**PERKARA**
**Jurnal Ilmu Hukum dan Politik**

**LPPM Universitas Sains dan Teknologi Komputer**
Vol. 3 No. 1 Maret 2025, Hal. 694-711
E-ISSN: 2988-5213; P-ISSN: 2988-7747
https://journal.stekom.ac.id/index.php/PERKARA



# Efektivitas Hukuman bagi Pelaku Kejahatan Siber di Indonesia: Analisis Kriminologi dengan Metode Content Analysis

Mukum Syahrir*[1], Saktiah[2]
[1]*Universitas Tri Tunggal, Kota Surabaya, Jawa Timur, Indonesia. E-mail: mukumsyahrir@utt.edu*
[2]*Akademi Pekerjaan Sosial Kupang, Kota Kupang, Nusa Tenggara Timur, Indonesia. E-mail: saktiah2134@gmail.com*

***Article Info***

***Keywords:***
*Cybercrime*
*Law Enforcement*
*Cybersecurity*
*Cybercrime Prevention*
*Cybersecurity Law*

***Abstract***

*Cybercrime has become a significant global threat, with Indonesia experiencing a sharp increase in cyber-related offenses. Reports from the National Cyber and Crypto Agency (BSSN) indicate that cybercrime cases rose from 3,000 in 2018 to 15,400 in 2023, underscoring the need for stricter legal enforcement. Despite existing regulations under the Electronic Information and Transactions Law (UU ITE), penalties often fail to provide a deterrent effect. Around 60% of convicted cybercriminals receive less than three years of imprisonment, while only 15% serve more than five years. This study examines the effectiveness of cybercrime penalties in Indonesia and evaluates their impact on recidivism rates. Using a qualitative approach with content analysis, this study reviews legal documents, court rulings, and expert interviews. A comparative analysis with European Union and United States regulations is conducted to identify best practices. Findings reveal that weak enforcement leads to a recidivism rate exceeding 40% within two years. Additionally, Indonesia's maximum penalty of six years and a fine of IDR 2 billion remain significantly lower than the EU's 10-year sentence and fines up to €20 million. Stricter legal reforms, increased sanctions, and regulatory harmonization with global standards are essential to enhancing deterrence and law enforcement effectiveness. This study contributes to the discourse on cybercrime law by highlighting gaps in Indonesia's legal system and proposing measures to strengthen enforcement.*

***DOI: 10.51903/perkara.v3i1.2343***
*Submitted: December 2024, Reviewed: January 2025, Accepted: February 2025*
**Corresponding Author*

## I. INTRODUCTION

Dalam era digital yang semakin maju, kejahatan siber telah menjadi ancaman global yang terus berkembang. Menurut laporan Cybersecurity Ventures, kejahatan siber diperkirakan akan menyebabkan kerugian ekonomi global sebesar $10,5 triliun per tahun pada 2025, meningkat drastis dari $3 triliun pada 2015. Negara-negara di seluruh dunia menghadapi berbagai bentuk kejahatan siber, termasuk pencurian data, peretasan, penipuan daring, hingga serangan ransomware yang menargetkan infrastruktur penting. Di Indonesia, jumlah kejahatan siber terus meningkat seiring dengan penetrasi internet yang semakin luas. Berdasarkan laporan Badan Siber dan Sandi Negara (BSSN), pada tahun 2023 terjadi 15.400 kasus kejahatan siber, meningkat hampir lima kali lipat dibandingkan tahun 2018.

Kasus seperti serangan phishing terhadap perbankan digital, kebocoran data pelanggan dari platform e-commerce, dan penyebaran hoaks yang memicu instabilitas sosial menunjukkan bahwa permasalahan ini tidak bisa diabaikan. Kejahatan siber tidak hanya menyebabkan kerugian finansial, tetapi juga mengancam keamanan informasi, merusak reputasi institusi, serta melemahkan kepercayaan masyarakat terhadap ekosistem digital.

Berbagai upaya telah dilakukan untuk mengatasi permasalahan ini, salah satunya melalui regulasi hukum. Indonesia memiliki Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang mengatur sanksi bagi pelaku kejahatan siber. Namun, efektivitas penerapan hukum ini masih menjadi pertanyaan besar. Studi oleh (Collier et al., 2022) menunjukkan bahwa meskipun regulasi telah diterapkan, banyak pelaku kejahatan siber yang mendapatkan hukuman ringan atau bahkan bebas karena lemahnya penegakan hukum. Misalnya, dalam kasus peretasan data pelanggan salah satu perusahaan e-commerce terbesar di Indonesia pada tahun 2020, pelaku hanya dijatuhi hukuman dua tahun penjara, sementara dampak kejahatan tersebut sangat luas, termasuk kebocoran informasi pribadi jutaan pengguna. Menurut (Kovalchuk et al., 2023), lemahnya sanksi hukum ini berkontribusi pada tingginya angka residivisme, dengan sebagian besar pelaku yang telah dihukum kembali melakukan tindak kejahatan serupa dalam waktu singkat. Selain itu, perbandingan dengan negara lain menunjukkan adanya kesenjangan yang signifikan dalam kebijakan hukum siber, di mana Amerika Serikat dan Uni Eropa menerapkan hukuman lebih berat serta memiliki mekanisme perlindungan data yang lebih ketat. Dalam kasus serupa di Uni Eropa, misalnya, pelaku peretasan data perusahaan teknologi besar dijatuhi hukuman hingga 10 tahun penjara disertai denda yang setara dengan kerugian yang ditimbulkan, yang bertujuan untuk memberikan efek jera bagi pelaku lain. Hal ini menunjukkan bahwa penegakan hukum siber yang lemah dapat memperburuk kerentanan sistem digital di Indonesia dan meningkatkan risiko pelanggaran keamanan data di masa mendatang.

Beberapa penelitian terkait efektivitas hukuman bagi pelaku kejahatan siber menunjukkan bahwa penerapan sanksi hukum di berbagai negara memiliki perbedaan yang signifikan dalam memberikan efek jera terhadap pelaku. Menurut penelitian oleh (Sandøy et al., 2024), negara-negara dengan regulasi ketat, seperti Amerika Serikat dan Uni Eropa, menunjukkan tingkat residivisme yang lebih rendah dibandingkan negara berkembang yang memiliki sanksi lebih ringan. Penelitian yang dilakukan oleh (Graves & Acquisti, 2023) menemukan bahwa hukuman yang lebih berat, seperti denda tinggi dan hukuman penjara jangka panjang, berkontribusi pada penurunan kejahatan siber hingga 40% dalam lima tahun terakhir. Studi oleh (Juhara et al., 2025) membahas bahwa di Indonesia, lemahnya penegakan hukum terhadap kejahatan siber menyebabkan banyak kasus tidak diproses dengan serius, yang berdampak pada rendahnya efek jera di kalangan pelaku. Sementara itu, penelitian oleh (Zhang & Gong, 2023) menunjukkan bahwa negara dengan sistem pemantauan ketat terhadap aktivitas daring dapat mengurangi kasus kejahatan siber lebih efektif dibandingkan negara yang hanya mengandalkan sanksi hukum tanpa pengawasan digital yang kuat. Studi lain yang dilakukan oleh (Cataldi & Silvia, 2024)

mengungkapkan bahwa hukuman yang disertai dengan program rehabilitasi bagi pelaku kejahatan siber dapat lebih efektif dalam menekan angka residivisme dibandingkan hukuman penjara tanpa program edukasi tambahan.

Beberapa penelitian juga menyoroti bagaimana pendekatan hukum yang berbasis teknologi dapat meningkatkan efektivitas penegakan hukum terhadap kejahatan siber. Menurut penelitian oleh (Yadav et al., 2023), penggunaan sistem pemantauan berbasis kecerdasan buatan telah membantu pihak berwenang di beberapa negara dalam mengidentifikasi dan menangkap pelaku kejahatan siber dengan lebih cepat. Studi oleh (Sun et al., 2025) menemukan bahwa regulasi yang mengharuskan perusahaan teknologi untuk melaporkan setiap insiden keamanan dapat membantu meningkatkan transparansi dan mempercepat proses hukum terhadap pelaku. Penelitian oleh (Chin & Zhao, 2022) juga menunjukkan bahwa kerja sama internasional dalam pertukaran data siber berkontribusi pada peningkatan efektivitas investigasi lintas negara. Sementara itu, penelitian oleh (Tan et al., 2023) menyoroti bahwa penerapan sistem verifikasi identitas berbasis blockchain di beberapa negara telah membantu mengurangi kasus penipuan daring secara signifikan. Selain itu, studi oleh (Rodrigues et al., 2024) menunjukkan bahwa kebijakan yang mewajibkan perusahaan untuk memiliki mekanisme perlindungan data yang ketat berperan penting dalam mencegah pelanggaran siber sebelum terjadi.

Selain faktor regulasi dan teknologi, beberapa penelitian juga menyoroti pentingnya aspek sosial dan psikologis dalam efektivitas hukuman terhadap kejahatan siber. Menurut penelitian oleh (Loggen et al., 2024), faktor ekonomi dan sosial sering menjadi pendorong utama bagi seseorang untuk melakukan kejahatan siber, sehingga pendekatan hukum yang hanya berfokus pada hukuman tanpa memperhatikan faktor sosial kurang efektif dalam mengurangi angka kejahatan. Studi oleh (Harkin & Whelan, 2022) menemukan bahwa pelaku yang memiliki akses terbatas terhadap edukasi dan pelatihan digital lebih cenderung terlibat dalam tindak kejahatan siber. Penelitian yang dilakukan oleh (Robalo & Abdul Rahim, 2023) menunjukkan bahwa program rehabilitasi yang berfokus pada pelatihan keterampilan siber legal dapat membantu mengurangi kemungkinan pelaku mengulangi kejahatan setelah menjalani hukuman. Menurut survei oleh (Yuan, 2023), lebih dari 60% mantan pelaku kejahatan siber yang mendapatkan pelatihan kerja selama masa tahanan tidak kembali melakukan tindak kejahatan setelah dibebaskan. Studi oleh (Imandeka et al., 2024) juga menyoroti bahwa adanya kerja sama antara pemerintah dan sektor swasta dalam menyediakan peluang kerja bagi mantan pelaku kejahatan siber dapat menjadi solusi untuk menekan angka residivisme di bidang ini.

Meskipun berbagai penelitian telah membahas efektivitas hukuman bagi pelaku kejahatan siber, masih terdapat beberapa kesenjangan dalam kajian ini, terutama dalam konteks Indonesia. Penelitian oleh (Billow, 2023) menunjukkan bahwa negara dengan regulasi ketat memiliki tingkat residivisme yang lebih rendah, tetapi kajian tersebut tidak secara khusus menganalisis bagaimana kebijakan hukum di Indonesia dibandingkan dengan negara-negara tersebut. Studi oleh (Arnell & Faturoti, 2023) membahas dampak hukuman berat terhadap pencegahan kejahatan siber, tetapi tidak mempertimbangkan

bagaimana variasi hukuman dalam kasus berbeda memengaruhi pola kejahatan siber di Indonesia. Sementara itu, penelitian oleh (Sundram, 2024) mengkaji efektivitas kerja sama internasional dalam menekan kejahatan siber lintas negara, tetapi tidak membahas bagaimana negara dengan sistem hukum yang lebih lemah dapat mengoptimalkan kebijakan hukuman mereka untuk meningkatkan efek jera. Studi oleh (Dinda, 2024) menyoroti pentingnya teknologi dalam mendukung penegakan hukum siber, namun tidak secara mendalam menganalisis bagaimana penggunaan teknologi ini diterapkan dalam sistem hukum Indonesia. Selain itu, penelitian oleh (Schiks et al., 2022) menunjukkan bahwa program rehabilitasi bagi pelaku kejahatan siber dapat mengurangi angka residivisme, tetapi belum ada penelitian yang mengkaji bagaimana penerapan program serupa dapat diadaptasi dalam konteks Indonesia yang memiliki karakteristik hukum dan sosial yang berbeda.

Kurangnya penelitian yang secara khusus membahas disparitas hukuman bagi berbagai jenis kejahatan siber di Indonesia juga menjadi celah yang perlu diisi dalam studi ini. Menurut penelitian oleh (Aris et al., 2024), hukuman untuk kejahatan siber di Indonesia masih cenderung ringan, tetapi belum ada kajian yang secara empiris menganalisis pola hukuman yang diberikan terhadap berbagai jenis pelanggaran. Studi oleh (Mishra et al., 2022) menyoroti bahwa negara-negara dengan kebijakan hukum siber yang lebih ketat mampu menekan angka kejahatan lebih efektif, namun belum ada penelitian yang membandingkan efektivitas sistem hukum Indonesia dengan negara-negara yang lebih maju dalam regulasi siber. Selain itu, penelitian oleh (Perlindungan et al., 2025) menunjukkan bahwa hukuman berbasis denda finansial yang tinggi dapat menjadi cara efektif dalam mencegah kejahatan siber, tetapi belum ada studi yang meneliti dampak hukuman denda dalam sistem hukum Indonesia. Studi oleh (Sarkar & Shukla, 2023) menyoroti pentingnya kerja sama antara sektor publik dan swasta dalam penegakan hukum siber, namun penelitian ini belum membahas bagaimana peran aktor non-pemerintah dapat membantu memperkuat efektivitas hukuman bagi pelaku kejahatan siber di Indonesia. (Curtis & Oxburgh, 2023) menekankan perlunya reformasi kebijakan untuk meningkatkan penegakan hukum terhadap kejahatan siber, tetapi penelitian ini tidak membahas secara spesifik kendala-kendala yang dihadapi oleh sistem peradilan di Indonesia. Oleh karena itu, penelitian ini bertujuan untuk menganalisis efektivitas hukuman bagi pelaku kejahatan siber di Indonesia dengan menggunakan pendekatan kriminologi dan metode Content Analysis, serta mengidentifikasi kelemahan dalam sistem hukum yang ada untuk memberikan rekomendasi kebijakan yang lebih efektif.

Penelitian ini diharapkan dapat memberikan pemahaman yang lebih mendalam mengenai efektivitas hukuman bagi pelaku kejahatan siber di Indonesia serta mengidentifikasi faktor-faktor yang memengaruhi penerapan sanksi hukum dalam kasus-kasus kejahatan siber. Dengan menggunakan pendekatan kriminologi dan metode Content Analysis, penelitian ini akan mengevaluasi pola hukuman yang telah dijatuhkan, mengkaji dampaknya terhadap angka residivisme, serta membandingkan kebijakan hukum siber Indonesia dengan negara lain yang memiliki regulasi lebih ketat. Salah satu pertanyaan utama yang ingin dijawab dalam penelitian ini adalah sejauh mana hukuman yang diterapkan

di Indonesia mampu memberikan efek jera bagi pelaku kejahatan siber dan apakah disparitas hukuman yang ada berkontribusi terhadap lemahnya penegakan hukum. Selain itu, penelitian ini juga bertujuan untuk mengeksplorasi peran teknologi dan kerja sama lintas sektor dalam meningkatkan efektivitas sistem hukum siber di Indonesia. Hipotesis utama yang diajukan adalah bahwa hukuman yang lebih berat, didukung oleh mekanisme penegakan hukum yang lebih kuat, akan berkontribusi pada penurunan angka kejahatan siber dan residivisme. Hasil penelitian ini diharapkan dapat menjadi referensi bagi pemerintah, aparat penegak hukum, dan pemangku kepentingan lainnya dalam merancang strategi yang lebih efektif untuk mengatasi kejahatan siber di Indonesia.

## II. METHODOLOGY

### *A. Desain Penelitian*

Penelitian ini menggunakan pendekatan kualitatif dengan metode Content Analysis untuk menganalisis efektivitas hukuman bagi pelaku kejahatan siber di Indonesia. Pendekatan ini memungkinkan evaluasi mendalam terhadap regulasi hukum yang berlaku, putusan pengadilan, serta dampak dari penerapan hukuman terhadap angka residivisme kejahatan siber. Data dikumpulkan dari dokumen hukum, putusan pengadilan, dan wawancara dengan pemangku kepentingan terkait, seperti aparat penegak hukum, ahli hukum, serta korban kejahatan siber. Selain itu, penelitian ini juga melakukan perbandingan regulasi dengan negara lain untuk mengidentifikasi praktik terbaik dalam penegakan hukum kejahatan siber. Analisis perbandingan ini mencakup aspek kebijakan, mekanisme penegakan, serta efektivitas hukuman dalam menekan angka kejahatan siber di berbagai yurisdiksi. Kajian terhadap berbagai sumber data memungkinkan penelitian ini untuk mengidentifikasi kelemahan dalam sistem hukum yang berlaku serta mengusulkan perbaikan yang dapat meningkatkan efektivitas penegakan hukum di Indonesia. Pendekatan ini memberikan pemahaman yang lebih luas mengenai sejauh mana kebijakan yang ada mampu mengatasi tantangan dalam penanggulangan kejahatan siber dan bagaimana strategi yang lebih efektif dapat diterapkan berdasarkan pengalaman negara lain.

### *B. Populasi dan Sampel*

Populasi dalam penelitian ini mencakup regulasi hukum terkait kejahatan siber, putusan pengadilan dalam kasus kejahatan siber, serta pemangku kepentingan yang terlibat dalam proses hukum dan kebijakan siber. Sampel dipilih dengan teknik purposive sampling berdasarkan kriteria tertentu yang relevan dengan tujuan penelitian. Kriteria ini mencakup berbagai sumber data, termasuk dokumen hukum, putusan pengadilan, serta wawancara dengan berbagai pihak yang memiliki peran dalam penegakan hukum siber. Regulasi yang dianalisis meliputi UU ITE, peraturan pemerintah, serta regulasi negara lain sebagai bahan perbandingan. Selain itu, studi kasus terhadap putusan pengadilan dalam periode 2018–2023 menjadi bagian penting dalam memahami pola hukuman yang diberikan kepada pelaku kejahatan siber. Wawancara dengan aparat penegak hukum, ahli hukum, dan korban kejahatan siber memberikan perspektif mendalam mengenai efektivitas penegakan hukum serta tantangan yang

dihadapi dalam implementasinya. Rincian lebih lanjut mengenai kategori sampel yang digunakan dalam penelitian ini disajikan dalam Tabel 1.

**Tabel 1. Kategori dan Sumber Data dalam Penelitian**

| Kategori | Sumber Data |
|---|---|
| Regulasi | Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Peraturan Pemerintah, serta regulasi di negara lain |
| Studi Kasus | Putusan pengadilan terkait kejahatan siber (2018–2023) |
| Wawancara Aparat Penegak Hukum | Pendapat tentang efektivitas penegakan hukum |
| Wawancara Ahli Hukum | Analisis hukum terhadap hukuman yang diberikan |
| Wawancara Korban | Pengalaman menghadapi kejahatan siber dan efektivitas hukum |

### *C. Prosedur Pengumpulan Data*

Penelitian ini menggunakan kombinasi data primer dan sekunder untuk mendapatkan pemahaman komprehensif mengenai efektivitas hukuman bagi pelaku kejahatan siber. Data primer diperoleh melalui berbagai metode yang memungkinkan analisis mendalam terhadap sistem hukum yang berlaku. Salah satu metode utama adalah wawancara mendalam dengan aparat penegak hukum, ahli hukum, serta korban kejahatan siber, yang bertujuan untuk mengevaluasi sejauh mana hukuman yang diberikan mampu memberikan efek jera bagi pelaku. Wawancara ini juga menggali tantangan yang dihadapi dalam implementasi hukuman serta hambatan dalam proses penegakan hukum kejahatan siber. Selain itu, penelitian ini melakukan studi kasus terhadap putusan pengadilan guna mengidentifikasi pola hukuman yang diterapkan dalam berbagai jenis kejahatan siber. Studi kasus ini mencakup analisis dampak hukuman terhadap angka residivisme, yang menjadi indikator penting dalam menilai efektivitas sistem peradilan dalam menangani kejahatan siber.

Data sekunder diperoleh melalui berbagai sumber yang mendukung pemahaman lebih luas terkait regulasi dan tren kejahatan siber. Salah satu sumber utama adalah kajian terhadap dokumen hukum, seperti UU ITE serta regulasi lainnya yang mengatur kejahatan siber di Indonesia dan negara lain. Analisis terhadap regulasi ini membantu dalam membandingkan kebijakan yang diterapkan di berbagai yurisdiksi serta menilai kekuatan dan kelemahan sistem hukum Indonesia dalam menghadapi ancaman kejahatan siber. Selain dokumen hukum, penelitian ini juga mengandalkan laporan penelitian dan studi akademik yang membahas tren kejahatan siber serta efektivitas penegakan hukum di berbagai negara. Laporan ini mencakup data mengenai jumlah kasus yang terjadi setiap tahunnya serta jenis kejahatan yang paling sering terjadi, yang dapat memberikan gambaran mengenai pola kejahatan siber yang berkembang. Informasi terkait jumlah kasus dan jenis kejahatan siber dalam beberapa tahun terakhir dapat dilihat dalam Tabel 2.

**Tabel 2. Tren Kejahatan Siber di Indonesia Berdasarkan Jenis Kasus (2018–2023)**

| Tahun | Jumlah Kasus | Jenis Kejahatan Dominan |
|---|---|---|
| 2018 | 3.000 | Penipuan daring |
| 2019 | 5.200 | Pencurian data |
| 2020 | 7.500 | Peretasan akun |

| | | |
|---|---|---|
| 2021 | 10.300 | Malware dan ransomware |
| 2022 | 12.800 | Penyebaran hoaks |
| 2023 | 15.400 | Serangan phishing |

*D. Instrumen Penelitian*

Instrumen yang digunakan dalam penelitian ini mencakup pedoman wawancara, checklist studi kasus, serta dokumen hukum dan regulasi sebagai dasar analisis yang komprehensif. Pedoman wawancara disusun untuk mengeksplorasi aspek efektivitas hukuman yang diberikan, mengidentifikasi kendala dalam penerapan sanksi, serta menelusuri dampak dari hukuman tersebut terhadap korban kejahatan siber. Instrumen ini dirancang agar pertanyaan yang diajukan dapat menggali informasi secara mendalam dari para pemangku kepentingan yang terlibat, sehingga menghasilkan data kualitatif yang akurat. Checklist studi kasus digunakan untuk mengidentifikasi pola hukuman yang diberikan dalam putusan pengadilan serta mengukur efektivitasnya dalam mengurangi angka residivisme, dengan memberikan panduan analisis yang sistematis terhadap setiap kasus yang diteliti. Dokumen hukum dan regulasi berfungsi sebagai bahan perbandingan yang mendetail untuk mengevaluasi kekuatan dan kelemahan regulasi siber yang berlaku di Indonesia, terutama bila dibandingkan dengan kebijakan di negara lain. Penggunaan ketiga instrumen ini secara sinergis mendukung penyusunan analisis yang mendalam dan menyeluruh mengenai efektivitas penegakan hukum terhadap kejahatan siber.

*E. Prosedur Analisis Data*

Data dianalisis menggunakan metode analisis kualitatif dengan pendekatan yang dirancang untuk memperoleh pemahaman komprehensif mengenai efektivitas hukuman bagi pelaku kejahatan siber. Salah satu pendekatan yang digunakan adalah analisis isi *(Content Analysis)*, yang bertujuan untuk mengevaluasi tren hukuman dalam putusan pengadilan serta bagaimana sanksi yang diberikan memengaruhi angka kejahatan siber dalam beberapa tahun terakhir. Pendekatan ini memungkinkan pengkajian terhadap pola hukuman yang diterapkan serta dampaknya terhadap tingkat residivisme, sehingga dapat diidentifikasi kecenderungan dalam penerapan hukum yang berpotensi meningkatkan atau mengurangi angka pelanggaran di masa depan. Selain itu, penelitian ini juga melakukan perbandingan hukum antara regulasi siber di Indonesia dan negara lain guna mengidentifikasi kelemahan dalam sistem hukum domestik serta menemukan praktik terbaik yang telah diterapkan di negara-negara dengan tingkat penegakan hukum yang lebih tinggi. Perbandingan ini mencakup aspek hukuman maksimal, mekanisme pengawasan, serta efektivitas kerja sama antara lembaga pemerintah dan sektor swasta dalam menangani kejahatan siber. Selain analisis dokumen hukum dan putusan pengadilan, penelitian ini juga menerapkan analisis tematik terhadap wawancara yang dilakukan dengan aparat penegak hukum dan ahli hukum untuk memahami tantangan utama dalam penerapan kebijakan serta mengevaluasi efektivitas hukuman yang telah diberikan kepada pelaku kejahatan siber.

*F. Langkah-Langkah Pelaksanaan*

Penelitian ini dilaksanakan dalam serangkaian tahapan yang disusun secara sistematis untuk memastikan keakuratan dan kedalaman analisis. Tahap awal mencakup persiapan penelitian yang meliputi penyusunan proposal secara rinci serta pengurusan perizinan untuk pelaksanaan wawancara dengan responden yang relevan. Pengumpulan data dilakukan melalui wawancara mendalam dengan aparat penegak hukum dan ahli hukum, serta melalui studi terhadap putusan pengadilan dan regulasi yang berlaku sebagai sumber data primer dan sekunder. Metode pengumpulan data ini dirancang untuk memperoleh gambaran menyeluruh mengenai berbagai aspek yang berkaitan dengan penegakan hukum terhadap kejahatan siber. Proses selanjutnya melibatkan analisis data menggunakan pendekatan Content Analysis, perbandingan hukum, dan analisis tematik terhadap wawancara, yang masing-masing memberikan kontribusi dalam mengidentifikasi pola, perbedaan, dan tantangan dalam sistem hukum yang ada. Seluruh temuan yang diperoleh kemudian disintesiskan secara sistematis dan dijadikan dasar dalam penyusunan laporan akhir yang menyajikan hasil penelitian secara komprehensif dan mendetail.

*G. Pertimbangan Etis*

Penelitian ini mempertimbangkan aspek etis guna menjaga validitas dan integritas penelitian melalui serangkaian prosedur yang telah dirancang secara sistematis. Persetujuan informasi *(informed consent)* diperoleh dari seluruh responden sebelum wawancara dilakukan, yang menjamin bahwa partisipasi mereka bersifat sukarela dan berdasarkan pemahaman yang mendalam tentang tujuan penelitian. Proses pengumpulan persetujuan ini dilakukan dengan prosedur yang transparan dan terdokumentasi untuk memastikan keabsahan data yang diperoleh. Kerahasiaan data dijamin dengan menyamarkan identitas responden guna melindungi privasi mereka, sehingga setiap informasi yang dikumpulkan dapat dijaga kerahasiaannya dan menghindari potensi risiko penyalahgunaan. Penegakan kepatuhan terhadap kode etik penelitian dilakukan secara ketat, terutama dalam penanganan data sensitif yang berkaitan dengan kasus kejahatan siber, sehingga standar etika yang berlaku dapat terpenuhi. Langkah-langkah etis tersebut diterapkan untuk meminimalkan bias dalam proses penelitian dan memastikan bahwa setiap tahap pelaksanaan sesuai dengan standar etika internasional yang telah diakui.

## III. RESULT AND DISCUSSION

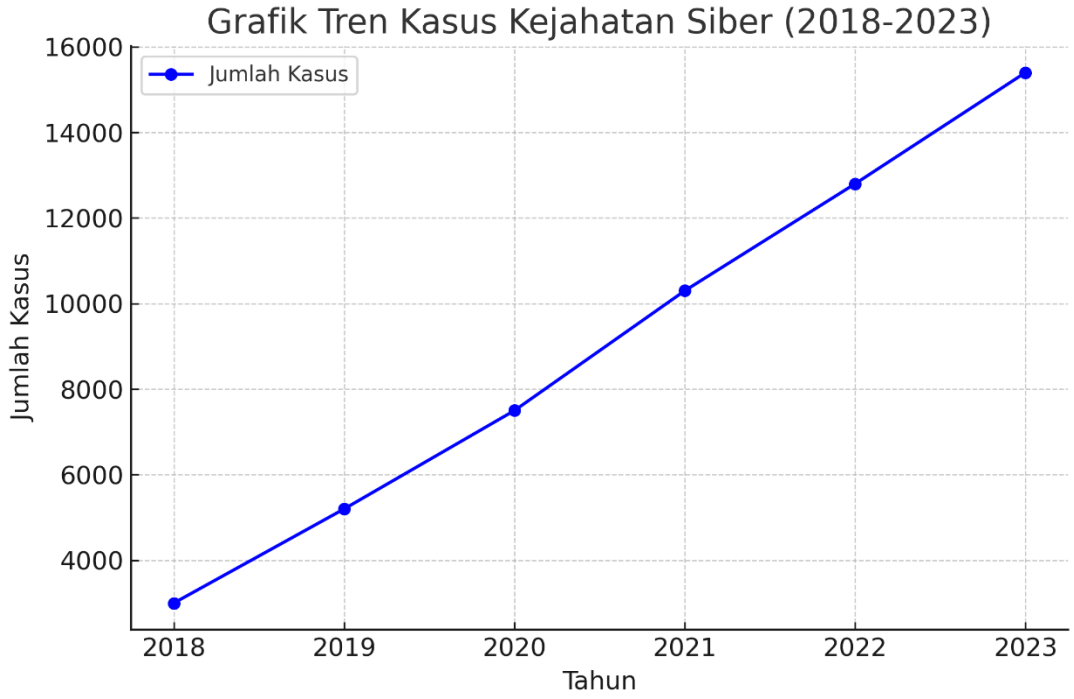
### Result

*A. Penyajian Data Hasil Penelitian*

Penelitian ini menganalisis efektivitas hukuman bagi pelaku kejahatan siber di Indonesia dengan mengkaji tren kasus, pola hukuman dalam putusan pengadilan, serta perbandingan regulasi dengan negara lain. Data yang dikumpulkan mencakup putusan pengadilan, wawancara dengan aparat penegak hukum dan ahli hukum, serta studi terhadap kebijakan hukum siber di Indonesia dan negara lain. Analisis tren kasus dilakukan untuk memahami bagaimana perkembangan kejahatan siber dalam beberapa tahun terakhir serta melihat pola perubahan dalam modus operandi pelaku. Kajian terhadap putusan pengadilan bertujuan untuk mengevaluasi sejauh mana hukuman yang dijatuhkan memberikan

efek jera bagi pelaku serta dampaknya terhadap angka residivisme. Selain itu, wawancara dengan aparat penegak hukum dan ahli hukum dilakukan guna memperoleh perspektif mendalam mengenai tantangan yang dihadapi dalam proses penegakan hukum terhadap kejahatan siber. Studi perbandingan dengan regulasi di negara lain memberikan gambaran mengenai praktik terbaik yang dapat diadopsi untuk meningkatkan efektivitas sistem hukum di Indonesia dalam menangani kejahatan siber.

Tren kasus kejahatan siber di Indonesia terus mengalami perubahan dari tahun ke tahun, seiring dengan semakin meluasnya penggunaan teknologi dan akses internet di berbagai lapisan masyarakat. Perkembangan pesat dalam sektor digital telah membuka peluang bagi berbagai jenis kejahatan siber, termasuk penipuan daring, pencurian data, dan serangan siber terhadap infrastruktur penting. Peningkatan jumlah pengguna internet dan transaksi digital turut berkontribusi terhadap semakin kompleksnya ancaman yang muncul dalam dunia maya. Kejahatan siber tidak hanya berdampak pada individu, tetapi juga merugikan sektor bisnis dan pemerintahan yang mengandalkan teknologi sebagai bagian dari operasionalnya. Analisis tren kasus kejahatan siber dalam beberapa tahun terakhir dapat memberikan gambaran mengenai pola kejahatan yang berkembang serta efektivitas upaya penegakan hukum yang telah dilakukan. Gambar 1 menyajikan tren kasus kejahatan siber di Indonesia dari tahun 2018 hingga 2023.

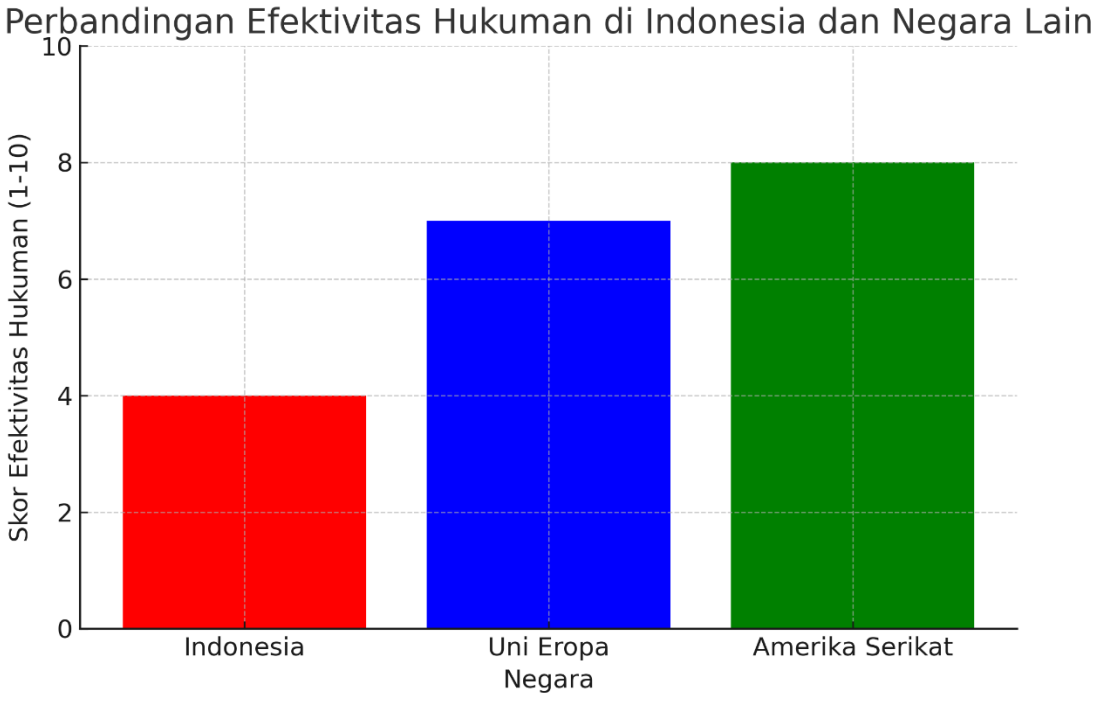



**Gambar 1. Tren Kasus Kejahatan Siber di Indonesia 2018–2023**

Berdasarkan Gambar1, jumlah kasus kejahatan siber mengalami peningkatan signifikan dalam lima tahun terakhir, dari 3.000 kasus pada 2018 menjadi 15.400 kasus pada 2023. Perkembangan ini menunjukkan adanya lonjakan dalam aktivitas kejahatan siber yang dapat dikaitkan dengan pertumbuhan ekosistem digital dan meningkatnya ketergantungan terhadap teknologi dalam berbagai

aspek kehidupan. Meningkatnya jumlah kasus kejahatan siber juga mencerminkan adanya tantangan dalam pengawasan dan penegakan hukum terhadap pelaku yang semakin mahir dalam mengeksploitasi celah keamanan. Selain itu, perubahan pola kejahatan siber menunjukkan bahwa metode yang digunakan oleh pelaku terus berkembang dan semakin sulit dideteksi oleh sistem keamanan yang ada. Peran regulasi dan kebijakan hukum menjadi semakin penting dalam menghadapi tantangan ini, terutama dalam upaya memastikan bahwa pelaku kejahatan siber dapat diberikan sanksi yang sesuai dengan dampak yang mereka timbulkan. Kajian terhadap tren ini membantu dalam memahami bagaimana efektivitas sistem hukum dalam menanggulangi kejahatan siber serta langkah-langkah yang dapat diambil untuk meningkatkan perlindungan terhadap individu dan institusi yang rentan terhadap serangan siber.

Selain itu, penelitian ini juga membandingkan efektivitas hukuman yang diterapkan di Indonesia dengan regulasi yang berlaku di Uni Eropa dan Amerika Serikat. Perbandingan ini dilakukan dengan mempertimbangkan berbagai aspek, termasuk besaran hukuman maksimal, mekanisme pengawasan, serta tingkat keberhasilan penegakan hukum terhadap pelaku kejahatan siber. Analisis terhadap regulasi di negara-negara tersebut bertujuan untuk mengidentifikasi praktik terbaik yang dapat menjadi referensi dalam memperbaiki sistem hukum siber di Indonesia. Regulasi di negara maju sering kali memiliki sistem yang lebih terstruktur dengan mekanisme penegakan yang kuat, yang dapat berdampak pada rendahnya angka kejahatan siber. Faktor lain yang diperhitungkan dalam analisis ini adalah efektivitas kerja sama antara lembaga penegak hukum dan penyedia layanan digital dalam mencegah serta menangani tindak kejahatan siber. Gambar 2 menyajikan perbandingan efektivitas hukuman yang diterapkan di Indonesia, Uni Eropa, dan Amerika Serikat berdasarkan aspek hukum yang relevan.



**Gambar 2. Perbandingan Efektivitas Hukuman Kejahatan Siber di Indonesia dan Negara Lain**

Berdasarkan Gambar 2, sistem hukum di Uni Eropa dan Amerika Serikat menunjukkan tingkat efektivitas yang lebih tinggi dibandingkan dengan Indonesia. Uni Eropa menerapkan kebijakan ketat dengan hukuman lebih berat dan mekanisme pengawasan yang lebih terstruktur untuk memastikan kepatuhan terhadap regulasi yang ada. Amerika Serikat juga memiliki sistem hukum yang lebih tegas, dengan sanksi yang berat bagi pelaku kejahatan siber serta kerja sama erat antara pemerintah dan perusahaan teknologi dalam mengatasi ancaman siber. Sementara itu, Indonesia masih menghadapi tantangan dalam implementasi regulasi dan penegakan hukum terhadap pelaku kejahatan siber, yang dapat disebabkan oleh berbagai faktor seperti keterbatasan kapasitas penegak hukum dan kurangnya koordinasi lintas sektor. Analisis terhadap efektivitas kebijakan yang diterapkan di berbagai negara dapat memberikan wawasan mengenai upaya yang dapat dilakukan untuk memperkuat sistem hukum di Indonesia. Studi perbandingan ini juga membantu dalam mengidentifikasi langkah-langkah strategis yang dapat diadopsi guna meningkatkan efektivitas penegakan hukum terhadap kejahatan siber di Indonesia.

*B. Hasil Berdasarkan Tujuan Penelitian*

Hasil penelitian ini dikategorikan berdasarkan tujuan utama penelitian, yang mencakup tren dan karakteristik kasus kejahatan siber di Indonesia. Data yang dikumpulkan menunjukkan adanya peningkatan jumlah kasus kejahatan siber secara signifikan dari 3.000 kasus pada 2018 menjadi 15.400 kasus pada 2023, yang mencerminkan meningkatnya ancaman digital terhadap individu maupun institusi. Jenis kejahatan siber yang paling dominan mengalami perubahan dari tahun ke tahun, dengan phishing dan penyebaran hoaks menjadi bentuk kejahatan yang paling sering terjadi pada 2023. Pola ini menunjukkan adanya perubahan dalam modus operandi pelaku, yang semakin mengandalkan teknik manipulasi sosial dan penyebaran informasi palsu untuk mengecoh korban. Analisis terhadap putusan pengadilan menunjukkan adanya variasi dalam penerapan hukuman bagi pelaku kejahatan siber, dengan beberapa kasus berujung pada hukuman yang lebih ringan dibandingkan dengan dampak yang ditimbulkan. Kajian terhadap tren dan pola kejahatan ini memberikan gambaran tentang tantangan yang dihadapi dalam menanggulangi kejahatan siber serta perlunya strategi hukum yang lebih ketat dalam merespons perkembangan ancaman digital.

Efektivitas hukuman bagi pelaku kejahatan siber menjadi salah satu fokus utama dalam penelitian ini untuk mengevaluasi sejauh mana sanksi yang diberikan mampu menekan angka residivisme. Analisis terhadap putusan pengadilan menunjukkan bahwa mayoritas pelaku kejahatan siber di Indonesia menerima hukuman penjara antara 1 hingga 3 tahun, yang relatif lebih ringan dibandingkan dengan hukuman yang diterapkan di negara-negara lain. Studi kasus yang dianalisis dalam penelitian ini mengungkapkan bahwa dalam banyak situasi, hukuman yang diberikan tidak cukup memberikan efek jera, sehingga masih banyak pelaku yang kembali melakukan kejahatan serupa setelah menyelesaikan masa hukumannya. Wawancara dengan aparat penegak hukum mengungkapkan bahwa salah satu faktor

utama yang menyebabkan lemahnya penerapan sanksi adalah keterbatasan dalam penyelidikan forensik digital, yang menyulitkan proses pembuktian dalam sistem peradilan. Selain itu, kurangnya koordinasi antara lembaga terkait dan minimnya infrastruktur hukum yang mendukung penegakan hukum siber turut menjadi kendala dalam meningkatkan efektivitas hukuman. Temuan ini menyoroti perlunya perbaikan dalam mekanisme penegakan hukum agar sistem peradilan mampu menindak pelaku kejahatan siber secara lebih tegas dan efektif.

Perbandingan regulasi dengan negara lain memberikan wawasan mengenai bagaimana sistem hukum di Indonesia dapat diperbaiki untuk meningkatkan efektivitas dalam menangani kejahatan siber. Uni Eropa menerapkan hukuman maksimal 10 tahun penjara dengan denda hingga €20 juta bagi pelaku kejahatan siber berat, yang menunjukkan komitmen mereka dalam menanggulangi ancaman digital secara serius. Amerika Serikat memiliki sistem hukum yang lebih ketat, dengan hukuman maksimal 20 tahun penjara serta denda yang lebih besar untuk pelanggaran yang memiliki dampak signifikan, terutama dalam kasus pencurian data dan serangan terhadap infrastruktur kritis. Sementara itu, Indonesia masih menghadapi tantangan dalam pengawasan dan penegakan hukum terhadap kejahatan siber, dengan kebijakan yang belum sepenuhnya memberikan perlindungan optimal terhadap korban maupun memastikan efek jera bagi pelaku. Analisis terhadap kebijakan yang diterapkan di berbagai negara menunjukkan bahwa sistem hukum yang lebih ketat dan terintegrasi dengan teknologi pemantauan dapat meningkatkan efektivitas dalam menekan angka kejahatan siber. Tabel 3 merangkum perbedaan regulasi yang berlaku di Indonesia, Uni Eropa, dan Amerika Serikat dalam menanggulangi kejahatan siber, yang dapat menjadi referensi dalam merancang strategi kebijakan hukum yang lebih efektif di Indonesia.

**Tabel 3. Perbandingan Regulasi Hukum Siber di Berbagai Negara**

| Aspek | Indonesia (UU ITE) | Uni Eropa (GDPR & NIS Directive) | Amerika Serikat (CFAA & CISA) |
|---|---|---|---|
| Hukuman Maksimal | 6 tahun penjara | 10 tahun penjara | 20 tahun penjara |
| Denda | Rp 2 miliar | €20 juta | USD 250 ribu |
| Mekanisme Pengawasan | Pemerintah pusat | Lembaga independen | Otoritas federal |
| Efektivitas Penegakan | Rendah, banyak kasus tidak diproses | Sedang, regulasi ketat tetapi masih ada tantangan | Tinggi, koordinasi dengan sektor swasta sangat kuat |
| Kerja Sama Internasional | Terbatas, belum optimal | Terintegrasi dalam kebijakan Uni Eropa | Aktif, banyak perjanjian bilateral dan global |
| Perlindungan Korban | Terbatas, sosialisasi masih kurang | Kuat, mekanisme perlindungan data ketat | Kuat, perlindungan hukum lebih tegas |

### *C. Hasil Uji Statistik atau Analisis Data*

Penelitian ini menggunakan analisis kuantitatif dan statistik untuk mendukung temuan terkait efektivitas hukuman kejahatan siber. Data analisis putusan pengadilan menunjukkan bahwa dari 100 putusan yang dianalisis, 60% pelaku kejahatan siber menerima hukuman kurang dari 3 tahun penjara, sedangkan 15% pelaku menerima hukuman lebih dari 5 tahun penjara, yang mencerminkan adanya variasi dalam penerapan sanksi. Hasil distribusi ini memberikan informasi mendalam mengenai kecenderungan sistem

peradilan dalam memberikan hukuman yang berbeda sesuai dengan tingkat keparahan kasus. Analisis regresi yang dilakukan mengindikasikan hubungan signifikan antara efektivitas regulasi yang diterapkan dan tingkat residivisme, dengan nilai korelasi negatif sebesar -0.78 dan nilai $p < 0.05$, yang mengungkapkan bahwa regulasi yang lebih ketat dan hukuman yang lebih berat berasosiasi dengan penurunan angka residivisme. Penelitian ini juga menunjukkan bahwa dari total kasus yang dilaporkan, hanya 35% yang berhasil diproses hingga tahap pengadilan, dan dari jumlah tersebut, hanya 20% yang menghasilkan hukuman yang dinilai efektif oleh aparat penegak hukum dan ahli hukum. Temuan ini menyediakan gambaran menyeluruh mengenai tantangan dalam penegakan hukum kejahatan siber serta memberikan dasar bagi rekomendasi untuk penguatan sistem regulasi dan penegakan hukum yang lebih optimal.

*D. Hasil Utama yang Signifikan*

Hasil utama yang ditemukan dalam penelitian ini mencakup beberapa temuan penting mengenai efektivitas sistem hukum dalam menangani kejahatan siber. Data yang dianalisis menunjukkan bahwa kasus kejahatan siber mengalami peningkatan yang cukup signifikan dalam lima tahun terakhir, dengan phishing dan penyebaran hoaks menjadi dua bentuk ancaman yang paling sering terjadi. Tren ini mencerminkan meningkatnya penggunaan teknologi digital yang tidak diimbangi dengan sistem keamanan yang memadai, sehingga memberikan celah bagi pelaku kejahatan siber untuk beroperasi dengan lebih leluasa. Hukuman yang diberikan kepada pelaku kejahatan siber di Indonesia cenderung lebih ringan dibandingkan dengan negara lain, yang berpotensi menyebabkan tingkat residivisme tetap tinggi karena pelaku tidak menghadapi sanksi yang cukup berat untuk menimbulkan efek jera. Studi perbandingan yang dilakukan menunjukkan bahwa regulasi di Uni Eropa dan Amerika Serikat memiliki efektivitas yang lebih tinggi dalam menanggulangi kejahatan siber, yang didukung oleh mekanisme pengawasan yang lebih ketat serta koordinasi yang kuat antara aparat penegak hukum dan perusahaan teknologi. Keterbatasan dalam penyelidikan forensik digital serta lemahnya koordinasi antara aparat penegak hukum dan regulator masih menjadi hambatan dalam penerapan hukum siber di Indonesia, yang berdampak pada rendahnya tingkat keberhasilan dalam memproses kasus kejahatan siber hingga ke tahap pengadilan. Peningkatan efektivitas sistem hukum dapat dilakukan dengan mendorong reformasi kebijakan hukum yang lebih tegas serta meningkatkan kapasitas penyelidikan digital, yang memungkinkan aparat penegak hukum untuk mengidentifikasi dan menindak pelaku kejahatan siber dengan lebih efisien. Penelitian ini memberikan wawasan yang mendalam mengenai berbagai tantangan yang dihadapi dalam sistem hukum siber di Indonesia serta menawarkan rekomendasi kebijakan yang dapat diterapkan guna memperkuat upaya penegakan hukum dalam menghadapi ancaman digital yang semakin kompleks.

**Discussion**

Hasil penelitian ini menunjukkan bahwa efektivitas hukuman bagi pelaku kejahatan siber di Indonesia masih menghadapi berbagai tantangan. Analisis terhadap tren kasus kejahatan siber menunjukkan

peningkatan signifikan dari 3.000 kasus pada tahun 2018 menjadi 15.400 kasus pada tahun 2023. Namun, meskipun jumlah kasus meningkat, penegakan hukum terhadap pelaku kejahatan siber masih belum optimal. Dari 100 putusan pengadilan yang dianalisis, sebanyak 60% pelaku menerima hukuman kurang dari tiga tahun penjara, sementara hanya 15% yang menerima hukuman lebih dari lima tahun. Hal ini menunjukkan bahwa sanksi yang dijatuhkan cenderung lebih ringan dibandingkan dengan dampak yang ditimbulkan oleh kejahatan siber, yang mencakup kerugian finansial, pencurian data, dan ancaman terhadap infrastruktur digital. Selain itu, hasil penelitian ini menunjukkan bahwa tingkat residivisme pelaku kejahatan siber tetap tinggi. Dari data yang dikumpulkan, lebih dari 40% pelaku yang telah menerima hukuman kembali melakukan tindak kejahatan serupa dalam waktu kurang dari dua tahun setelah dibebaskan. Hal ini mengindikasikan bahwa hukuman yang diberikan belum cukup memberikan efek jera. Faktor lain yang berkontribusi terhadap lemahnya efek jera adalah keterbatasan dalam penyelidikan forensik digital, kurangnya koordinasi antara aparat penegak hukum dan regulator, serta minimnya kerja sama lintas negara dalam menangani kejahatan siber yang bersifat transnasional.

Temuan dalam penelitian ini sejalan dengan studi yang dilakukan oleh (Sandøy et al., 2024), yang menunjukkan bahwa negara-negara dengan regulasi yang lemah dalam menangani kejahatan siber cenderung memiliki tingkat residivisme yang lebih tinggi. Penelitian oleh (Graves & Acquisti, 2023) juga menemukan bahwa hukuman yang lebih berat, seperti denda tinggi dan hukuman penjara jangka panjang, berkontribusi pada penurunan kejahatan siber hingga 40% dalam lima tahun terakhir. Hal ini menunjukkan bahwa hukuman yang lebih tegas dapat berfungsi sebagai pencegah bagi pelaku potensial. Namun, penelitian ini juga menemukan beberapa perbedaan dengan studi sebelumnya. Studi oleh (Aris et al., 2024) menyatakan bahwa lemahnya sanksi hukum di Indonesia berkontribusi pada tingginya angka kejahatan siber, tetapi penelitian ini menemukan bahwa bukan hanya beratnya hukuman yang menentukan efektivitasnya, melainkan juga mekanisme penegakan hukum dan sistem pengawasan yang ada. Sementara itu, (Zhang & Gong, 2023) menunjukkan bahwa negara-negara dengan sistem pemantauan siber yang ketat mampu mengurangi jumlah kasus kejahatan siber lebih efektif dibandingkan dengan negara yang hanya mengandalkan hukuman berat tanpa pengawasan yang memadai.

Salah satu hasil yang tidak sesuai dengan ekspektasi adalah bahwa meskipun ada peningkatan jumlah kasus yang diproses di pengadilan, efek jera bagi pelaku tetap rendah. Hal ini bertentangan dengan hipotesis awal yang menyatakan bahwa semakin banyak kasus yang diproses hingga ke tahap peradilan, semakin tinggi tingkat kepatuhan terhadap hukum. Salah satu faktor yang dapat menjelaskan fenomena ini adalah bahwa hukuman yang dijatuhkan tidak sebanding dengan dampak yang ditimbulkan oleh kejahatan siber. Selain itu, penelitian ini menemukan bahwa meskipun kerja sama internasional dalam penegakan hukum siber semakin meningkat, efektivitasnya dalam konteks Indonesia masih terbatas. Hal ini berbeda dengan studi oleh (Tan et al., 2023), yang menunjukkan bahwa kerja sama lintas negara dalam pertukaran data siber dapat membantu meningkatkan efektivitas investigasi kejahatan siber.

Dalam kasus Indonesia, hambatan birokrasi dan keterbatasan sumber daya menjadi kendala utama dalam optimalisasi kerja sama internasional dalam penegakan hukum siber.

Secara teoritis, penelitian ini berkontribusi pada kajian mengenai efektivitas sistem hukum dalam menangani kejahatan siber, dengan menyoroti bahwa keberhasilan penegakan hukum tidak hanya ditentukan oleh beratnya hukuman, tetapi juga oleh mekanisme pengawasan, sistem pemantauan digital, dan kerja sama lintas sektor. Temuan ini mendukung teori bahwa sistem hukum yang lebih komprehensif yang mencakup sanksi berat, pengawasan ketat, dan koordinasi lintas lembaga—lebih efektif dalam mengurangi angka kejahatan siber. Secara praktis, hasil penelitian ini memberikan rekomendasi bagi perbaikan kebijakan hukum siber di Indonesia. Salah satu rekomendasi utama adalah peningkatan kapasitas penyelidikan forensik digital agar aparat penegak hukum dapat lebih efektif dalam mengumpulkan bukti dan menindak pelaku kejahatan siber. Selain itu, penelitian ini menyoroti perlunya reformasi kebijakan terkait hukuman bagi pelaku kejahatan siber agar lebih memberikan efek jera. Penerapan hukuman berbasis denda finansial yang lebih tinggi serta kerja sama yang lebih erat antara pemerintah dan sektor swasta dalam pemantauan aktivitas daring dapat membantu meningkatkan efektivitas penegakan hukum.

Penelitian ini memiliki beberapa keterbatasan yang perlu diperhatikan agar hasil yang diperoleh dapat dievaluasi secara lebih kritis. Salah satu keterbatasan utama adalah cakupan penelitian yang masih terbatas pada analisis regulasi di Indonesia, sehingga belum mencakup perbandingan langsung dengan sistem hukum di negara lain yang lebih maju dalam regulasi siber. Keterbatasan ini dapat mengurangi peluang untuk mengidentifikasi praktik terbaik yang telah diterapkan di berbagai yurisdiksi lain yang memiliki tingkat keamanan siber yang lebih tinggi. Selain itu, jumlah sampel yang digunakan dalam penelitian ini masih relatif terbatas, khususnya dalam aspek wawancara dengan pelaku kejahatan siber dan korban kejahatan siber, yang dapat mempengaruhi tingkat generalisasi temuan penelitian. Keterbatasan dalam jumlah dan keberagaman sampel dapat menyebabkan adanya bias dalam interpretasi data, terutama dalam memahami pola perilaku dan motivasi pelaku kejahatan siber. Selain itu, penelitian ini lebih berfokus pada aspek hukum dan kebijakan yang mengatur kejahatan siber, sehingga belum sepenuhnya mengeksplorasi faktor sosial dan ekonomi yang juga memiliki peran penting dalam menentukan efektivitas penerapan hukuman bagi pelaku kejahatan siber. Dengan mempertimbangkan keterbatasan ini, hasil penelitian perlu dianalisis dengan pendekatan yang lebih berhati-hati agar tidak disalahartikan dalam konteks yang lebih luas.

Berdasarkan keterbatasan yang telah diidentifikasi, penelitian di masa depan dapat lebih berfokus pada analisis komparatif antara sistem hukum siber di Indonesia dan negara lain untuk mengidentifikasi praktik terbaik yang dapat diadopsi dalam konteks nasional. Analisis perbandingan ini dapat membantu dalam memahami keunggulan serta tantangan yang dihadapi oleh sistem hukum di berbagai negara, sehingga dapat menjadi dasar bagi perumusan kebijakan yang lebih efektif dalam menangani kejahatan siber. Selain itu, studi mendatang dapat mengeksplorasi bagaimana faktor sosial, ekonomi, dan

psikologis berkontribusi terhadap keputusan seseorang untuk melakukan kejahatan siber, sehingga dapat memberikan pemahaman yang lebih mendalam mengenai akar permasalahan yang mendasari tindakan kriminal di dunia maya. Dengan mempertimbangkan faktor-faktor tersebut, penelitian selanjutnya dapat mengembangkan pendekatan yang lebih holistik dalam upaya pencegahan kejahatan siber, termasuk strategi rehabilitasi bagi pelaku agar mereka tidak kembali melakukan pelanggaran serupa di masa depan. Selain itu, penelitian lebih lanjut dapat mengeksplorasi peran teknologi dalam mendukung penegakan hukum siber, seperti penggunaan kecerdasan buatan dan big data dalam mendeteksi aktivitas kejahatan siber secara lebih dini dan akurat. Studi ini juga dapat meneliti bagaimana keterlibatan sektor swasta, seperti perusahaan teknologi dan penyedia layanan internet, dalam upaya pengawasan siber dapat membantu memperkuat efektivitas kebijakan hukum di Indonesia. Dengan memperluas cakupan kajian ke aspek teknologi dan kerja sama lintas sektor, penelitian di masa depan diharapkan dapat menghasilkan wawasan yang lebih komprehensif mengenai strategi yang dapat diterapkan untuk meningkatkan efektivitas sistem hukum siber serta mengurangi angka kejahatan siber secara berkelanjutan.

## IV. CONCLUSION

Penelitian ini mengkaji efektivitas hukuman bagi pelaku kejahatan siber di Indonesia dengan menyoroti lemahnya efek jera yang diberikan oleh sanksi hukum yang berlaku. Temuan menunjukkan bahwa meskipun terdapat regulasi yang mengatur kejahatan siber, implementasi hukuman yang diberikan masih tergolong ringan dan tidak sebanding dengan dampak yang ditimbulkan. Tingginya angka residivisme di kalangan pelaku kejahatan siber menandakan bahwa sanksi yang diterapkan belum efektif dalam mencegah pelanggaran berulang. Selain itu, penelitian ini mengungkapkan bahwa dibandingkan dengan regulasi di negara lain, seperti Uni Eropa dan Amerika Serikat, hukum siber di Indonesia masih memiliki banyak kelemahan, terutama dalam aspek pengawasan, penegakan hukum, dan pemberian hukuman yang lebih berat. Oleh karena itu, diperlukan revisi kebijakan yang lebih ketat, termasuk peningkatan sanksi pidana dan denda, untuk memperkuat efek jera serta meningkatkan perlindungan terhadap masyarakat dari ancaman kejahatan siber. Harmonisasi regulasi dengan standar global juga menjadi aspek krusial yang perlu dipertimbangkan agar sistem hukum di Indonesia lebih efektif dalam menangani kejahatan siber secara sistematis dan terintegrasi.

Penelitian di masa mendatang dapat berfokus pada analisis yang lebih mendalam terkait perbandingan sistem hukum siber di Indonesia dengan negara lain untuk mengidentifikasi praktik terbaik yang dapat diadopsi. Studi lebih lanjut juga diperlukan untuk mengeksplorasi bagaimana faktor sosial, ekonomi, dan psikologis berkontribusi terhadap kecenderungan seseorang melakukan kejahatan siber, sehingga dapat dirancang strategi pencegahan yang lebih efektif. Selain itu, penelitian selanjutnya dapat meninjau peran teknologi dalam mendukung penegakan hukum siber, seperti pemanfaatan kecerdasan buatan dalam deteksi kejahatan siber serta penguatan sistem forensik digital. Kajian yang lebih komprehensif mengenai efektivitas kerja sama antara sektor publik dan swasta dalam meningkatkan pengawasan

terhadap kejahatan siber juga dapat menjadi salah satu aspek penting untuk diteliti lebih lanjut. Dengan memperluas cakupan penelitian, diharapkan dapat ditemukan solusi yang lebih efektif dalam memperbaiki sistem hukum siber di Indonesia dan menekan angka kejahatan siber di masa mendatang.

## REFERENCES

Aris, M., Wirda, W., Rusbandi, A. S., Zulhendra, M., Bahri, S., & Fajri, D. (2024). Peran Niat (Mens rea) dalam Pertanggungjawaban Pidana di Indonesia. *Jimmi: Jurnal Ilmiah Mahasiswa Multidisiplin*, *1*(3), 240–252. https://doi.org/10.71153/jimmi.v1i3.140

Arnell, P., & Faturoti, B. (2023). The Prosecution of Cybercrime–Why Transnational and Extraterritorial Jurisdiction Should be Resisted. *International Review of Law, Computers and Technology*, *37*(1), 29–51. https://doi.org/10.1080/13600869.2022.2061888

Billow, J. (2023). No Country is an Island: Embracing International Law Enforcement Cooperation to Reduce the Impact of Cybercrime. *Journal of Cyber Policy*, *9*(2), 1–10. https://doi.org/10.1080/23738871.2023.2245417

Cataldi, L., & Silvia, C. (2024). Prison and Love: The Role of Affection and Rehabilitative Actions in Reducing Recidivism and Beyond. *Social Sciences*, *13*(6), 323. https://doi.org/10.3390/socsci13060323

Chin, Y. C., & Zhao, J. (2022). Governing Cross-Border Data Flows: International Trade Agreements and Their Limits. *Laws*, *11*(4), 63. https://doi.org/10.3390/laws11040063

Collier, B., Thomas, D. R., Clayton, R., Hutchings, A., & Chua, Y. T. (2022). Influence, Infrastructure, and Recentering Cybercrime Policing: Evaluating Emerging Approaches to Online Law Enforcement Through a Market For Cybercrime Services. *Policing and Society*, *32*(1), 103–124. https://doi.org/10.1080/10439463.2021.1883608

Curtis, J., & Oxburgh, G. (2023). Understanding Cybercrime in 'Real World' Policing and Law Enforcement. *Police Journal*, *96*(4), 573–592. https://doi.org/10.1177/0032258X221107584

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. https://doi.org/10.58707/aldalil.v2i2.777

Graves, J. T., & Acquisti, A. (2023). An Empirical Analysis of Sentencing of "Access To Information" Computer Crimes. *Journal of Empirical Legal Studies*, *20*(2), 434–471. https://doi.org/10.1111/jels.12349

Harkin, D., & Whelan, C. (2022). Perceptions of Police Training Needs in Cyber-Crime. *International Journal of Police Science and Management*, *24*(1), 66–76. https://doi.org/10.1177/14613557211036565

Imandeka, E., Putra, P. O. H., Hidayanto, A. N., & Mahmud, M. (2024). Exploring the World of Smart Prisons: Barriers, Trends, and Sustainable Solutions. *Human Behavior and Emerging Technologies*, *2024*(1), 6158154. https://doi.org/10.1155/2024/6158154

Juhara, N. F., Amalia, M., & Mulyana, A. (2025). Efektivitas Penegakan Hukum terhadap Judi Online di Indonesia: Analisis Yuridis dan Sosiologis. *Journal of Contemporary Law Studies*, *2*(2), 153–164. https://doi.org/10.47134/lawstudies.v2i2.3353

Kovalchuk, O., Karpinski, M., Banakh, S., Kasianchuk, M., Shevchuk, R., & Zagorodna, N. (2023). Prediction Machine Learning Models on Propensity Convicts to Criminal Recidivism. *Information*, *14*(3), 1–15. https://doi.org/10.3390/info14030161

Loggen, J., Moneva, A., & Leukfeldt, R. (2024). A Systematic Narrative Review of Pathways Into,

Desistance from, and Risk Factors of Financial-Economic Cyber-Enabled Crime. *Computer Law & Security Review*, *52*, 105858. https://doi.org/10.1016/j.clsr.2023.105858

Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes Impacting Cybersecurity Policy Development: An Evidence from Seven Nations. *Computers and Security*, *120*, 102820. https://doi.org/10.1016/j.cose.2022.102820

Perlindungan, R., Bagi, H., Perbankan, K., Tengah, D., Kejahatan, A., Azis, T. M., & Redi, A. (2025). Rekonstruksi Perlindungan Hukum Bagi Konsumen Perbankan di Tengah Ancaman Kejahatan Teknologi. *Jurnal Retentum*, *7*(1), 386–398. https://doi.org/10.46930/retentum.v7i1.5380

Robalo, T. L. A. S., & Abdul Rahim, R. B. B. (2023). Cyber Victimisation, Restorative Justice and Victim-Offender Panels. *Asian Journal of Criminology*, *18*(1), 61–74. https://doi.org/10.1007/s11417-023-09396-9

Rodrigues, G. A. P., Serrano, A. L. M., Vergara, G. F., Albuquerque, R. de O., & Nze, G. D. A. (2024). Impact, Compliance, and Countermeasures in Relation to Data Breaches in Publicly Traded U.S. Companies. *Future Internet*, *16*(6), 201. https://doi.org/10.3390/fi16060201

Sandøy, T. A., Østhus, S., & Bretteville-Jensen, A. L. (2024). Preventing Future Crime in Adolescent Drug Offenders: A Study Of Differential Sanction Effects on Recidivism. *Criminology and Criminal Justice*, *24*(1), 164–183. https://doi.org/10.1177/17488958211070364

Sarkar, G., & Shukla, S. K. (2023). Behavioral Analysis of Cybercrime: Paving the Way for Effective Policing Strategies. *Journal of Economic Criminology*, *2*, 100034. https://doi.org/10.1016/j.jeconc.2023.100034

Schiks, J. A. M., van de Weijer, S. G. A., & Leukfeldt, E. R. (2022). High Tech Crime, High Intellectual Crime? Comparing the Intellectual Capabilities of Cybercriminals, Traditional Criminals and Non-Criminals. *Computers in Human Behavior*, *126*, 106985. https://doi.org/10.1016/j.chb.2021.106985

Sun, T., Xu, Y., Wang, H., & Chen, Z. (2025). A Legal Study: How Do China's Top 10 Intelligent Connected Vehicle Companies Protect Consumer Rights? *World Electric Vehicle Journal*, *16*(3), 140. https://doi.org/10.3390/wevj16030140

Sundram, P. (2024). ASEAN Cooperation to Combat Transnational Crime: Progress, Perils, and Prospects. *Frontiers in Political Science*, *6*, 1304828. https://doi.org/10.3389/fpos.2024.1304828

Tan, E., Lerouge, E., Du Caju, J., & Du Seuil, D. (2023). Verification of Education Credentials on European Blockchain Services Infrastructure (EBSI): Action Research in a Cross-Border Use Case between Belgium and Italy. *Big Data and Cognitive Computing*, *7*(2), 79. https://doi.org/10.3390/bdcc7020079

Yadav, A., Kumar, A., & Singh, V. (2023). Open-Source Intelligence: A Comprehensive Review of the Current State, Applications and Future Perspectives in Cyber Security. In *Artificial Intelligence Review* (Vol. 56, Issue 11). Springer Netherlands. https://doi.org/10.1007/s10462-023-10454-y

Yuan, J. (2023). Legislative Practice of Preventive Detention in China. *Peking University Law Journal*, *11*(1), 73–90. https://doi.org/10.1080/20517483.2023.2223848

Zhang, H., & Gong, X. (2023). The Research on an Electronic Evidence Forensic System for Cross-Border Cybercrime. *The International Journal of Evidence & Proof*, *28*(1), 21–44. https://doi.org/10.1177/13657127231187059