

PERBANDINGAN HUKUM PIDANA TERHADAP KEJAHATAN DUNIA MAYA DI INDONESIA DAN AMERIKA SERIKAT

Bielqis Sahara Salsabilah Maharani¹, Nurul Khatama Putri², Suci Rusmiarni³, Septi Emiliyah⁴, Nesta Putra Side⁵, Asep Suherman⁶

^{1,2,3,4,5,6}Universitas Bengkulu

bielqissahara@gmail.com¹, putrinurul4556@gmail.com², sucirusmiarni@gmail.com³, septiemiliyah@gmail.com⁴, sidenestaputra@gmail.com⁵, asepsuherman@unib.ac.id⁶

ABSTRACT; *This study aims to analyze the comparative regulation and application of criminal law against cybercrime in Indonesia and the United States. The method used is normative legal research with a statute approach to analyze the legal provisions in force in both countries. The results of the study indicate that although Indonesia and the United States have regulations to deal with cybercrime, there are differences in the legal approaches applied. Indonesia focuses more on the Electronic Information and Transactions Act (UU ITE), while the United States relies on several laws such as the Computer Fraud and Abuse Act (CFAA) and the Identity Theft and Assumption Deterrence Act. On the other hand, the challenges faced by both countries in enforcing cybercrime law include issues of jurisdiction, international cooperation, and protection of individual privacy rights. This study suggests the need to update the ITE Law in Indonesia, increase the capacity of law enforcement agencies, and strengthen international cooperation to face the growing challenges of cybercrime.*

Keywords: *Cybercrime, Criminal Law, ITE Law, Law Enforcement, International Cooperation.*

ABSTRAK; Penelitian ini bertujuan untuk menganalisis perbandingan pengaturan dan penerapan hukum pidana terhadap kejahatan dunia maya (cybercrime) di Indonesia dan Amerika Serikat. Metode yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan (statute approach) untuk menganalisis ketentuan hukum yang berlaku di kedua negara. Hasil penelitian menunjukkan bahwa meskipun Indonesia dan Amerika Serikat memiliki regulasi untuk menangani cybercrime, terdapat perbedaan dalam pendekatan hukum yang diterapkan. Indonesia lebih fokus pada Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), sementara Amerika Serikat mengandalkan beberapa undang-undang seperti Computer Fraud and Abuse Act (CFAA) dan Identity Theft and Assumption Deterrence Act. Di sisi lain, tantangan yang dihadapi kedua negara dalam penegakan hukum cybercrime termasuk masalah yurisdiksi, kerjasama internasional, serta perlindungan hak privasi individu. Penelitian ini menyarankan perlunya pembaruan UU ITE di Indonesia, peningkatan kapasitas lembaga penegak hukum, dan penguatan kerjasama internasional untuk menghadapi tantangan cybercrime yang semakin berkembang.

Kata Kunci: Cybercrime, Hukum Pidana, UU ITE, Penegakan Hukum, Kerjasama Internasional.

PENDAHULUAN

Perbandingan hukum pidana terhadap kejahatan dunia maya di Indonesia dan Amerika Serikat dapat dilihat dalam konteks perkembangan teknologi informasi yang sangat pesat. Dalam beberapa dekade terakhir, kemajuan teknologi telah membawa revolusi besar dalam berbagai aspek kehidupan masyarakat, baik dalam bidang perdagangan, komunikasi, hingga layanan perbankan. Teknologi informasi, khususnya internet dan komputer, telah memberikan kemudahan bagi masyarakat untuk mengakses informasi, bertransaksi, serta berinteraksi dalam kehidupan sosial dan politik. Namun, di balik kemudahan tersebut, terdapat sisi gelap yang merugikan, yakni munculnya tindak kejahatan dunia maya (cybercrime) yang semakin kompleks dan meresahkan.¹

Di Indonesia, perkembangan teknologi informasi telah mengubah banyak aspek kehidupan, namun juga membuka celah bagi munculnya kejahatan dunia maya. Dalam konteks ini, fenomena seperti penipuan online, peretasan data pribadi, serta penyebaran konten ilegal, seperti pornografi dan ujaran kebencian, semakin sering terjadi. Kejahatan dunia maya ini tidak hanya merugikan individu, tetapi juga dapat merusak integritas sistem keuangan, keamanan nasional, dan moral masyarakat. Hal ini mengarah pada kebutuhan untuk mengembangkan undang-undang yang lebih efektif dalam menanggulangi cybercrime. Meskipun Indonesia telah mengadopsi berbagai peraturan hukum, seperti Undang-Undang Informasi dan Transaksi Elektronik (ITE), implementasi hukum terhadap kejahatan dunia maya masih menghadapi berbagai tantangan, terutama dalam hal penegakan hukum yang seringkali tertinggal dibandingkan dengan perkembangan teknologi.²

Sementara itu, di Amerika Serikat, perkembangan cybercrime juga tidak kalah signifikan. Negara ini memiliki infrastruktur digital yang sangat maju, namun hal ini juga membuka peluang bagi para pelaku kejahatan dunia maya untuk melakukan aksinya. Kejahatan dunia maya di AS melibatkan berbagai bentuk, mulai dari peretasan data pribadi hingga serangan siber terhadap infrastruktur kritis negara. Untuk mengatasi masalah ini,

¹ Anggoro, S. B., Amrullah, M. A., Tanuwijaya, F., & Anggono, B. D. (2024). Perbandingan Sistem Penegakan Hukum Kejahatan Perbankan Di Era Digital Di Negara Maju Dan Berkembang. *Journal of Syntax Literate*, 9(10). https://openurl.ebsco.com/EPDB%3A9%3A20051241/detailv2?sid=ebsco%3Aplink%3Ascholar&id=ebsco%3A9cd%3A180872203&crl=c&link_origin=scholar.google.com

² Rifat, E. M., & Dompok, T. (2025). Hak asasi manusia di era digital: Tantangan dan peluang dalam mengatasi kejahatan siber. *Jurnal Ilmu Multidisiplin*, 3(1), 86-98. <https://multi.risetakademik.com/index.php/jim/article/view/30>

Amerika Serikat telah mengembangkan sejumlah undang-undang yang khusus mengatur kejahatan dunia maya, seperti Computer Fraud and Abuse Act (CFAA) dan Digital Millennium Copyright Act (DMCA). Meskipun demikian, dengan sifat kejahatan dunia maya yang lintas batas negara, penegakan hukum di AS juga menghadapi kesulitan, terutama terkait dengan yurisdiksi dan kerjasama internasional dalam penanganan kasus-kasus tersebut.

Landasan normatif dalam hukum pidana untuk menangani cybercrime di Indonesia diatur dalam beberapa undang-undang, seperti Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), yang kemudian diubah menjadi Undang-Undang No. 19 Tahun 2016. Undang-undang ini memberikan dasar hukum untuk memerangi berbagai bentuk kejahatan yang terjadi di dunia maya, termasuk penipuan, penyebaran informasi palsu, hingga penyalahgunaan data pribadi. Namun, meskipun ada landasan hukum, penegakan hukum terhadap kejahatan dunia maya di Indonesia masih terkendala oleh faktor keterbatasan sumber daya, ketidaktahuan masyarakat, dan kesulitan dalam melacak pelaku yang beroperasi di luar negeri.

Di Amerika Serikat, hukum pidana terhadap kejahatan dunia maya didasarkan pada berbagai peraturan, salah satunya adalah Computer Fraud and Abuse Act (CFAA),³ yang pertama kali diterapkan pada tahun 1986 dan telah mengalami beberapa revisi. Undang-undang ini mengatur tentang tindak pidana yang melibatkan komputer, mulai dari peretasan hingga pencurian identitas. Selain itu, Amerika Serikat juga memiliki Digital Millennium Copyright Act (DMCA) yang mengatur tentang pelanggaran hak cipta di dunia maya.⁴ Landasan normatif ini memberikan kerangka hukum yang cukup lengkap untuk mengatasi berbagai bentuk cybercrime yang terus berkembang.

Isu hukum yang muncul dalam perbandingan antara hukum pidana Indonesia dan Amerika Serikat terkait cybercrime adalah terkait dengan perbedaan pendekatan dalam penegakan hukum, perlindungan data pribadi, serta kerjasama internasional dalam mengatasi kejahatan dunia maya yang sifatnya lintas negara. Di Indonesia, meskipun terdapat berbagai upaya untuk meningkatkan regulasi terkait cybercrime, masih ada kesenjangan antara

³ Soullier, B. A. (2024). Decriminalizing Trivial Computer Use: The Need to Narrow the Computer Fraud and Abuse Act (CFAA) After Van Buren. *Federal Communications Law Journal*, 76(2), 239-269. http://www.fclj.org/wp-content/uploads/2024/01/76.2.2_Decriminalizing-Trivial-Computer-Use-The-Need-to-Narrow-the-Computer-Fraud-and-Abuse-Act-CFAA-After-Van-Buren.pdf

⁴ Rafli, Z. (2024). Examining Legal Precedents and Social Implications-Interplay Between Intellectual Property Rights and Digital Piracy in the Age of DMCA. *Moccasin Journal De Public Perspective*, 1(1), 6-15. <https://gensain.com/index.php/mjdpp/article/view/21>

peraturan yang ada dan implementasinya di lapangan. Selain itu, tantangan utama yang dihadapi adalah keterbatasan dalam hal teknologi dan sumber daya manusia untuk menanggulangi kejahatan dunia maya.

Sementara itu, di Amerika Serikat, meskipun hukum yang ada lebih matang, tantangan utama terletak pada penerapan undang-undang yang bersifat federal namun juga melibatkan yurisdiksi negara bagian. Selain itu, meningkatnya ancaman kejahatan dunia maya yang semakin canggih menuntut adanya kerjasama internasional yang lebih erat untuk mengatasi permasalahan ini secara efektif. Amerika Serikat, sebagai negara yang memiliki pengaruh besar dalam dunia maya, terus berupaya untuk mengembangkan kebijakan dan strategi yang dapat memerangi cybercrime dengan lebih efektif.

Dampak dari kejahatan dunia maya sangat luas, tidak hanya bagi individu yang menjadi korban, tetapi juga bagi sektor ekonomi, keamanan negara, dan kepercayaan masyarakat terhadap teknologi.⁵ Di Indonesia, kejahatan dunia maya yang merugikan ekonomi digital dan menurunkan kepercayaan publik terhadap transaksi elektronik menjadi isu yang perlu segera ditangani. Di sisi lain, Amerika Serikat, yang menjadi pusat kegiatan digital global, menghadapi tantangan besar dalam melindungi data dan informasi pribadi dari serangan siber yang terus berkembang.

Dalam rangka mengatasi masalah tersebut, perlu adanya evaluasi dan pembaruan regulasi yang ada di kedua negara. Penegakan hukum terhadap cybercrime harus dilakukan secara lebih terkoordinasi dan melibatkan kerjasama internasional, mengingat sifat kejahatan dunia maya yang lintas batas. Selain itu, peningkatan kapasitas teknis aparat penegak hukum dan edukasi kepada masyarakat mengenai potensi risiko dan cara perlindungan diri dari kejahatan dunia maya juga sangat penting untuk mengurangi angka kejahatan ini.

Secara keseluruhan, perbandingan hukum pidana terkait cybercrime antara Indonesia dan Amerika Serikat menunjukkan adanya kesamaan dalam tantangan yang dihadapi, meskipun kedua negara memiliki pendekatan hukum yang berbeda. Oleh karena itu, penting untuk terus memperbaharui undang-undang yang ada, serta meningkatkan kerjasama internasional dalam menangani kejahatan dunia maya yang semakin canggih dan merusak.

Rumusan Masalah

⁵ Bego, K. C., Aziz, F. R., & Rahmad, R. A. (2025). Tindak Pidana Cybercrime: Tantangan Hukum Pidana Dalam Menanggulangi Kejahatan Di Dunia Maya. *Jurnal Kolaboratif Sains*, 8(1). <https://www.jurnal.unismuhpalu.ac.id/index.php/JKS/article/view/6740>

1. Bagaimana perbandingan pengaturan dan penerapan hukum pidana terhadap kejahatan dunia maya (cybercrime) di Indonesia dan Amerika Serikat?
2. Bagaimana peran lembaga penegak hukum dalam mengatasi fenomena ini di Indonesia dan Amerika Serikat?

METODE PENELITIAN

Jenis penelitian yang digunakan dalam penelitian ini adalah penelitian hukum normatif, yang bertujuan untuk menganalisis dan menggali norma-norma hukum yang berlaku dalam peraturan perundang-undangan yang mengatur tentang cybercrime di Indonesia dan Amerika Serikat. Penelitian ini lebih berfokus pada kajian terhadap teks-teks hukum yang ada, baik itu yang tercantum dalam undang-undang, peraturan pemerintah, maupun doktrin hukum yang berlaku. Pendekatan penelitian yang diterapkan adalah pendekatan perundang-undangan (statute approach), yang menganalisis ketentuan hukum yang mengatur tentang cybercrime baik di Indonesia maupun di Amerika Serikat untuk membandingkan perbedaan dan persamaan dalam pengaturannya.

Dalam penelitian ini, bahan hukum yang digunakan terdiri dari dua jenis, yaitu bahan hukum primer dan bahan hukum sekunder. Bahan hukum primer mencakup peraturan perundang-undangan yang mengatur tentang cybercrime, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia dan Computer Fraud and Abuse Act (CFAA) di Amerika Serikat. Bahan hukum sekunder mencakup buku-buku, artikel ilmiah, dan pendapat para ahli yang relevan dengan pembahasan penelitian. Bahan hukum tersebut akan digunakan untuk menggali pemahaman yang lebih dalam mengenai pengaturan kejahatan dunia maya di kedua negara serta untuk menganalisis apakah ada perbedaan mendasar dalam pendekatan hukum yang diterapkan.

Analisis bahan hukum dalam penelitian ini dilakukan dengan menggunakan metode interpretasi hukum, yang mencakup penafsiran terhadap teks-teks hukum yang ada serta membandingkannya antara hukum di Indonesia dan di Amerika Serikat. Selain itu, analisis dilakukan secara komparatif untuk melihat kesamaan dan perbedaan dalam pengaturan dan penerapan hukum pidana terhadap kejahatan dunia maya di kedua negara. Dengan pendekatan ini, diharapkan dapat diperoleh gambaran yang jelas mengenai efektivitas peraturan hukum yang ada serta tantangan yang dihadapi dalam penegakan hukum terhadap cybercrime di Indonesia dan Amerika Serikat

HASIL DAN PEMBAHASAN

1. Perbandingan Pengaturan Dan Penerapan Hukum Pidana Terhadap Kejahatan Dunia Maya (Cybercrime) Di Indonesia Dan Amerika Serikat

Perbandingan pengaturan dan penerapan hukum pidana terhadap kejahatan dunia maya (cybercrime) di Indonesia dan Amerika Serikat menunjukkan adanya perbedaan dan persamaan dalam pendekatan hukum terhadap tindak pidana yang terjadi di dunia maya. Kejahatan dunia maya, yang mencakup berbagai jenis pelanggaran seperti peretasan, pencurian data, dan penyebaran konten ilegal, memiliki dampak yang signifikan bagi keamanan nasional, ekonomi, dan privasi individu.⁶ Oleh karena itu, baik Indonesia maupun Amerika Serikat telah mengadopsi kebijakan hukum untuk menangani ancaman ini melalui legislasi yang mengatur transaksi elektronik dan informasi di dunia maya. Meskipun kedua negara ini memiliki kesamaan dalam mengakui pentingnya regulasi terhadap cybercrime, terdapat perbedaan mendasar dalam cara masing-masing negara mengaturnya, terutama dalam hal ruang lingkup, bentuk pelanggaran, dan sanksi hukum yang dikenakan.

Di Indonesia, pengaturan terhadap cybercrime diatur dalam Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (ITE). Undang-Undang ITE ini merupakan perubahan kedua dari UU Nomor 11 Tahun 2008 yang sebelumnya mengatur tentang hal yang sama. Undang-Undang ini berfokus pada pengaturan informasi dan transaksi elektronik serta memberikan dasar hukum untuk menanggulangi berbagai jenis tindak pidana yang terjadi di dunia maya. Salah satu pasal yang sangat relevan dalam pengaturan cybercrime adalah Pasal 27 ayat (3) yang mengatur tentang penyebaran informasi elektronik yang bersifat melanggar kesusilaan. Pasal ini menjadi landasan hukum bagi penindakan terhadap konten pornografi dan penyebaran informasi yang merugikan pihak lain. Selain itu, Pasal 28 ayat (2) UU ITE juga mengatur tentang pencemaran nama baik secara elektronik, yang sering digunakan dalam kasus-kasus penghinaan melalui media sosial.

Penerapan hukum pidana terhadap kejahatan dunia maya di Indonesia seringkali dihadapkan pada tantangan terkait dengan penegakan hukum yang efektif di dunia digital yang

⁶ Pradyanda, A. S., Sibuea, A. M., Khosyi, N. J., & Wijaya, S. H. (2023). Analisis Perbandingan Hukum Pidana Atas Tindak Pidana Pornografi Terhadap Anak Antara Indonesia Dengan Amerika Serikat. *Indonesian Journal of Criminal Law*, 5(1), 18-36. <https://journal.ilinstitute.com/index.php/IJoCL/article/view/2054>

sangat cepat berkembang.⁷ Salah satu tantangan terbesar adalah masalah yurisdiksi, karena pelaku kejahatan dunia maya seringkali beroperasi di luar negeri, yang membuat penegakan hukum menjadi lebih kompleks. Di samping itu, kurangnya pemahaman masyarakat tentang hukum yang berlaku juga menjadi kendala, mengingat banyaknya kasus yang melibatkan pelanggaran terhadap UU ITE yang tidak disertai dengan pemahaman yang cukup tentang hak dan kewajiban dalam dunia digital. Dalam hal ini, penting bagi pemerintah Indonesia untuk terus memperbarui regulasi dan memberikan edukasi kepada masyarakat tentang pentingnya menjaga etika dalam berinteraksi di dunia maya.⁸

Sementara itu, di Amerika Serikat, pengaturan terhadap cybercrime diatur dalam berbagai undang-undang, dengan salah satu yang paling terkenal adalah **Computer Fraud and Abuse Act (CFAA)** yang pertama kali diundangkan pada tahun 1986. Undang-undang ini mengatur berbagai jenis kejahatan terkait dengan komputer, termasuk peretasan, pencurian data, dan penyalahgunaan akses komputer. CFAA telah mengalami beberapa perubahan seiring berjalannya waktu, dengan perubahan signifikan pada tahun 1994, 1996, dan 2001. Dalam CFAA, terdapat pasal yang mengatur tentang akses komputer tanpa izin, yang dapat dikenakan sanksi pidana yang berat. Misalnya, Pasal 1030 yang mengatur tentang akses tanpa izin pada komputer yang dilindungi, yang tidak hanya mencakup peretasan tetapi juga penggunaan komputer untuk tujuan penipuan, pencurian data, dan penyebaran malware.

Salah satu aspek penting yang membedakan pengaturan cybercrime di Amerika Serikat adalah perhatian yang lebih besar terhadap kejahatan yang melibatkan data pribadi dan perlindungan privasi. Undang-undang seperti **Identity Theft and Assumption Deterrence Act** (1998) memberikan dasar hukum untuk melawan pencurian identitas yang terjadi di dunia maya, yang merupakan salah satu bentuk kejahatan yang berkembang pesat di Amerika Serikat⁹. Kejahatan ini biasanya melibatkan penggunaan informasi pribadi seseorang tanpa izin untuk melakukan tindakan penipuan atau pencurian. Selain itu, Amerika Serikat juga memiliki

⁷ Suseno, S., Ramli, A. M., Mayana, R. F., Safiranita, T., & Aurellia Nathania Tiarna, B. (2025). Cybercrime in the new criminal code in Indonesia. *Cogent Social Sciences*, 11(1), 2439543. <https://www.tandfonline.com/doi/full/10.1080/23311886.2024.2439543>

⁸ Imran, M. F. (2023). Cyber Criminology: An analysis of the Indonesian and the United States Police Perception. *International Journal of Cyber Criminology*, 17(2), 250-261. <https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/224>

⁹ Dearden, T. E., Parti, K., & Hawdon, J. (2021). Institutional anomie theory and cybercrime—cybercrime and the American dream, now available online. *Journal of Contemporary Criminal Justice*, 37(3), 311-332. <https://journals.sagepub.com/doi/abs/10.1177/10439862211001590>

undang-undang yang mengatur tentang **cyberbullying** dan konten pornografi anak, yang menjadi isu besar dalam dunia maya. Undang-undang seperti **Child Protection and Obscenity Enforcement Act** (1988) dan **Communications Decency Act** (1996) memberikan dasar hukum untuk menindak penyebaran konten yang merugikan anak-anak, seperti pornografi anak, dan juga mengatur tentang larangan penyebaran materi yang dianggap cabul.

Perbedaan antara Indonesia dan Amerika Serikat dalam pengaturan cybercrime terletak pada pendekatan masing-masing negara dalam mengatasi pelaku yang beroperasi lintas negara. Di Amerika Serikat, dengan kekuatan hukum yang lebih terintegrasi, pemerintah dapat bekerja sama dengan negara-negara lain melalui mekanisme internasional untuk menindak pelaku yang berada di luar yurisdiksi mereka. Sebagai contoh, melalui perjanjian internasional dan kerjasama antara lembaga penegak hukum, seperti yang tercermin dalam **Convention on Cybercrime** yang diadopsi oleh Dewan Eropa pada tahun 2001, Amerika Serikat dapat melakukan ekstradisi atau meminta bantuan hukum kepada negara-negara lain dalam memproses kejahatan dunia maya. Di sisi lain, meskipun Indonesia juga berpartisipasi dalam perjanjian internasional terkait cybercrime, penerapan kerjasama internasional dalam menangani pelaku cybercrime di Indonesia masih terbatas oleh masalah teknis dan birokrasi.

Dari sisi penerapan hukum, di Indonesia, meskipun UU ITE memberikan sanksi yang tegas terhadap pelanggaran yang terjadi di dunia maya, namun implementasi penegakan hukum masih menghadapi berbagai kendala. Salah satu kendala utama adalah kurangnya sumber daya manusia yang terlatih di bidang forensik digital dan teknologi informasi yang dapat mendalami serta mengungkap pelaku cybercrime secara efektif. Selain itu, ada kekhawatiran bahwa UU ITE seringkali digunakan untuk menekan kebebasan berpendapat, terutama dalam kasus penghinaan dan pencemaran nama baik di media sosial. Hal ini menciptakan ketegangan antara perlindungan terhadap individu dan kebebasan berekspresi, yang menjadi isu kontroversial dalam penerapan UU ITE.

Sementara itu, di Amerika Serikat, penerapan hukum terhadap cybercrime cukup ketat dan lebih sistematis. Pemerintah Amerika Serikat memiliki berbagai lembaga yang menangani kejahatan dunia maya, seperti **Federal Bureau of Investigation (FBI)** dan **United States Secret Service**, yang memiliki divisi khusus untuk menangani kejahatan terkait komputer dan informasi. Selain itu, lembaga ini juga bekerja sama dengan lembaga penegak hukum

internasional untuk menangani kejahatan dunia maya yang melibatkan pelaku lintas negara.¹⁰ Dalam hal ini, Amerika Serikat memiliki infrastruktur dan sistem penegakan hukum yang lebih maju dibandingkan dengan Indonesia.

Namun demikian, meskipun Amerika Serikat telah memiliki sistem yang lebih mapan dalam penegakan hukum terhadap cybercrime, tantangan tetap ada. Salah satunya adalah permasalahan mengenai perlindungan data pribadi dan hak asasi manusia, di mana ada kekhawatiran bahwa kebijakan yang terlalu keras dapat mengarah pada pelanggaran privasi individu. Oleh karena itu, meskipun Amerika Serikat memiliki pendekatan yang lebih komprehensif dalam menangani cybercrime, perdebatan mengenai keseimbangan antara keamanan dan privasi tetap menjadi topik yang relevan dalam konteks peraturan yang berlaku.

Secara keseluruhan, meskipun Indonesia dan Amerika Serikat memiliki dasar hukum yang jelas untuk menangani kejahatan dunia maya, terdapat perbedaan dalam hal penerapan hukum dan tantangan yang dihadapi. Indonesia lebih fokus pada regulasi domestik melalui UU ITE, sedangkan Amerika Serikat mengandalkan berbagai undang-undang dan kebijakan yang lebih terintegrasi dengan sistem penegakan hukum yang lebih maju¹¹. Kedua negara menghadapi tantangan yang sama dalam menangani cybercrime yang terus berkembang, terutama terkait dengan aspek teknis, kolaborasi internasional, dan perlindungan hak-hak individu.

2. Peran Lembaga Penegak Hukum Dalam Mengatasi Fenomena Ini Di Indonesia Dan Amerika Serikat

Di Indonesia, peran lembaga penegak hukum dalam mengatasi fenomena cybercrime atau kejahatan siber semakin penting seiring dengan perkembangan teknologi informasi yang pesat. Kejahatan siber di Indonesia, yang meliputi berbagai jenis tindak pidana seperti penipuan online, peretasan, penyebaran konten ilegal, dan penyalahgunaan data pribadi, telah menuntut adanya penyesuaian dalam sistem hukum. Hingga saat ini, sebagian besar kejahatan siber di Indonesia masih diatur secara tidak jelas dalam norma hukum yang berlaku, dengan

¹⁰ Caneppele, S. (2025). Observing, Measuring, and Researching Cybercrime: A Scoping Review of Systematic Reviews Since 2010s. *Understanding Crime Trends in a Hybrid Society*, 101. <https://library.oapen.org/bitstream/handle/20.500.12657/98612/1/9783031723872.pdf#page=111>

¹¹ Oktari, I. (2024). Law Enforcement Policy In Handling Cyber Crime In Indonesia: Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Di Indonesia. *UPMI Proceeding Series*, 2(2), 89-97. <https://upmi-proceeding.com/index.php/ups/article/view/225>

banyaknya penerapan pasal-pasal dalam Kitab Undang-Undang Hukum Pidana (KUHP) yang diberlakukan secara ekstensif. Misalnya, pasal yang mengatur tentang penipuan (Pasal 378 KUHP), pencurian (Pasal 362-367 KUHP), atau penghancuran barang (Pasal 406-412 KUHP) yang digunakan untuk menangani kasus kejahatan siber. Namun, dengan adanya fenomena kejahatan siber yang semakin kompleks, diperlukan sebuah payung hukum yang lebih spesifik dan jelas untuk memfasilitasi penegakan hukum yang lebih efektif.

Seiring dengan tuntutan tersebut, Indonesia telah mengeluarkan Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE) yang menggantikan UU ITE sebelumnya. Undang-Undang ini bertujuan untuk memperkuat pengaturan terhadap transaksi elektronik dan penggunaan teknologi informasi secara aman serta untuk mengatasi masalah kejahatan siber yang terus berkembang. Dalam konteks penegakan hukum, UU ITE terbaru memberikan kewenangan yang lebih jelas kepada lembaga penegak hukum, seperti Kepolisian Negara Republik Indonesia (POLRI), untuk menangani kasus-kasus kejahatan siber, seperti pemerasan online, penyebaran konten negatif, dan pencurian data pribadi. Penegakan hukum dalam kasus kejahatan siber di Indonesia masih menghadapi berbagai tantangan, termasuk kurangnya kapasitas sumber daya manusia yang terlatih, keterbatasan teknologi yang dimiliki oleh lembaga penegak hukum, serta minimnya pemahaman masyarakat mengenai bahaya dan dampak dari kejahatan siber. Oleh karena itu, penegak hukum di Indonesia memerlukan sinergi yang lebih baik dengan berbagai pihak, baik itu pemerintah, sektor swasta, maupun masyarakat untuk mengoptimalkan penanganan kasus cybercrime ini.¹²

Selain itu, salah satu aspek penting yang menjadi perhatian dalam penegakan hukum terhadap kejahatan siber adalah adanya hambatan dalam hal kerjasama internasional. Kejahatan siber sering kali bersifat lintas negara, sehingga penegakan hukum yang efektif membutuhkan kerjasama antara lembaga penegak hukum dari berbagai negara. Misalnya, Indonesia dapat bekerja sama dengan negara-negara lain yang memiliki sistem hukum yang lebih maju dalam hal pengaturan dan penanggulangan kejahatan siber. Dengan adanya kerjasama ini, informasi yang diperoleh dari penyidikan di negara lain dapat digunakan untuk mempercepat proses penegakan hukum di Indonesia. Namun, kerjasama internasional ini

¹² Judijanto, L. (2025). Hukum Pidana dan Kejahatan Siber:: Menanggulangi Ancaman Kejahatan Digital di Era Teknologi. Indonesian Research Journal on Education, 5(1), 968-972. <https://www.irje.org/irje/article/view/2114>

masih dibatasi oleh perbedaan regulasi yang ada di masing-masing negara, serta adanya kendala dalam hal pengaturan hukum yang dapat menyulitkan proses ekstradisi tersangka atau pertukaran bukti yang sah. Oleh karena itu, perlu adanya pembaharuan dan harmonisasi peraturan hukum di tingkat internasional untuk memudahkan penegakan hukum terhadap kejahatan siber di seluruh dunia.

Di Amerika Serikat, peran lembaga penegak hukum dalam menangani kejahatan siber juga sangat penting dan telah didukung oleh regulasi yang sangat spesifik mengenai cybercrime. Negara ini telah memiliki berbagai undang-undang dan kebijakan yang diadaptasi untuk menangani fenomena ini, salah satunya adalah Computer Fraud and Abuse Act (CFAA) yang telah diberlakukan sejak tahun 1986. Undang-Undang ini memberi kewenangan kepada lembaga penegak hukum, seperti Federal Bureau of Investigation (FBI) dan United States Secret Service (USSS), untuk menyelidiki dan menindak kejahatan siber di seluruh negara.¹³ Amerika Serikat, sebagai negara yang sangat maju dalam hal teknologi dan sistem informasi, telah membuat berbagai upaya untuk melindungi warganya dari ancaman kejahatan siber yang semakin canggih dan meluas. Berbagai jenis kejahatan siber seperti peretasan (hacking), pencurian identitas, dan penipuan online, menjadi fokus utama dalam kebijakan penegakan hukum di negara ini.

Seiring dengan perkembangan teknologi dan semakin kompleksnya modus operandi yang digunakan oleh pelaku kejahatan siber, lembaga penegak hukum di Amerika Serikat terus melakukan pembaruan dan penyesuaian dalam regulasi dan pendekatan penanganannya. Pada tahun 2002, Amerika Serikat juga mengeluarkan Cybersecurity Enhancement Act yang mengatur mengenai perlindungan data pribadi dan sistem informasi kritis dari ancaman kejahatan siber. Lembaga penegak hukum di Amerika Serikat, seperti FBI dan USSS, memiliki unit khusus yang menangani kejahatan siber yang terorganisir dan memiliki tingkat keahlian yang tinggi dalam menangani kasus-kasus yang melibatkan teknologi canggih, seperti peretasan terhadap sistem infrastruktur kritis, pencurian data perusahaan besar, hingga serangan ransomware. Selain itu, lembaga ini juga berkoordinasi dengan lembaga-lembaga internasional seperti Interpol dan Europol untuk menghadapi ancaman kejahatan siber yang bersifat lintas negara.

¹³ Buçaj, E., & Idrizaj, K. (2025). The need for cybercrime regulation on a global scale by the international law and cyber convention. *Multidisciplinary Reviews*, 8(1), 2025024-2025024. <https://www.malque.pub/ojs/index.php/mr/article/view/5348>

Namun, meskipun Amerika Serikat memiliki sistem hukum yang sangat terstruktur dan lembaga penegak hukum yang terlatih, mereka juga menghadapi tantangan besar dalam menangani kejahatan siber. Salah satunya adalah ancaman dari serangan siber yang semakin canggih dan terus berkembang, seperti serangan denial of service (DDoS), serangan ransomware yang menargetkan perusahaan dan lembaga pemerintahan, serta penipuan melalui cryptocurrency. Selain itu, permasalahan privasi data juga menjadi isu penting, mengingat adanya konflik antara upaya penegakan hukum dan perlindungan hak privasi individu. Dalam beberapa kasus, lembaga penegak hukum di Amerika Serikat harus menyeimbangkan antara melakukan penyelidikan dan perlindungan terhadap data pribadi yang ada pada korban atau pelaku. Hal ini sering kali menimbulkan dilema terkait dengan hak privasi dan kebebasan individu versus kebutuhan untuk melindungi keamanan negara dan masyarakat dari ancaman kejahatan siber yang semakin kompleks.

Lembaga penegak hukum di kedua negara ini, Indonesia dan Amerika Serikat, juga menghadapi tantangan terkait dengan keterbatasan sumber daya manusia dan teknologi yang dimiliki dalam menghadapi ancaman kejahatan siber yang terus berkembang.¹⁴ Baik di Indonesia maupun di Amerika Serikat, terdapat kebutuhan yang mendesak untuk meningkatkan kapasitas lembaga penegak hukum dalam hal pelatihan personel, pengembangan teknologi, dan pemahaman mengenai berbagai jenis kejahatan siber yang dapat terjadi. Di Indonesia, meskipun UU ITE terbaru memberikan landasan hukum yang lebih kuat, tetapi masih terdapat kendala dalam hal implementasi, baik dari sisi regulasi maupun dari sisi fasilitas dan teknologi yang dimiliki oleh aparat penegak hukum. Oleh karena itu, penting untuk terus melakukan peningkatan kapasitas dalam hal ini agar dapat menanggulangi kejahatan siber secara lebih efektif.¹⁵

Di sisi lain, kerjasama internasional juga memainkan peranan yang sangat penting dalam memerangi kejahatan siber, baik di Indonesia maupun di Amerika Serikat. Kejahatan siber yang sering kali bersifat lintas negara memerlukan koordinasi yang kuat antara negara-negara

¹⁴ Nabila, A. P., Manabung, N. A., & Ramadhansha, A. C. (2024). Peran Hukum Internasional Dalam Menanggulangi Cyber Crime Pada Kejahatan Transnasional. *Indonesian Journal of Law*, 1(1), 26-37. <https://jurnal.intekom.id/index.php/inlaw/article/view/290>

¹⁵ Putri, E. H. A. D., Kasim, R., & Nurmala, L. D. (2024). Analisis Yuridis Terhadap Penegakan dan Pengaturan Hukum Kejahatan Dunia Maya (Cybercrime) di Indonesia. *ALADALAH: Jurnal Politik, Sosial, Hukum dan Humaniora*, 2(3), 102-111. <https://ejurnalqarnain.stisnq.ac.id/index.php/ALADALAH/article/view/865>

yang terlibat, baik melalui kerjasama antara lembaga penegak hukum maupun dalam bentuk perjanjian internasional. Sebagai contoh, di Amerika Serikat, lembaga penegak hukum bekerja sama dengan Interpol dan Europol dalam melakukan investigasi kasus-kasus yang melibatkan pelaku kejahatan siber dari negara lain. Di Indonesia, meskipun kerjasama internasional ini masih dalam tahap pengembangan, namun sudah ada upaya-upaya untuk memperkuat koordinasi dengan negara-negara lain guna memerangi kejahatan siber yang semakin berkembang.

Dengan demikian, dapat disimpulkan bahwa meskipun Indonesia dan Amerika Serikat telah memiliki regulasi yang mendukung dalam penegakan hukum terhadap kejahatan siber, masih ada tantangan besar yang harus dihadapi dalam hal implementasi, pengembangan kapasitas lembaga penegak hukum, serta kerjasama internasional. Penanganan yang efektif terhadap kejahatan siber memerlukan kesadaran yang tinggi dari seluruh pihak yang terlibat, baik pemerintah, lembaga penegak hukum, maupun masyarakat luas, untuk bersama-sama melawan ancaman yang ada demi menciptakan dunia maya yang aman dan terlindungi

KESIMPULAN DAN SARAN

Kesimpulan

1. Perbandingan pengaturan dan penerapan hukum pidana terhadap kejahatan dunia maya di Indonesia dan Amerika Serikat menunjukkan adanya persamaan dan perbedaan mendasar. Kedua negara mengakui pentingnya regulasi dalam menangani cybercrime, namun Indonesia lebih fokus pada UU ITE yang mengatur transaksi elektronik dan informasi di dunia maya, sementara Amerika Serikat menggunakan berbagai undang-undang seperti Computer Fraud and Abuse Act (CFAA) dan Identity Theft and Assumption Deterrence Act. Meski demikian, kedua negara menghadapi tantangan terkait penegakan hukum, terutama dalam hal yurisdiksi, kerjasama internasional, dan perlindungan hak-hak individu.
2. Peran lembaga penegak hukum dalam mengatasi fenomena cybercrime di Indonesia dan Amerika Serikat sangat penting dan memiliki tantangan tersendiri. Di Indonesia, meskipun sudah ada UU ITE yang memberikan kewenangan kepada lembaga penegak hukum seperti POLRI, penegakan hukum masih terbentur dengan keterbatasan kapasitas SDM dan teknologi serta masalah kerjasama internasional. Sementara di Amerika Serikat, lembaga penegak hukum seperti FBI dan USSS telah memiliki regulasi yang

lebih terintegrasi dan infrastruktur yang lebih maju, meskipun tetap menghadapi tantangan dalam melindungi privasi individu serta mengatasi kejahatan lintas negara.

Saran

1. Penting bagi Indonesia untuk terus memperbarui UU ITE dan meningkatkan kapasitas lembaga penegak hukum melalui pelatihan dan penguatan teknologi informasi agar mampu menanggulangi kejahatan dunia maya dengan lebih efektif. Selain itu, kerjasama internasional dalam penanganan cybercrime perlu ditingkatkan, dengan mengadopsi mekanisme yang lebih efisien untuk memproses pelaku yang berada di luar yurisdiksi Indonesia.
2. Di Indonesia, peran lembaga penegak hukum dalam menghadapi kejahatan siber harus diperkuat dengan penambahan pelatihan bagi aparat penegak hukum serta penguatan kerjasama internasional untuk mempercepat penanganan kasus kejahatan dunia maya. Selain itu, pemerintah perlu menyusun peraturan yang lebih harmonis dengan negara lain agar memudahkan proses ekstradisi dan pertukaran bukti dalam kasus kejahatan lintas negara.

DAFTAR PUSTAKA

- Anggoro, S. B., Amrullah, M. A., Tanuwijaya, F., & Anggono, B. D. (2024). Perbandingan sistem penegakan hukum kejahatan perbankan di era digital di negara maju dan berkembang. *Journal of Syntax Literate*, 9(10). https://openurl.ebsco.com/EPDB%3Aagcd%3A9%3A2005124%201/detailv2?sid=ebsco%3Aplink%3Ascholar&id=ebsco%3Aagcd%3A180872203&crl=c&link_origin=scholar.google.com
- Bego, K. C., Aziz, F. R., & Rahmad, R. A. (2025). Tindak pidana cybercrime: Tantangan hukum pidana dalam menanggulangi kejahatan di dunia maya. *Jurnal Kolaboratif Sains*, 8(1). <https://www.jurnal.unismuhpalu.ac.id/index.php/JKS/article/view/6740>
- Buçaj, E., & Idrizaj, K. (2025). The need for cybercrime regulation on a global scale by international law and cyber convention. *Multidisciplinary Reviews*, 8(1), 2025024-2025024. <https://www.malque.pub/ojs/index.php/mr/article/view/5348>
- Caneppele, S. (2025). Observing, measuring, and researching cybercrime: A scoping review of systematic reviews since the 2010s. In *Understanding Crime Trends in a Hybrid Society* (p. 101).

<https://library.oapen.org/bitstream/handle/20.500.12657/98612/1/9783031723872.pdf#page=111>

- Dearden, T. E., Parti, K., & Hawdon, J. (2021). Institutional anomie theory and cybercrime—cybercrime and the American dream, now available online. *Journal of Contemporary Criminal Justice*, 37(3), 311-332. <https://journals.sagepub.com/doi/abs/10.1177/10439862211001590>
- Imran, M. F. (2023). Cyber criminology: An analysis of the Indonesian and the United States police perception. *International Journal of Cyber Criminology*, 17(2), 250-261. <https://cybercrimejournal.com/manuscript/index.php/cybercrimejournal/article/view/224>
- Judijanto, L. (2025). Hukum pidana dan kejahatan siber: Menanggulangi ancaman kejahatan digital di era teknologi. *Indonesian Research Journal on Education*, 5(1), 968-972. <https://www.irje.org/irje/article/view/2114>
- Marzuki, Peter Mahmud, Penelitian Hukum. Cet 2, Jakarta : Kencana, 2008.
- Nabila, A. P., Manabung, N. A., & Ramadhansha, A. C. (2024). Peran hukum internasional dalam menanggulangi cybercrime pada kejahatan transnasional. *Indonesian Journal of Law*, 1(1), 26-37. <https://jurnal.intekom.id/index.php/inlaw/article/view/290>
- Oktari, I. (2024). Law enforcement policy in handling cybercrime in Indonesia: Kebijakan penegakan hukum dalam upaya penanganan cybercrime di Indonesia. *UPMI Proceeding Series*, 2(2), 89-97. <https://upmi-proceeding.com/index.php/ups/article/view/225>
- Pradyanda, A. S., Sibuea, A. M., Khosyi, N. J., & Wijaya, S. H. (2023). Analisis perbandingan hukum pidana atas tindak pidana pornografi terhadap anak antara Indonesia dengan Amerika Serikat. *Indonesian Journal of Criminal Law*, 5(1), 18-36. <https://journal.ilinstitute.com/index.php/IJoCL/article/view/2054>
- Putri, E. H. A. D., Kasim, R., & Nurmala, L. D. (2024). Analisis yuridis terhadap penegakan dan pengaturan hukum kejahatan dunia maya (cybercrime) di Indonesia. *ALADALAH: Jurnal Politik, Sosial, Hukum dan Humaniora*, 2(3), 102-111. <https://ejurnalqarnain.stisnq.ac.id/index.php/ALADALAH/article/view/865>
- Rafli, Z. (2024). Examining legal precedents and social implications: Interplay between intellectual property rights and digital piracy in the age of DMCA. *Moccasin Journal De Public Perspective*, 1(1), 6-15. <https://gensain.com/index.php/mjdpp/article/view/21>

- Rif'at, E. M., & Dompok, T. (2025). Hak asasi manusia di era digital: Tantangan dan peluang dalam mengatasi kejahatan siber. *Jurnal Ilmu Multidisiplin*, 3(1), 86-98. <https://multi.risetakademik.com/index.php/jim/article/view/30>
- Soullier, B. A. (2024). Decriminalizing trivial computer use: The need to narrow the Computer Fraud and Abuse Act (CFAA) after Van Buren. *Federal Communications Law Journal*, 76(2), 239-269. http://www.fclj.org/wp-content/uploads/2024/01/76.2.2_Decriminalizing-Trivial-Computer-Use-The-Need-to-Narrow-the-Computer-Fraud-and-Abuse-Act-CFAA-After-Van-Buren.pdf
- Suseno, S., Ramli, A. M., Mayana, R. F., Safiranita, T., & Aurellia Nathania Tiarma, B. (2025). Cybercrime in the new criminal code in Indonesia. *Cogent Social Sciences*, 11(1), 2439543. <https://www.tandfonline.com/doi/full/10.1080/23311886.2024.2439543>.