

STUDI PERBANDINGAN HUKUM PIDANA DALAM PENANGANAN KEJAHATAN  
SIBER: PERSPEKTIF INDONESIA DAN AMERIKA SERIKATYunita Sekar Ety Arabel<sup>1</sup>, Ida Musofiana<sup>2</sup><sup>1,2</sup>Prodi Ilmu Hukum, Fakultas Hukum, Universitas Islam Sultan AgungE-mail: [aarabel98@gmail.com](mailto:aarabel98@gmail.com)<sup>1</sup>, [ida.musofiana@unissula.ac.id](mailto:ida.musofiana@unissula.ac.id)<sup>2</sup>

## ABSTRAK

Dalam era globalisasi dan teknologi informasi yang pesat, kejahatan siber menjadi isu utama di seluruh dunia, termasuk di Indonesia dan Amerika Serikat. Penelitian ini bertujuan untuk menganalisis dan membandingkan peraturan dan undang-undang yang mengatur kejahatan siber serta efektivitas penegakan hukum di kedua negara. Di Indonesia, meskipun terdapat Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), tantangan dalam penegakan hukum menghambat efektivitasnya. Sebaliknya, Amerika Serikat memiliki kerangka hukum yang lebih matang dan lembaga penegak hukum yang lebih siap. Penelitian ini juga mempertimbangkan faktor sosial dan budaya yang memengaruhi kebijakan hukum di kedua negara. Hasil penelitian menunjukkan bahwa AS memiliki pendekatan yang lebih efektif dalam menangani kejahatan siber, sementara Indonesia perlu meningkatkan kerangka hukum dan kesadaran masyarakat untuk memperbaiki penanganan kejahatan siber.

**Kata kunci:** Kejahatan Siber, Penegakan Hukum, Indonesia, Amerika Serikat

## Article History

Received: Oktober 2024

Reviewed: Oktober 2024

Published: Oktober 2024

Plagiarism Checker No 234

Prefix DOI : Prefix DOI :

10.8734/CAUSA.v1i2.365

**Copyright : Author****Publish by : CAUSA**

This work is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/).

## PENDAHULUAN

Dalam era globalisasi dan perkembangan teknologi informasi yang pesat, kejahatan siber telah menjadi salah satu isu utama yang dihadapi oleh banyak negara di seluruh dunia. Kejahatan siber mencakup berbagai tindakan ilegal yang dilakukan melalui jaringan komputer dan internet, termasuk pencurian data, penipuan online, penyebaran virus, dan pelanggaran privasi. Dengan semakin banyaknya individu dan organisasi yang bergantung pada teknologi digital, potensi kerugian akibat kejahatan siber juga semakin meningkat. Oleh karena itu, negara perlu merespons ancaman ini dengan kebijakan dan kerangka hukum yang efektif (Ginting, 2024).

Indonesia dan Amerika Serikat (AS) adalah dua negara yang menghadapi tantangan signifikan terkait kejahatan siber, meskipun konteks hukum dan sosial mereka berbeda. Di Indonesia, meskipun terdapat beberapa undang-undang yang mengatur kejahatan siber, seperti Undang-Undang ITE (Informasi dan Transaksi Elektronik), implementasi dan penegakan hukum sering kali terhambat oleh berbagai faktor, termasuk kurangnya sumber daya, pemahaman hukum yang belum merata di masyarakat, dan tantangan dalam kolaborasi antar lembaga penegak hukum. Sementara itu, AS memiliki kerangka hukum yang lebih matang terkait kejahatan siber, dengan berbagai undang-undang federal dan negara bagian yang dirancang

untuk mengatasi isu ini, termasuk Computer Fraud and Abuse Act (CFAA) dan Digital Millennium Copyright Act (DMCA). Penegakan hukum di AS didukung oleh institusi yang kuat dan sumber daya yang memadai, serta adanya kerjasama internasional dalam memerangi kejahatan siber (Dinda, 2024).

Perbedaan ini menciptakan kesempatan untuk menganalisis dan membandingkan pendekatan hukum pidana yang diambil oleh kedua negara dalam menangani kejahatan siber. Melalui studi ini, diharapkan dapat ditemukan praktik terbaik yang dapat diadopsi oleh Indonesia untuk memperbaiki penanganan kejahatan siber di dalam negeri. Dengan membandingkan kerangka hukum, proses penegakan, dan hasil yang dicapai dalam menangani kasus-kasus kejahatan siber, studi ini akan mengidentifikasi kekuatan dan kelemahan masing-masing sistem hukum serta memberikan rekomendasi yang relevan.

Aspek lain yang perlu dipertimbangkan adalah perbedaan dalam budaya dan pandangan masyarakat terhadap kejahatan siber. Di AS, kesadaran masyarakat akan risiko dan dampak kejahatan siber cenderung lebih tinggi, yang berkontribusi pada penegakan hukum yang lebih proaktif. Sebaliknya, di Indonesia, kesadaran dan pemahaman masyarakat tentang kejahatan siber masih terbatas, yang dapat menghambat upaya pencegahan dan penegakan hukum. Penelitian ini akan mengeksplorasi bagaimana faktor-faktor sosial dan budaya ini memengaruhi kebijakan hukum pidana di kedua negara.

Dengan demikian, penelitian ini tidak hanya bertujuan untuk memberikan analisis yang mendalam tentang perbandingan hukum pidana dalam penanganan kejahatan siber antara Indonesia dan Amerika Serikat, tetapi juga untuk memberikan kontribusi pada pengembangan kebijakan yang lebih efektif di Indonesia. Melalui pemahaman yang lebih baik tentang praktik dan pengalaman negara lain, diharapkan dapat dihasilkan rekomendasi yang pragmatis untuk meningkatkan penanganan kejahatan siber di Indonesia, sehingga masyarakat dapat merasa lebih aman dan terlindungi dalam era digital yang terus berkembang (Nurisman, 2023).

## PEMBAHASAN

### 1. Peraturan Dan Undang-Undang Yang Mengatur Kejahatan Siber Di Indonesia Dan Amerika Serikat

Dalam konteks hukum pidana, penanganan kejahatan siber memerlukan perhatian khusus karena karakteristiknya yang unik dan terus berkembang. Salah satu rumusan masalah utama dalam penelitian ini adalah identifikasi peraturan dan undang-undang yang mengatur kejahatan siber di Indonesia dan Amerika Serikat. Di Indonesia, meskipun telah ada Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang diimplementasikan untuk menangani berbagai bentuk kejahatan di dunia maya, terdapat tantangan signifikan dalam penegakan hukum yang efektif. Beberapa isu seperti ambiguitas dalam pengaturan, rendahnya pemahaman masyarakat, dan keterbatasan sumber daya menjadi hambatan utama dalam implementasi hukum. Di sisi lain, Amerika Serikat memiliki kerangka hukum yang lebih matang, dengan berbagai undang-undang seperti Computer Fraud and Abuse Act (CFAA) dan Digital Millennium Copyright Act (DMCA) yang secara khusus ditujukan untuk mengatasi kejahatan siber (Soullier, 2023).

Selain itu, penelitian ini juga bertujuan untuk mengeksplorasi apakah terdapat kesenjangan dalam kebijakan hukum yang dapat memengaruhi efektivitas penegakan hukum. Dengan memahami perbedaan regulasi yang ada, penelitian ini akan

mengidentifikasi elemen-elemen kunci yang dapat menjadi acuan bagi Indonesia dalam mengembangkan kebijakan hukum yang lebih komprehensif dan responsif terhadap tantangan kejahatan siber. Melalui analisis mendalam terhadap kerangka hukum di kedua negara, diharapkan dapat diperoleh wawasan yang dapat berkontribusi pada pengembangan kebijakan dan penegakan hukum yang lebih baik dalam menghadapi kejahatan siber di Indonesia.

Di Indonesia, regulasi yang mengatur kejahatan siber diatur dalam beberapa perundang-undangan, di antaranya adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang kemudian direvisi dengan UU Nomor 19 Tahun 2016. UU ITE mengatur berbagai aspek terkait informasi elektronik dan transaksi, termasuk kejahatan siber seperti penipuan, pencemaran nama baik, dan penyebaran konten ilegal. Selain itu, terdapat Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi dan Undang-Undang Nomor 35 Tahun 2013 tentang Perlindungan Anak, yang juga memiliki ketentuan terkait dengan penggunaan teknologi informasi dalam konteks kejahatan. Namun, meskipun terdapat berbagai regulasi, tantangan dalam implementasi dan penegakan hukum sering kali dihadapi, seperti ambigu dalam definisi, kurangnya sosialisasi kepada masyarakat, dan keterbatasan sumber daya (Leahy, 2022).

Sementara itu, di Amerika Serikat, terdapat sejumlah undang-undang yang secara khusus mengatur kejahatan siber. Salah satu yang paling penting adalah Computer Fraud and Abuse Act (CFAA) yang mengkriminalisasi berbagai tindakan penipuan dan penyalahgunaan komputer. Selain itu, Digital Millennium Copyright Act (DMCA) juga menjadi dasar hukum untuk menangani pelanggaran hak cipta di dunia digital. Undang-undang lainnya, seperti Electronic Communications Privacy Act (ECPA), mengatur privasi dalam komunikasi elektronik. Dalam konteks ini, AS memiliki pendekatan yang lebih terstruktur dan komprehensif dalam penanganan kejahatan siber, didukung oleh lembaga penegak hukum yang lebih siap dan sumber daya yang memadai. Perbedaan dalam kerangka hukum ini menunjukkan bahwa setiap negara memiliki tantangan dan kebijakan yang berbeda dalam menghadapi ancaman kejahatan siber, serta pentingnya kolaborasi internasional dalam mengatasi isu ini.

## **2. Efektivitas Penegakan Hukum Terhadap Kejahatan Siber Di Indonesia Dibandingkan Dengan Amerika Serikat**

Efektivitas penegakan hukum terhadap kejahatan siber di Indonesia dan Amerika Serikat menunjukkan perbedaan yang signifikan, dipengaruhi oleh berbagai faktor, termasuk infrastruktur hukum, sumber daya, dan kesadaran masyarakat. Di Indonesia, meskipun telah ada regulasi yang mengatur kejahatan siber, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), implementasinya seringkali terhambat oleh berbagai tantangan. Salah satu masalah utama adalah kurangnya pemahaman hukum di kalangan masyarakat dan penegak hukum itu sendiri. Banyak individu, baik korban maupun pelaku, yang tidak sepenuhnya menyadari adanya regulasi yang ada, yang mengakibatkan rendahnya pelaporan kejahatan siber. Selain itu, penegakan hukum di Indonesia sering kali terganggu oleh kekurangan sumber daya, baik dari segi tenaga ahli maupun teknologi. Penegakan hukum cenderung lambat, dengan banyak kasus yang tidak terungkap atau terhenti di tengah jalan,

terutama ketika melibatkan pelanggaran yang kompleks, seperti pencurian data atau penipuan online.

Di sisi lain, Amerika Serikat memiliki pendekatan yang lebih sistematis dan terintegrasi dalam penegakan hukum terhadap kejahatan siber. Negara ini memiliki sejumlah lembaga penegak hukum yang khusus menangani kejahatan siber, seperti FBI melalui Cyber Division dan Departemen Keamanan Dalam Negeri (DHS). Selain itu, AS memiliki kerangka hukum yang lebih kuat, didukung oleh undang-undang yang komprehensif seperti Computer Fraud and Abuse Act (CFAA). Dalam hal ini, penegakan hukum lebih responsif dan proaktif, dengan adanya kolaborasi antara berbagai lembaga dan sektor swasta untuk berbagi informasi dan sumber daya (Febriyanti, 2023).

Kesadaran masyarakat di AS mengenai kejahatan siber juga lebih tinggi. Banyak kampanye pendidikan dan pelatihan yang dilakukan untuk meningkatkan pemahaman tentang risiko kejahatan siber dan langkah-langkah pencegahan yang bisa diambil. Hal ini berkontribusi pada tingkat pelaporan yang lebih tinggi dan dukungan bagi penegakan hukum. Meskipun AS memiliki sistem yang lebih matang, tidak berarti bahwa mereka bebas dari tantangan. Isu privasi, penyalahgunaan kekuasaan, dan ketidakadilan dalam penegakan hukum tetap menjadi perhatian. Namun, secara keseluruhan, efektivitas penegakan hukum terhadap kejahatan siber di Amerika Serikat terlihat lebih baik dibandingkan dengan Indonesia. Oleh karena itu, Indonesia perlu melakukan upaya untuk memperbaiki kerangka hukum, meningkatkan kesadaran masyarakat, dan mengoptimalkan sumber daya dalam menangani kejahatan siber secara lebih efektif.

## KESIMPULAN

Penelitian ini menunjukkan perbedaan yang signifikan dalam penanganan kejahatan siber antara Indonesia dan Amerika Serikat. Di Indonesia, meskipun telah ada upaya melalui regulasi seperti UU ITE, tantangan dalam implementasi dan penegakan hukum menghambat efektivitasnya. Kendala seperti kurangnya pemahaman hukum, keterbatasan sumber daya, dan rendahnya kesadaran masyarakat menjadi faktor penghambat. Di sisi lain, Amerika Serikat menunjukkan pendekatan yang lebih sistematis dan terintegrasi, didukung oleh kerangka hukum yang lebih komprehensif dan lembaga penegak hukum yang lebih siap. Kesadaran masyarakat yang lebih tinggi di AS juga berkontribusi pada efektivitas penegakan hukum. Untuk memperbaiki situasi di Indonesia, perlu dilakukan reformasi dalam kerangka hukum, meningkatkan pemahaman masyarakat tentang kejahatan siber, serta meningkatkan kolaborasi antar lembaga penegak hukum. Dengan demikian, diharapkan masyarakat dapat merasa lebih aman dan terlindungi dari ancaman kejahatan siber di era digital ini.

## DAFTAR PUSTAKA

- Dinda, A. L. S. (2024). Efektivitas Penegakan Hukum Terhadap Kejahatan Siber di Indonesia. *AL-DALIL: Jurnal Ilmu Sosial, Politik, dan Hukum*, 2(2), 69-77.
- FEBRIYANTI, D. N. A. (2023). Kekerasan Berbasis Gender Di Pakistan Pada Tahun 2017-2019.
- Ginting, Y. P., Tumbelaka, A. C. G., Yogeta, A., Tjahaja, B. D. O., Hambran, B. F., Gani, M. A., ... & Kimberly, V. (2024). Sosialisasi Perbandingan Hukum Pidana: Tindak Pidana ITE di Indonesia dan Singapura. *Jurnal Pengabdian West Science*, 3(04), 429-442.

- Leahy, G. F. (2022). Keeping Gates Down: Further Narrowing the Computer Fraud and Abuse Act in the Wake of Van Buren. *Wm. & Mary Bus. L. Rev.*, 14, 215.
- Nurisman, E., & Febriyani, E. (2023). KRITIKAL ANALISIS PENEGAKAN HUKUM TERHADAP TINDAK PIDANA CYBER PORNOGRAPHY: KAJIAN PERBANDINGAN HUKUM NEGARA INDONESIA DAN CHINA. *JIL: Journal of Indonesian Law*, 4(2), 115-142.
- Soullier, B. A. (2023). Decriminalizing Trivial Computer Use: The Need to Narrow the Computer Fraud and Abuse Act (CFAA) After Van Buren. *Fed. Comm. LJ*, 76, 239.