Jurnal Hukum Terapan dan Inovasi Hukum

https://journalversa.com/s/index.php/jhtih Vol. 7, No. 1, Februari 2025

MODERNISASI SISTEM HUKUM PIDANA DALAM MENANGGAPI PERKEMBANGAN KEJAHATAN SIBER GLOBAL

Suryo Wijoyo[1], Zainal Arifin Hoessein[2]

[1,2]Universitas Borobudur

suryowijoyo.uki@gmail.com[1], zainal.arifin@umj.ac.id[2]

ABSTRAK

Perkembangan teknologi informasi telah membawa tantangan baru bagi sistem hukum pidana, terutama dalam menghadapi kejahatan siber yang bersifat lintas negara. Modernisasi sistem hukum pidana menjadi keharusan untuk menjamin perlindungan hukum yang efektif dan adaptif terhadap perkembangan ini. Penelitian ini bertujuan untuk menganalisis langkah-langkah modernisasi sistem hukum pidana Indonesia dalam merespons kejahatan siber global, dengan mengacu pada standar internasional dan praktik terbaik dari berbagai negara. Penelitian menggunakan metode yuridis normatif dengan pendekatan perundang-undangan, konseptual, dan komparatif. Data dikumpulkan melalui kajian pustaka terhadap regulasi nasional, perjanjian internasional, dan literatur akademik yang relevan. Pembahasan difokuskan pada analisis terhadap kelemahan regulasi hukum pidana siber di Indonesia serta perbandingan dengan regulasi di negara-negara lain, seperti Amerika Serikat dan Uni Eropa, yang telah menerapkan kerangka hukum siber yang lebih maju. Hasil penelitian menunjukkan bahwa sistem hukum pidana Indonesia masih menghadapi tantangan dalam mengakomodasi karakteristik unik kejahatan siber, termasuk aspek lintas yurisdiksi, anonimitas pelaku, dan penggunaan teknologi canggih. Modernisasi diperlukan dalam bentuk pembaruan regulasi, penguatan kapasitas penegak hukum, serta peningkatan kerja sama internasional. Kesimpulannya, modernisasi sistem hukum pidana tidak hanya melibatkan pembaruan undang-undang, tetapi juga transformasi kelembagaan dan penguatan koordinasi global.

Kata Kunci: Hukum Pidana, Kejahatan Siber, Modernisasi Hukum, Sistem Hukum Global, Teknologi Informasi.

ABSTRACT

The development of information technology has brought new challenges to the criminal justice system, especially in dealing with cross-border cyber crimes. Modernization of the criminal law system is a necessity to ensure legal protection that is effective and adaptive to these developments. This research aims to analyze steps to modernize the Indonesian criminal law system in response to global cyber crime, by referring to international standards and best practices from various countries. The research uses normative juridical methods with statutory, conceptual and comparative approaches. Data was collected through a literature review of

national regulations, international agreements and relevant academic literature. The discussion focuses on analyzing the weaknesses of cyber criminal law regulations in Indonesia as well as comparisons with regulations in other countries, such as the United States and the European Union, which have implemented a more advanced cyber legal framework. The research results show that the Indonesian criminal law system still faces challenges in accommodating the unique characteristics of cybercrime, including cross-jurisdictional aspects, perpetrator anonymity, and the use of advanced technology. Modernization is needed in the form of regulatory updates, strengthening law enforcement capacity, and increasing international cooperation. In conclusion, modernizing the criminal justice system does not only involve legislative reform, but also institutional transformation and strengthening global coordination.

Keywords: *Criminal Law, Cyber Crime, Legal Modernization, Global Legal System, Information Technology.*

A. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa transformasi besar dalam berbagai aspek kehidupan manusia, mulai dari ekonomi, pendidikan, hingga sistem pemerintahan. Namun, di sisi lain, kemajuan ini juga melahirkan tantangan serius berupa meningkatnya kejahatan siber yang bersifat global. Kejahatan siber mencakup berbagai bentuk tindakan melawan hukum yang memanfaatkan teknologi informasi, seperti peretasan, pencurian data, hingga penipuan daring[1]. Kejahatan ini tidak hanya mengancam individu tetapi juga stabilitas ekonomi dan keamanan nasional. Fenomena ini menuntut sistem hukum pidana untuk beradaptasi dan mampu memberikan respons yang memadai dalam menangani dinamika kejahatan yang terus berkembang[2].

Indonesia telah memiliki sejumlah regulasi untuk menangani kejahatan siber, salah satunya adalah Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Pasal 27 hingga Pasal 30 UU ITE mengatur tindak pidana seperti pencemaran nama baik, akses ilegal, dan manipulasi data elektronik. Meskipun UU ITE menjadi langkah awal yang penting,

[1] Lc., MA. Dr. Husamuddin MZ et al., HUKUM ACARA PIDANA & PIDANA CYBER, Medan: PT Media Penerbit Indonesia, 2024). Hlm. 35

[2] Miftakhur Rokhman Habibi and Isnatul Liviani, "Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia" *Al-Qānūn: Jurnal Pemikiran dan Pembaharuan Hukum Islam*. 23.2 (2020).

tantangan global dalam kejahatan siber sering kali melampaui batas yurisdiksi nasional. Oleh karena itu, diperlukan modernisasi yang lebih komprehensif terhadap sistem hukum pidana untuk menghadapi karakteristik kejahatan siber yang unik, seperti anonimitas pelaku dan sifat lintas negara.

Sebagai tindak lanjut, Indonesia juga telah meratifikasi Konvensi Budapest tentang Kejahatan Siber melalui Undang-Undang Nomor 11 Tahun 2020 tentang Cipta Kerja. Konvensi ini memberikan kerangka hukum internasional untuk menangani kejahatan siber dan meningkatkan kerja sama antarnegara dalam investigasi dan penuntutan kasus-kasus siber. Namun, pelaksanaan konvensi ini di tingkat nasional menghadapi berbagai hambatan, termasuk kurangnya kapasitas teknologi di lembaga penegak hukum dan terbatasnya harmonisasi dengan peraturan lain dalam sistem hukum Indonesia.

Kejahatan siber global memiliki sifat yang sangat dinamis, dengan modus operandi yang terus berkembang seiring kemajuan teknologi[3]. Contoh nyata adalah serangan ransomware yang meningkat dalam beberapa tahun terakhir, di mana pelaku meminta tebusan dalam bentuk mata uang kripto setelah mengenkripsi data korban. Hal ini menunjukkan bahwa pelaku kejahatan siber tidak hanya menggunakan teknologi canggih, tetapi juga memanfaatkan celah hukum yang belum diatur secara spesifik. Situasi ini menggarisbawahi urgensi untuk memperbarui kerangka hukum pidana agar mampu mengantisipasi tren kejahatan siber di masa depan.

Sistem hukum pidana di Indonesia masih menghadapi berbagai tantangan dalam menangani kejahatan siber. Salah satu tantangan utama adalah kurangnya aturan yang secara khusus mengatur pengumpulan bukti digital dalam proses penyelidikan dan penuntutan. Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (KUHAP) belum sepenuhnya mengakomodasi kebutuhan ini, sehingga sering kali menimbulkan kendala dalam pembuktian kasus-kasus siber di pengadilan. Hal ini menegaskan perlunya revisi hukum acara pidana yang lebih selaras dengan era digital.

Modernisasi sistem hukum pidana tidak hanya mencakup pembaruan regulasi, tetapi juga memerlukan penguatan kapasitas kelembagaan dan teknologi di tingkat penegakan

[3] Rafi Septia Budianto Pansariadi and Noenik Soekorini, "Tindak Pidana Cyber Crime dan Penegakan Hukumnya" *Binamulia Hukum*. 12.2 (2023): 287–298.

hukum. Polri dan lembaga terkait lainnya perlu dilengkapi dengan perangkat teknologi mutakhir dan pelatihan khusus untuk menangani kejahatan siber. Di samping itu, penguatan literasi hukum digital di kalangan masyarakat menjadi langkah preventif yang penting untuk mengurangi potensi menjadi korban kejahatan siber.

Kerja sama internasional menjadi elemen penting dalam upaya penanggulangan kejahatan siber. Banyak negara telah membangun kerangka kerja kolaboratif untuk berbagi informasi intelijen, mengintegrasikan mekanisme penegakan hukum, dan mengejar pelaku kejahatan lintas negara. Indonesia perlu memanfaatkan kerja sama ini secara optimal untuk menutup celah-celah dalam sistem hukum yang dapat dimanfaatkan oleh pelaku kejahatan siber[4]. Hal ini tidak hanya meningkatkan efektivitas penegakan hukum, tetapi juga memperkuat posisi Indonesia dalam forum internasional.

Kejahatan siber global adalah ancaman serius yang memerlukan respons komprehensif dari sistem hukum pidana. Perubahan yang mencakup pembaruan regulasi, penguatan kelembagaan, serta kolaborasi internasional menjadi langkah kunci untuk memastikan sistem hukum pidana Indonesia mampu menghadapi tantangan ini secara efektif. Penelitian ini bertujuan untuk menganalisis kebutuhan modernisasi tersebut dan memberikan rekomendasi strategis untuk memperkuat sistem hukum pidana Indonesia dalam menghadapi kejahatan siber global.

Rumusan Masalah :

1. Bagaimana modernisasi hukum pidana Indonesia mengakomodasi teknologi informasi untuk menangani kejahatan siber lintas negara?
2. Mengapa hukum pidana saat ini belum efektif menghadapi tantangan unik kejahatan siber?
3. Bagaimana penerapan Konvensi Budapest mendukung pembaruan hukum pidana Indonesia untuk menangani kejahatan siber global?

B. METODE PENELITIAN

[4] Andi Mohammad Agus Mustam, "MEMERANGI KEJAHATAN SIBER DI INDONESIA: ANALISIS REGULASI HUKUM PIDANA YANG BERLAKU DAN TANTANGANNYA" *Journal homepage: https://journal.uniba.ac.id/index.php/GM/index/*. 35.01 (2023): 10–14.

Penelitian ini menggunakan metode yuridis normatif, yang merupakan pendekatan dalam penelitian hukum yang berfokus pada analisis normatif terhadap peraturan perundang-undangan, doktrin hukum, dan prinsip-prinsip yang berlaku[5]. Pendekatan ini bertujuan untuk mengkaji aturan hukum yang terkait dengan kejahatan siber, baik dalam konteks nasional maupun internasional. Penelitian ini mengedepankan pemahaman mendalam tentang bagaimana sistem hukum pidana dapat dimodernisasi untuk menghadapi tantangan kejahatan siber global.

Pendekatan yang digunakan dalam penelitian ini mencakup beberapa metode, yaitu pendekatan perundang-undangan (statute approach), pendekatan konseptual (conceptual approach), dan pendekatan komparatif (comparative approach). Pendekatan perundang-undangan dilakukan dengan meneliti berbagai regulasi yang relevan, seperti Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Nomor 11 Tahun 2020 tentang Cipta Kerja, serta ketentuan internasional seperti Konvensi Budapest tentang Kejahatan Siber. Pendekatan konseptual digunakan untuk menggali konsep-konsep dasar terkait kejahatan siber dan modernisasi sistem hukum pidana, sedangkan pendekatan komparatif bertujuan untuk membandingkan regulasi hukum pidana di Indonesia dengan negara-negara lain yang lebih maju dalam menangani kejahatan siber.

Sumber bahan hukum dalam penelitian ini dibagi menjadi dua kategori, yaitu bahan hukum primer dan bahan hukum sekunder. Bahan hukum primer meliputi peraturan perundang-undangan, putusan pengadilan, serta dokumen internasional yang relevan, seperti Konvensi Budapest. Sementara itu, bahan hukum sekunder mencakup literatur hukum, artikel jurnal ilmiah bereputasi, buku teks, dan pendapat ahli hukum terkemuka. Bahan hukum ini dianalisis untuk memahami kelemahan dalam sistem hukum pidana Indonesia dan untuk merumuskan langkah-langkah modernisasi yang diperlukan.

Pengumpulan bahan hukum dilakukan melalui studi pustaka yang mendalam. Peneliti memanfaatkan berbagai sumber seperti jurnal bereputasi nasional dan internasional, buku hukum, serta artikel yang relevan dari basis data seperti Scopus, HeinOnline, dan ScienceDirect. Selain itu, pendapat ahli hukum diperoleh dari wawancara tidak langsung

[5] Kornelius Benuf and Muhamad Azhar, "Metodologi Penelitian Hukum sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer" *Jurnal Gema Keadilan* . 7.1 (2020): 20–33.

melalui literatur yang mendokumentasikan pandangan mereka tentang kejahatan siber dan modernisasi hukum pidana. Studi pustaka ini memberikan landasan teoritis yang kokoh bagi analisis yang dilakukan dalam penelitian ini.

Analisis bahan hukum dilakukan secara sistematis dengan menggunakan metode deduktif dan komparatif. Pendekatan deduktif digunakan untuk menelaah ketentuan hukum yang ada dan mengidentifikasi kesenjangan antara regulasi dan kebutuhan praktis dalam menghadapi kejahatan siber. Pendekatan komparatif memberikan perspektif baru dengan melihat bagaimana negara-negara lain menangani tantangan serupa, sehingga menghasilkan rekomendasi yang relevan dan aplikatif untuk konteks Indonesia. Proses ini memastikan bahwa hasil penelitian memiliki nilai akademik yang tinggi dan memberikan kontribusi praktis bagi pengembangan sistem hukum pidana.

C. HASIL DAN PEMBAHASAN

1. Modernisasi hukum pidana Indonesia mengakomodasi teknologi informasi untuk menangani kejahatan siber lintas negara.

Modernisasi hukum pidana Indonesia dalam menghadapi kejahatan siber lintas negara menjadi kebutuhan mendesak seiring dengan meningkatnya kompleksitas kejahatan siber. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) merupakan salah satu instrumen utama dalam penanganan kejahatan siber di Indonesia. Pasal 27 hingga Pasal 30 UU ITE mengatur tindak pidana seperti pencemaran nama baik secara elektronik, akses ilegal, dan manipulasi data. Namun, implementasi regulasi ini menunjukkan adanya keterbatasan dalam menjangkau pelaku kejahatan lintas negara yang memanfaatkan teknologi canggih dan anonimitas jaringan.

Karakteristik kejahatan siber yang bersifat lintas yurisdiksi menciptakan tantangan baru bagi sistem hukum pidana Indonesia[6]. Dalam konteks ini, Konvensi Budapest tentang Kejahatan Siber, yang diadopsi melalui Undang-Undang Nomor 11 Tahun 2020 tentang Cipta Kerja, memberikan kerangka internasional untuk mengatasi keterbatasan tersebut. Konvensi ini mengatur prinsip-prinsip kerja sama antarnegara, termasuk pertukaran informasi dan

[6] Dr. Sahat Maruli T. Situmeang, S.H., M.H. CYBER LAW, vols. (Bandung: CV. Cakra, 2020).

penyelidikan lintas batas. Namun, di tingkat nasional, implementasi konvensi ini masih menghadapi kendala, terutama dalam hal harmonisasi dengan regulasi domestik dan kapasitas teknologi lembaga penegak hukum.

Aspek penting lain dari modernisasi hukum pidana adalah pengakuan terhadap bukti digital sebagai elemen kunci dalam pembuktian kejahatan siber. Dalam praktiknya, Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (KUHAP) belum sepenuhnya mengakomodasi pengumpulan dan validasi bukti digital. Hal ini menyebabkan hambatan signifikan dalam proses penuntutan, terutama ketika bukti tersebut berasal dari lintas negara. Perluasan pengaturan tentang pengakuan bukti digital melalui revisi KUHAP menjadi langkah penting dalam modernisasi ini.

Undang-Undang Nomor 5 Tahun 2018 tentang Pemberantasan Tindak Pidana Terorisme turut memuat pengaturan tentang kejahatan siber yang berpotensi digunakan untuk pendanaan terorisme. Pasal 43A undang-undang ini menekankan pentingnya kerja sama internasional dalam mengidentifikasi, melacak, dan memblokir aliran dana yang melibatkan teknologi digital. Pengaturan ini mencerminkan bahwa modernisasi hukum pidana tidak hanya menyangkut adaptasi terhadap teknologi, tetapi juga memperluas cakupan kejahatan yang dapat ditangani secara efektif.

Dalam konteks pembaruan regulasi, integrasi teknologi informasi dalam penegakan hukum pidana menjadi salah satu fokus utama. Penggunaan teknologi digital, seperti perangkat lunak forensik dan sistem pengawasan siber, telah mulai diadopsi oleh kepolisian dan lembaga terkait lainnya[7]. Namun, adopsi ini masih terbatas pada kasus-kasus tertentu dan memerlukan penguatan lebih lanjut agar dapat diterapkan secara luas. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik juga memberikan landasan bagi lembaga penegak hukum untuk mengakses data dalam upaya investigasi kejahatan siber.

Kerja sama internasional menjadi elemen penting dalam upaya modernisasi hukum pidana. Melalui Interpol dan forum lainnya, Indonesia berpartisipasi dalam pertukaran data dan pelatihan penanganan kejahatan siber. Namun, tantangan utama dalam kerja sama ini adalah

[7] Amsori, Fakhri Awaluddin, and Momon Mulyana, "Tantangan dan Peran Digital Forensik dalam Penegakan Hukum terhadap Kejahatan di Ranah Digital" *Journal Humaniora: Jurnal Hukum dan Ilmu Sosial*. 02.01 (2024).

perbedaan yurisdiksi hukum antarnegara, yang sering kali memperlambat proses penyelidikan. Harmonisasi hukum pidana Indonesia dengan standar internasional menjadi langkah strategis untuk mengoptimalkan kerja sama tersebut.

Modernisasi hukum pidana juga memerlukan penguatan kapasitas penegak hukum dalam memahami dan memanfaatkan teknologi informasi. Pelatihan khusus untuk penyidik dan penuntut umum telah dilakukan, tetapi keberlanjutannya menjadi isu yang perlu diperhatikan. Kurikulum pelatihan yang berbasis teknologi, seperti analisis data besar dan forensik digital, menjadi krusial untuk meningkatkan efektivitas penanganan kejahatan siber.

Transformasi digital yang terjadi secara global telah mendorong peningkatan signifikan dalam berbagai bentuk kejahatan siber. Kejahatan ini memiliki karakteristik yang unik, seperti anonimitas pelaku, sifat lintas negara, dan penggunaan teknologi canggih, yang sering kali menyulitkan penegakan hukum. Sistem hukum pidana Indonesia, meskipun telah memiliki dasar regulasi melalui Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), masih perlu dimodernisasi untuk mengatasi tantangan tersebut. Pasal-pasal dalam UU ITE, seperti Pasal 27-30, memberikan landasan hukum untuk menangani tindak pidana pencemaran nama baik, akses ilegal, dan manipulasi data elektronik, tetapi belum sepenuhnya mampu mengakomodasi kompleksitas kejahatan siber lintas negara.

Sebagai upaya modernisasi, pemerintah Indonesia telah meratifikasi beberapa instrumen internasional, seperti Konvensi Budapest, melalui kebijakan nasional yang tertuang dalam Undang-Undang Nomor 11 Tahun 2020 tentang Cipta Kerja. Instrumen ini memberikan pedoman internasional dalam menangani kejahatan siber, terutama yang melibatkan yurisdiksi lintas negara. Namun, pelaksanaan Konvensi Budapest di Indonesia memerlukan harmonisasi lebih lanjut dengan sistem hukum nasional, termasuk revisi terhadap KUHAP untuk mengakomodasi bukti elektronik sebagai elemen penting dalam proses pembuktian.

Pemanfaatan teknologi informasi dalam sistem hukum pidana juga mencakup pengembangan infrastruktur yang mendukung digitalisasi proses hukum[8]. Sistem manajemen perkara berbasis elektronik dapat membantu meningkatkan transparansi dan efisiensi dalam

[8] Andy Satria et al., "Penggunaan Teknologi Informasi Dalam Penegakan Hukum Pada Bidang Sistem Politik" *Doktrin: Jurnal Dunia Ilmu Hukum dan Politik* . 2.2 (2024).

proses penanganan kasus kejahatan siber. Langkah ini tidak hanya relevan untuk mempercepat proses hukum, tetapi juga sebagai upaya untuk menghadapi dinamika perkembangan teknologi yang terus berubah.

Di tingkat nasional, langkah modernisasi hukum pidana harus mencakup revisi regulasi yang memastikan perlindungan data pribadi yang lebih kuat. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi memberikan dasar hukum untuk melindungi hak individu atas data pribadi mereka. Namun, implementasi yang lebih ketat diperlukan agar regulasi ini dapat mendukung pengamanan terhadap risiko kejahatan siber yang semakin kompleks.

2. Hukum pidana saat ini belum efektif menghadapi tantangan unik kejahatan siber

Kejahatan siber merupakan fenomena global yang semakin berkembang, mengancam berbagai sektor, mulai dari keamanan data hingga stabilitas ekonomi. Di Indonesia, upaya penanggulangan kejahatan siber telah diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang kemudian diperbarui melalui Undang-Undang Nomor 19 Tahun 2016. Pasal 27 hingga Pasal 30 UU ITE mengatur berbagai bentuk tindak pidana siber, termasuk pelanggaran privasi, akses ilegal, dan manipulasi data elektronik. Namun, dalam praktiknya, implementasi hukum pidana ini sering kali kurang efektif dalam mengatasi kompleksitas kejahatan siber.

Salah satu tantangan utama yang dihadapi oleh hukum pidana adalah anonimitas pelaku kejahatan siber[9]. Modus operandi seperti penggunaan perangkat lunak enkripsi dan jaringan anonim seperti *dark web* menyulitkan identifikasi dan pelacakan pelaku. Dalam konteks ini, Pasal 30 UU ITE yang mengatur tentang akses ilegal sering kali tidak cukup untuk menangkap pelaku yang memanfaatkan teknologi canggih untuk menyembunyikan identitas mereka. Hal ini menunjukkan bahwa pendekatan regulasi yang ada belum mampu mengimbangi kecepatan perkembangan teknologi informasi.

Selain itu, sifat lintas yurisdiksi dari kejahatan siber menambah lapisan kompleksitas dalam penegakan hukum. Kejahatan seperti penipuan daring atau serangan ransomware

[9] Nurul Aini and Fauziah Lubis, "TANTANGAN PEMBUKTIAN DALAM KASUS KEJAHATAN " *Judge : Jurnal Hukum*. 05.02 (2024): 55–63.

sering melibatkan pelaku dan korban yang berada di negara berbeda. Meskipun Indonesia telah meratifikasi beberapa perjanjian internasional, termasuk Konvensi Budapest melalui Undang-Undang Nomor 11 Tahun 2020 tentang Cipta Kerja, implementasi di tingkat nasional belum optimal. Harmonisasi antara hukum nasional dan kerangka kerja internasional masih menjadi kendala besar dalam penanganan kejahatan siber lintas negara.

Pembuktian dalam kasus kejahatan siber juga menjadi tantangan serius bagi sistem hukum pidana. Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (KUHAP) belum sepenuhnya mengakomodasi pembuktian digital sebagai alat bukti sah. Sering kali, bukti digital seperti jejak IP, metadata, atau komunikasi terenkripsi sulit diakui dalam proses peradilan. Ketidakjelasan prosedur dalam pengumpulan dan validasi bukti digital ini melemahkan posisi hukum dalam menuntut pelaku kejahatan siber.

Di sisi lain, penguatan kapasitas teknologi lembaga penegak hukum juga menjadi kebutuhan mendesak. Banyak kasus kejahatan siber tidak dapat diselesaikan karena keterbatasan teknologi dan pengetahuan di kalangan penegak hukum. Meskipun Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia memberikan kewenangan kepada Polri untuk menangani kejahatan teknologi tinggi, pelaksanaan kewenangan ini sering kali terbatas oleh minimnya sumber daya teknologi yang diperlukan untuk investigasi siber yang efektif[10].

Ketidakharmonisan antara UU ITE dengan undang-undang lain, seperti Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan dan Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi, juga menghambat efektivitas penanganan kejahatan siber. Sebagai contoh, kasus peretasan data keuangan sering kali berada di persimpangan antara UU ITE dan regulasi perbankan, sehingga menciptakan ambiguitas yurisdiksi. Hal ini menimbulkan masalah koordinasi antar lembaga dalam menyelesaikan kasus yang terkait dengan kejahatan siber.

Selain kelemahan dalam regulasi, rendahnya kesadaran masyarakat tentang risiko kejahatan siber memperburuk situasi. Kurangnya literasi hukum digital di kalangan masyarakat menjadikan individu maupun institusi lebih rentan terhadap serangan siber. Pasal

[10] Alexander Kennedy, "PERLINDUNGAN DATA PRIBADI DALAM DUNIA SIBER DI INDONESIA DITINJAU BERDASARKAN HUKUM TATA NEGARA" 06.2 (2024): 82–98.

28 UU ITE yang mengatur tentang penyebaran informasi elektronik berisi hoaks atau fitnah, misalnya, sering kali tidak dipahami secara mendalam oleh masyarakat sehingga penegakan hukumnya tidak berjalan optimal.

Dalam menghadapi tantangan-tantangan tersebut, modernisasi sistem hukum pidana menjadi kebutuhan yang tidak dapat diabaikan. Penanganan kejahatan siber memerlukan pendekatan yang holistik, mencakup pembaruan regulasi, peningkatan kapasitas teknologi penegak hukum, dan harmonisasi dengan kerangka hukum internasional. Dengan demikian, meskipun berbagai upaya telah dilakukan, sistem hukum pidana di Indonesia saat ini masih jauh dari optimal dalam menghadapi tantangan unik yang ditimbulkan oleh kejahatan siber.

Meskipun Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) telah mengatur berbagai aspek kejahatan siber seperti dalam Pasal 27 hingga Pasal 30, regulasi ini belum mampu mengakomodasi kompleksitas tindak pidana siber yang sering melibatkan pelaku dari berbagai yurisdiksi. Perbandingan dengan negara-negara lain menunjukkan bahwa regulasi hukum pidana Indonesia masih tertinggal dalam mengatasi tantangan global ini.

Amerika Serikat menjadi salah satu negara dengan kerangka hukum siber yang komprehensif melalui *Computer Fraud and Abuse Act* (CFAA) yang diadopsi sejak tahun 1986[11]. Undang-undang ini secara khusus dirancang untuk mengatasi kejahatan berbasis komputer, termasuk akses ilegal dan peretasan. CFAA memberikan landasan hukum yang jelas bagi otoritas penegak hukum untuk menangani kasus kejahatan siber, termasuk yang bersifat lintas negara. Keberadaan aturan yang fleksibel dalam CFAA memungkinkan penyidik untuk mengajukan tuntutan terhadap pelaku yang beroperasi di luar yurisdiksi Amerika Serikat, sesuatu yang belum diakomodasi sepenuhnya dalam UU ITE.

Di Uni Eropa, *General Data Protection Regulation* (GDPR) menjadi tonggak penting dalam perlindungan data pribadi dan penanganan pelanggaran siber[12]. GDPR memberikan kewenangan luas kepada otoritas hukum untuk menindak pelanggaran, bahkan jika pelaku berada di luar wilayah Uni Eropa. Pendekatan ini relevan untuk mengatasi sifat lintas

[11] Yunita Sekar Ety Arabel and Ida Musofiana, "STUDI PERBANDINGAN HUKUM PIDANA DALAM PENANGANAN KEJAHATAN SIBER: PERSPEKTIF INDONESIA DAN AMERIKA SERIKAT" *Hukum dan Kewarganegaraan*. 06.12 (2024).

[12] Yahya Ziqra et al., "Analisis Hukum General Data Protection Regulation (GDPR) Terhadap Data Pribadi Konsumen Dalam Melakukan Transaksi Online" *IURIS STUDIA: Jurnal Kajian Hukum*. 2.2 (2021): 330–336.

yurisdiksi dari kejahatan siber yang sering melibatkan pelaku internasional. Dalam konteks ini, sistem hukum Indonesia belum memiliki perangkat hukum yang serupa untuk melindungi data pribadi secara efektif maupun untuk menangani kejahatan yang bersifat transnasional.

Selain itu, Singapura melalui *Computer Misuse Act* (CMA) telah menunjukkan efektivitas dalam menghadapi kejahatan siber dengan memperkenalkan pasal-pasal yang secara eksplisit mengatur akses ilegal, peretasan, dan penyalahgunaan data digital. CMA memberikan penekanan pada sanksi yang berat dan langkah-langkah preventif untuk menekan kejahatan siber. Dalam hal ini, pendekatan preventif dan sanksi tegas di Singapura dapat menjadi model bagi Indonesia untuk meningkatkan efektivitas penegakan hukum pidana dalam kasus-kasus siber.

Jepang juga memiliki sistem hukum yang mumpuni melalui *Unauthorized Computer Access Law*. Undang-undang ini memberikan regulasi terperinci tentang pembatasan akses ke sistem komputer tanpa izin, termasuk pengumpulan bukti digital yang sah di pengadilan. Di Indonesia, pengumpulan dan validasi bukti digital masih menjadi kendala, terutama karena KUHAP belum mengakomodasi teknologi digital secara memadai. Ketidakharmonisan antara UU ITE dan KUHAP ini menghambat proses penuntutan kasus siber, sesuatu yang diatasi dengan baik oleh Jepang melalui integrasi hukum acara yang relevan.

Kerangka kerja internasional seperti *Convention on Cybercrime* atau Konvensi Budapest juga menjadi acuan penting bagi negara-negara dalam menangani kejahatan siber[13]. Konvensi ini menyediakan pedoman bagi penyusunan regulasi nasional dan mekanisme kerja sama internasional. Indonesia telah mengadopsi sebagian prinsip Konvensi Budapest melalui UU Nomor 11 Tahun 2020 tentang Cipta Kerja, tetapi implementasinya masih menghadapi hambatan dalam harmonisasi dengan regulasi domestik lainnya. Sebagai perbandingan, negara-negara yang sepenuhnya mengadopsi Konvensi Budapest, seperti Jerman dan Prancis, menunjukkan tingkat efektivitas yang lebih tinggi dalam menangani kejahatan siber lintas negara.

Keberhasilan sistem hukum negara lain dalam menangani kejahatan siber juga tidak terlepas dari penguatan kapasitas lembaga penegak hukum. Di Inggris, *National Cyber*

[13] Elza Qorina Pangestika et al., "PENERAPAN PRINSIP HUKUM INTERNASIONAL DALAM PENEGAKAN HUKUM TERHADAP KEJAHATAN SIBER DAN SERANGAN SIBER" *Jurnal Review Pendidikan dan Pengajaran*. 7.2 (2024).

Security Centre (NCSC) menjadi lembaga khusus yang bertugas menangani ancaman siber. Lembaga ini berperan sebagai penghubung antara penegak hukum, sektor swasta, dan masyarakat untuk memperkuat respons terhadap kejahatan siber. Indonesia belum memiliki lembaga serupa yang secara khusus menangani ancaman siber, sehingga koordinasi antarinstansi sering kali menjadi kendala dalam penegakan hukum.

Perbandingan dengan sistem hukum negara lain menunjukkan bahwa keberhasilan dalam menangani kejahatan siber tidak hanya bergantung pada regulasi, tetapi juga pada integrasi teknologi, penguatan kelembagaan, dan kerja sama internasional. Indonesia dapat mengambil pelajaran dari pendekatan komprehensif yang diterapkan oleh negara-negara seperti Amerika Serikat, Uni Eropa, Singapura, Jepang, dan Inggris. Keberhasilan mereka menunjukkan bahwa penanganan kejahatan siber memerlukan kolaborasi yang erat antara hukum pidana nasional, kerangka hukum internasional, dan pemanfaatan teknologi modern.

3. Penerapan Konvensi Budapest mendukung pembaruan hukum pidana Indonesia untuk menangani kejahatan siber global

Konvensi Budapest merupakan instrumen hukum internasional pertama yang secara khusus dirancang untuk menangani kejahatan siber[14]. Ditetapkan oleh Dewan Eropa pada tahun 2001, konvensi ini bertujuan untuk mengharmonisasi hukum pidana di tingkat nasional, memperkuat kerja sama internasional, dan meningkatkan kapasitas nasional dalam menghadapi kejahatan siber. Sebagai kerangka kerja yang bersifat komprehensif, Konvensi Budapest mencakup ketentuan mengenai kriminalisasi berbagai bentuk kejahatan siber, seperti akses ilegal, intersepsi data tanpa izin, dan penyalahgunaan perangkat lunak. Prinsip ini memberikan landasan yang penting bagi negara-negara anggota untuk mengembangkan regulasi hukum pidana yang lebih adaptif terhadap perkembangan teknologi.

Dalam konteks Indonesia, Konvensi Budapest menjadi acuan penting bagi pembaruan regulasi hukum pidana, khususnya setelah pengesahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan perubahannya melalui Undang-Undang Nomor 19 Tahun 2016. Pasal 27 hingga Pasal 30 UU ITE mengatur tindak

[14] Dina Melina and Diki Zukriadi, "PERKEMBANGAN HUKUM DI DUNIA DIGITAL: EVOLUSI HUKUM KEJAHATAN DUNIA MAYA" *Scientia Jurnal* . (n.d.).

pidana siber, termasuk penghinaan, pencemaran nama baik, akses ilegal, dan manipulasi data. Namun, ketentuan ini masih memiliki keterbatasan dalam menjangkau sifat lintas yurisdiksi dari kejahatan siber, yang menjadi perhatian utama dalam Konvensi Budapest.

Salah satu prinsip utama dalam Konvensi Budapest adalah harmonisasi hukum pidana di tingkat nasional agar sejalan dengan standar internasional. Prinsip ini relevan bagi Indonesia, mengingat sistem hukum pidana yang ada saat ini masih didasarkan pada Kitab Undang-Undang Hukum Pidana (KUHP) peninggalan kolonial Belanda. KUHP tidak memiliki ketentuan khusus yang mengatur kejahatan siber, sehingga diperlukan langkah pembaruan yang mengintegrasikan elemen-elemen Konvensi Budapest. Upaya harmonisasi ini juga tercermin dalam pengesahan Undang-Undang Nomor 11 Tahun 2020 tentang Cipta Kerja, yang membuka peluang untuk mengadopsi standar internasional dalam hukum nasional.

Konvensi Budapest juga menekankan pentingnya pengumpulan bukti digital sebagai bagian dari proses penegakan hukum. Dalam Pasal 19 hingga Pasal 21, konvensi ini mengatur prosedur pencarian dan penyitaan data elektronik, pengungkapan data lalu lintas, serta pengumpulan data terkait yang relevan untuk keperluan investigasi. Di Indonesia, aspek ini masih menjadi tantangan karena KUHAP (Undang-Undang Nomor 8 Tahun 1981) belum sepenuhnya mengakomodasi kebutuhan pembuktian digital. Hal ini menimbulkan kesenjangan dalam proses penyelidikan dan penuntutan kasus-kasus siber, yang membutuhkan perhatian lebih dalam pembaruan hukum pidana.

Kerja sama internasional menjadi elemen kunci yang diusung oleh Konvensi Budapest dalam menangani kejahatan siber global[15]. Melalui Pasal 23 hingga Pasal 35, konvensi ini mendorong negara-negara anggota untuk saling bekerja sama dalam penyelidikan lintas batas, ekstradisi pelaku, dan pertukaran informasi. Prinsip kerja sama ini relevan dengan situasi Indonesia, mengingat banyak kasus kejahatan siber melibatkan pelaku yang beroperasi di luar yurisdiksi nasional. Dalam praktiknya, Indonesia telah menjalin kerja sama dengan Interpol dan negara-negara anggota ASEAN, tetapi perluasan cakupan kerja sama ini sangat diperlukan untuk meningkatkan efektivitas penegakan hukum.

[15] Siti Aura Fadhillah, Michelle Sharon Anastasia Matakupan, and Britney Wilhelmina Berlian Mingga, "Peran Interpol dalam Penyelesaian Kasus Kejahatan Siber Berdasarkan Konvensi Budapest On Cybercrimes" *Journal on Education* . 05.04 (2023): 16553–16564.

Selain itu, Konvensi Budapest memberikan pedoman yang jelas tentang kriminalisasi perangkat lunak berbahaya, sebagaimana diatur dalam Pasal 6. Ketentuan ini dapat menjadi landasan bagi Indonesia untuk mengembangkan regulasi yang lebih spesifik terkait penyebaran malware dan aktivitas serupa. Saat ini, ketentuan serupa hanya diatur secara terbatas dalam Pasal 30 UU ITE, sehingga pembaruan hukum pidana yang lebih komprehensif dapat meningkatkan perlindungan terhadap keamanan siber nasional.

Prinsip perlindungan hak asasi manusia juga menjadi perhatian utama dalam Konvensi Budapest. Pasal 15 menegaskan bahwa setiap tindakan penegakan hukum harus mematuhi standar internasional dalam hal penghormatan terhadap hak privasi dan kebebasan individu. Indonesia dapat memanfaatkan prinsip ini untuk memastikan bahwa pembaruan hukum pidana yang dilakukan tidak hanya berfokus pada aspek penegakan hukum, tetapi juga menjaga keseimbangan antara keamanan dan hak-hak warga negara.

Dengan latar belakang yang kuat dalam regulasi internasional, Konvensi Budapest menyediakan kerangka yang komprehensif untuk pembaruan hukum pidana Indonesia[16]. Penerapan prinsip-prinsip konvensi ini tidak hanya mendukung penanggulangan kejahatan siber secara lebih efektif, tetapi juga meningkatkan posisi Indonesia dalam komunitas internasional sebagai negara yang berkomitmen terhadap keamanan siber global.

Sebelum penerapan prinsip-prinsip Konvensi Budapest, sistem hukum pidana Indonesia menghadapi berbagai kendala dalam penanganan kejahatan siber. Salah satu kendala utamanya adalah ketidaksesuaian antara regulasi nasional dengan sifat global dari kejahatan siber. Contoh kasus yang sering terjadi adalah peretasan yang dilakukan oleh pelaku asing terhadap sistem di Indonesia, di mana pengumpulan bukti digital sering kali terhambat oleh batasan yurisdiksi hukum. Dalam hal ini, Pasal 43 UU ITE telah memberikan kewenangan penyidik untuk mengakses data digital sebagai alat bukti. Namun, peraturan ini masih memerlukan penguatan dalam kerangka hukum acara pidana untuk menjamin keabsahan bukti digital dalam proses peradilan.

Penerapan Konvensi Budapest juga relevan untuk mendukung pembaruan Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (KUHAP) di Indonesia. KUHAP

[16] Dewi Bunga, "Legal Response to Cybercrime in Global and National Dimensions" *PADJADJARAN Journal of Law* . 6.1 (2019).

saat ini belum mengakomodasi secara spesifik prosedur pengumpulan bukti elektronik yang sah, sehingga menyulitkan aparat penegak hukum dalam menangani kasus-kasus siber. Dalam Konvensi Budapest, terdapat ketentuan yang mengatur tentang "preservation order" dan "production order" yang memungkinkan otoritas untuk menyimpan dan mengakses data digital dengan cepat. Penerapan prinsip ini di Indonesia dapat memberikan landasan hukum yang lebih kuat untuk mendukung investigasi kejahatan siber.

Konvensi Budapest juga berperan penting dalam mendorong kerja sama internasional yang lebih efektif. Pasal 32 Konvensi ini, misalnya, mengatur tentang akses lintas batas terhadap data yang tersimpan di server di luar negeri. Ketentuan ini sangat relevan bagi Indonesia, mengingat banyaknya kejahatan siber yang melibatkan pelaku asing dan data yang disimpan di server global. Saat ini, kerja sama internasional Indonesia dalam penanganan kejahatan siber didukung oleh Undang-Undang Nomor 1 Tahun 2006 tentang Bantuan Timbal Balik dalam Masalah Pidana. Namun, peraturan ini masih perlu disesuaikan dengan ketentuan Konvensi Budapest untuk memastikan bahwa kerja sama internasional dapat dilakukan secara lebih efisien.

Selain itu, penerapan Konvensi Budapest dapat membantu mengatasi tantangan teknologi yang sering kali digunakan oleh pelaku kejahatan siber. Misalnya, kejahatan seperti ransomware, di mana pelaku mengenkripsi data korban dan meminta tebusan, memerlukan kemampuan investigasi yang melibatkan teknologi tinggi. Dalam hal ini, Konvensi Budapest memberikan pedoman tentang teknik investigasi modern yang dapat diterapkan oleh aparat penegak hukum. Hal ini relevan dengan upaya Indonesia dalam meningkatkan kapasitas teknologi lembaga penegak hukum, seperti yang diamanatkan dalam Pasal 45C UU ITE.

Penguatan regulasi nasional berdasarkan prinsip-prinsip Konvensi Budapest juga berimplikasi pada perlindungan hak asasi manusia[17]. Pasal 15 Konvensi ini menggarisbawahi pentingnya menjaga keseimbangan antara penegakan hukum dan perlindungan hak-hak individu, termasuk hak atas privasi. Dalam konteks Indonesia, regulasi terkait privasi digital telah diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

[17] Muhammad Mutawalli, “Implementasi Prinsip Konvensi Internasional dalam Mengurai Pelanggaran HAM di Indonesia ” *Arajang : Jurnal Ilmu Sosial Politik Volume* . 6.1 (2023).

(UU PDP). Integrasi antara UU PDP dan prinsip Konvensi Budapest dapat memperkuat pengaturan hukum yang adil dalam menangani kejahatan siber.

Penerapan Konvensi Budapest dalam sistem hukum pidana Indonesia membawa pengaruh signifikan terhadap pembaruan regulasi hukum terkait kejahatan siber. Sebagai instrumen internasional yang mengatur tindak pidana siber, Konvensi Budapest menawarkan panduan yang komprehensif untuk mengharmonisasi hukum pidana dengan perkembangan teknologi global. Dalam konteks ini, Indonesia telah mengadopsi prinsip-prinsip Konvensi melalui berbagai regulasi, termasuk Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Pasal 27 hingga Pasal 30 UU ITE, misalnya, mengatur kriminalisasi terhadap akses ilegal, manipulasi data elektronik, dan penyebaran informasi yang melanggar hukum, sebagaimana diamanatkan oleh Konvensi Budapest.

Pembaruan regulasi hukum pidana yang selaras dengan Konvensi Budapest juga terlihat dalam pengaturan tentang pembuktian digital. Salah satu aspek utama dalam Konvensi ini adalah penekanan pada pengumpulan dan autentikasi bukti elektronik sebagai alat yang sah dalam proses peradilan. Dalam konteks Indonesia, regulasi terkait pembuktian digital diatur dalam Pasal 5 ayat (1) UU ITE, yang mengakui dokumen elektronik sebagai alat bukti hukum. Namun, implementasi pengaturan ini menghadapi tantangan teknis dan kelembagaan, termasuk kebutuhan akan peningkatan kapasitas teknologi di lembaga penegak hukum.

Di sisi lain, adopsi prinsip-prinsip Konvensi Budapest juga memengaruhi pengembangan regulasi mengenai perlindungan data dan privasi di Indonesia. Perlindungan data menjadi elemen penting dalam memerangi kejahatan siber, sebagaimana diatur dalam Pasal 9 Konvensi Budapest. Dalam konteks ini, Indonesia telah mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), yang menjadi landasan penting untuk memastikan keamanan data dalam ruang digital. UU ini diharapkan dapat mendukung upaya penegakan hukum terhadap pelanggaran data yang sering kali menjadi bagian dari kejahatan siber.

D. KESIMPULAN DAN SARAN

Kesimpulan

1. Modernisasi hukum pidana Indonesia dalam menghadapi kejahatan siber global memerlukan pendekatan komprehensif yang mengintegrasikan perkembangan teknologi informasi ke dalam regulasi dan mekanisme penegakan hukum. Upaya pembaruan regulasi, seperti revisi Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), telah memberikan langkah awal yang signifikan untuk mengakomodasi kebutuhan hukum di era digital. Namun, respons terhadap tantangan lintas negara dalam kejahatan siber membutuhkan penguatan kerangka hukum yang lebih adaptif dan selaras dengan standar internasional, termasuk dalam pengaturan yurisdiksi, pengumpulan bukti digital, dan mekanisme kerja sama internasional.
2. Efektivitas hukum pidana Indonesia dalam menghadapi kejahatan siber saat ini masih terbatas oleh berbagai kendala, seperti kesenjangan teknologi, kurangnya kapasitas penegak hukum, dan lemahnya harmonisasi antarregulasi. Keterbatasan dalam hukum acara pidana, khususnya dalam pengaturan terkait bukti elektronik, menjadi hambatan utama dalam penegakan hukum yang efektif. Hal ini menunjukkan perlunya revisi menyeluruh terhadap hukum acara pidana dan penguatan kelembagaan untuk memastikan bahwa sistem hukum mampu menghadapi kompleksitas kejahatan siber, termasuk karakteristik unik seperti anonimitas pelaku dan sifat lintas yurisdiksi.
3. Penerapan Konvensi Budapest memberikan landasan yang kuat bagi pembaruan hukum pidana Indonesia untuk menghadapi kejahatan siber global. Harmonisasi dengan prinsip-prinsip dalam Konvensi Budapest, seperti kriminalisasi tindakan siber tertentu dan mekanisme kerja sama lintas negara, memungkinkan sistem hukum Indonesia untuk lebih efektif dalam menanggapi ancaman kejahatan siber. Dengan adopsi regulasi seperti Undang-Undang Perlindungan Data Pribadi (UU PDP) dan penguatan kapasitas teknologi di lembaga penegak hukum, Indonesia dapat meningkatkan efisiensi penegakan hukum dan memperkuat posisinya dalam kerja sama internasional. Hasil penelitian ini menunjukkan bahwa pembaruan hukum pidana yang berbasis pada Konvensi Budapest memberikan peluang besar untuk meningkatkan keamanan digital di Indonesia.

Saran

1. Pemerintah perlu segera merevisi Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (KUHAP) untuk mengakomodasi pengaturan yang lebih jelas mengenai pembuktian digital. Pengaturan ini harus mencakup mekanisme pengumpulan, autentikasi, dan penyimpanan bukti elektronik, sesuai dengan prinsip-prinsip yang diatur dalam Konvensi Budapest. Dengan adanya penguatan dalam hukum acara pidana, proses penegakan hukum terhadap kejahatan siber dapat berjalan lebih efektif dan sesuai dengan standar internasional.
2. Peningkatan kapasitas penegak hukum melalui pelatihan khusus tentang investigasi siber dan penguasaan teknologi informasi menjadi prioritas utama. Lembaga penegak hukum, seperti Polri dan kejaksaan, perlu dilengkapi dengan perangkat teknologi mutakhir dan pelatihan berkelanjutan untuk menghadapi karakteristik unik kejahatan siber, termasuk anonimitas pelaku dan sifat lintas yurisdiksi. Langkah ini tidak hanya akan meningkatkan efektivitas penyelidikan tetapi juga mengurangi ketergantungan pada bantuan pihak luar dalam menangani kejahatan siber lintas negara.
3. Optimalisasi kerja sama internasional perlu dilakukan melalui implementasi lebih lanjut dari Konvensi Budapest, khususnya dalam penguatan mekanisme ekstradisi, pertukaran informasi, dan penyelarasan kebijakan dengan negara lain. Pemerintah juga perlu memanfaatkan forum internasional untuk memperkuat posisi Indonesia sebagai mitra strategis dalam pemberantasan kejahatan siber. Dengan kerja sama yang lebih intensif, Indonesia dapat memastikan bahwa pelaku kejahatan siber lintas negara tidak dapat lolos dari proses hukum, sekaligus meningkatkan keamanan digital secara global.

DAFTAR PUSTAKA

Alexander Kennedy. “PERLINDUNGAN DATA PRIBADI DALAM DUNIA SIBER DI INDONESIA DITINJAU BERDASARKAN HUKUM TATA NEGARA” 06.2 (2024): 82–98.

Amsori, Fakhri Awaluddin, and Momon Mulyana. “Tantangan dan Peran Digital Forensik dalam Penegakan Hukum terhadap Kejahatan di Ranah Digital.” *Journal Humaniora: Jurnal Hukum dan Ilmu Sosial* 02.01 (2024).

Andi Mohammad Agus Mustam. “MEMERANGI KEJAHATAN SIBER DI INDONESIA: ANALISIS REGULASI HUKUM PIDANA YANG BERLAKU DAN

TANTANGANNYA." *Journal homepage: https://journal.uniba.ac.id/index.php/GM/index/* 35.01 (2023): 10–14.

Andy Satria et al. "Penggunaan Teknologi Informasi Dalam Penegakan Hukum Pada Bidang Sistem Politik." *Doktrin: Jurnal Dunia Ilmu Hukum dan Politik* 2.2 (2024).

Dewi Bunga. "Legal Response to Cybercrime in Global and National Dimensions." *PADJADJARAN Journal of Law* 6.1 (2019).

Dina Melina, and Diki Zukriadi. "PERKEMBANGAN HUKUM DI DUNIA DIGITAL: EVOLUSI HUKUM KEJAHATAN DUNIA MAYA." *Scientia Jurnal* (n.d.).

Dr. Husamuddin MZ, Lc., MA. et al. *HUKUM ACARA PIDANA & PIDANA CYBER*. Medan: PT Media Penerbit Indonesia, 2024.

Dr. Sahat Maruli T. Situmeang, S.H., M.H. *CYBER LAW*. Bandung: CV. Cakra, 2020.

Elza Qorina Pangestika et al. "PENERAPAN PRINSIP HUKUM INTERNASIONAL DALAM PENEGAKAN HUKUM TERHADAP KEJAHATAN SIBER DAN SERANGAN SIBER." *Jurnal Review Pendidikan dan Pengajaran* 7.2 (2024).

Kornelius Benuf, and Muhamad Azhar. "Metodologi Penelitian Hukum sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer." *Jurnal Gema Keadilan* 7.1 (2020): 20–33.

Miftakhur Rokhman Habibi, and Isnatul Liviani. "Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia." *Al-Qānūn: Jurnal Pemikiran dan Pembaharuan Hukum Islam* 23.2 (2020).

Muhammad Mutawalli. "Implementasi Prinsip Konvensi Internasional dalam Mengurai Pelanggaran HAM di Indonesia ." *Arajang : Jurnal Ilmu Sosial Politik Volume* 6.1 (2023).

Nurul Aini, and Fauziah Lubis. "TANTANGAN PEMBUKTIAN DALAM KASUS KEJAHATAN ." *Judge : Jurnal Hukum* 05.02 (2024): 55–63.

Rafi Septia Budianto Pansariadi, and Noenik Soekorini. "Tindak Pidana Cyber Crime dan Penegakan Hukumnya." *Binamulia Hukum* 12.2 (2023): 287–298.

Siti Aura Fadhillah, Michelle Sharon Anastasia Matakupan, and Britney Wilhelmina Berlian Mingga. "Peran Interpol dalam Penyelesaian Kasus Kejahatan Siber Berdasarkan Konvensi Budapest On Cybercrimes." *Journal on Education* 05.04 (2023): 16553–16564.

Yahya Ziqra et al. "Analisis Hukum General Data Protection Regulation (GDPR) Terhadap Data Pribadi Konsumen Dalam Melakukan Transaksi Online." *IURIS STUDIA: Jurnal Kajian Hukum* 2.2 (2021): 330–336.

Yunita Sekar Ety Arabel, and Ida Musofiana. "STUDI PERBANDINGAN HUKUM PIDANA DALAM PENANGANAN KEJAHATAN SIBER: PERSPEKTIF INDONESIA DAN AMERIKA SERIKAT." *Hukum dan Kewarganegaraan* 06.12 (2024).