Volume 1 Nomor 1
Tahun 2024

Lex Researchia

https://jurnal.htp.ac.id/index.php/lex

Dinamika Hukum Dalam Penanganan Kejahatan Siber Di Indonesia

Legal Dynamics in Handling Cyber Crime in Indonesia

Dedy Saputra
Prodi Hukum, Universitas Hang Tuah Pekanbaru
dedysaputra@htp.ac.id

Histori artikel

***Received:* 02-7-2024**

***Accepted*: 16-7-2024**

***Published:* 30-7-2024**

Abstrak
Abstract

Perkembangan teknologi informasi telah membawa perubahan signifikan dalam berbagai aspek kehidupan, termasuk peningkatan aktivitas kejahatan siber. Artikel ini mengkaji perkembangan hukum terkait penanganan kejahatan siber di Indonesia, dengan fokus pada peraturan perundang-undangan yang ada, tantangan implementasi, dan usulan perbaikan untuk memperkuat penegakan hukum di bidang siber. Penelitian ini menggunakan metode yuridis normatif dengan pendekatan studi kasus, mengumpulkan data melalui analisis dokumen hukum, wawancara dengan praktisi hukum dan ahli teknologi, serta studi kasus penanganan kejahatan siber di Indonesia. Hasil penelitian menunjukkan bahwa meskipun sudah ada peraturan yang mengatur kejahatan siber, tantangan dalam hal kapasitas penegak hukum, kesadaran publik, dan kerjasama internasional masih menjadi hambatan utama. Artikel ini memberikan rekomendasi yang mencakup peningkatan pelatihan bagi penegak hukum, penguatan regulasi, dan peningkatan edukasi publik untuk memperkuat sistem penegakan hukum siber di Indonesia..

Kata kunci: ***Kejahatan Siber, Hukum Siber, Penegakan Hukum, Yuridis***

The development of information technology has brought significant changes in various aspects of life, including an increase in cybercrime activities. This article examines legal developments related to handling cyber crime in Indonesia, with a focus on existing laws and regulations, implementation challenges, and proposed improvements to strengthen law enforcement in the cyber sector. This research uses a normative juridical method with a case study approach, collecting data through analysis of legal documents, interviews with legal practitioners and technology experts, as well as case studies on handling cyber crime in Indonesia. The research results show that even though there are regulations governing cybercrime, challenges in terms of law enforcement capacity, public awareness and international cooperation are still the main obstacles. This article provides recommendations that include increasing training for law enforcers, strengthening regulations, and increasing public education to strengthen the cyber law enforcement system in Indonesia.

Keywords: crime, cyber, cyber law,law enforcement, juridical

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah memberikan banyak manfaat yang signifikan bagi masyarakat global, termasuk Indonesia. Teknologi ini telah mengubah cara orang berkomunikasi, bekerja, dan bertransaksi. Namun, di sisi lain, perkembangan ini juga membawa tantangan baru, terutama dalam bentuk kejahatan siber. Kejahatan siber mencakup berbagai kegiatan ilegal yang memanfaatkan teknologi komputer dan internet, seperti pencurian data, penipuan online, peretasan, dan penyebaran konten ilegal.

https://doi.org/10.56466/lex/Vol1.Iss1.1987

Kejahatan siber berbeda dari kejahatan konvensional karena sifatnya yang tidak mengenal batas wilayah dan dapat dilakukan dari jarak jauh dengan menggunakan perangkat teknologi. Hal ini menyebabkan tantangan tersendiri dalam penegakan hukum, karena sering kali melibatkan berbagai yurisdiksi internasional. Selain itu, modus operandi yang digunakan dalam kejahatan siber sangat beragam dan terus berkembang seiring dengan kemajuan teknologi.

Di Indonesia, penanganan kejahatan siber memerlukan pendekatan hukum yang adaptif dan efektif untuk mengatasi ancaman yang terus berkembang. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) No. 11 Tahun 2008, yang kemudian diubah dengan UU No. 19 Tahun 2016, merupakan landasan hukum utama dalam penanganan kejahatan siber di Indonesia. UU ini mencakup berbagai jenis kejahatan siber, seperti pencurian data, penipuan online, dan penyebaran konten ilegal.

Namun, meskipun sudah ada peraturan yang mengatur kejahatan siber, implementasi dan penegakan hukum di lapangan masih menghadapi banyak tantangan. Salah satu tantangan utama adalah keterbatasan kapasitas dan sumber daya penegak hukum dalam menangani kejahatan siber yang kompleks dan seringkali melibatkan berbagai yurisdiksi internasional. Selain itu, kurangnya kesadaran dan edukasi publik tentang risiko kejahatan siber membuat banyak masyarakat Indonesia rentan menjadi korban.

Penelitian ini bertujuan untuk menganalisis perkembangan hukum terkait penanganan kejahatan siber di Indonesia, mengidentifikasi tantangan dalam implementasi peraturan perundang-undangan, dan memberikan rekomendasi untuk memperkuat penegakan hukum di bidang siber. Dengan menggunakan metode yuridis normatif dan pendekatan studi kasus, penelitian ini mengumpulkan data melalui analisis dokumen hukum, wawancara dengan praktisi hukum dan ahli teknologi, serta studi kasus mengenai penanganan kejahatan siber di Indonesia.

Melalui penelitian ini, diharapkan dapat ditemukan solusi yang lebih efektif dalam menangani kejahatan siber di Indonesia, sehingga dapat memberikan perlindungan yang lebih baik bagi masyarakat dan mendukung perkembangan ekonomi digital yang aman dan terpercaya.

METODOLOGI PENELITIAN

Penelitian ini menggunakan metode yuridis normatif dengan pendekatan studi kasus. Data dikumpulkan melalui analisis dokumen hukum, wawancara dengan praktisi hukum dan ahli teknologi, serta studi kasus mengenai penanganan kejahatan siber di Indonesia. Analisis dilakukan untuk mengevaluasi efektivitas peraturan perundang-undangan yang ada dan memberikan rekomendasi untuk memperkuat penegakan hukum.

PEMBAHASAN

1. Perkembangan Peraturan Perundang-Undangan Terkait Kejahatan Siber

https://doi.org/10.56466/lex/Vol1.Iss1.1987

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) No. 11 Tahun 2008, yang kemudian diubah dengan UU No. 19 Tahun 2016, merupakan landasan hukum utama dalam penanganan kejahatan siber di Indonesia. UU ini mencakup berbagai jenis kejahatan siber, seperti pencurian data, penipuan online, dan penyebaran konten ilegal[1].

2. Tantangan dalam Implementasi Hukum Siber

1. Keterbatasan Kapasitas Penegak Hukum Salah satu tantangan utama adalah keterbatasan kapasitas dan sumber daya penegak hukum dalam menangani kejahatan siber yang kompleks dan seringkali melibatkan berbagai yurisdiksi internasional[2].
2. Kurangnya Kesadaran dan Edukasi Publik Banyak masyarakat Indonesia yang masih kurang menyadari risiko kejahatan siber dan cara melindungi diri. Hal ini membuat mereka lebih rentan menjadi korban kejahatan siber[3].

3. Studi Kasus: Penanganan Kejahatan Siber di Indonesia

1. Kasus Penipuan Online Kasus penipuan online yang melibatkan platform e-commerce besar menunjukkan kelemahan dalam sistem pengawasan dan penegakan hukum. Banyak korban yang tidak melaporkan kasus mereka karena merasa prosesnya rumit dan tidak ada jaminan pengembalian dana[4].
2. Kasus Pencurian Data Pencurian data dari beberapa institusi besar di Indonesia menunjukkan pentingnya keamanan siber yang kuat. Kasus ini menyoroti perlunya peraturan yang lebih ketat dan teknologi yang lebih canggih untuk melindungi data sensitif[5].

4. Rekomendasi untuk Memperkuat Penegakan Hukum Siber

1. Peningkatan Kapasitas Penegak Hukum Diperlukan pelatihan dan peningkatan kapasitas bagi penegak hukum untuk memahami teknologi terbaru dan teknik penanganan kejahatan siber[6].
2. Kerjasama Internasional Mengingat kejahatan siber seringkali melibatkan pelaku dari berbagai negara, diperlukan kerjasama internasional yang lebih erat untuk menangani kasus-kasus ini secara efektif[7].
3. Edukasi Publik Meningkatkan kesadaran publik tentang risiko kejahatan siber dan cara melindungi diri sangat penting untuk mencegah meningkatnya jumlah korban[8].

KESIMPULAN

Penelitian ini menunjukkan bahwa meskipun telah ada peraturan perundang-undangan terkait penanganan kejahatan siber di Indonesia, masih banyak tantangan dalam implementasinya. Diperlukan peningkatan kapasitas penegak hukum, kerjasama internasional, dan edukasi publik untuk memperkuat penegakan hukum di bidang siber..

https://doi.org/10.56466/lex/Vol1.Iss1.1987

DAFTAR PUSTAKA

Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). ↩

Simarmata, Rudi. (2020). Tantangan Penegakan Hukum dalam Kasus Kejahatan Siber di Indonesia. Jurnal Hukum dan Teknologi, 17(2), 105-118. ↩

Wicaksono, Ahmad. (2019). Kurangnya Kesadaran Publik tentang Kejahatan Siber di Indonesia. Jurnal Keamanan Informasi, 13(2), 75-85. ↩

Prasetyo, Andi. (2021). Kasus Penipuan Online di Indonesia: Analisis dan Studi Kasus. Jurnal Teknologi Informasi, 17(3), 120-130. ↩

Rahmawati, Siti. (2018). Pencurian Data di Indonesia: Tantangan dan Solusi. Jurnal Keamanan Siber, 10(4), 200-215. ↩

Hardiyanto, Rudi. (2019). Peningkatan Kapasitas Penegak Hukum dalam Penanganan Kejahatan Siber. Jurnal Hukum dan Regulasi, 13(2), 150-165. ↩

Permana, Dian. (2020). Kerjasama Internasional dalam Penanganan Kejahatan Siber. Jurnal Kebijakan Publik, 16(3), 180-195. ↩

Yulianto, Agus. (2022). Edukasi Publik tentang Kejahatan Siber di Indonesia. Jurnal Pendidikan Keamanan Informasi, 14(1), 33-44. ↩