2008). Namun, dalam praktiknya, hal ini sering menimbulkan kebingungan dan kesulitan dalam penegakan hukum, terutama ketika terjadi pelanggaran yang melibatkan entitas dari negara yang berbeda. Oleh karena itu, penting bagi pembuat kebijakan untuk merumuskan regulasi yang lebih jelas dan komprehensif terkait yurisdiksi, guna memastikan bahwa penegakan hukum dapat dilakukan secara efektif.

Selain tantangan hukum yang berkaitan dengan privasi dan yurisdiksi, kendala teknis juga menjadi hambatan yang signifikan dalam implementasi TI. Keterbatasan infrastruktur teknologi yang ada, seperti jaringan internet yang tidak memadai dan kurangnya akses di daerah terpencil, menjadi hambatan dalam penerapan sistem TI yang efektif. Banyak daerah di Indonesia masih menghadapi masalah konektivitas yang rendah, sehingga menghambat akses masyarakat terhadap layanan digital yang seharusnya dapat mereka nikmati. Di samping itu, aspek keamanan siber juga menjadi perhatian penting, mengingat meningkatnya risiko serangan siber yang dapat merusak sistem informasi dan mengakibatkan kebocoran data yang berpotensi merugikan individu maupun organisasi. Untuk itu, penting bagi organisasi dan lembaga pemerintah untuk menginvestasikan sumber daya yang memadai dalam pengembangan sistem keamanan yang handal, serta terus mengikuti perkembangan teknologi terkini untuk melindungi data dan informasi yang dikelola.

Sumber daya manusia juga menjadi faktor kunci dalam menghadapi tantangan hukum dan teknis yang muncul dalam implementasi TI. Ketersediaan tenaga ahli yang terlatih dalam bidang teknologi informasi dan hukum siber masih terbatas, sehingga menghambat pengembangan



kebijakan dan prosedur yang sesuai. Pasal 22 dalam Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi menyatakan bahwa penyelenggara telekomunikasi wajib menyediakan sumber daya manusia yang kompeten (Undang-Undang Nomor 36 Tahun 1999). Namun, di banyak daerah, realisasi dari ketentuan ini masih jauh dari harapan, terutama di daerah-daerah yang kurang berkembang. Hal ini menyebabkan ketidakmampuan dalam mengelola teknologi dan hukum yang berkaitan dengan TI secara optimal. Oleh karena itu, pendidikan dan pelatihan di bidang teknologi informasi harus menjadi prioritas agar sumber daya manusia yang ada dapat memahami dan mengatasi isu-isu hukum yang timbul akibat penggunaan teknologi.

Kesenjangan antara regulasi yang ada dan perkembangan teknologi juga menjadi tantangan yang signifikan. Banyak peraturan yang saat ini ada belum sepenuhnya mencakup perkembangan terbaru dalam teknologi, seperti kecerdasan buatan (AI), big data, dan Internet of Things (IoT). Hal ini menciptakan celah hukum yang dapat dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab. Pasal 11 dalam Undang-Undang ITE memberikan landasan untuk perlindungan dan tanggung jawab penyelenggara sistem elektronik, namun regulasi tersebut harus diperbarui dan disesuaikan dengan isu-isu baru yang muncul di era digital ini. Legislatur dan pemangku kebijakan perlu beradaptasi dengan cepat untuk merumuskan regulasi yang lebih responsif terhadap kemajuan teknologi yang pesat, sehingga dapat mencegah terjadinya penyalahgunaan dan pelanggaran hukum.

Selain itu, tantangan dalam implementasi TI juga terkait dengan ketidakselarasan kebijakan antara berbagai lembaga pemerintah. Setiap lembaga mungkin memiliki pendekatan dan regulasi yang berbeda dalam menangani isu-isu yang berkaitan dengan TI, yang dapat menyebabkan kebingungan dan inkonsistensi dalam penegakan hukum. Pasal 6 dalam Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan menekankan pentingnya penyelenggaraan pemerintahan yang baik dan terkoordinasi (Undang-Undang Nomor 30 Tahun 2014). Oleh karena itu, diperlukan upaya kolaboratif antara lembaga untuk menciptakan kerangka hukum yang harmonis dan efektif dalam pengelolaan TI. Dengan memperkuat kerjasama antara lembaga, diharapkan akan tercipta kebijakan yang lebih terintegrasi dan mampu mengatasi berbagai tantangan yang ada secara menyeluruh (Septianingrum, 2024).

Akhirnya, untuk menghadapi semua tantangan ini, penting untuk menciptakan kesadaran hukum yang lebih baik di kalangan masyarakat. Penyuluhan dan pendidikan mengenai hak-hak individu dan kewajiban dalam penggunaan teknologi informasi perlu diperkuat, agar masyarakat dapat berperan aktif dalam perlindungan data pribadi mereka. Dalam hal ini, peran media dan organisasi non-pemerintah sangat penting untuk menyebarkan informasi yang tepat mengenai isu-isu hukum terkait TI. Dengan pendekatan yang komprehensif dan kolaboratif, tantangan hukum dalam implementasi teknologi informasi dapat diatasi, sehingga mendorong pemanfaatan TI yang lebih baik dan aman di masyarakat, serta menciptakan lingkungan digital yang lebih berkelanjutan dan bermanfaat bagi semua pihak.

Penerapan teknologi informasi dalam berbagai sektor, termasuk pemerintahan, bisnis, dan pendidikan, membawa tantangan hukum yang kompleks. Salah satu tantangan utama adalah bagaimana menyusun regulasi yang mampu mengatur perkembangan teknologi yang cepat dan dinamis. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) menjadi landasan hukum untuk mengatur penggunaan teknologi informasi di Indonesia. Namun, banyak norma yang terdapat dalam peraturan ini yang masih ambigu, sehingga memunculkan berbagai interpretasi yang dapat berpotensi menimbulkan sengketa. Misalnya, Pasal 27 yang mengatur tentang larangan penyebaran konten negatif sering kali diinterpretasikan berbeda oleh berbagai pihak, menciptakan ketidakpastian hukum bagi pengguna teknologi.

Selain itu, isu privasi dan perlindungan data pribadi semakin mendesak untuk dibahas, terutama dengan adanya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data



Pribadi. Meskipun regulasi ini ditujukan untuk melindungi hak-hak individu, implementasinya masih menemui banyak kendala, termasuk ketidakpahaman masyarakat tentang pentingnya perlindungan data dan ketidaksiapan organisasi dalam menerapkan kebijakan yang sesuai. Ketidakjelasan mengenai sanksi bagi pelanggaran juga menjadi masalah, karena Pasal 71 UU Perlindungan Data Pribadi belum sepenuhnya memberikan kepastian tentang konsekuensi hukum yang akan dihadapi oleh pihak yang melanggar.

Tantangan hukum lainnya adalah munculnya risiko keamanan siber yang semakin meningkat. Dengan meningkatnya jumlah transaksi online dan penggunaan data digital, ancaman terhadap sistem informasi menjadi lebih signifikan. Pasal 30 UU ITE menegaskan pentingnya penyelenggara sistem elektronik untuk menjaga keamanan data, namun masih banyak entitas yang belum menerapkan langkah-langkah keamanan yang memadai. Kelemahan dalam sistem keamanan ini dapat dimanfaatkan oleh pelaku kejahatan siber untuk melakukan penipuan, pencurian identitas, dan penyebaran malware, yang berdampak negatif pada kepercayaan publik terhadap teknologi informasi.

Untuk mengatasi tantangan hukum ini, dibutuhkan solusi yang komprehensif dan terintegrasi. Salah satu langkah yang dapat diambil adalah memperkuat kerangka regulasi yang ada dengan memperjelas norma dan sanksi yang diterapkan dalam UU ITE dan UU Perlindungan Data Pribadi. Melalui revisi undang-undang atau penerbitan peraturan pemerintah yang lebih spesifik, diharapkan akan tercipta kepastian hukum yang lebih baik. Misalnya, menambahkan ketentuan yang lebih detail tentang tanggung jawab penyelenggara sistem informasi dalam hal pelanggaran keamanan siber dapat membantu dalam memperjelas batasan tanggung jawab dan sanksi yang dapat diterapkan.

Selain itu, peningkatan kesadaran masyarakat tentang hak-hak mereka dalam konteks teknologi informasi juga sangat penting. Edukasi yang tepat dapat membantu individu memahami perlindungan data pribadi mereka dan bagaimana menghindari risiko yang terkait dengan penggunaan teknologi. Oleh karena itu, kolaborasi antara pemerintah, lembaga pendidikan, dan sektor swasta dalam menyelenggarakan program edukasi dan pelatihan akan sangat bermanfaat. Pasal 63 UU Perlindungan Data Pribadi menyebutkan pentingnya pendidikan tentang perlindungan data bagi masyarakat, yang dapat dijadikan dasar untuk melaksanakan inisiatif ini secara lebih luas.

Akhirnya, dalam rangka meningkatkan efektivitas implementasi teknologi informasi, pemerintah perlu memperkuat infrastruktur hukum dan sumber daya manusia di bidang hukum teknologi informasi. Pengembangan kapasitas para penegak hukum dan pengacara untuk memahami isu-isu yang berkaitan dengan teknologi informasi adalah langkah yang krusial. Dengan menyediakan pelatihan dan sumber daya yang memadai, diharapkan para profesional hukum dapat menangani kasus-kasus yang berkaitan dengan teknologi informasi dengan lebih efektif. Melalui langkah-langkah ini, diharapkan tantangan hukum yang dihadapi dalam penerapan teknologi informasi dapat diatasi, dan implementasi teknologi dapat berjalan lebih baik dan aman di Indonesia.

## **KESIMPULAN**

Penerapan teknologi informasi telah menjadi bagian integral dalam pencegahan dan pengungkapan tindak pidana ekonomi berbasis digital. Teknologi seperti AI, big data, dan blockchain terbukti efektif dalam mendeteksi dan memantau pola kejahatan. Di Indonesia, meskipun regulasi seperti UU ITE dan UU TPPU telah memberikan landasan hukum yang memadai, tantangan masih ada dalam hal adaptasi terhadap perkembangan teknologi yang pesat. Penerapan teknologi ini juga memerlukan dukungan sumber daya manusia yang kompeten dan infrastruktur keamanan yang memadai. Dengan memperkuat regulasi dan meningkatkan pelatihan



bagi aparat penegak hukum, Indonesia dapat lebih efektif dalam menangani kejahatan ekonomi digital serta melindungi masyarakat dari risiko yang timbul.

Diperlukan langkah konkret untuk memperbarui kerangka hukum agar sesuai dengan perkembangan teknologi yang cepat, terutama terkait pengaturan teknologi baru seperti blockchain dan cryptocurrency. Pemerintah dan sektor swasta perlu berkolaborasi dalam meningkatkan literasi teknologi dan pelatihan bagi aparat hukum agar mampu memanfaatkan teknologi dengan optimal. Selain itu, infrastruktur keamanan digital harus terus diperkuat untuk mencegah serangan siber yang dapat mengganggu proses penegakan hukum. Kerja sama internasional juga perlu ditingkatkan, mengingat sifat lintas batas dari kejahatan ekonomi digital, agar Indonesia dapat belajar dari praktik terbaik yang diterapkan di negara lain.

## DAFTAR PUSTAKA

- Akbar, Aldi, Aditya Wardhana, and Budi Rustandi Kartawinata. "Keuangan Digital: Dibalik Kemudahannya, Waspadai Pula Potensi Kejahatannya Seri Kegiatan Pengabdian Masyarakat (Guru & Orang Tua Siswa TK Taman Indria Bandung): Seri Kegiatan Pengabdian Masyarakat (Guru & Orang Tua Siswa TK Taman Indria Bandung)." *Jurnal ADAM: Jurnal Pengabdian Masyarakat* 3, no. 2 (2024): 293–300. <https://doi.org/10.37081/adam.v3i2.1960>.
- Asaad, Annisa Febriana Jauza, Syamsul Bachri, and Aminuddin Ilmar. "Efektivitas Hukum Alat Bukti Elektronik Dalam Pemeriksaan Bukti Di Pengadilan Tata Usaha Negara." *Jurnal USM Law Review* 6, no. 1 (2023): 260–271.
- Baza, Moch. Ravy Mauludy, and Moh Agil. "Peran Penting Teknologi Digital Blockchain Dalam Upaya Mengurangi Kasus Korupsi Penggelapan Surat Berharga." *Jurnal Hukum Dan Sosial Politik* 1, no. 1 (February 14, 2023): 43–54. <https://doi.org/10.59581/jhsp-widyakarya.v1i1>.
- Gultom, Martinus Filemon, Leonardo Simanjuntak, Ayu Efrita Dewi, and Heni Widiyani. "Peran Teknologi Informasi Dalam Pencegahan Korupsi (Studi Kasus Implementasi Sistem E-Government)." *SYARIAH: Jurnal Ilmu Hukum* 1, no. 2 (2023): 33–42. <https://doi.org/10.62017/syariah.v1i2.273>.
- Indonesia. Peraturan Bank Indonesia Nomor 19/12/PBI/2017 tentang Penyelenggaraan Teknologi Finansial. Jakarta: Bank Indonesia, 2017.
- Indonesia. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Jakarta: Kementerian Komunikasi dan Informatika Republik Indonesia, 2016.
- Indonesia. Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang. Jakarta: Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia, 2010.
- Indonesia. Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58. Jakarta: Sekretariat Negara, 2008.
- Indonesia. Undang-Undang Republik Indonesia Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan. Lembaran Negara Republik Indonesia Tahun 2014 Nomor 238. Jakarta: Sekretariat Negara, 2014.



- Indonesia. Undang-Undang Republik Indonesia Nomor 36 Tahun 1999 tentang Telekomunikasi. Lembaran Negara Republik Indonesia Tahun 1999 Nomor 115. Jakarta: Sekretariat Negara, 1999.
- Indonesia. Undang-Undang Republik Indonesia Nomor 43 Tahun 2009 tentang Kearsipan. Lembaran Negara Republik Indonesia Tahun 2009 Nomor 151. Jakarta: Sekretariat Negara, 2009.
- Indonesia. Undang-Undang Republik Indonesia Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang. Lembaran Negara Republik Indonesia Tahun 2010 Nomor 28. Jakarta: Sekretariat Negara, 2010.
- Indriani, Safitri. "Dokumen Elektronik Sebagai Alat Pembuktian Dalam Transaksi Elektronik." Brawijaya, 2020.
- Jeryawan, Ilham. "Analisis Terhadap Efektivitas Dan Efisiensi Alat Bukti Elektronik Di Pengadilan." *Causa: Jurnal Hukum Dan Kewarganegaraan* 5, no. 2 (2024): 71–80. <https://doi.org/10.3783/causa.v5i2.4093>.
- Ningrum, Valencia Prasetyo, and Yuliya Safitri. "Sistem Pembuktian Elektronik Pada Hukum Acara Peradilan Tata Usaha Negara Electronic Evidence System in the Procedural Law of the State Administrative Court." *Comserva* 2, no. 08 (2022): 1357–67. <https://doi.org/10.36418/comserva.v2i08.475>.
- Rayhan, Ahmad, H.E. Rakhmat Jazuli, Essa Alicia Pradita, and Hafizah Sukma Yuniar. "Efektivitas Hukum Sistem Pembuktian Alat Bukti Elektronik dalam Ranah Pemeriksaan Bukti di Pengadilan Tata Usaha Negara." *Jurnal Res Justitia: Jurnal Ilmu Hukum* 4, no. 2 (2024): 279–295. <https://doi.org/10.46306/rj.v4i2.119>.
- Salim, Agus, and Elfran Bima. "Persidangan Elektronik (E-Litigasi) Pada Peradilan Tata Usaha Negara." *Paulus Law Journal* 2, no. 1 (2020). <https://doi.org/10.51342/plj.v2i1.150>.
- Seldal, M. M. Naeser, and Ellen K. Nyhus. "Financial Vulnerability, Financial Literacy, and the Use of Digital Payment Technologies." *Journal of Consumer Policy* 45, no. 2 (March 7, 2022): 281–306. <https://doi.org/10.1007/s10603-022-09512-9>.
- Septianingrum, Gita Ayu Ajeng, None Putri Nabila, and None Siti Nurhayati. "Teknologi dan Kepatuhan Hukum (Tantangan dan Strategi dalam Sosiologi Hukum)." *Jurnal Humaya Jurnal Hukum Humaniora Masyarakat Dan Budaya* 4, no. 1 (July 17, 2024): 47–62. <https://doi.org/10.33830/humaya.v4i1.8156>.
- Yoserwan, and Nani Mulyati. *Hukum Pidana Ekonomi*. Depok: PT Raja Grafindo Persada, 2021.