CAUSA
ISSN 3031-0369

Jurnal Hukum dan Kewarganegaraan
Vol. 10 No. 12 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

SISTEM PEMIDANAAN TINDAK PIDANA CYBERCRIME DI INDONESIA DAN AMERIKA SERIKAT: STUDI PERBANDINGAN HUKUM PIDANA

Aurelia Salsabila
Universitas Bengkulu
aurelisalsabila004@gmail.com

Abstrak

Perkembangan teknologi digital telah meningkatkan jumlah kejahatan siber (cybercrime) yang mengancam individu, institusi, dan negara. Indonesia dan Amerika Serikat memiliki sistem pemidanaan cybercrime yang berbeda berdasarkan hukum yang berlaku di masing-masing negara. Penelitian ini bertujuan untuk menganalisis perbedaan sistem pemidanaan cybercrime di kedua negara serta faktor yang mempengaruhi penerapannya. Metode yang digunakan adalah penelitian hukum normatif dengan pendekatan perbandingan hukum, yang menelaah regulasi seperti UU ITE di Indonesia dan Computer Fraud and Abuse Act di Amerika Serikat. Hasil penelitian menunjukkan bahwa Indonesia masih menghadapi kendala dalam penegakan hukum cybercrime, seperti kurangnya alat bukti elektronik dan keterbatasan sumber daya manusia yang ahli di bidang forensik digital. Sementara itu, Amerika Serikat memiliki regulasi lebih spesifik serta lembaga penegak hukum yang lebih siap menangani kejahatan siber. Selain itu, Amerika Serikat menerapkan mekanisme plea bargaining yang memungkinkan terdakwa bekerja sama dengan aparat hukum untuk meringankan hukuman.

Kata Kunci: cybercrime, sistem pemidanaan, perbandingan hukum, Indonesia, Amerika Serikat.

Abstract

The advancement of digital technology has led to a rise in cybercrime, posing threats to individuals, institutions, and nations. Indonesia and the United States have different cybercrime sentencing systems based on their respective legal frameworks. This study aims to analyze the differences in cybercrime sentencing between the two countries and the factors influencing its implementation. The research method used is normative legal research with a comparative law approach, examining regulations such as Indonesia's Electronic Information and Transactions Law (UU ITE) and the United States' Computer Fraud and Abuse Act (CFAA). The findings reveal that Indonesia faces challenges in enforcing cybercrime laws, including a lack of electronic evidence and limited expertise in digital forensics. In contrast, the United States has more specific regulations and law enforcement agencies better equipped to handle cybercrime. Additionally, the U.S. employs a plea-bargaining mechanism that allows defendants to

Article History
Received: February 2025
Reviewed: February 2025
Published: February 2025
Plagirism Checker No 234
Prefix DOI : Prefix DOI : 10.8734/CAUSA.v1i2.365
Copyright : Author
Publish by : CAUSA

cooperate with law enforcement in exchange for reduced sentences. This study concludes that Indonesia can learn from the U.S.
***Keywords**: cybercrime, sentencing system, legal comparison, Indonesia, United States*

LATAR BELAKANG

Perkembangan teknologi informasi dan komunikasi yang pesat telah membawa perubahan besar dalam berbagai aspek kehidupan, termasuk dalam dunia kejahatan. Digitalisasi yang semakin luas membuka peluang bagi munculnya bentuk-bentuk kejahatan baru yang dilakukan melalui dunia maya, yang dikenal dengan istilah cybercrime. Kejahatan siber ini meliputi berbagai tindak pidana, seperti pencurian data pribadi, penipuan daring (online fraud), peretasan (hacking), penyebaran malware, hingga tindak pidana pencucian uang melalui sistem digital. Fenomena ini tidak hanya terjadi di Indonesia, tetapi juga di berbagai negara, termasuk Amerika Serikat. Seiring dengan meningkatnya intensitas kejahatan siber, sistem pemidanaan terhadap pelaku cybercrime menjadi isu hukum yang krusial dan perlu mendapatkan perhatian lebih dalam konteks perbandingan hukum antara Indonesia dan Amerika Serikat.[1]

Di Indonesia, fenomena cybercrime semakin marak seiring dengan meningkatnya jumlah pengguna internet. Menurut laporan We Are Social dan Hootsuite (2023), jumlah pengguna internet di Indonesia mencapai lebih dari 212 juta orang, yang berarti lebih dari 77% penduduk telah terhubung dengan internet. Namun, di balik kemajuan ini, angka kejahatan siber juga meningkat drastis. Pusat Operasi Keamanan Siber Nasional (National Cyber Security Operations Center/NCSOC) Badan Siber dan Sandi Negara (BSSN) mencatat lebih dari 700 juta serangan siber sepanjang tahun 2022. Bentuk-bentuk cybercrime yang sering terjadi di Indonesia meliputi pembobolan rekening bank, pencurian data pribadi, penyebaran hoaks, hingga kejahatan berbasis fintech seperti pinjaman online ilegal.

Dampak dari kejahatan siber di Indonesia sangat signifikan, baik terhadap individu, lembaga keuangan, perusahaan, hingga sektor pemerintahan. Salah satu contoh nyata adalah kasus dugaan kebocoran data 1,3 miliar SIM card pengguna di Indonesia pada tahun 2022, yang diduga melibatkan peretasan terhadap sistem Direktorat Jenderal Kependudukan dan Pencatatan Sipil (Dukcapil). Selain itu, maraknya kasus scamming dan phishing juga menyebabkan kerugian finansial yang besar bagi masyarakat. Dengan meningkatnya jumlah kejahatan siber, sistem pemidanaan terhadap pelaku cybercrime di Indonesia masih menghadapi tantangan, terutama dalam hal efektivitas penegakan hukum dan ketepatan sanksi pidana.[2]

Dalam aspek hukum, landasan normatif sistem pemidanaan cybercrime di Indonesia diatur dalam beberapa peraturan perundang-undangan, seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016, serta beberapa ketentuan dalam Kitab Undang-Undang Hukum Pidana (KUHP) dan Kitab Undang-Undang Hukum Acara Pidana (KUHAP). Selain itu, terdapat peraturan sektoral lain, seperti Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, yang juga berperan dalam mengatur aspek kejahatan siber. Namun, meskipun telah memiliki kerangka hukum yang cukup lengkap, Indonesia masih menghadapi berbagai kendala dalam penerapan sistem pemidanaan terhadap

[1] Gojali, D. S. (2023). Identifying the Prevalence of Cybercrime in Indonesian Corporations: A Corporate Legislation Perspective. *International Journal of Cyber Criminology*, *17*(1), 1-11.

[2] Imran, M. F. (2023). Preventing and Combating Cybercrime in Indonesia. *International Journal of Cyber Criminology*, *17*(1), 223-235.

Jurnal Hukum dan Kewarganegaraan
Vol. 10 No. 12 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

pelaku cybercrime, seperti kesulitan dalam pembuktian, keterbatasan alat bukti elektronik, kurangnya koordinasi antar lembaga penegak hukum, serta lemahnya kerja sama internasional dalam menangani kejahatan lintas negara.

Sementara itu, di Amerika Serikat, sistem pemidanaan terhadap pelaku cybercrime jauh lebih berkembang dan memiliki mekanisme yang lebih kompleks. Negara ini memiliki berbagai undang-undang yang secara khusus mengatur kejahatan siber, di antaranya Computer Fraud and Abuse Act (CFAA) tahun 1986, Electronic Communications Privacy Act (ECPA) tahun 1986, serta Cybersecurity Information Sharing Act (CISA) tahun 2015. Selain itu, Federal Bureau of Investigation (FBI), Department of Justice (DOJ), dan Cybersecurity and Infrastructure Security Agency (CISA) memiliki peran besar dalam menangani kasus-kasus kejahatan siber, termasuk dalam aspek investigasi dan pemidanaan. Amerika Serikat memiliki pendekatan yang lebih tegas dalam memberikan sanksi terhadap pelaku cybercrime. Dalam beberapa kasus besar, pelaku kejahatan siber dijatuhi hukuman berat, seperti hukuman penjara puluhan tahun dan denda jutaan dolar. Sebagai contoh, dalam kasus hacking yang dilakukan oleh kelompok kejahatan siber terhadap Equifax pada tahun 2017, para pelaku diancam dengan hukuman hingga 20 tahun penjara, mengingat besarnya dampak yang ditimbulkan, yaitu kebocoran data lebih dari 147 juta warga Amerika.

Sistem pemidanaan di Amerika Serikat juga menerapkan pendekatan berbasis deterrence (efek jera) dengan menjatuhkan hukuman berat kepada pelaku untuk mencegah kejahatan serupa terjadi di masa mendatang. Selain itu, terdapat mekanisme plea bargaining, di mana terdakwa dapat mengurangi masa hukuman dengan bekerja sama dalam investigasi atau mengungkap jaringan kejahatan yang lebih besar. Hal ini berbeda dengan sistem di Indonesia yang cenderung masih bergantung pada hukum pidana klasik, tanpa adanya mekanisme yang fleksibel seperti plea bargaining dalam proses hukum pidana siber. Dari perbandingan di atas, terlihat bahwa terdapat perbedaan signifikan dalam sistem pemidanaan tindak pidana cybercrime antara Indonesia dan Amerika Serikat. Beberapa perbedaan utama terletak pada kerangka hukum, efektivitas penegakan hukum, sistem sanksi, serta kerja sama internasional dalam menangani kejahatan siber lintas negara. Indonesia masih menghadapi tantangan besar dalam meningkatkan efektivitas sistem pemidanaannya, terutama dalam aspek penegakan hukum, penyempurnaan regulasi, serta peningkatan kapasitas aparat penegak hukum dalam menangani kasus-kasus siber yang semakin kompleks.[3]

Isu hukum yang muncul dalam sistem pemidanaan cybercrime di Indonesia mencakup beberapa aspek penting, antara lain ketidakpastian hukum dalam regulasi cybercrime, kurangnya efektivitas dalam sistem pembuktian kejahatan siber, lemahnya koordinasi antar lembaga penegak hukum, serta belum optimalnya kerja sama internasional dalam menangani cybercrime lintas negara. UU ITE, sebagai regulasi utama terkait kejahatan siber di Indonesia, masih kerap menimbulkan multitafsir dan kontroversi dalam penerapannya. Selain itu, sistem pembuktian yang masih bergantung pada alat bukti elektronik sering kali menghadapi kendala dalam verifikasi, sementara koordinasi antar lembaga, seperti Polri, Kementerian Kominfo, dan BSSN, masih belum berjalan optimal dalam menangani kejahatan siber secara terpadu. Dari perspektif perbandingan hukum, sistem pemidanaan di Amerika Serikat dapat menjadi bahan evaluasi bagi Indonesia dalam meningkatkan efektivitas hukum pidana siber. Beberapa langkah yang dapat diadaptasi dari sistem hukum Amerika Serikat antara lain penguatan regulasi cybercrime, peningkatan kapasitas aparat penegak hukum, penerapan mekanisme plea

[3] Nugroho, A., & Chandrawulan, A. A. (2022). Research synthesis of cybercrime laws and COVID-19 in Indonesia: lessons for developed and developing countries. *Security Journal*, 1.

Jurnal Hukum dan Kewarganegaraan
Vol. 10 No. 12 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

bargaining, serta penguatan kerja sama internasional dalam menangani kejahatan siber lintas negara.[4]

RUMUSAN MASALAH

1. Bagaimana Sistem Pemidanaan Tindak Pidana Cybercrime Di Indonesia Dan Amerika Serikat Diterapkan Berdasarkan Hukum Yang Berlaku?
2. Mengapa Terdapat Perbedaan Dalam Sistem Pemidanaan Tindak Pidana Cybercrime Antara Indonesia Dan Amerika Serikat?

METODE PENELITIAN HUKUM

Metode penelitian yang digunakan dalam kajian mengenai sistem pemidanaan tindak pidana cybercrime di Indonesia dan Amerika Serikat ini adalah penelitian hukum normatif. Menurut Peter Mahmud Marzuki dalam bukunya Penelitian Hukum (2017), penelitian hukum normatif dilakukan dengan cara meneliti bahan hukum yang terdiri dari peraturan perundang-undangan, putusan pengadilan, doktrin, serta prinsip-prinsip hukum yang relevan. Pendekatan yang digunakan dalam penelitian ini adalah pendekatan perundang-undangan (statute approach), pendekatan perbandingan (comparative approach), dan pendekatan konseptual (conceptual approach). Pendekatan perundang-undangan digunakan untuk menganalisis regulasi yang mengatur sistem pemidanaan cybercrime di Indonesia dan Amerika Serikat, sedangkan pendekatan perbandingan digunakan untuk membandingkan efektivitas penerapan sistem pemidanaan di kedua negara. Sementara itu, pendekatan konseptual berfungsi untuk memahami konsep dasar pemidanaan dalam hukum pidana siber.

Bahan hukum yang digunakan dalam penelitian ini meliputi bahan hukum primer, yaitu Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia, Computer Fraud and Abuse Act (CFAA) di Amerika Serikat, serta peraturan terkait lainnya. Selain itu, digunakan pula bahan hukum sekunder, seperti buku, jurnal hukum, serta artikel ilmiah yang relevan. Analisis bahan hukum dalam penelitian ini dilakukan dengan metode deskriptif-analitis, yaitu menguraikan, membandingkan, serta mengevaluasi efektivitas sistem pemidanaan cybercrime di kedua negara guna memberikan rekomendasi bagi penguatan regulasi dan kebijakan hukum pidana siber di Indonesia.[5]

HASIL DAN PEMBAHASAN

1. Sistem Pemidanaan Tindak Pidana Cybercrime Di Indonesia Dan Amerika Serikat Diterapkan Berdasarkan Hukum Yang Berlaku

Perkembangan teknologi informasi yang pesat telah melahirkan bentuk-bentuk kejahatan baru yang dilakukan di dunia maya, yang dikenal sebagai cybercrime. Kejahatan ini mencakup berbagai tindak pidana seperti peretasan (hacking), pencurian data pribadi, penipuan daring (online fraud), penyebaran malware, serta tindak pidana pencucian uang melalui sistem digital. Seiring dengan meningkatnya kejahatan siber, berbagai negara, termasuk Indonesia dan Amerika Serikat, telah menerapkan sistem pemidanaan berdasarkan hukum yang berlaku untuk menanggulangi dan menindak pelaku cybercrime. Namun, terdapat perbedaan mendasar dalam pendekatan, regulasi, dan sistem sanksi yang diterapkan di kedua negara.[6]

---

[4] 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.
[5] Marzuki, Peter Mahmud. 2016, Penelitian Hukum (Edisi Revisi), Jakarta : Kencana Prenada Media Group.
[6] Widijowati, D. (2022). Legal Complexity in Dealing with Cyber Crime in Indonesia. *Research Horizon*, *2*(6), 597-606.

Jurnal Hukum dan Kewarganegaraan
Vol. 10 No. 12 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

Di Indonesia, sistem pemidanaan terhadap pelaku cybercrime diatur dalam berbagai peraturan perundang-undangan, dengan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 sebagai regulasi utama. UU ITE mengatur berbagai bentuk kejahatan siber dan sanksi pidana yang dapat dikenakan kepada pelaku. Selain itu, beberapa ketentuan dalam Kitab Undang-Undang Hukum Pidana (KUHP) serta Kitab Undang-Undang Hukum Acara Pidana (KUHAP) juga turut digunakan dalam proses penegakan hukum terhadap tindak pidana cybercrime. Menurut Pasal 27 hingga Pasal 36 UU ITE, beberapa tindak pidana siber yang diatur dalam hukum Indonesia meliputi penyebaran informasi elektronik yang melanggar kesusilaan dengan ancaman pidana paling lama enam tahun penjara dan/atau denda maksimal Rp1 miliar, penghinaan dan pencemaran nama baik melalui media elektronik dengan ancaman pidana empat tahun penjara dan/atau denda hingga Rp750 juta, serta penyebaran berita bohong yang menimbulkan kerugian konsumen dalam transaksi elektronik dengan ancaman pidana enam tahun penjara dan denda maksimal Rp1 miliar. Selain itu, akses ilegal terhadap sistem elektronik orang lain atau hacking diancam dengan hukuman hingga delapan tahun penjara dan denda maksimal Rp800 juta, sedangkan manipulasi, perusakan, atau penghancuran data elektronik (cyber sabotage) dapat dikenai ancaman pidana sepuluh tahun penjara dan denda hingga Rp5 miliar. Selain UU ITE, beberapa regulasi lain juga mendukung sistem pemidanaan cybercrime di Indonesia, seperti Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, yang mengatur tata kelola keamanan siber serta perlindungan data pribadi. Namun, meskipun memiliki dasar hukum yang cukup kuat, sistem pemidanaan terhadap kejahatan siber di Indonesia masih menghadapi berbagai kendala, seperti keterbatasan dalam pembuktian alat bukti elektronik, lemahnya koordinasi antar lembaga penegak hukum, serta kurangnya mekanisme kerja sama internasional dalam menangani kejahatan lintas negara.[7]

Berbeda dengan Indonesia, Amerika Serikat memiliki sistem pemidanaan cybercrime yang lebih kompleks dan terstruktur. Regulasi utama yang mengatur tindak pidana siber di Amerika Serikat adalah Computer Fraud and Abuse Act (CFAA) tahun 1986, yang telah mengalami beberapa amandemen untuk menyesuaikan dengan perkembangan teknologi. CFAA mengatur berbagai bentuk kejahatan siber, seperti akses ilegal terhadap sistem komputer, pencurian informasi elektronik, dan sabotase digital, dengan ancaman hukuman yang bervariasi tergantung pada tingkat kejahatan yang dilakukan. Selain CFAA, terdapat beberapa undang-undang lain yang turut mengatur pemidanaan cybercrime di Amerika Serikat, di antaranya Electronic Communications Privacy Act (ECPA) tahun 1986 yang melindungi komunikasi elektronik dari penyadapan ilegal dan akses tanpa izin, Cybersecurity Information Sharing Act (CISA) tahun 2015 yang memungkinkan sektor swasta dan pemerintah berbagi informasi mengenai ancaman keamanan siber untuk mencegah serangan siber lebih lanjut, serta Identity Theft and Assumption Deterrence Act tahun 1998 yang mengatur sanksi bagi pelaku pencurian identitas dalam dunia maya. Dalam sistem hukum pidana Amerika Serikat, hukuman bagi pelaku cybercrime umumnya lebih berat dibandingkan dengan di Indonesia, terutama bagi kejahatan yang berdampak besar terhadap masyarakat atau perekonomian negara. Misalnya, dalam kasus peretasan terhadap perusahaan Equifax pada tahun 2017, di mana data pribadi lebih dari 147 juta warga Amerika Serikat dicuri, pelaku dapat dijatuhi hukuman hingga dua puluh tahun penjara dan denda jutaan dolar. Salah satu karakteristik sistem pemidanaan di Amerika Serikat adalah penerapan plea bargaining, yang memungkinkan terdakwa untuk mengurangi

[7] Siregar, G., & Sinaga, S. (2021). The law globalization in cybercrime prevention. *International Journal of Law Reconstruction*, *5*(2), 211-227.

Jurnal Hukum dan Kewarganegaraan
Vol. 10 No. 12 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

masa hukuman dengan bekerja sama dalam penyelidikan atau mengungkap jaringan kejahatan yang lebih besar. Mekanisme ini memberikan fleksibilitas dalam sistem hukum dan sering digunakan dalam kasus cybercrime yang melibatkan sindikat internasional.

Dari pemaparan di atas, terlihat adanya perbedaan mendasar antara sistem pemidanaan cybercrime di Indonesia dan Amerika Serikat. Beberapa perbedaan utama dapat diuraikan sebagai berikut. Dari segi kerangka hukum, Indonesia mengandalkan UU ITE sebagai regulasi utama, dengan tambahan aturan dalam KUHP dan KUHAP, sedangkan Amerika Serikat memiliki berbagai undang-undang khusus, seperti CFAA, ECPA, dan CISA, yang secara rinci mengatur berbagai bentuk cybercrime. Dari segi efektivitas penegakan hukum, Indonesia masih menghadapi berbagai kendala dalam pembuktian kejahatan siber, keterbatasan alat bukti elektronik, dan koordinasi antar lembaga, sementara Amerika Serikat memiliki sistem yang lebih kuat dengan dukungan dari FBI, Department of Justice (DOJ), dan Cybersecurity and Infrastructure Security Agency (CISA), yang secara khusus menangani kejahatan siber. Dari segi sistem sanksi, sanksi di Indonesia cenderung lebih ringan dibandingkan Amerika Serikat. Hukuman maksimal dalam UU ITE umumnya berkisar antara empat hingga sepuluh tahun penjara dengan denda hingga Rp5 miliar, sementara di Amerika Serikat, hukuman bagi pelaku cybercrime bisa mencapai puluhan tahun penjara dan denda jutaan dolar, terutama dalam kasus yang merugikan banyak pihak. Dari segi mekanisme fleksibilitas hukum, sistem di Indonesia masih bergantung pada hukum pidana klasik, tanpa adanya mekanisme seperti plea bargaining, sementara Amerika Serikat menerapkan plea bargaining, yang memungkinkan pengurangan hukuman bagi pelaku yang bekerja sama dengan aparat penegak hukum.[8]

Sistem pemidanaan cybercrime di Indonesia dan Amerika Serikat memiliki karakteristik yang berbeda berdasarkan hukum yang berlaku di masing-masing negara. Indonesia masih menghadapi berbagai tantangan dalam efektivitas penegakan hukum terhadap cybercrime, sedangkan Amerika Serikat telah memiliki sistem yang lebih matang, dengan regulasi yang lebih terperinci dan mekanisme penegakan hukum yang lebih ketat. Oleh karena itu, Indonesia dapat mengevaluasi dan mengambil pelajaran dari sistem hukum Amerika Serikat, khususnya dalam hal penguatan regulasi, peningkatan kapasitas penegak hukum, serta penerapan kerja sama internasional dalam menangani kejahatan siber lintas negara.

Meskipun sistem pemidanaan cybercrime di Indonesia dan Amerika Serikat memiliki perbedaan mendasar, keduanya sama-sama menghadapi tantangan dalam menangani kejahatan siber yang semakin kompleks. Di era digital, kejahatan siber tidak hanya bersifat domestik tetapi juga berskala global, melibatkan pelaku lintas negara dan menargetkan korban di berbagai belahan dunia. Oleh karena itu, kerja sama internasional dalam pemberantasan cybercrime menjadi aspek krusial yang perlu diperkuat oleh setiap negara, termasuk Indonesia. Salah satu upaya yang dapat dilakukan adalah dengan meningkatkan kolaborasi melalui organisasi internasional seperti Interpol dan ASEAN Cybersecurity Cooperation Strategy, serta memperkuat perjanjian ekstradisi untuk mempermudah proses hukum terhadap pelaku yang berada di luar yurisdiksi nasional. Dalam hal ini, Amerika Serikat telah memiliki sistem yang lebih maju dalam menangani kejahatan lintas batas dengan menjalin kerja sama erat dengan negara-negara lain melalui Mutual Legal Assistance Treaty (MLAT), yang memungkinkan pertukaran informasi serta penyerahan tersangka kejahatan siber antarnegara.[9]

---

[8] Sumadinata, W. S. (2023). Cybercrime And Global Security Threats: A Challenge In International Law. *Russian Law Journal*, *11*(3), 438-444.

[9] Manthovani, R. (2023). Indonesian Cybercrime Assessment and Prosecution: Implications for Criminal Law. *International Journal of Criminal Justice Sciences*, *18*(1), 439-452.

Jurnal Hukum dan Kewarganegaraan
Vol. 10 No. 12 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

Selain kerja sama internasional, peningkatan kapasitas aparat penegak hukum dan penyediaan alat bukti digital yang memadai menjadi tantangan tersendiri dalam sistem pemidanaan cybercrime. Di Indonesia, keterbatasan sumber daya manusia yang memiliki keahlian di bidang digital forensik masih menjadi kendala dalam penyidikan kasus kejahatan siber. Banyak kasus yang gagal diproses karena kurangnya alat bukti elektronik yang sah secara hukum atau ketidaksiapan aparat dalam menangani kasus yang melibatkan teknologi canggih. Dalam praktiknya, pembuktian dalam kejahatan siber memang lebih rumit dibandingkan dengan kejahatan konvensional, karena sering kali melibatkan jaringan internet global dan berbagai bentuk enkripsi data yang sulit dipecahkan. Oleh karena itu, Indonesia perlu meningkatkan investasi dalam teknologi digital forensik serta mengembangkan pelatihan khusus bagi aparat penegak hukum agar dapat lebih efektif dalam menangani kasus cybercrime. Di sisi lain, Amerika Serikat telah memiliki lembaga-lembaga khusus seperti Federal Bureau of Investigation (FBI) dan Cybersecurity and Infrastructure Security Agency (CISA), yang memiliki divisi khusus untuk menangani serangan siber dan melakukan investigasi berbasis digital forensik. Hal ini memungkinkan mereka untuk lebih sigap dalam menanggulangi kejahatan siber, baik dalam skala domestik maupun internasional.[10]

Perlindungan terhadap korban kejahatan siber juga menjadi aspek penting dalam sistem pemidanaan cybercrime yang perlu mendapatkan perhatian. Di Indonesia, perlindungan terhadap korban masih terbatas pada aspek hukum pidana, di mana fokus utama adalah menghukum pelaku, sementara mekanisme pemulihan bagi korban, seperti ganti rugi atau pemulihan psikologis, masih belum optimal. Dalam kasus pencurian data pribadi atau penipuan daring, misalnya, banyak korban yang mengalami kerugian finansial besar tanpa mendapatkan kompensasi yang memadai. Amerika Serikat memiliki sistem yang lebih baik dalam memberikan perlindungan terhadap korban, termasuk mekanisme kompensasi serta layanan pemulihan identitas bagi korban pencurian data pribadi. Beberapa negara bagian di Amerika Serikat juga memiliki undang-undang khusus yang mewajibkan perusahaan untuk memberikan notifikasi kepada pelanggan jika terjadi kebocoran data, sehingga masyarakat dapat lebih waspada terhadap potensi penyalahgunaan informasi pribadi mereka.

Selain itu, dalam menghadapi tantangan cybercrime di masa depan, Indonesia perlu memperbarui regulasi yang ada agar lebih adaptif terhadap perkembangan teknologi. Kejahatan siber terus berkembang dengan metode yang semakin canggih, seperti penggunaan kecerdasan buatan (artificial intelligence) dalam serangan siber, deepfake untuk penipuan identitas, serta penggunaan cryptocurrency dalam transaksi ilegal. Regulasi yang ada saat ini belum sepenuhnya mampu mengakomodasi dinamika baru tersebut, sehingga diperlukan reformasi hukum yang lebih fleksibel dan progresif. Amerika Serikat telah lebih dulu mengadaptasi regulasi mereka dengan melakukan amandemen terhadap undang-undang terkait, serta mengembangkan kebijakan keamanan siber yang lebih komprehensif, termasuk melalui kerja sama dengan sektor swasta dalam meningkatkan keamanan digital. Indonesia dapat mengambil pelajaran dari pendekatan ini dengan memperkuat kebijakan keamanan siber nasional serta mendorong keterlibatan sektor swasta dalam pengamanan data dan sistem elektronik. Dengan berbagai tantangan dan peluang yang ada, sistem pemidanaan cybercrime di Indonesia perlu terus mengalami perbaikan agar lebih efektif dalam menanggulangi kejahatan siber. Selain memperkuat regulasi dan penegakan hukum, Indonesia juga perlu mengembangkan mekanisme kerja sama internasional, meningkatkan kapasitas aparat penegak hukum, serta memastikan

[10] Husamuddin, M. Z., Sumardi Efendi, S. H. I., Syaibatul Hamdi, M. H., & Ida Rahma, S. H. I. (2024). Hukum acara pidana & pidana cyber: buku ajar.

perlindungan yang lebih baik bagi korban kejahatan siber. Dengan demikian, Indonesia dapat lebih siap dalam menghadapi ancaman cybercrime di era digital yang semakin maju dan kompleks.[11]

2. Mengapa Terdapat Perbedaan Dalam Sistem Pemidanaan Tindak Pidana Cybercrime Antara Indonesia Dan Amerika Serikat?

Perbedaan dalam sistem pemidanaan tindak pidana cybercrime antara Indonesia dan Amerika Serikat disebabkan oleh berbagai faktor, termasuk perbedaan sistem hukum, perkembangan teknologi, kesiapan regulasi, tingkat ancaman kejahatan siber, serta kapasitas penegakan hukum di masing-masing negara. Cybercrime merupakan bentuk kejahatan yang berkembang seiring dengan kemajuan teknologi informasi, sehingga setiap negara memiliki kebijakan dan regulasi yang berbeda dalam menanganinya. Indonesia dan Amerika Serikat, meskipun sama-sama menghadapi tantangan kejahatan siber, memiliki pendekatan hukum yang berbeda dalam menentukan bentuk pemidanaan terhadap pelaku cybercrime. Hal ini tidak terlepas dari struktur hukum yang dianut oleh kedua negara, di mana Indonesia menganut sistem hukum civil law yang berbasis pada kodifikasi undang-undang, sedangkan Amerika Serikat menggunakan sistem hukum common law yang lebih fleksibel dalam penerapannya.[12]

Salah satu faktor utama yang menyebabkan perbedaan dalam sistem pemidanaan cybercrime adalah perbedaan sistem hukum yang diterapkan. Indonesia menganut sistem civil law, di mana hukum pidana diatur secara tertulis dalam undang-undang yang bersifat rigid dan harus diterapkan sebagaimana tertulis. Sistem ini mengutamakan kepastian hukum, tetapi sering kali kurang fleksibel dalam menghadapi perubahan teknologi yang berkembang dengan cepat. Dasar hukum utama pemidanaan cybercrime di Indonesia adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang telah diperbarui dengan Undang-Undang Nomor 19 Tahun 2016. Selain itu, beberapa ketentuan dalam Kitab Undang-Undang Hukum Pidana (KUHP) dan peraturan sektoral lainnya juga digunakan sebagai dasar hukum dalam menindak kejahatan siber.

Di sisi lain, Amerika Serikat menganut sistem common law, di mana hukum berkembang berdasarkan putusan pengadilan (precedents) dan interpretasi hakim terhadap undang-undang yang ada. Sistem ini lebih fleksibel dalam merespons perkembangan teknologi dan perubahan modus operandi kejahatan siber. Dalam konteks cybercrime, Amerika Serikat memiliki regulasi yang lebih rinci dan spesifik, seperti Computer Fraud and Abuse Act (CFAA) 1986, Electronic Communications Privacy Act (ECPA) 1986, serta Cybersecurity Information Sharing Act (CISA) 2015. Selain itu, pengadilan di Amerika Serikat memiliki kebebasan untuk memberikan interpretasi terhadap kasus-kasus cybercrime, sehingga memungkinkan penerapan hukum yang lebih dinamis dibandingkan dengan Indonesia.

Perbedaan dalam sistem pemidanaan cybercrime juga disebabkan oleh kelengkapan dan spesifikasi regulasi yang dimiliki oleh masing-masing negara. Indonesia masih dalam tahap pengembangan regulasi yang komprehensif terkait kejahatan siber, sedangkan Amerika Serikat telah memiliki berbagai undang-undang khusus yang mengatur cybercrime secara lebih mendalam. Misalnya, di Indonesia, UU ITE masih menjadi regulasi utama dalam pemidanaan cybercrime, tetapi sering kali mengalami multitafsir, terutama dalam pasal-pasal terkait pencemaran nama baik, penyebaran berita bohong, dan akses ilegal terhadap sistem elektronik.

[11] Amin, K., & Oktavia, M. O. (2024). Pengelolaan Lembaga Pemasyarakatan Oleh Perusahaan Swasta di Indonesia Studi Perbandingan Dengan Negara Amerika Serikat. *UNES Law Review*, *6*(3), 8135-8146.

[12] Oktaviani, A. (2023). Alternatif Pidana Bagi Pelaku Tindak Pidana Peretasan Di Indonesia Dalam Undang-Undang Informasi Dan Transaksi Elektronik. *Novum: Jurnal Hukum*, 249-264.

Jurnal Hukum dan Kewarganegaraan
Vol. 10 No. 12 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

Sebaliknya, Amerika Serikat memiliki undang-undang yang lebih terperinci dalam menangani berbagai bentuk kejahatan siber. Computer Fraud and Abuse Act (CFAA), misalnya, mengatur secara spesifik mengenai akses tanpa izin terhadap sistem komputer, pencurian informasi elektronik, dan sabotase digital. Selain itu, Cybersecurity Information Sharing Act (CISA) 2015 mendorong kerja sama antara pemerintah dan sektor swasta dalam berbagi informasi tentang ancaman siber, sesuatu yang belum sepenuhnya diterapkan di Indonesia. Keberadaan regulasi yang lebih spesifik ini membuat sistem pemidanaan cybercrime di Amerika Serikat lebih tegas dan efektif dibandingkan dengan di Indonesia.[13]

Selain perbedaan dalam sistem hukum dan regulasi, pendekatan dalam penegakan hukum juga menjadi faktor yang membedakan sistem pemidanaan cybercrime di kedua negara. Indonesia masih menghadapi berbagai tantangan dalam menegakkan hukum terhadap kejahatan siber, terutama terkait dengan keterbatasan alat bukti elektronik, kurangnya tenaga ahli di bidang digital forensik, serta lemahnya koordinasi antar lembaga penegak hukum. Dalam banyak kasus, aparat penegak hukum di Indonesia masih kesulitan dalam melakukan investigasi terhadap kasus cybercrime yang kompleks, terutama yang melibatkan pelaku lintas negara. Di Amerika Serikat, penegakan hukum terhadap cybercrime jauh lebih maju dan terstruktur. Lembaga seperti Federal Bureau of Investigation (FBI), Department of Justice (DOJ), dan Cybersecurity and Infrastructure Security Agency (CISA) memiliki divisi khusus untuk menangani kejahatan siber. Mereka tidak hanya bertugas untuk menangkap pelaku, tetapi juga melakukan analisis mendalam terhadap pola kejahatan siber dan mengembangkan strategi pencegahan yang lebih efektif. Selain itu, sistem peradilan di Amerika Serikat juga lebih tegas dalam menjatuhkan hukuman bagi pelaku cybercrime. Dalam beberapa kasus, pelaku kejahatan siber di Amerika Serikat bisa dijatuhi hukuman puluhan tahun penjara dan denda jutaan dolar, sedangkan di Indonesia, hukuman yang diberikan umumnya jauh lebih ringan.[14]

Perbedaan lainnya dalam sistem pemidanaan cybercrime antara Indonesia dan Amerika Serikat adalah adanya mekanisme fleksibilitas hukum yang lebih berkembang di Amerika Serikat. Salah satu mekanisme yang sering digunakan dalam sistem peradilan pidana di Amerika Serikat adalah plea bargaining, yaitu kesepakatan antara terdakwa dan jaksa untuk mengurangi hukuman dengan memberikan informasi atau bekerja sama dalam penyelidikan kasus yang lebih besar. Mekanisme ini sering digunakan dalam kasus cybercrime yang melibatkan sindikat internasional, di mana seorang terdakwa dapat mengungkap jaringan kejahatan yang lebih luas untuk mendapatkan hukuman yang lebih ringan. Di Indonesia, mekanisme seperti plea bargaining belum diterapkan dalam sistem peradilan pidana, sehingga semua kasus harus melalui proses persidangan yang panjang dan formal. Hal ini sering kali menyebabkan penegakan hukum terhadap cybercrime menjadi kurang efektif, terutama dalam kasus-kasus yang membutuhkan kerja sama dengan pelaku yang telah ditangkap untuk mengungkap jaringan kejahatan yang lebih besar.[15]

Cybercrime sering kali melibatkan pelaku lintas negara, sehingga kerja sama internasional menjadi sangat penting dalam penegakannya. Amerika Serikat telah memiliki berbagai perjanjian internasional untuk mempermudah penanganan kasus kejahatan siber, seperti Mutual Legal Assistance Treaty (MLAT) yang memungkinkan pertukaran informasi dan ekstradisi

[13] Sari, U. I. P. (2021). Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia. *Jurnal Studia Legalia*, *2*(01), 58-77.

[14] Wijaya, T. H. D. (2022). Penerapan sanksi sosial sebagai alternatif pemidanaan terhadap pelaku tindak pidana kejahatan siber (cyber crime). *Al-Qisth Law Review*, *5*(2), 371-404.

[15] Jumadiyanto, E. (2024). Penerapan Yurisdiksi Pribadi Dalam Penegakan Hukum Di Internet Dan E-Commerce Law. *Pancasila Law Review*, *1*(2), 116-130.

Jurnal Hukum dan Kewarganegaraan
Vol. 10 No. 12 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

tersangka antarnegara. Selain itu, Amerika Serikat juga aktif dalam kerja sama dengan organisasi internasional seperti Interpol dan Europol untuk menangani kasus cybercrime lintas negara. Di Indonesia, kerja sama internasional dalam menangani cybercrime masih terbatas. Meskipun telah menjalin beberapa kerja sama dengan negara lain dan organisasi internasional, Indonesia masih menghadapi kendala dalam hal efektivitas koordinasi serta akses terhadap data dan pelaku yang berada di luar yurisdiksi nasional. Hal ini sering kali menyebabkan kasus kejahatan siber yang dilakukan oleh pelaku dari luar negeri sulit untuk ditindaklanjuti.[16]

Perbedaan dalam sistem pemidanaan cybercrime antara Indonesia dan Amerika Serikat disebabkan oleh berbagai faktor, seperti perbedaan sistem hukum, regulasi yang lebih rinci di Amerika Serikat, pendekatan yang lebih tegas dalam penegakan hukum, serta mekanisme fleksibilitas hukum yang lebih berkembang di Amerika Serikat. Selain itu, kerja sama internasional yang lebih kuat membuat sistem pemidanaan cybercrime di Amerika Serikat lebih efektif dalam menangani kejahatan siber lintas negara. Indonesia dapat mengambil pelajaran dari sistem hukum Amerika Serikat dengan memperkuat regulasi, meningkatkan kapasitas aparat penegak hukum, serta memperluas kerja sama internasional dalam menangani cybercrime di era digital yang semakin kompleks. Selain perbedaan sistem hukum dan regulasi, faktor sosial, ekonomi, dan politik juga berperan dalam membentuk perbedaan sistem pemidanaan tindak pidana cybercrime antara Indonesia dan Amerika Serikat. Setiap negara memiliki kondisi sosial dan tingkat kesadaran hukum yang berbeda dalam menghadapi kejahatan siber. Di Indonesia, tingkat literasi digital masih relatif rendah dibandingkan dengan Amerika Serikat, sehingga banyak masyarakat yang belum sepenuhnya memahami ancaman cybercrime serta mekanisme hukum yang berlaku. Hal ini sering kali menyebabkan kasus-kasus cybercrime sulit dilaporkan dan ditindaklanjuti oleh aparat penegak hukum. Selain itu, kurangnya kesadaran masyarakat mengenai pentingnya perlindungan data pribadi membuat banyak orang menjadi korban penipuan daring, pencurian identitas, serta penyalahgunaan informasi pribadi tanpa menyadarinya.

Di Amerika Serikat, tingkat kesadaran hukum masyarakat terhadap cybercrime jauh lebih tinggi karena adanya edukasi yang lebih baik serta peran aktif pemerintah dalam mencegah kejahatan siber. Pemerintah Amerika Serikat secara rutin mengadakan kampanye kesadaran siber untuk meningkatkan pemahaman masyarakat tentang pentingnya keamanan digital. Selain itu, sektor swasta di Amerika Serikat juga memiliki peran yang lebih aktif dalam mencegah kejahatan siber melalui program-program keamanan siber yang ketat, terutama bagi perusahaan yang menyimpan data sensitif pengguna. Berbeda dengan Indonesia, di mana masih banyak perusahaan yang belum menerapkan sistem keamanan siber yang kuat, sehingga lebih rentan terhadap serangan hacker dan pencurian data. Dari segi ekonomi, Amerika Serikat memiliki infrastruktur teknologi yang lebih maju dan sistem keamanan siber yang lebih canggih dibandingkan dengan Indonesia. Negara ini menginvestasikan miliaran dolar setiap tahun untuk memperkuat pertahanan siber nasionalnya melalui berbagai program penelitian dan pengembangan teknologi keamanan digital. Selain itu, adanya keterlibatan perusahaan teknologi besar seperti Google, Microsoft, dan Facebook dalam penanganan kejahatan siber membuat sistem pemidanaan di Amerika Serikat lebih efektif. Sebaliknya, Indonesia masih menghadapi

[16] Husnita, N. (2022). Pembaruan Special Defence dalam Tindak Pidana Pencemaran Nama Baik Melalui Media Elektronik di Indonesia (Studi Komparasi dengan Malaysia). *Jurnal Hukum Lex Generalis*, *3*(7), 589-608.

CAUSA
ISSN 3031-0369

Jurnal Hukum dan Kewarganegaraan
Vol. 10 No. 12 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

kendala dalam hal pendanaan dan pengembangan teknologi keamanan siber, sehingga sistem penegakan hukum terhadap cybercrime belum sekuat di Amerika Serikat.[17]

Dari perspektif politik, perbedaan dalam kebijakan keamanan siber juga memengaruhi sistem pemidanaan cybercrime di kedua negara. Amerika Serikat memiliki kebijakan yang lebih tegas dalam menangani ancaman siber, terutama dalam konteks keamanan nasional. Pemerintah Amerika Serikat secara aktif memantau aktivitas siber yang berpotensi membahayakan kepentingan negara, baik yang dilakukan oleh individu, kelompok, maupun aktor negara asing. Salah satu contoh kebijakan yang menunjukkan ketegasan Amerika Serikat dalam menindak cybercrime adalah tindakan hukum terhadap peretas yang berasal dari luar negeri, seperti kasus penangkapan hacker asal Rusia dan Tiongkok yang dianggap membahayakan keamanan nasional Amerika Serikat. Di Indonesia, kebijakan terkait keamanan siber masih mengalami berbagai tantangan, terutama dalam hal koordinasi antar lembaga pemerintah dan implementasi regulasi yang efektif. Meskipun Indonesia telah memiliki Badan Siber dan Sandi Negara (BSSN) yang bertugas menangani isu keamanan siber, namun koordinasi antara BSSN dengan lembaga penegak hukum lainnya seperti Polri dan Kementerian Komunikasi dan Informatika masih perlu ditingkatkan agar sistem pemidanaan cybercrime dapat berjalan lebih efektif. Selain itu, proses legislasi di Indonesia cenderung lebih lambat dibandingkan Amerika Serikat, sehingga sering kali regulasi yang ada tidak dapat mengikuti perkembangan teknologi yang cepat.[18]

KESIMPULAN DAN SARAN

Kesimpulan dari pembahasan pertama menunjukkan bahwa sistem pemidanaan tindak pidana cybercrime di Indonesia dan Amerika Serikat memiliki perbedaan mendasar dalam aspek regulasi, efektivitas penegakan hukum, serta sistem sanksi yang diterapkan. Indonesia masih menghadapi berbagai kendala dalam penegakan hukum terhadap kejahatan siber, seperti keterbatasan alat bukti elektronik dan lemahnya koordinasi antar lembaga, sementara Amerika Serikat memiliki sistem yang lebih matang dengan regulasi yang lebih spesifik serta mekanisme penegakan hukum yang lebih tegas. Selain itu, fleksibilitas dalam sistem hukum, seperti penerapan plea bargaining di Amerika Serikat, membuat penanganan kasus cybercrime menjadi lebih efisien dibandingkan dengan Indonesia. Oleh karena itu, Indonesia perlu memperkuat regulasi, meningkatkan kapasitas aparat penegak hukum, serta memperluas kerja sama internasional dalam menanggulangi kejahatan siber yang semakin kompleks.

Kesimpulan dari pembahasan kedua mengungkap bahwa perbedaan sistem pemidanaan cybercrime antara Indonesia dan Amerika Serikat dipengaruhi oleh berbagai faktor, seperti sistem hukum yang berbeda, kelengkapan regulasi, pendekatan dalam penegakan hukum, serta mekanisme fleksibilitas hukum yang diterapkan. Amerika Serikat yang menganut sistem common law lebih fleksibel dalam merespons perkembangan teknologi dan ancaman cybercrime dibandingkan Indonesia yang menggunakan sistem civil law. Selain itu, perbedaan dalam kerja sama internasional dan tingkat literasi digital masyarakat turut memengaruhi efektivitas pemidanaan cybercrime di kedua negara. Oleh karena itu, Indonesia perlu melakukan reformasi hukum agar lebih adaptif terhadap perkembangan teknologi, memperkuat koordinasi antar lembaga penegak hukum, serta meningkatkan kesadaran masyarakat tentang pentingnya keamanan digital untuk mengurangi risiko menjadi korban kejahatan siber.

[17] Rismawati, J. (2023). Pemberian Pidana pada Kasus Cybercrime dalam Perspektif Hukum Pidana Positif. *De Juncto Delicti: Journal of Law*, *3*(2), 93-107.

[18] Ramadani, N., & Ratna, D. (2023). *KORELASI Penggunaan Teknologi Dalam Penindakan Cybercrime di Indonesia* (Doctoral dissertation, Sekolah Tinggi Ilmu Hukum IBLAM).

Jurnal Hukum dan Kewarganegaraan
Vol. 10 No. 12 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

DAFTAR PUSTAKA

Amin, K., & Oktavia, M. O. (2024). Pengelolaan Lembaga Pemasyarakatan Oleh Perusahaan Swasta di Indonesia Studi Perbandingan Dengan Negara Amerika Serikat. *UNES Law Review*, *6*(3), 8135-8146.

Gojali, D. S. (2023). Identifying the Prevalence of Cybercrime in Indonesian Corporations: A Corporate Legislation Perspective. *International Journal of Cyber Criminology*, *17*(1), 1-11.

Husamuddin, M. Z., Sumardi Efendi, S. H. I., Syaibatul Hamdi, M. H., & Ida Rahma, S. H. I. (2024). Hukum acara pidana & pidana cyber: buku ajar.

Husnita, N. (2022). Pembaruan Special Defence dalam Tindak Pidana Pencemaran Nama Baik Melalui Media Elektronik di Indonesia (Studi Komparasi dengan Malaysia). *Jurnal Hukum Lex Generalis*, *3*(7), 589-608.

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.

Imran, M. F. (2023). Preventing and Combating Cybercrime in Indonesia. *International Journal of Cyber Criminology*, *17*(1), 223-235.

Jumadiyanto, E. (2024). Penerapan Yurisdiksi Pribadi Dalam Penegakan Hukum di Internet Dan E-Commerce Law. *Pancasila Law Review*, *1*(2), 116-130.

Manthovani, R. (2023). Indonesian Cybercrime Assessment and Prosecution: Implications for Criminal Law. *International Journal of Criminal Justice Sciences*, *18*(1), 439-452.

Marzuki, Peter Mahmud. 2016, Penelitian Hukum (Edisi Revisi), Jakarta: Kencana Prenada Media Group.

Nugroho, A., & Chandrawulan, A. A. (2022). Research synthesis of cybercrime laws and COVID-19 in Indonesia: lessons for developed and developing countries. *Security Journal*, 1.

Oktaviani, A. (2023). Alternatif Pidana Bagi Pelaku Tindak Pidana Peretasan Di Indonesia Dalam Undang-Undang Informasi Dan Transaksi Elektronik. *Novum: Jurnal Hukum*, 249-264.

Ramadani, N., & Ratna, D. (2023). *KORELASI Penggunaan Teknologi Dalam Penindakan Cybercrime di Indonesia* (Doctoral dissertation, Sekolah Tinggi Ilmu Hukum IBLAM).

Rismawati, J. (2023). Pemberian Pidana pada Kasus Cybercrime dalam Perspektif Hukum Pidana Positif. *De Juncto Delicti: Journal of Law*, *3*(2), 93-107.

Sari, U. I. P. (2021). Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia. *Jurnal Studia Legalia*, *2*(01), 58-77.

Siregar, G., & Sinaga, S. (2021). The law globalization in cybercrime prevention. *International Journal of Law Reconstruction*, *5*(2), 211-227.

Sumadinata, W. S. (2023). Cybercrime And Global Security Threats: A Challenge In International Law. *Russian Law Journal*, *11*(3), 438-444.

Widijowati, D. (2022). Legal Complexity in Dealing with Cyber Crime in Indonesia. *Research Horizon*, *2*(6), 597-606.

Wijaya, T. H. D. (2022). Penerapan sanksi sosial sebagai alternatif pemidanaan terhadap pelaku tindak pidana kejahatan siber (cyber-crime). *Al-Qisth Law Review*, *5*(2), 371-404.