Jurnal Panah Keadilan **P-ISSN 2775-3116**
Vol. 3 No. 2 Edisi Agustus 2024 **E-ISSN 2776-3560**

ANALISIS PERAN DAN EFEKTIVITAS HUKUM DALAM MELAWAN ANCAMAN CYBERCRIME DI INDONESIA

Muhammad Hisyam Fahmi[1], Henri Marusaha Tambunan[2]
[1,2]Universitas Negeri Semarang
(mimieeee22@gmail.com[1], henritambunan@gmail.com[2])

Abstract

This article discusses the challenges faced and the role of law in dealing with the threat of cybercrime in Indonesia amidst the rapid progress of digital technology. The main focus of this article is on the Information and Electronic Transactions Law (UU ITE) as the main legal framework, and the role of the National Cyber and Crypto Agency (BSSN) in coordinating and dealing with cyber threats. In addition, this article identifies several crucial challenges such as technical limitations, rapid technological developments, and digital anonymity of cybercriminals. Evaluation of the effectiveness of regulations and personal data protection is also the focus of this discussion, while providing recommendations for strengthening technological infrastructure, increasing training, strengthening international cooperation, and revising existing regulations to be able to face increasingly complex threats in today's digital era.

Keywords: *Cybercrime; Cyberlaw; Technical Challenges*

Abstrak

Artikel ini membahas tantangan yang dihadapi serta peran hukum dalam menghadapi ancaman cybercrime di Indonesia di tengah pesatnya kemajuan teknologi digital. Fokus utama artikel ini adalah pada Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) sebagai kerangka hukum utama, dan peran Badan Siber dan Sandi Negara (BSSN) dalam koordinasi dan penanggulangan ancaman siber. Selain itu, artikel ini mengidentifikasi beberapa tantangan krusial seperti keterbatasan teknis, perkembangan teknologi yang cepat, dan anonimitas digital dari pelaku kejahatan siber. Evaluasi efektivitas regulasi dan perlindungan data pribadi juga menjadi fokus dalam diskusi ini, sambil memberikan rekomendasi untuk memperkuat infrastruktur teknologi, meningkatkan pelatihan, memperkuat kerjasama internasional, dan merevisi regulasi yang ada agar dapat menghadapi ancaman yang semakin kompleks dalam era digital saat ini.

Kata Kunci; Kejahatan siber, UU ITE, Tantangan teknis

A. Pendahuluan

Perkembangan teknologi informasi dan komunikasi yang pesat telah membawa banyak manfaat, tetapi juga menghadirkan tantangan baru, terutama dalam bentuk cybercrime atau kejahatan siber. Cybercrime mencakup berbagai jenis aktivitas ilegal yang dilakukan melalui internet atau melibatkan sistem komputer dan jaringan digital, mulai dari penipuan online, pencurian identitas, hingga serangan terhadap infrastruktur digital yang vital. Di Indonesia, dengan populasi yang besar dan penetrasi internet yang meningkat pesat, ancaman cybercrime telah menjadi masalah yang semakin serius dan kompleks, memerlukan perhatian khusus dari semua pemangku kepentingan,

termasuk pemerintah, sektor swasta, dan masyarakat umum.

Cybercrime tidak hanya menimbulkan kerugian finansial yang signifikan tetapi juga mengancam stabilitas sosial dan keamanan nasional. Berbagai kasus cybercrime, seperti pencurian data pribadi, penipuan online, dan serangan siber terhadap instansi pemerintah, menunjukkan betapa rentannya infrastruktur digital Indonesia terhadap ancaman ini. Misalnya pada tahun 2020 kasus kebocoran data di Tokopedia, salah satu platform e-commerce terbesar di Indonesia, mengungkapkan informasi pribadi jutaan pengguna, menyebabkan kerugian finansial yang besar dan menimbulkan kekhawatiran serius tentang keamanan data pribadi di Indonesia. Selain itu, serangan terhadap sistem informasi pemerintah juga telah terjadi.

Dalam menghadapi ancaman cybercrime yang semakin kompleks, peran hukum menjadi sangat penting. Hukum berfungsi sebagai instrumen yang mendefinisikan dan mengkriminalisasi berbagai bentuk kejahatan siber serta menyediakan kerangka kerja untuk penegakan hukum dan perlindungan hak-hak individu dan organisasi. Di Indonesia, sejumlah peraturan telah diterapkan untuk mengatasi cybercrime, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan berbagai peraturan terkait keamanan siber. UU ITE, yang diundangkan pada tahun 2008 dan diperbarui pada tahun 2016, adalah salah satu undang-undang utama yang mengatur aktivitas di ruang digital, termasuk tindakan-tindakan yang dianggap sebagai kejahatan siber. Selain itu, Badan Siber dan Sandi Negara (BSSN) dibentuk untuk mengkoordinasikan upaya nasional dalam menghadapi ancaman siber dan melindungi infrastruktur digital negara.

Namun, meskipun berbagai langkah hukum telah diambil, efektivitas hukum dalam melawan ancaman cybercrime di Indonesia masih menjadi perdebatan. Salah satu tantangan utama adalah kecepatan perubahan teknologi yang sering kali melampaui kecepatan pembuatan dan penerapan regulasi. Selain itu, penegakan hukum yang efektif juga memerlukan pemahaman teknis yang mendalam dan kapasitas yang memadai untuk mengatasi kejahatan siber yang semakin canggih dan lintas batas. Kasus-kasus seperti kebocoran data Tokopedia dan serangan siber terhadap sistem informasi pemerintah menunjukkan bahwa masih ada kelemahan dalam sistem perlindungan dan penegakan hukum yang harus segera diatasi.

Penelitian ini menggunakan metode penelitian hukum normatif, yang berarti fokusnya adalah pada analisis norma hukum yang tertulis. Metode ini, yang juga dikenal sebagai penelitian hukum doktrinal, dogmatik, atau teoritis, berlandaskan pada data sekunder seperti peraturan perundang-undangan. Karakteristik utama penelitian hukum normatif adalah berfokus pada hukum yang tertulis. Artinya, hukum dipelajari dan dianalisis berdasarkan teks peraturan perundang-undangan yang ada. Peneliti menggunakan data sekunder yang bersumber dari dokumen tertulis untuk memahami dan menjelaskan norma hukum yang berlaku.

B. Metodelogi Penelitian

Jenis Penelitian

Penelitian ini menggunakan metode normatif (yuridis normatif) yang fokus pada analisis hukum tertulis: undang-undang, regulasi, doktrin, putusan pengadilan, serta kebijakan terkait

cybercrime. Karena ingin mengevaluasi efektivitas hukum, juga akan ditambahkan unsur empiris sebagai pelengkap jika memungkinkan.

Pendekatan

Pendekatan penelitian dalam analisis peran dan efektivitas hukum dalam melawan ancaman cybercrime di Indonesia menggunakan tiga pendekatan utama, yaitu pendekatan perundang-undangan, kelembagaan, dan empiris. Pendekatan perundang-undangan (statute approach) digunakan untuk menganalisis isi dari Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), beserta regulasi turunannya seperti Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, serta undang-undang lain yang relevan, termasuk Kitab Undang-Undang Hukum Pidana (KUHP) dan peraturan yang berkaitan dengan keamanan siber dan perlindungan data pribadi. Analisis ini bertujuan untuk menilai kesesuaian dan kelengkapan norma hukum dalam menghadapi perkembangan kejahatan siber yang dinamis.

Selanjutnya, pendekatan kelembagaan (institutional approach) digunakan untuk melihat bagaimana peran dan koordinasi lembaga seperti Badan Siber dan Sandi Negara (BSSN), Kepolisian, Kejaksaan, serta lembaga pengawas dan sektor swasta dalam implementasi kebijakan keamanan siber dan penegakan hukum.

Sebagai pelengkap, pendekatan empiris digunakan secara opsional melalui wawancara dengan penyidik, analis forensik digital, dan praktisi hukum, serta melalui studi kasus dan analisis putusan pengadilan. Pendekatan ini memberikan gambaran nyata tentang efektivitas hukum di lapangan, tantangan teknis, serta respons aparat penegak hukum terhadap ancaman cybercrime yang terus berkembang.

Sumber Data

Sumber data penelitian ini terdiri atas data primer dan sekunder. Data primer mencakup teks peraturan perundang-undangan seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) beserta revisinya, Kitab Undang-Undang Hukum Pidana (KUHP), peraturan pemerintah, regulasi Badan Siber dan Sandi Negara (BSSN), serta putusan pengadilan yang berkaitan dengan kasus cybercrime. Sementara itu, data sekunder diperoleh dari berbagai artikel ilmiah, buku teks hukum, jurnal akademik, dan laporan institusi seperti BSSN, kepolisian, maupun lembaga swadaya masyarakat (LSM) yang membahas isu keamanan siber dan penegakan hukum terhadap kejahatan digital di Indonesia.

Teknik Pengumpulan Data

Teknik pengumpulan data dalam penelitian ini dilakukan melalui beberapa metode. Pertama, studi pustaka atau analisis dokumen hukum digunakan untuk menelaah peraturan perundang-undangan, literatur akademik, serta putusan pengadilan yang berkaitan dengan cybercrime di Indonesia. Kedua, dilakukan wawancara semi-struktural atau penyebaran kuesioner kepada pihak-pihak terkait, seperti aparat penegak hukum, ahli forensik digital, dan praktisi hukum, guna memperoleh pandangan langsung mengenai efektivitas penegakan hukum siber. Ketiga, observasi studi kasus diterapkan untuk menelusuri peristiwa nyata, seperti kasus kebocoran data berskala besar, guna memahami penerapan regulasi dan respons lembaga terhadap ancaman keamanan digital di lapangan.

Analisis Data

Analisis data dalam penelitian ini dilakukan dengan menggunakan beberapa pendekatan yang saling melengkapi. Pertama, analisis kualitatif deskriptif digunakan untuk menelaah norma hukum yang terkandung dalam peraturan perundang-undangan terkait cybercrime, mengidentifikasi kelemahan

regulasi, serta mengevaluasi implementasi dan praktik penegakan hukum di lapangan. Kedua, dilakukan analisis perbandingan (benchmarking) terhadap praktik internasional apabila data tersedia, dengan tujuan memahami bagaimana negara lain merumuskan kebijakan dan menegakkan hukum dalam menghadapi ancaman siber serupa. Ketiga, diterapkan analisis efektivitas, yaitu mengevaluasi sejauh mana regulasi dan lembaga penegak hukum di Indonesia berhasil mencegah atau menyelesaikan kasus cybercrime, melalui pengukuran terhadap indikator seperti jumlah kasus yang ditangani, durasi proses penyelesaian, tingkat hukuman, serta dampak kebijakan terhadap penurunan kejahatan siber.

Validitas dan Kredibilitas

Untuk memastikan validitas dan kredibilitas hasil penelitian, digunakan metode triangulasi data dengan membandingkan berbagai sumber informasi, seperti dokumen hukum, hasil wawancara, dan temuan dari studi kasus. Pendekatan ini bertujuan untuk memperoleh gambaran yang lebih objektif dan komprehensif mengenai efektivitas hukum dalam menghadapi cybercrime. Selain itu, dilakukan pula pemeriksaan silang terhadap putusan pengadilan dan laporan empiris dari lembaga terkait, seperti BSSN atau kepolisian, guna memastikan bahwa analisis dan kesimpulan penelitian tidak hanya bersifat teoritis, tetapi juga mencerminkan realitas implementasi hukum dan penegakan keadilan di lapangan.

C. Hasil Penelitian dan Pembahasan

Di tengah pesatnya perkembangan digital di Indonesia, interaksi antara hukum dan keamanan siber menjadi kunci penting untuk menjaga keamanan nasional. Cybercrime atau kejahatan dunia maya telah menjadi ancaman serius bagi keamanan dan stabilitas di berbagai sektor di Indonesia. Oleh karena itu, penting untuk memahami peran dan efektivitas hukum dalam upaya melawan ancaman ini. Analisis ini akan membahas bagaimana regulasi dan penegakan hukum di Indonesia berfungsi dalam menghadapi tantangan cybercrime, serta mengevaluasi efektivitas langkah-langkah tersebut dalam menciptakan lingkungan digital yang aman dan terlindungi.

Indonesia termasuk rawan di dunia tehadap serangan cyber, harusnya ada biro security yang mengawasi dan menjaga BSSN dan untuk melihat seberapa besar serangan siber. Apalagi cyberspace itu tak ada batas dan tidak ada sensor, semuanya bebas dan ini menimbulkan berbagai macam risiko. Risiko itu bisa hubungan perdata maupun pidana. Yang harus diperhatikan pembentuk hukum harus melihat kemajuan teknologi dan mengetahui pola kejahatannya, Ungkap wasis dalam sebuah webinar.

Ketentuan hukum yang ada di Indonesia saat ini dalam menangani ancaman cybercrime

Ketentuan hukum di Indonesia untuk menangani ancaman cybercrime saat ini terutama diatur oleh Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), yang diundangkan pertama kali pada tahun 2008 dan direvisi pada tahun 2016. UU ITE menjadi landasan utama untuk mengatur aktivitas digital dan menangani berbagai bentuk kejahatan siber, termasuk akses ilegal, penyadapan, peretasan, dan penyebaran konten yang melanggar hukum. Selain UU ITE, terdapat sejumlah peraturan lain seperti Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik yang memperjelas tanggung jawab penyedia layanan dalam menjaga keamanan data dan sistem elektronik. Namun, meskipun UU ITE menyediakan dasar hukum yang penting, tantangan dalam penerapan dan penegakan hukum

masih cukup signifikan, seperti ketidakmampuan mengikuti perkembangan teknologi yang cepat dan kompleksitas kejahatan siber yang sering kali melintasi batas negara.

Apakah peraturan yang ada sudah cukup efektif? Kepala Pusat Studi Cyber Law dan Transformasi Digital Fakultas Hukum Universitas Padjadjaran Dr. Tasya Safiranita Ramli, S.H., M..H. mengatakan bahwa "sistem Perundang-undangan Indonesia belum mengatur secara khusus tentang kejahatan pada media internet atau layanan over the top, dan pada saat bersamaan modus operasi kejahatan dunia maya atau cyber crime cukup beragam serta terus berkembang". Efektivitas UU ITE dan regulasi terkait dalam mengatur dan menanggulangi berbagai bentuk cybercrime masih menjadi perdebatan. Di satu sisi, UU ITE telah memberikan kerangka hukum yang jelas untuk penegakan hukum terhadap berbagai kejahatan cyber, dengan penetapan sanksi yang cukup ketat bagi pelaku. Namun, di sisi lain masih terdapat kelemahan dalam hal penegakan dan adaptasi regulasi terhadap teknologi yang terus berkembang. Misalnya, beberapa kasus besar seperti kebocoran data pengguna di platform online menunjukkan bahwa perlindungan data pribadi di Indonesia masih perlu diperkuat, dan koordinasi antara lembaga pemerintah serta dengan sektor swasta masih perlu ditingkatkan untuk memperkuat upaya pencegahan dan penanggulangan cybercrime.

Badan Siber dan Sandi Negara (BSSN) berperan penting dalam kerangka hukum tersebut sebagai lembaga yang bertanggung jawab atas koordinasi dan penanggulangan ancaman siber di Indonesia. Dibentuk melalui Peraturan Presiden No. 53 Tahun 2017, BSSN memiliki tanggung jawab untuk mengembangkan kebijakan keamanan siber nasional, memantau dan merespons insiden siber, serta meningkatkan kapasitas penegak hukum dan masyarakat dalam menghadapi ancaman siber. BSSN juga berfungsi sebagai penghubung antara berbagai instansi pemerintah dan sektor swasta dalam penanganan masalah siber, serta menjalin kerjasama internasional untuk mengatasi kejahatan siber lintas negara. Meskipun peran BSSN sangat strategis, lembaga ini masih menghadapi tantangan dalam hal sumber daya dan kapasitas, serta dalam menjaga koordinasi yang efektif di tengah kompleksitas lanskap ancaman siber yang terus berubah.

Tantangan utama dalam penegakan hukum cybercrime di Indonesia

Penegakan hukum terhadap cybercrime di Indonesia merupakan sebuah tantangan kompleks yang melibatkan berbagai aspek, mulai dari keterbatasan teknis hingga dinamika perkembangan teknologi yang cepat. Berikut adalah bebrapa poin utama yang menjadi t:antangan:

1. Keterbatasan Teknis dan Kurangnya Sumber Daya

Penegakan hukum cybercrime memerlukan infrastruktur teknologi yang canggih dan sumber daya manusia yang terlatih secara khusus. Namun, di Indonesia masih ada beberapa keterbatasan yang signifikan:

a. Infrastruktur Teknologi yang Terbatas: Banyak lembaga penegak hukum masih menghadapi tantangan dalam hal infrastruktur teknologi yang memadai untuk melakukan analisis forensik digital, pelacakan pelaku kejahatan siber, dan pengumpulan bukti elektronik yang diperlukan dalam kasus-kasus cybercrime. Kurangnya akses terhadap

perangkat lunak dan peralatan yang diperlukan sering kali memperlambat proses penyelidikan dan penegakan hukum.

b. Kurangnya Keahlian Teknis: Keberhasilan dalam menangani kasus cybercrime sangat bergantung pada keahlian teknis dari penyidik dan analis forensik digital. Sayangnya, jumlah ahli yang memiliki keahlian khusus dalam keamanan siber dan forensik digital masih terbatas di Indonesia. Pelatihan yang teratur dan peningkatan kapasitas dalam bidang ini menjadi sangat penting untuk meningkatkan kemampuan penegak hukum dalam menghadapi ancaman cybercrime yang semakin kompleks.
c. Keterbatasan Anggaran: Pengembangan infrastruktur teknologi yang diperlukan untuk menangani cybercrime membutuhkan investasi finansial yang signifikan. Namun, anggaran yang terbatas sering kali menjadi hambatan dalam memperbarui infrastruktur dan memperluas kapasitas penegak hukum dalam hal teknologi dan sumber daya manusia.

2. Perkembangan Teknologi yang Cepat dan Kompleksitas Kejahatan Siber

Perkembangan teknologi digital terus berlangsung dengan cepat, menciptakan tantangan baru bagi penegakan hukum dalam menyesuaikan diri dengan teknik baru yang digunakan oleh pelaku kejahatan siber. Misalnya, penggunaan teknologi blockchain untuk melakukan transaksi ilegal atau teknik enkripsi yang canggih untuk menyembunyikan jejak kriminalitas digital. Kompleksitas modus operandi Pelaku sering kali menggunakan jaringan yang kompleks dan sulit dilacak, sering kali melintasi batas negara. Hal ini menambah tingkat kesulitan dalam penyidikan dan penegakan hukum, karena memerlukan kerja sama lintas negara yang efektif dan pemahaman mendalam tentang hukum yang berlaku di berbagai yurisdiksi. Dan juga Anonimitas Digital yang sering kali dapat dipertahankan oleh pelaku kejahatan siber membuat proses identifikasi dan penangkapan menjadi lebih sulit. Penggunaan alat dan teknik untuk menyembunyikan identitas digital membutuhkan pendekatan investigasi yang canggih dan waktu yang lebih lama untuk memperoleh bukti yang cukup kuat secara hukum.

Dampak Perkembangan Teknologi terhadap Efektivitas Hukum. Yang pertama Tantangan Regulasi, Hukum yang ada mungkin tidak selalu mampu menanggapi dengan cepat dan efektif terhadap perubahan teknologi baru. Tantangan ini bisa membuat kejahatan siber sulit untuk diidentifikasi dan diberantas, karena regulasi yang tidak selaras atau kurang tepat waktu. Dan yang kedua Perlindungan Data Pribadi, Perlindungan data pribadi dalam UU ITE merupakan salah satu aspek penting dalam upaya mencegah cybercrime. Namun, kelemahan dalam implementasi dan kesadaran yang rendah tentang pentingnya keamanan data pribadi dapat meningkatkan risiko kebocoran informasi sensitif yang dapat dieksploitasi oleh pelaku kejahatan siber.

Berkembang seiring dengan kemajuan teknologi dan meningkatnya ketergantungan pada sistem digital serta meningkatnya jumlah insiden cybercrime, penting untuk mengambil langkah-langkah yang tepat untuk melindungi sistem dan informasi vital dari serangan. Berikut beberapa langkah strategis yang dapat dipertimbangkan:

a. Peningkatan Investasi dan Infrastruktur: Pemerintah perlu meningkatkan

investasi dalam infrastruktur teknologi yang diperlukan dan memastikan bahwa lembaga penegak hukum memiliki akses terhadap teknologi yang mutakhir untuk mendukung upaya penegakan hukum.

b. Pelatihan dan Pengembangan Keahlian: Program pelatihan intensif dan pengembangan keahlian teknis dalam bidang keamanan siber dan forensik digital harus diprioritaskan untuk meningkatkan kemampuan penyidik dan analis dalam menghadapi ancaman cybercrime yang semakin canggih.
c. Kerjasama Internasional: Peningkatan kerjasama dengan lembaga penegak hukum internasional untuk pertukaran informasi dan koordinasi dalam penyelidikan dan penanggulangan ancaman cybercrime yang melintasi batas negara.
d. Revisi Regulasi dan Kebijakan: Evaluasi dan penyesuaian regulasi yang ada untuk memastikan bahwa mereka tetap relevan dan efektif dalam menghadapi tantangan baru dari perkembangan teknologi.
e. Peningkatan Kesadaran Publik: Kampanye penyuluhan dan peningkatan kesadaran masyarakat tentang ancaman cybercrime dan praktik keamanan digital yang aman untuk mengurangi kerentanan terhadap serangan cyber.

Selain itu, mengidentifikasi dan mengejar pelaku kejahatan siber menghadirkan berbagai tantangan kompleks. Salah satu masalah utamanya adalah anonimitas di dunia maya, yang memungkinkan pelaku menyembunyikan identitas dengan menggunakan alamat IP palsu atau layanan penyamaran online. Selain itu, kejahatan siber sering kali melibatkan lintas batas negara, membuat koordinasi dengan yurisdiksi lain menjadi sulit dalam proses penyelidikan dan penangkapan. Kurangnya keterampilan dan sumber daya dalam penegakan hukum untuk menangani kasus kejahatan siber juga menjadi kendala. Terakhir, perkembangan teknologi yang cepat membuat penegak hukum sulit untuk terus memperbarui pengetahuan dan keterampilan mereka dalam menghadapi ancaman baru. Ada beberapa tantangan yang dihadapi dalam mengidentifikasi dan mengejar pelaku kejahatan siber:

1. Anonimitas dan Penggunaan Alat Penyamaran: Pelaku kejahatan siber sering menggunakan alamat IP palsu atau layanan penyamaran online untuk menyembunyikan identitas mereka, sehingga sulit melacak sumber serangan atau aktivitas kriminal mereka.
2. Transparansi Antar-Negara: Kejahatan siber sering terjadi lintas batas negara tanpa hambatan, menciptakan tantangan dalam berkoordinasi dengan yurisdiksi lain untuk penyelidikan dan penangkapan pelaku.
3. Kompleksitas Teknologi: Pelaku kejahatan siber terus memperbarui metode dan menggunakan teknologi canggih seperti enkripsi dan malware, yang menuntut penegak hukum untuk selalu memperbarui pengetahuan dan keterampilan mereka.
4. Kerjasama Industri dan Pemerintah: Diperlukan kerjasama antara industri swasta, pemerintah, dan lembaga internasional untuk menghadapi ancaman kejahatan siber secara efektif. Namun, koordinasi ini sering sulit karena perbedaan kepentingan dan regulasi di berbagai negara.

Untuk mengatasi tantangan ini, diperlukan kerjasama yang erat antara berbagai pihak, termasuk lembaga penegak hukum, pemerintah, industri, dan masyarakat umum. Selain itu, dibutuhkan

investasi dalam pengembangan sumber daya manusia, teknologi, dan kerjasama lintas-batas untuk meningkatkan kemampuan dalam mengidentifikasi dan menangkap pelaku kejahatan cyber.

D. Kesimpulan

Di Indonesia, pertumbuhan teknologi digital yang pesat telah menimbulkan ancaman serius terhadap keamanan siber dan memperlihatkan perlunya peningkatan efektivitas hukum dalam menanggapi cybercrime. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) merupakan landasan utama yang mengatur aktivitas digital, meskipun masih menghadapi tantangan dalam penerapan dan penegakan hukum yang cepat dan kompleks. Badan Siber dan Sandi Negara (BSSN) berperan sentral dalam koordinasi penanggulangan ancaman siber, meski menghadapi keterbatasan sumber daya dan koordinasi lintas sektor. Tantangan utama dalam penegakan hukum cybercrime meliputi keterbatasan teknis, kekurangan tenaga ahli yang terlatih, serta kompleksitas kejahatan yang melintasi batas negara. Langkah-langkah strategis yang diperlukan meliputi peningkatan investasi dalam infrastruktur teknologi, pelatihan intensif untuk keahlian teknis, revisi regulasi yang responsif terhadap perkembangan teknologi, dan peningkatan kesadaran masyarakat tentang keamanan digital. Dengan kolaborasi yang kuat antara pemerintah, sektor swasta, dan masyarakat, diharapkan dapat menciptakan lingkungan digital yang lebih aman dan terlindungi di Indonesia.

E. Daftar Pustaka

Adinda Agis Fitria Cahyani, & Nadia Elvin Eka Azaria. (2024). Sumba Tribal Catch Marriage Tradition In The Perspective Of Legal Pluralism. *JURNAL PANAH KEADILAN*, *3*(1), 48-58. https://doi.org/10.57094/jpk.v3i1.1533

Antonius Ndruru. (2022). Penerapan Pemidanaan Di Bawah Ancaman Minimal Pada Tindak Pidana Penempatan Tenaga Kerja Indonesia Di Luar Negeri. *JURNAL PANAH KEADILAN*, *1*(2), 34-51. https://doi.org/10.57094/jpk.v1i2.450

Arianus Harefa, & Antonius Ndruru. (2022). Perspektif Psikologi Kriminil Terhadap Penyebab Terjadinya Juvenile Delinquency Ditinjau Dari Aspek Kriminologi. *JURNAL PANAH KEADILAN*, *1*(1), 55-69. https://doi.org/10.57094/jpk.v1i1.445

Fariaman Laia. (2022). Analisis Yuridis Terhadap Perlindungan Hukum Bagi Saksi Peradilan Pidana Di Indonesia. *JURNAL PANAH KEADILAN*, *1*(1), 24-39. https://doi.org/10.57094/jpk.v1i1.443

Hasan Zainudin , Aldi Yansah, dkk. (2024). Tinjauan Cyberlaw terhadap Ancaman dan Strategi Penanggulangan Cybercrime. MANDUB, 2(2), 136-137.

Hasaziduhu Möhö, & Fariaman Laia. (2022). Kajian Kontrak Dalam Perspektif Filsafat Hukum. *JURNAL PANAH KEADILAN*, *1*(1), 12-23. https://doi.org/10.57094/jpk.v1i1.442

Hasaziduhu Möhö. (2022). Hakikat Upah Dalam Hubungan Ketenagakerjaan. *JURNAL PANAH KEADILAN*, *1*(2), 117-127. https://doi.org/10.57094/jpk.v1i2.457

Heriani, Fitri Novia. (2022). Minim Regulasi, Pemberantasan Cybercrime di Indonesia Menjadi

Rumit. Hukum Online.com. https://www.hukumonline.com/berita/a/minim-regulasi--pemberantasan-cybercrime-di-indonesia-menjadi-rumit-lt6244385d4a100/?page=all

Indonesia, CNN. (2020). Kronologi Lengkap 91 Juta Akun Tokopedia Bocor dan Dijual. CNN INDONESIA. https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual

Kosmas Dohu Amajihono. (2022). Kekuatan Hukum Kontrak Elektronik. *JURNAL PANAH KEADILAN*, *1*(2), 128-139. https://doi.org/10.57094/jpk.v1i2.458

Najwa, Fadhila Rahman. (2024). Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia. AL-BAHST, 2(1), 9-10.

Nurdin, Merry Kurniawati, Chika Aurel Rivaldi, dkk. (2023). Peran Hukum Telematika Dalam Penyelesaian Kasus Cybercrime. ResearchGate. https://www.researchgate.net/publication/375792129

S H Bachtiar and others, Mendesain Penelitian Hukum (Deepublish, 2021). hlm. 93.

S.M, P. P., & Rony Andre Christian Naldo. (2025). Pemotongan Gaji Peserta Tabungan Perumahan Rakyat (TAPERA). *JURNAL PANAH KEADILAN*, *4*(2), 1-13. https://doi.org/10.57094/jpk.v4i2.2659

Sari, Utin Indah Permata. (2021). Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cybercrime Yang Dilakukan Oleh Virtual Police Di Indonesia. Mimbar Jurnal Hukum, 2(1).

Yonathan Sebastian Laowo. (2022). Kajian Hukum Tindak Pidana Pencucian Uang (Money Loundring). *JURNAL PANAH KEADILAN*, *1*(1), 70-87. https://doi.org/10.57094/jpk.v1i1.447