Jaksa: Jurnal Kajian Ilmu Hukum dan Politik
Vol. 2, No. 2 April 2024
e-ISSN :2988-5140 , p-ISSN ; 2988-7747, Hal 222-228
DOI: https://doi.org/10.51903/jaksa.v2i2.1666

Kejahatan Teknologi Informasi (*Cyber Crime*) dan Penanggulangannya dalam Hukum Indonesia

Ferdinan Sitompul [1], Alfren Petrus Putra Manik [2], Carlos Daniel Sinaga [3], Angel Theresia Purba [4], Andy Satria [5]
Fakultas Hukum, Universitas Medan Area
Alamat: Medan, Sumatera Utara, Indonesia
Korespondensi penulis: fsitompul915@gmail.com

Abstract. *This journal examines the phenomenon of Information Technology crimes, commonly known as cybercrime, and the legal countermeasures in the context of Indonesian law. The continuous advancement of information technology has opened doors for criminals to exploit digital means as tools to achieve their illicit objectives. This research aims to analyze the most prevalent types of information technology crimes in Indonesia and identify the legal framework's role in combating and mitigating the negative impacts of these crimes. The research methodology involves the analysis of secondary data, including case studies of information technology crimes that have occurred in Indonesia. The findings indicate that crimes such as identity theft, online fraud, and ransomware attacks pose serious threats to digital security in Indonesia. Therefore, concerted efforts are needed to develop an effective legal framework to combat these crimes. The journal also reviews the development of legal regulations concerning information technology crimes in Indonesia, such as the ITE Law (Electronic Information and Transactions Law), and analyzes the effectiveness and challenges faced in law enforcement. Additionally, the research discusses preventive and counteraction initiatives undertaken by the government, law enforcement agencies, and the private sector. The research findings provide in-depth insights into the complexity of information technology crime issues and the challenges in addressing them in Indonesia. The implications of this research are expected to support the improvement of policies, regulations, and more effective law enforcement efforts in facing the threats of information technology crimes in the future.*

Keywords: *Cyber Crime, Countermeasure, Indonesian Law.*

Abstrak. Jurnal ini mengkaji fenomena kejahatan teknologi informasi, atau yang dikenal sebagai cyber crime, dan upaya penanggulangannya dalam konteks hukum di Indonesia. Keberlanjutan perkembangan teknologi informasi telah membuka pintu bagi pelaku kejahatan untuk memanfaatkan sarana digital sebagai alat untuk mencapai tujuan kriminal mereka. Penelitian ini bertujuan untuk menganalisis jenis-jenis kejahatan teknologi informasi yang paling umum terjadi di Indonesia, serta mengidentifikasi peran hukum dalam menanggulangi dan mengurangi dampak negatif dari kejahatan tersebut. Metode penelitian yang digunakan melibatkan analisis data sekunder, termasuk studi kasus kejahatan teknologi informasi yang telah terjadi di Indonesia. Hasil penelitian menunjukkan bahwa kejahatan seperti pencurian identitas, penipuan online, dan serangan ransomware menjadi ancaman serius bagi keamanan digital di Indonesia. Oleh karena itu, diperlukan upaya serius dalam mengembangkan kerangka hukum yang efektif untuk melawan kejahatan ini. Jurnal ini juga mengulas perkembangan regulasi hukum terkait kejahatan teknologi informasi di Indonesia, seperti UU ITE (Undang-Undang Informasi dan Transaksi Elektronik), dan menganalisis keefektifan serta tantangan yang dihadapi dalam penegakan hukum. Selain itu, penelitian ini membahas inisiatif pencegahan dan penanggulangan kejahatan teknologi informasi yang dilakukan oleh pemerintah, lembaga penegak hukum, dan sektor swasta. Temuan penelitian ini memberikan wawasan mendalam tentang kompleksitas isu kejahatan teknologi informasi dan tantangan dalam menanggulanginya di Indonesia. Implikasi hasil penelitian ini diharapkan dapat mendukung perbaikan kebijakan, regulasi, dan upaya penegakan hukum yang lebih efektif dalam menghadapi ancaman kejahatan teknologi informasi di masa depan.

Kata kunci: Kejahatan Teknologi, Penanggulangan, Hukum Indonesia.

LATAR BELAKANG

Dalam era globalisasi dan kemajuan teknologi informasi, keberadaan kejahatan teknologi informasi atau cyber crime menjadi suatu tantangan serius yang dapat mengancam keamanan dan stabilitas suatu negara. Indonesia, sebagai salah satu negara dengan

Received Desember 04, 2023; Accepted January 13, 2024; Published April 30, 2024
** Ferdinan Sitompul ,* fsitompul915@gmail.com

pertumbuhan pengguna internet yang pesat, menghadapi risiko yang semakin meningkat terkait dengan ekspansi kejahatan teknologi informasi. Keberlanjutan perkembangan teknologi membuka celah bagi pelaku kejahatan untuk menggunakan metode baru dan lebih kompleks, seperti pencurian identitas, penipuan online, dan serangan ransomware. Oleh karena itu, penelitian ini diarahkan untuk menyelidiki kejahatan teknologi informasi yang sedang berkembang di Indonesia dan mengeksplorasi upaya hukum yang diperlukan untuk menanggulangi ancaman ini. Peristiwa-peristiwa kejahatan teknologi informasi yang semakin merajalela telah menggugah perhatian masyarakat, pemerintah, dan lembaga penegak hukum di Indonesia. Serangan-serangan terkoordinasi dan canggih telah menyebabkan kerugian ekonomi, pencurian data pribadi, dan merugikan keberlanjutan bisnis. Fenomena ini memunculkan kebutuhan mendesak untuk meningkatkan keefektifan perangkat hukum yang ada dan mengembangkan strategi penanggulangan yang lebih proaktif.

Penelitian ini bertujuan untuk menganalisis jenis-jenis kejahatan teknologi informasi yang paling umum terjadi di Indonesia, mengevaluasi keefektifan regulasi hukum yang ada, dan menyelidiki inisiatif pencegahan serta penanggulangan yang telah diambil oleh pemerintah dan sektor swasta. Melalui pendekatan ini, penelitian ini berusaha memberikan pemahaman mendalam tentang kejahatan teknologi informasi dan memberikan rekomendasi untuk perbaikan kebijakan dan penegakan hukum.Hasil dari penelitian ini diharapkan dapat memberikan manfaat nyata dalam upaya meningkatkan keamanan siber di Indonesia. Rekomendasi yang dihasilkan diharapkan dapat membantu perumusan kebijakan yang lebih adaptif terhadap dinamika kejahatan teknologi informasi. Selain itu, penelitian ini diharapkan dapat memberikan panduan bagi lembaga penegak hukum dan sektor swasta untuk meningkatkan ketahanan terhadap serangan teknologi informasi dan mengurangi potensi kerugian yang diakibatkan oleh kejahatan tersebut. Dengan menyelidiki fenomena kejahatan teknologi informasi dan merinci upaya penanggulangannya, penelitian ini memberikan kontribusi pada pemahaman kita tentang kompleksitas tantangan yang dihadapi oleh Indonesia dalam menghadapi ancaman keamanan siber.

KAJIAN TEORITIS

Dalam konteks kejahatan teknologi informasi (cyber crime), literatur mengidentifikasi sejumlah jenis kejahatan yang semakin merajalela di berbagai negara, termasuk Indonesia. Pencurian identitas, sebagai salah satu bentuk kejahatan teknologi informasi, mencuat sebagai ancaman utama yang dapat mengakibatkan kerugian finansial dan reputasi bagi individu maupun perusahaan (Bocij, 2018). Selain itu, penipuan online menjadi perhatian serius, dengan

metode-metode baru yang terus berkembang, seperti phishing dan social engineering, membingungkan korban dan mengakibatkan kerugian yang signifikan (Holt, T. J., Bossler, A. M., & May, 2019). Keberlanjutan serangan ransomware juga menjadi fokus literatur, dengan penekanan pada potensi dampak serius terhadap sektor bisnis dan infrastruktur kritis (Baryamureeba, 2020).

Dalam upaya menanggulangi kejahatan teknologi informasi, regulasi hukum memegang peran kunci. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia menjadi landasan hukum utama dalam menangani kejahatan di dunia maya (Ramadhan, 2017). Meskipun telah mengalami beberapa amendemen, efektivitas UU ITE dalam menghadapi kejahatan teknologi informasi tetap menjadi subjek perdebatan. Beberapa literatur (Anggraini, 2019) dan (Wijaya, 2020) mencatat bahwa ketidakjelasan dan potensi penyalahgunaan UU ITE telah menimbulkan kekhawatiran terkait kebebasan berekspresi dan hak asasi manusia.

Selain regulasi hukum, literatur juga membahas inisiatif pencegahan dan penanggulangan yang dilakukan oleh pemerintah dan sektor swasta. Upaya-upaya tersebut termasuk peningkatan kapasitas lembaga penegak hukum, kampanye kesadaran masyarakat, dan kerjasama antara pemerintah dan industri (Ismail, 2021). Dalam kerangka ini, literatur menyajikan evaluasi terhadap keefektifan inisiatif-inisiatif ini dan menyoroti tantangan yang dihadapi dalam menghadapi keberlanjutan dan evolusi kejahatan teknologi informasi di Indonesia.

Kajian pustaka ini mengilustrasikan kompleksitas isu kejahatan teknologi informasi dan menyoroti perlunya pendekatan holistik yang melibatkan regulasi hukum yang adaptif, upaya pencegahan yang proaktif, dan kerjasama lintas sektor untuk menghadapi ancaman ini secara efektif.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan analisis data sekunder. Data utama diperoleh dari studi kasus kejahatan teknologi informasi yang terjadi di Indonesia dalam beberapa tahun terakhir. Sumber data melibatkan laporan resmi dari lembaga penegak hukum, dokumen pengadilan, dan publikasi terkait kejahatan teknologi informasi. Analisis data dilakukan melalui proses kategorisasi dan tema, yang memungkinkan identifikasi pola, tren, dan karakteristik dari berbagai kejahatan teknologi informasi. Selain itu, penelitian ini juga melakukan evaluasi terhadap regulasi hukum yang berkaitan dengan kejahatan teknologi informasi di Indonesia. Analisis mendalam dilakukan terhadap Undang-Undang Informasi dan

Transaksi Elektronik (UU ITE) dan peraturan terkait lainnya. Pemahaman kontekstual terhadap perkembangan hukum ini membantu dalam mengevaluasi keefektifan dan kecukupannya dalam menanggapi dinamika kejahatan teknologi informasi.

Adapun untuk mendapatkan perspektif praktis terkait upaya penanggulangan, penelitian ini melakukan wawancara dengan para ahli hukum, perwakilan lembaga penegak hukum, dan pelaku industri teknologi informasi. Wawancara ini bertujuan untuk menggali pandangan dan pengalaman praktis mereka dalam menghadapi dan menanggulangi kejahatan teknologi informasi di Indonesia.

Dengan kombinasi pendekatan kualitatif, analisis data sekunder, dan wawancara, penelitian ini berusaha memberikan gambaran komprehensif tentang kejahatan teknologi informasi di Indonesia serta mengidentifikasi tantangan dan potensi solusi dari perspektif hukum dan praktis. Pendekatan ini diharapkan dapat menyediakan pemahaman mendalam tentang dinamika kompleks kejahatan teknologi informasi dan kontribusi bagi pemikiran kebijakan dan penegakan hukum di masa mendatang.

HASIL DAN PEMBAHASAN

Analisis data sekunder mengungkapkan bahwa kejahatan teknologi informasi di Indonesia telah mengalami peningkatan yang signifikan selama beberapa tahun terakhir. Berdasarkan data dari Kepolisian Republik Indonesia (Polri), terdapat peningkatan sebesar 25% dalam jumlah kasus kejahatan teknologi informasi pada tahun 2023 dibandingkan dengan tahun sebelumnya. Jenis kejahatan yang paling umum melibatkan pencurian identitas, yang mencatatkan lonjakan sebesar 30%, diikuti oleh penipuan online dengan peningkatan 20%. Serangan ransomware juga menunjukkan tren peningkatan yang mencolok, mencapai 15% pada tahun yang sama. Pemeriksaan lebih lanjut terhadap regulasi hukum menunjukkan bahwa Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) telah mengalami beberapa amendemen dalam upaya menanggapi perkembangan kejahatan teknologi informasi. Namun, evaluasi terhadap efektivitas UU ITE menunjukkan bahwa ketidakjelasan dalam beberapa pasal masih menjadi kendala utama. Dari data wawancara dengan ahli hukum, ditemukan bahwa terdapat perbedaan interpretasi dan penegakan hukum yang tidak konsisten terkait dengan UU ITE.

Wawancara dengan para praktisi dan lembaga terkait menggambarkan bahwa upaya penanggulangan kejahatan teknologi informasi terus dilakukan. Namun, data menunjukkan bahwa terdapat kebutuhan mendesak untuk peningkatan kapasitas lembaga penegak hukum. Dari responden wawancara, sekitar 65% menyatakan bahwa kurangnya sumber daya dan

pelatihan yang memadai menjadi hambatan utama dalam menangani kejahatan teknologi informasi. Dengan demikian, hasil penelitian ini menyimpulkan bahwa kejahatan teknologi informasi di Indonesia merupakan tantangan serius yang memerlukan pembaruan dan perbaikan dalam regulasi hukum serta peningkatan kapasitas lembaga penegak hukum. Rekomendasi kebijakan dapat mencakup perubahan lebih lanjut pada UU ITE, peningkatan sumber daya manusia dan teknologi untuk lembaga penegak hukum, serta kampanye kesadaran masyarakat untuk mengurangi risiko kejahatan teknologi informasi.

Peningkatan signifikan dalam kasus kejahatan teknologi informasi di Indonesia, sebagaimana tercermin dari data yang dikumpulkan, menyoroti urgensi untuk mengambil tindakan preventif dan korektif yang lebih serius. Fokus penelitian ini adalah pada evaluasi regulasi hukum, perbandingan dengan tren kejahatan aktual, dan identifikasi tantangan yang dihadapi oleh lembaga penegak hukum.

Pertama, dari segi regulasi hukum, UU ITE telah mengalami beberapa perubahan untuk mencakup perkembangan teknologi dan tantangan baru dalam kejahatan teknologi informasi. Meski demikian, ketidakjelasan dalam beberapa pasal tetap menjadi isu yang perlu diatasi. Rekomendasi pembaharuan lanjutan pada UU ITE perlu dipertimbangkan, dengan menggali masukan dari para ahli hukum dan pemangku kepentingan terkait untuk memastikan kejelasan dan ketepatan regulasi. Kedua, dari analisis data wawancara, terlihat bahwa kurangnya sumber daya dan pelatihan yang memadai bagi lembaga penegak hukum merupakan hambatan serius dalam menangani kejahatan teknologi informasi. Peningkatan investasi dalam pelatihan sumber daya manusia, serta pengadaan teknologi terkini untuk mendukung investigasi dan penegakan hukum, menjadi langkah krusial. Kerjasama antara sektor publik dan swasta juga dapat memainkan peran penting dalam memberikan dukungan dan sumber daya yang dibutuhkan.

Rekomendasi kebijakan dapat mencakup inisiatif untuk meningkatkan kejelasan dan ketepatan UU ITE, mengadakan pelatihan rutin untuk lembaga penegak hukum, serta menggalakkan kolaborasi antara pemerintah, industri, dan masyarakat dalam mendukung upaya penanggulangan kejahatan teknologi informasi. Secara keseluruhan, pembahasan ini menggarisbawahi perlunya pendekatan holistik yang melibatkan perubahan hukum, penguatan kapasitas lembaga, dan partisipasi aktif seluruh lapisan masyarakat untuk menghadapi tantangan kompleks kejahatan teknologi informasi di Indonesia.

KESIMPULAN DAN SARAN

Kesimpulan dari penelitian ini menegaskan bahwa kejahatan teknologi informasi di Indonesia telah mencapai tingkat yang memerlukan perhatian serius dan tindakan proaktif dari pemerintah, lembaga penegak hukum, dan sektor swasta. Peningkatan jumlah kasus, khususnya dalam pencurian identitas dan penipuan online, menciptakan urgensi untuk memperbarui dan memperkuat regulasi hukum. Evaluasi terhadap UU ITE menyoroti perlunya revisi untuk mengatasi ketidakjelasan yang masih ada dan memastikan keberlanjutan dalam menghadapi keberlanjutan dan evolusi kejahatan teknologi informasi.

Saran yang dapat diambil dari penelitian ini mencakup perlunya peningkatan investasi dalam pelatihan dan sumber daya manusia bagi lembaga penegak hukum. Hal ini dapat mencakup program pelatihan yang lebih intensif dalam bidang kejahatan teknologi informasi, serta pengadaan teknologi terkini untuk mendukung investigasi dan penegakan hukum yang efektif. Kerjasama antara sektor publik dan swasta perlu diperkuat untuk memberikan dukungan yang lebih baik dalam menanggulangi ancaman kejahatan teknologi informasi.

Secara keseluruhan, untuk melindungi masyarakat dan perusahaan dari risiko kejahatan teknologi informasi, perubahan regulasi yang cermat dan peningkatan kapasitas lembaga penegak hukum perlu diimplementasikan seiring dengan upaya pencegahan dan kerjasama lintas sektor. Dengan mengadopsi pendekatan holistik ini, diharapkan Indonesia dapat merespons dan menanggulangi kejahatan teknologi informasi dengan lebih efektif dan memastikan keberlanjutan keamanan siber di masa mendatang.

UCAPAN TERIMA KASIH

Kami ingin mengucapkan terima kasih yang tulus kepada semua pihak yang telah turut serta dalam penelitian ini. Terima kasih kepada responden wawancara, ahli hukum, dan perwakilan lembaga penegak hukum yang telah berbagi pengalaman dan wawasan yang berharga. Kami juga menghargai dukungan dari pemerintah, lembaga swasta, dan masyarakat yang telah memberikan data dan kerjasama yang memungkinkan penelitian ini terlaksana.

Ucapan terima kasih juga kami sampaikan kepada rekan-rekan peneliti dan tim penelitian yang telah memberikan kontribusi maksimal dalam mengumpulkan dan menganalisis data. Tanpa kerjasama dan dedikasi mereka, penelitian ini tidak akan mencapai tingkat kedalaman dan keberhasilan yang telah kami raih.

Semua bantuan dan dukungan ini sangat berarti dalam melahirkan hasil penelitian ini. Semoga temuan dan rekomendasi yang dihasilkan dapat memberikan kontribusi positif dalam

upaya mengatasi tantangan kejahatan teknologi informasi di Indonesia. Terima kasih atas kerjasama dan kontribusi berharga dari semua pihak.

DAFTAR REFERENSI

Anggraini, L. (2019). No The Evaluation of Indonesia's Electronic Information and Transactions (ITE) Law. *A Critical Review. International Journal of Cyber Criminology*, *13*(2), 209–224.

Baryamureeba, V. (2020). *Cybersecurity in Africa: An evolving challenge*. Spinger.

Bocij, P. (2018). *Cybercrime: Understanding and addressing the global threat*. Wiley.

Holt, T. J., Bossler, A. M., & May, D. C. (2019). *Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century*. Routledge.

Ismail, I. (2021). Combating Cybercrime in Indonesia: A Multi-stakeholder Approach. *International Journal of Advanced Computer Science and Applications*, *12*(2), 16–23.

Ramadhan, H. (2017). *Regulasi dan Penegakan Hukum Tindak Pidana Teknologi Informasi*. Fikahati Anoragito.

Wijaya, A. D. (2020). Electronic Information and Transactions (ITE) Law in Indonesia: Issues and Challenges. *Journal of Law, Policy and Globalization*, *97*, 121–129.