Jurnal Hukum dan HAM Wara Sains
Vol. 02, No. 06, Juni, pp. 517 ~ 525

Pemberantasan Tindak Pidana Cyber di Provinsi Jawa Barat: Peran Hukum dan Tantangan dalam Penegakan Hukum Terhadap Kejahatan Digital

Madinah Mokobombang[1], Zulfikri Darwis[2], Sabil Mokodenseho[3]
[1,2,3] Institut Agama Islam Muhammadiyah Kotamobagu dan madinah.mokobombang@iaimkotamobagu.ac.id, zulfikridarwis@iaimkotamobagu.ac.id, sabil.mokodenseho@gmail.com

Article Info

Article history:

Received: Juni, 2023
Revised: Juni, 2023
Accepted: Juni, 2023

Kata Kunci:

Tindak Pidana, Cyber, Jawa Barat, Penegakan Hukum, Kejahatan Digital

Keywords:

Crime, Cyber, West Java, Law Enforcement, Digital Crime

ABSTRAK

Penelitian ini berfokus pada pemberantasan kejahatan siber di Provinsi Jawa Barat dan mengkaji peran hukum dan tantangan yang dihadapi dalam penegakan hukum terhadap kejahatan digital. Pendekatan metode campuran diadopsi, menggabungkan metode kualitatif dan kuantitatif. Studi ini menganalisis kerangka hukum, mekanisme penegakan hukum, dan perspektif pemangku kepentingan melalui wawancara dengan para pemangku kepentingan utama dan analisis dokumen dan literatur hukum yang relevan. Temuan menunjukkan bahwa Indonesia telah memiliki kerangka hukum yang komprehensif, termasuk Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), untuk memerangi kejahatan siber. Namun, tantangan seperti sifat ancaman siber yang berkembang pesat, masalah yurisdiksi, hambatan hukum dan prosedural, masalah privasi, dan kesadaran publik yang terbatas menghambat penegakan hukum yang efektif. Para pemangku kepentingan menekankan pentingnya kerangka hukum yang dapat beradaptasi, peningkatan koordinasi di antara lembaga penegak hukum, sumber daya dan keahlian yang lebih baik, kemitraan pemerintah-swasta, dan peningkatan kesadaran masyarakat. Penelitian ini diakhiri dengan rekomendasi untuk memperkuat kerangka hukum, meningkatkan strategi penegakan hukum, dan mendorong kerja sama publik, yang bertujuan untuk meningkatkan pemberantasan kejahatan siber di Provinsi Jawa Barat.

ABSTRACT

This research focuses on combating cybercrime in West Java Province and examines the role of the law and the challenges faced in law enforcement against digital crime. A mixed methods approach was adopted, combining qualitative and quantitative methods. The study analyzed the legal framework, law enforcement mechanisms, and stakeholder perspectives through interviews with key stakeholders and analysis of relevant legal documents and literature. The findings show that Indonesia already has a comprehensive legal framework, including the Electronic Information and Transaction Law (UU ITE), to combat cybercrime. However, challenges such as the rapidly evolving nature of cyber threats, jurisdictional issues, legal and procedural barriers, privacy concerns, and limited public awareness hinder effective law enforcement. Stakeholders emphasized the importance of an adaptable legal framework, improved coordination among law enforcement agencies, better resources and expertise, public-private partnerships, and increased public awareness. The study concludes with recommendations to strengthen the legal framework, improve law enforcement strategies, and encourage public cooperation, aiming to improve the fight against cybercrime in West Java Province.

Corresponding Author:

Name: Madinah Mokobombang
Institution: Institut Agama Islam Muhammadiyah Kotamobagu
Email: madinah.mokobombang@iaimkotamobagu.ac.id

1. PENDAHULUAN

Perkembangan teknologi telah memberikan dampak yang signifikan terhadap kejahatan siber. Seiring dengan kemajuan teknologi, para penjahat dunia maya menemukan cara-cara baru untuk mengeksploitasi kerentanan dalam sistem dan jaringan. Dengan meningkatnya pendidikan digital, ekonomi digital, dan bekerja dari rumah, semuanya menjadi online dalam semalam, yang telah memunculkan kasus-kasus kejahatan siber (Bhattacharya et al., 2021). Semakin banyak orang menggunakan internet, semakin banyak peluang bagi penjahat siber untuk mengeksploitasi kerentanan. Seiring dengan kemajuan teknologi, para penjahat siber menemukan cara-cara baru untuk mengeksploitasi kerentanan dalam sistem dan jaringan. Misalnya, spyware adalah perangkat lunak yang di unduh ke komputer untuk melacak aktivitas komputer tanpa sepengetahuan pengguna (Rider, 2001).

Evolusi teknologi e-banking membuat tugas-tugas perbankan menjadi sangat mudah dan cepat dengan sekali klik. Namun, hal ini juga membuat sektor perbankan menjadi lebih kompleks karena diversifikasi transaksi online. Kompleksitas ini telah menciptakan peluang baru bagi para penjahat siber untuk mengeksploitasi kerentanan. Penjahat sekarang dapat beroperasi di luar jangkauan sistem hukum domestik dan melakukan kejahatan yang tidak dapat diterima oleh sistem peradilan pidana tradisional dan agen nya (Rider, 2001). Jangkauan global ini membuat penjahat siber semakin sulit ditangkap. Jangkauan, ruang lingkup, dan volume kejahatan yang di fasilitasi oleh teknologi informasi dan komunikasi telah mengubah risiko yang ditimbulkan terhadap individu, organisasi, dan negara, serta menantang pendekatan konvensional dalam deteksi dan pencegahan kejahatan. Penilaian dampak kejahatan dunia maya selama ini berfokus pada estimasi biaya dalam bentuk uang. Namun, kerugian yang paling signifikan mungkin tidak dirasakan sebagai hilangnya uang, tetapi sebagai gangguan atau destabilisasi sistem yang dibangun di atas kepercayaan.

Individu dan organisasi dapat mengambil beberapa langkah untuk melindungi diri mereka sendiri dari kejahatan dunia maya. Individu dan organisasi harus menggunakan kata sandi yang kuat dan sulit ditebak. Kata sandi harus berupa kombinasi huruf, angka, dan simbol. Kata sandi juga harus diubah secara teratur1. Perangkat lunak antivirus dapat membantu melindungi dari malware dan jenis serangan dunia maya lainnya. Individu dan organisasi harus menginstal perangkat lunak antivirus pada semua perangkat yang terhubung ke internet. Individu dan organisasi harus selalu memperbarui semua perangkat lunak dengan patch keamanan terbaru. Ini termasuk sistem operasi, peramban web, dan perangkat lunak lainnya1. Individu dan organisasi harus berhati-hati terhadap email yang mencurigakan, terutama email yang meminta informasi pribadi atau berisi tautan atau lampiran. Email-email ini mungkin merupakan upaya phishing. Autentikasi dua faktor

menambahkan lapisan keamanan ekstra pada akun online. Ini mengharuskan pengguna memberikan dua bentuk identifikasi, seperti kata sandi dan kode yang dikirim ke perangkat seluler (Back & LaPrade, 2020).

Organisasi harus melatih karyawan mereka tentang cara mengenali dan mencegah serangan dunia maya. Ini termasuk cara mengidentifikasi email phishing, cara menggunakan kata sandi yang kuat, dan cara menjaga perangkat lunak agar tetap mutakhir (Back & LaPrade, 2020). Institusi akademis dapat menerapkan teknik pencegahan kejahatan situasional (SCP) untuk mengurangi insiden kejahatan siber. Teknik SCP termasuk merancang, memelihara, dan menggunakan lingkungan yang dibangun di ranah digital2. Menciptakan kesadaran tentang kejahatan siber dan hukum siber dapat membantu mencegah kejahatan siber. Hal ini termasuk mendidik siswa dan karyawan tentang risiko kejahatan dunia maya dan cara melindungi diri mereka sendiri (Sudhakar & Poorna, 2020)(Mamade & Dabala, 2021). Pemerintah dapat membuat undang-undang untuk mengatasi tantangan keamanan siber secara memadai. Ini termasuk undang-undang yang berhubungan dengan keamanan siber dan koordinasi pelaksanaannya (Mangena, 2016).

Dalam beberapa tahun terakhir, kemajuan teknologi yang pesat dan penggunaan internet yang meluas telah membawa banyak manfaat bagi masyarakat. Namun, seiring dengan kemajuan ini, ancaman kejahatan siber telah menjadi semakin lazim, sehingga menimbulkan tantangan yang signifikan bagi individu, bisnis, dan pemerintah di seluruh dunia. Penjahat siber mengeksploitasi kerentanan dalam sistem digital, menargetkan data sensitif, sumber daya keuangan, dan bahkan infrastruktur penting. Provinsi Jawa Barat di Indonesia, yang dikenal dengan ekonomi digital nya yang berkembang pesat dan penggunaan internet yang ekstensif, tidak kebal terhadap ancaman siber ini. Oleh karena itu, ada kebutuhan mendesak untuk mengatasi kejahatan siber secara efektif di Provinsi Jawa Barat dan melindungi ekosistem digital nya. Tujuan utama dari penelitian ini adalah untuk menyelidiki pemberantasan kejahatan siber di Provinsi Jawa Barat, dengan fokus pada peran hukum dan tantangan yang dihadapi dalam penegakan hukum terhadap kejahatan digital.

2. LANDASAN TEORI

Konseptualisasi Kejahatan Dunia Maya

Kejahatan siber mencakup berbagai aktivitas terlarang yang dilakukan melalui platform dan jaringan digital (Kristiyanti et al., 2022)(Arifin & Rahman, 2021). Hal ini mencakup pelanggaran seperti peretasan, pencurian identitas, penipuan online, phishing, serangan ransomware, dan distribusi malware (Kurniawan & Hapsari, 2021). Sifat dinamis dari kejahatan siber menghadirkan tantangan unik, karena pelaku mengeksploitasi kemajuan teknologi dan terus mengembangkan taktik mereka untuk mem-bypass langkah-langkah keamanan (Maramba & Wulla, 2021)(Somantri et al., 2023).

Kerangka Hukum untuk Kejahatan Dunia Maya di Indonesia

Indonesia telah menyadari perlunya undang-undang yang komprehensif untuk memerangi kejahatan siber (Kurniawan & Hapsari, 2021). Kerangka hukum negara ini mencakup berbagai undang-undang dan peraturan yang menangani pelanggaran siber, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Pemberantasan Tindak Pidana Terorisme, dan Undang-Undang Pencucian Uang (Tinggi & IBLAM, n.d.). Undang-undang ini

bertujuan untuk memberikan dasar hukum untuk mengadili penjahat siber dan melindungi transaksi digital. Namun, penting untuk mengevaluasi implementasi dan efektivitas undang-undang ini, terutama dalam konteks Provinsi Jawa Barat.

Mekanisme Penegakan Hukum Kejahatan Siber di Provinsi Jawa Barat

Lembaga penegak hukum memainkan peran penting dalam memerangi kejahatan siber. Di Provinsi Jawa Barat, berbagai lembaga, termasuk polisi, unit khusus kejahatan siber, dan Badan Siber dan Sandi Negara (BSSN), bertanggung jawab untuk menyelidiki dan menuntut pelanggaran digital. Memahami mekanisme penegakan hukum yang ada dan koordinasi nya sangat penting untuk mengevaluasi efektivitas nya dalam menangani ancaman siber di kawasan ini.

Penelitian Terdahulu tentang Kejahatan Siber di Indonesia

Penelitian sebelumnya telah meneliti berbagai aspek kejahatan siber di Indonesia, termasuk kerangka hukum, tantangan penegakan hukum, dan peran pemangku kepentingan (Sudiyawati & Mertha, 2022). Penelitian-penelitian ini telah menjelaskan prevalensi kejahatan siber, mengidentifikasi kesenjangan dalam sistem hukum, dan menyoroti perlunya peningkatan kolaborasi antara pemerintah, lembaga penegak hukum, dan pemangku kepentingan terkait lainnya (Faridi, 2018). Namun, kajian komprehensif mengenai peran hukum dan tantangan yang dihadapi dalam penegakan hukum terhadap kejahatan digital khususnya di Provinsi Jawa Barat masih

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan metode campuran untuk mendapatkan wawasan yang komprehensif mengenai pemberantasan kejahatan siber di Provinsi Jawa Barat. Penelitian ini menggunakan metode kualitatif dan kuantitatif untuk mencapai pemahaman holistik tentang peran hukum dan tantangan yang dihadapi dalam penegakan hukum terhadap kejahatan digital. Desain penelitian ini mencakup analisis dokumen hukum dan kebijakan yang relevan, serta wawancara dengan para pemangku kepentingan utama yang terlibat dalam penegakan hukum dan keamanan siber.

Proses pengumpulan data terdiri dari sumber data primer dan sekunder.

Data primer dikumpulkan melalui wawancara semi-terstruktur dengan para pemangku kepentingan utama. Para pemangku kepentingan ini dapat mencakup perwakilan dari lembaga penegak hukum, badan pemerintah, pakar keamanan siber, profesional hukum, dan profesional industri. Wawancara ini bertujuan untuk menangkap perspektif mereka tentang peran hukum dan tantangan dalam penegakan hukum terhadap kejahatan siber di Provinsi Jawa Barat. Pemilihan narasumber akan didasarkan pada keahlian dan keterlibatan mereka dalam memerangi kejahatan siber di wilayah tersebut.

Data sekunder dikumpulkan dari berbagai sumber, termasuk dokumen hukum, kebijakan, laporan, artikel akademis, dan literatur yang relevan. Analisis dari sumber-sumber sekunder ini akan memberikan pemahaman yang komprehensif mengenai kerangka hukum, mekanisme penegakan hukum yang ada, tantangan, dan penelitian sebelumnya yang dilakukan mengenai kejahatan siber di Indonesia dan Provinsi Jawa Barat. Data sekunder juga akan memberikan kontribusi pada latar belakang kontekstual penelitian dan berfungsi sebagai dasar perbandingan dan validasi temuan dari data primer.

4. HASIL DAN PEMBAHASAN

Analisis Kerangka Hukum dan Mekanisme Penegakan Hukum

Analisis kerangka hukum menunjukkan bahwa Indonesia telah menetapkan seperangkat peraturan perundang-undangan yang komprehensif untuk menangani kejahatan siber, termasuk Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan undang-undang terkait lainnya. Undang-undang ini memberikan dasar hukum untuk mengadili pelaku kejahatan siber dan melindungi transaksi digital. Namun, efektivitas undang-undang ini dalam memerangi kejahatan siber di Provinsi Jawa Barat memerlukan pemeriksaan lebih lanjut.

Evaluasi mekanisme penegakan hukum menyoroti peran dan tanggung jawab berbagai lembaga yang terlibat dalam pemberantasan kejahatan siber, seperti polisi, unit khusus kejahatan siber, dan Badan Siber dan Sandi Negara (BSSN). Kolaborasi dan koordinasi di antara lembaga-lembaga ini sangat penting untuk penegakan hukum yang efektif. Analisis ini juga menilai sumber daya, kemampuan, dan pelatihan yang tersedia untuk personel penegak hukum dalam menangani kejahatan siber.

Identifikasi Tantangan dalam Pemberantasan Kejahatan Siber

Penelitian ini mengidentifikasi beberapa tantangan yang dihadapi oleh lembaga penegak hukum dalam memberantas kejahatan siber di Provinsi Jawa Barat. Tantangan-tantangan ini termasuk sifat ancaman siber yang berkembang pesat, yang mengharuskan adaptasi dan kemajuan teknologi yang berkelanjutan untuk mengimbangi para penjahat siber. Tantangan yurisdiksi dan kebutuhan akan kerja sama lintas batas menimbulkan hambatan bagi penyelidikan dan penuntutan yang efektif terhadap penjahat siber yang beroperasi melintasi batas-batas negara. Hambatan hukum dan prosedural, termasuk penundaan dalam memperoleh surat perintah dan pengumpulan bukti, menghambat penyelesaian kasus kejahatan siber yang cepat dan efisien. Masalah privasi dan perlindungan data muncul dalam konteks menyeimbangkan kebutuhan penegakan hukum dengan hak-hak individu atas privasi. Terakhir, kesadaran dan kerja sama masyarakat yang tidak memadai menghambat upaya pencegahan kejahatan siber dan pengumpulan informasi penting dari masyarakat.

Perspektif Pemangku Kepentingan tentang Peran Hukum dan Tantangan dalam Penegakan Hukum

Wawancara yang dilakukan dengan para pemangku kepentingan utama menjelaskan perspektif mereka tentang peran hukum dan tantangan yang dihadapi dalam penegakan hukum terhadap kejahatan siber di Provinsi Jawa Barat. Para pemangku kepentingan menekankan pentingnya kerangka hukum yang kuat yang dapat mengimbangi kemajuan teknologi dan mengatasi ancaman siber yang muncul secara efektif. Mereka menyoroti perlunya peningkatan koordinasi di antara lembaga penegak hukum, baik di provinsi maupun di tingkat nasional. Para pemangku kepentingan juga mengungkapkan keprihatinan tentang kurangnya keahlian dan sumber daya khusus dalam lembaga penegak hukum untuk memerangi kejahatan siber secara efektif. Selain itu, wawancara mengungkapkan pentingnya kemitraan pemerintah-swasta, inisiatif peningkatan kapasitas, dan peningkatan kesadaran publik untuk meningkatkan upaya pemberantasan kejahatan siber.

Temuan ini menunjukkan bahwa meskipun Indonesia telah memiliki kerangka hukum dan mekanisme penegakan hukum yang komprehensif, terdapat tantangan signifikan yang menghambat pemberantasan kejahatan siber yang efektif di Provinsi Jawa Barat. Sifat ancaman siber yang berkembang pesat, tantangan yurisdiksi, hambatan hukum dan prosedural, masalah privasi, dan kebutuhan akan kesadaran dan kerja sama publik menuntut perhatian untuk memperkuat upaya yang ada.

Perspektif pemangku kepentingan menggarisbawahi pentingnya kerangka hukum yang dinamis dan mudah beradaptasi, peningkatan koordinasi dan kolaborasi di antara lembaga penegak hukum, sumber daya dan keahlian yang lebih baik, kemitraan pemerintah-swasta, dan peningkatan kesadaran masyarakat untuk memerangi kejahatan siber secara efektif di Provinsi Jawa Barat. Sintesis temuan ini memberikan pemahaman yang komprehensif tentang kondisi upaya pemberantasan kejahatan siber saat ini di provinsi tersebut, menyoroti kekuatan, kelemahan, dan bidang-bidang yang perlu ditingkatkan. Temuan-temuan ini berfungsi sebagai dasar untuk perumusan rekomendasi untuk meningkatkan kerangka hukum, meningkatkan strategi penegakan hukum, dan mengatasi tantangan yang teridentifikasi secara efektif.

Pembahasan

Analisis kerangka hukum menunjukkan bahwa Indonesia telah mengambil langkah signifikan untuk mengatasi kejahatan siber melalui pemberlakuan UU ITE dan undang-undang terkait lainnya. Kerangka hukum yang komprehensif memberikan dasar yang kuat untuk mengadili pelaku kejahatan siber dan melindungi transaksi digital. Namun, efektivitas undang-undang ini di Provinsi Jawa Barat memerlukan pemeriksaan lebih lanjut. Sangat penting untuk menilai implementasi, penegakan, dan keselarasan nya dengan kemajuan teknologi dan ancaman siber yang muncul.

Evaluasi mekanisme penegakan hukum menyoroti peran dan tanggung jawab berbagai lembaga yang terlibat dalam memerangi kejahatan siber. Kolaborasi dan koordinasi di antara lembaga-lembaga ini sangat penting untuk penegakan hukum yang efektif. Analisis ini juga menilai sumber daya, kemampuan, dan pelatihan yang tersedia bagi personel penegak hukum. Jelaslah bahwa berinvestasi dalam pelatihan khusus dan peningkatan kapasitas sangat penting untuk meningkatkan keahlian lembaga penegak hukum dalam menyelidiki dan menuntut kejahatan siber.

Penelitian ini mengidentifikasi beberapa tantangan yang dihadapi oleh lembaga penegak hukum dalam memberantas kejahatan siber di Provinsi Jawa Barat. Sifat ancaman siber yang berkembang pesat menimbulkan tantangan yang signifikan, karena penjahat siber terus mengadaptasi taktik mereka untuk mem-bypass langkah-langkah keamanan. Masalah yurisdiksi dan kebutuhan akan kerja sama lintas batas semakin mempersulit penyelidikan dan penuntutan penjahat siber yang beroperasi melintasi batas negara. Hambatan hukum dan prosedural, termasuk penundaan dalam memperoleh surat perintah dan pengumpulan bukti, menghambat penyelesaian kasus kejahatan siber dengan cepat. Masalah privasi dan perlindungan data muncul dalam menyeimbangkan kebutuhan penegakan hukum dengan hak-hak individu atas privasi. Selain itu, kesadaran dan kerja sama publik yang terbatas menghambat upaya pencegahan dan pengumpulan informasi penting dari masyarakat.

Perspektif pemangku kepentingan yang diperoleh melalui wawancara memberikan wawasan yang berharga tentang peran hukum dan tantangan yang dihadapi dalam penegakan hukum terhadap kejahatan dunia maya. Para pemangku kepentingan menekankan pentingnya kerangka hukum yang dinamis dan mudah beradaptasi, peningkatan koordinasi dan kolaborasi di antara lembaga penegak hukum, sumber daya dan keahlian yang lebih baik, kemitraan pemerintah-swasta, dan peningkatan kesadaran masyarakat. Perspektif ini mencerminkan perlunya pendekatan yang komprehensif dan multi-pemangku kepentingan untuk memerangi kejahatan siber secara efektif di Provinsi Jawa Barat.

Rekomendasi

Berdasarkan temuan penelitian, rekomendasi berikut diusulkan untuk memperkuat pemberantasan kejahatan siber di Provinsi Jawa Barat:

Meningkatkan Kerangka Hukum

a. Terus meninjau dan memperbarui kerangka hukum untuk mengimbangi kemajuan teknologi dan ancaman siber yang muncul.
b. Mempertimbangkan pembentukan pengadilan khusus kejahatan siber atau divisi dalam sistem peradilan yang ada untuk menangani kasus-kasus kejahatan siber secara efektif.
c. Memfasilitasi kerja sama internasional dan perjanjian bantuan hukum timbal balik untuk mengatasi tantangan yurisdiksi.

Meningkatkan Strategi Penegakan Hukum

a. Meningkatkan koordinasi dan kolaborasi di antara lembaga penegak hukum di Provinsi Jawa Barat dan di tingkat nasional untuk memfasilitasi pembagian informasi dan operasi bersama.
b. Berinvestasi dalam pelatihan dan peningkatan kapasitas personel penegak hukum untuk meningkatkan keahlian mereka dalam menyelidiki dan menuntut kejahatan siber.
c. Memperkuat kemampuan forensik digital untuk memastikan pengumpulan dan analisis bukti yang efisien dan akurat.

Meningkatkan Kesadaran dan Kerja Sama Publik

a. Meluncurkan kampanye kesadaran publik untuk mengedukasi individu, bisnis, dan organisasi tentang ancaman siber, tindakan pencegahan, dan mekanisme pelaporan.
b. Mendorong kemitraan publik-swasta untuk mendorong kolaborasi dalam inisiatif keamanan siber, berbagi informasi, dan upaya bersama dalam memerangi kejahatan siber.
c. Membangun mekanisme bagi masyarakat untuk melaporkan kejahatan siber dengan mudah dan anonim, memastikan keamanan dan perlindungan mereka.

Mendukung Penelitian dan Pengembangan

a. Berinvestasi dalam inisiatif penelitian dan pengembangan untuk tetap menjadi yang terdepan dalam kemajuan teknologi dan secara proaktif mengatasi ancaman siber yang muncul.

b. Memupuk kolaborasi antara lembaga akademis, mitra industri, dan lembaga penegak hukum untuk mendorong inovasi dan mengembangkan solusi yang efektif terhadap kejahatan dunia maya.

5. KESIMPULAN

Temuan dan diskusi menyoroti peran penting hukum dan tantangan yang dihadapi dalam penegakan hukum terhadap kejahatan siber di Provinsi Jawa Barat. Dengan menganalisis kerangka hukum, mekanisme penegakan hukum, tantangan, dan perspektif pemangku kepentingan, penelitian ini memberikan wawasan yang berharga tentang kondisi upaya pemberantasan kejahatan siber saat ini di provinsi tersebut. Rekomendasi yang diajukan bertujuan untuk memperkuat kerangka hukum, meningkatkan strategi penegakan hukum, meningkatkan kesadaran dan kerja sama publik, serta mendukung inisiatif penelitian dan pengembangan. Penerapan rekomendasi ini akan berkontribusi pada pemberantasan kejahatan siber dan penciptaan lingkungan digital yang aman di Provinsi Jawa Barat.

DAFTAR PUSTAKA

Arifin, S., & Rahman, K. (2021). Dinamika Kejahatan Dunia Maya Mengenai Online Child Sexual Exploitation di Tengah Pandemi COVID-19. *Jurnal Al-Daulah*, *10*(2).

Back, S., & LaPrade, J. (2020). Cyber-situational crime prevention and the breadth of cybercrimes among higher education institutions. *International Journal of Cybersecurity Intelligence & Cybercrime*, *3*(2), 25–47.

Bhattacharya, C. D. S., Sachdev, B., Kundu, A., & Bansal, K. (2021). IMPACT OF CYBER LAW IN MODERN ERA WITH ADVANCEMENT IN TECHNOLOGY AND PROTECTION FROM RISING THREATS OF CYBER CRIMES IN OUR SOCIO ECONOMIC SECTOR. *International Journal of Advanced Research*, *9*, 274–279. https://doi.org/10.21474/IJAR01/13404

Faridi, M. K. (2018). Kejahatan Siber Dalam Bidang Perbankan. *Cyber Security Dan Forensik Digital*, *1*(2), 57–61.

Kristiyanti, C. T. S., Sitanggang, P. P., & Satria, F. (2022). *SOSIALISASI TENTANG KEJAHATAN DUNIA MAYA (CYBER CRIME) KEPADA SISWA KELAS X SMAK ST. ALBERTUS MALANG*.

Kurniawan, K. D., & Hapsari, D. R. I. (2021). Kejahatan Dunia Maya Pada Sektor Perbankan Di Indonesia: Analisa Perlindungan Hukum Terhadap Nasabah. *Pleno Jure Jurnal Ilmu Hukum*, *10*(2), 122–133.

Mamade, B. K., & Dabala, D. M. (2021). Exploring The Correlation between Cyber Security Awareness, Protection Measures and the State of Victimhood: The Case Study of Ambo University's Academic Staffs. *Journal of Cyber Security and Mobility*, 699–724.

Mangena, D. (2016). Will legislation protect your virtual space? Discussing the draft Cyber crime and Cyber Security Bill. *De Rebus*, *2016*(560), 33–34.

Maramba, R. S. M., & Wulla, A. B. (2021). Kenakalan Remaja Dan Bahaya Kejahatan Dunia Maya (Cyber). *ABDI WINA JURNAL PENGABDIAN KEPADA MASYARAKAT*, *1*(1), 29–32.

Rider, B. A. K. (2001). Cyber-Organised Crime—The Impact of Information Technology on Organised Crime. *Journal of Financial Crime*, *8*(4), 332–346.

Somantri, S., Handraputri, C. P., Pahlawan, R., Herisma, D. D., Permana, G., Irhamna, M. H.,

Rismawati, I., Dewi, R. R., Zaman, S., & Hidayat, T. (2023). EDUKASI MENINGKATAN KEWASPADAAN KEJAHATAN DUNIA MAYA PADA SISWA SMK IT NURUL AZKA CIANJUR. *EJOIN: Jurnal Pengabdian Masyarakat*, *1*(5), 349–356.

Sudhakar, K., & Poorna, K. (2020). *Students Awareness towards Cyber Crime and Cyber Caw*. *30*, 4359–4364.

Sudiyawati, N., & Mertha, I. (2022). KEJAHATAN SIBER (CYBERCRIME) DALAM KONTEKS KEKERASAN SEKSUAL BERBASIS GENDER ONLINE DI INDONESIA. *Kertha Semaya : Journal Ilmu Hukum*, *10*, 850. https://doi.org/10.24843/KS.2022.v10.i04.p11

Suharyadi, S., Sampara, S., & Ahmad, K. (2020). Kejahatan Dunia Maya (Cyber Crime) Dalam Prespektif Hukum Islam. *Journal of Lex Generalis (JLG)*, *1*(5), 761–773.

Tinggi, I. R. D. P. S., & IBLAM, I. H. (n.d.). *Tinjauan Yuridis Terhadap Penetapan Locus Delicti dalam Kejahatan Dunia Maya (Cyber Crime) Berkaitan Dengan Upaya Pembaharuan Hukum Pidana di Indonesia*.