Efektivitas Penegakan Hukum terhadap Kejahatan Siber Jenis Hacking Berdasarkan UU ITE di Indonesia

Oleh:

Ade Fatimah Zura, Astrid Indah Tri Ariany, Azzriel Al Bari Daulay, Julhadi Siregar, Dian Prildani Pasaribu, Muhammad Rafli Pratomo

Email: zurafatimahade@gmail.com, astridindahta19@gmail.com, albaridaulayazzriel@gmail.com, julhadisiregarhadi671@gmail.com, dianprildanipasaribu04@gmail.com, muhammadraflipratomo@gmail.com

Abstrak

Kejahatan siber, khususnya jenis hacking, semakin marak terjadi di Indonesia seiring dengan meningkatnya ketergantungan masyarakat terhadap teknologi informasi. Fenomena ini menjadi ancaman serius terhadap keamanan digital dan kedaulatan data pribadi serta lembaga pemerintahan dan swasta. Artikel ini bertujuan untuk menganalisis efektivitas penegakan hukum terhadap kejahatan siber jenis hacking berdasarkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia. Dengan menggunakan metode kualitatif deskriptif dan pendekatan yuridis normatif, penulis mengevaluasi kebijakan hukum serta hambatan dalam implementasi UU ITE. Hasil penelitian menunjukkan bahwa meskipun UU ITE telah mengatur secara tegas mengenai perbuatan ilegal terkait sistem elektronik, namun penegakan hukum masih menghadapi berbagai kendala, seperti keterbatasan sumber daya, minimnya literasi digital aparat penegak hukum, serta tantangan pembuktian teknis di ranah digital. Diperlukan sinergi antara pemerintah, aparat penegak hukum, dan masyarakat dalam memperkuat sistem perlindungan siber di Indonesia.

Kata Kunci: Kejahatan Siber, Hacking, Penegakan Hukum, UU ITE, Efektivitas.

Pendahuluan

Kemajuan teknologi informasi telah membawa perubahan besar dalam kehidupan manusia, baik dari sisi sosial, ekonomi, maupun politik. Namun, di balik berbagai kemudahan tersebut, muncul ancaman baru berupa kejahatan siber, salah satunya adalah *hacking*. Kejahatan ini dilakukan dengan mengakses sistem elektronik secara ilegal untuk mendapatkan, merusak, atau mencuri informasi. Di Indonesia, kasus hacking terhadap situs pemerintah, perbankan, maupun data pribadi pengguna internet semakin sering terjadi (Meirisah & Sutabri, 2023).

Untuk menghadapi kejahatan ini, pemerintah Indonesia telah mengesahkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU

ITE), yang kemudian diperbarui melalui Undang-Undang Nomor 19 Tahun 2016. UU ini menjadi dasar hukum utama dalam penanganan kejahatan siber di Indonesia. Namun demikian, efektivitas penegakan hukum terhadap pelaku hacking masih menjadi persoalan serius (Kasim et al., 2022).

Artikel ini mencoba menjawab pertanyaan utama: seberapa efektifkah penegakan hukum terhadap kejahatan siber jenis hacking berdasarkan UU ITE di Indonesia? Dan faktor-faktor apa saja yang menjadi hambatan dalam implementasinya?

Kajian Teori

A. Kejahatan Siber dan Hacking

Perkembangan teknologi informasi dan komunikasi telah memberikan dampak besar terhadap berbagai aspek kehidupan manusia, termasuk dalam hal kejahatan. Salah satu bentuk kejahatan modern yang paling mencolok saat ini adalah kejahatan siber (*cybercrime*), yakni tindak pidana yang dilakukan dengan memanfaatkan sistem komputer, jaringan internet, atau perangkat digital lainnya. Kejahatan ini sering kali bersifat lintas batas (borderless), tidak mengenal ruang dan waktu, serta dapat menimbulkan kerugian besar baik bagi individu, korporasi, maupun negara (Yudistira, 2023).

Kejahatan siber memiliki banyak jenis, salah satunya yang paling populer dan meresahkan adalah *hacking*. Dalam konteks hukum, hacking adalah tindakan mengakses sistem komputer atau jaringan milik pihak lain secara ilegal, tanpa izin, dan dilakukan dengan sengaja. Tindakan ini melanggar prinsip integritas, kerahasiaan, dan ketersediaan (*confidentiality, integrity, availability*) yang merupakan dasar dari keamanan siber (*cybersecurity*) (Yuswanto & Wibowo, 2021).

Motif pelaku hacking bisa beragam. Sebagian pelaku melakukan aksinya untuk kepentingan finansial, seperti mencuri data kartu kredit atau informasi pribadi pengguna untuk kemudian diperjualbelikan. Ada pula pelaku yang bertindak atas dasar ideologi, keinginan balas dendam, atau bahkan hanya untuk menunjukkan kemampuan teknisnya. Di dunia maya, mereka yang melakukan hacking dengan tujuan tertentu sering

diklasifikasikan sebagai *black hat hackers*, sementara mereka yang melakukan hacking untuk tujuan baik, seperti menguji keamanan sistem, dikenal sebagai *white hat hackers*. Ada pula kelompok *grey hat hackers* yang berada di antara keduanya (Djanggih, 2018).

Di Indonesia, kasus hacking bukanlah hal baru. Serangan terhadap situs pemerintah, lembaga pendidikan, rumah sakit, hingga perusahaan teknologi menunjukkan bahwa sistem keamanan digital di Indonesia masih cukup rentan. Bahkan, beberapa pelaku hacking diketahui masih berusia remaja, yang menunjukkan bahwa akses terhadap teknologi sangat mudah, tetapi tidak selalu diiringi dengan kesadaran hukum yang memadai (Mahira Dewantoro & Dian Alan Setiawan S.H., M.H., 2023).

B. Landasan Hukum: UU ITE

Sebagai respons terhadap ancaman kejahatan siber, Indonesia telah mengesahkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). UU ini menjadi tonggak penting dalam pengaturan aktivitas digital di Indonesia. Di dalamnya terkandung berbagai ketentuan mengenai informasi elektronik, transaksi elektronik, serta perlindungan terhadap data dan sistem elektronik dari penyalahgunaan (Laksana, 2024).

Pasal 30 UU ITE menyatakan bahwa:

"Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun."

Ketentuan ini jelas menunjukkan bahwa aktivitas hacking masuk dalam kategori tindak pidana. Tidak hanya soal masuk ke dalam sistem elektronik tanpa izin, tetapi juga termasuk segala tindakan yang bertujuan mengganggu, mengubah, merusak, atau mencuri informasi dari sistem tersebut (Djanggih & Qamar, 2018).

Lebih lanjut, Pasal 46 UU ITE mengatur sanksi pidana terhadap pelaku kejahatan sebagaimana dimaksud dalam Pasal 30. Ancaman pidana bervariasi berdasarkan tingkat keseriusan pelanggaran yang dilakukan, dengan ancaman maksimal delapan tahun penjara dan denda hingga Rp800 juta.

Revisi terhadap UU ITE pada tahun 2016 melalui Undang-Undang Nomor 19 Tahun 2016 tidak mengubah substansi utama terkait peretasan atau hacking, namun lebih menekankan aspek perlindungan terhadap masyarakat pengguna teknologi informasi, termasuk memperjelas batasan beberapa pasal yang semula multitafsir. Meski begitu, implementasi UU ini di lapangan masih menghadapi berbagai tantangan, terutama dalam membuktikan elemen pidana di dunia maya yang sangat teknis (Wijaya, 2022).

Di luar UU ITE, instrumen hukum lainnya seperti KUHP, Undang-Undang No. 8 Tahun 1981 tentang Hukum Acara Pidana (KUHAP), serta peraturan pelaksana seperti Peraturan Kapolri dan pedoman Kejaksaan turut berperan dalam memproses kasus hacking. Namun, UU ITE tetap menjadi basis utama dalam menentukan unsur perbuatan dan sanksi yang dikenakan.

C. Penegakan Hukum

Efektivitas penegakan hukum tidak hanya bergantung pada keberadaan norma hukum, tetapi juga sangat ditentukan oleh bagaimana hukum tersebut diimplementasikan secara nyata. Dalam teori yang dikemukakan oleh Soerjono Soekanto, efektivitas penegakan hukum dipengaruhi oleh lima faktor utama, yaitu:

1. **Hukum itu sendiri (Substansi)**

   Substansi hukum mencakup isi dari peraturan perundang-undangan. Dalam konteks kejahatan siber, substansi hukum Indonesia terutama UU ITE telah memuat norma yang cukup jelas terkait larangan dan sanksi terhadap peretasan sistem elektronik. Namun, beberapa kalangan menilai bahwa rumusan pasal-pasal tersebut perlu diperbaharui agar dapat menyesuaikan dengan perkembangan teknologi yang sangat cepat. Hukum yang tertinggal dari realitas teknologi akan kehilangan relevansinya dalam proses penegakan (Putri et al., 2022).

2. **Aparat Penegak Hukum (Struktur)**

   Aparat penegak hukum, seperti kepolisian, kejaksaan, hakim, hingga penyidik di Kementerian Komunikasi dan Informatika, memegang peran sentral dalam menindak pelaku kejahatan siber. Sayangnya, banyak di antara mereka belum

memiliki kompetensi teknis yang memadai dalam bidang *cybercrime*. Hal ini menyebabkan proses penyidikan berjalan lambat, atau bahkan tidak tuntas. Pelatihan dan pendidikan khusus perlu ditingkatkan agar aparat memiliki kemampuan forensik digital yang andal (Budiman, 2022).

3. **Sarana dan Prasarana (Fasilitas)**

   Penanganan kejahatan siber membutuhkan infrastruktur teknologi yang memadai. Alat pelacak IP, perangkat *digital forensic tools*, hingga perangkat lunak analisis data sangat dibutuhkan untuk mengungkap pelaku hacking. Namun, fasilitas semacam ini masih terkonsentrasi di kota besar dan belum menjangkau seluruh wilayah Indonesia. Akibatnya, kasus hacking yang terjadi di daerah sering kali tidak dapat ditindaklanjuti secara efektif (Vadila & Pratama, 2021).

4. **Masyarakat (Partisipasi dan Kesadaran Hukum)**

   Kesadaran hukum masyarakat juga berpengaruh terhadap efektivitas penegakan hukum. Banyak masyarakat yang belum memahami bahwa tindakan iseng seperti masuk ke sistem orang lain tanpa izin adalah bentuk kejahatan. Di sisi lain, masyarakat juga perlu tahu bagaimana melaporkan dan mendokumentasikan kasus kejahatan siber secara benar agar proses hukum bisa berjalan. Edukasi publik mengenai hukum dan etika digital perlu terus digencarkan (Rahmawati, 2017b).

5. **Kebudayaan Hukum (Legal Culture)**

   Kebudayaan hukum merujuk pada sikap dan nilai yang hidup dalam masyarakat terkait hukum. Dalam konteks digital, budaya hukum masih tertinggal dibandingkan dengan pertumbuhan penggunaan teknologi. Budaya untuk menggunakan internet secara etis, bertanggung jawab, dan menghormati privasi orang lain belum terbentuk secara menyeluruh. Oleh karena itu, pembentukan budaya hukum digital harus menjadi bagian dari pendidikan formal maupun non-formal (Sudiyawati & Mertha, 2022).

Dalam praktiknya, kelima faktor tersebut belum terwujud secara sinergis di Indonesia. Ketidakseimbangan antar faktor menjadi salah satu penyebab mengapa penegakan hukum terhadap kejahatan hacking belum berjalan maksimal. Di satu sisi, UU ITE sudah tersedia sebagai dasar hukum. Namun di sisi lain, penegaknya masih belum sepenuhnya siap, baik dari sisi keahlian teknis maupun dukungan teknologi (Purwani, 2023).

Oleh karena itu, untuk menciptakan sistem penegakan hukum yang efektif dalam menangani kejahatan hacking, diperlukan upaya reformasi yang menyeluruh: mulai dari penyempurnaan regulasi, penguatan kapasitas SDM, peningkatan infrastruktur, hingga pembentukan budaya hukum yang kuat di kalangan masyarakat digital (Syah, 2023).

Metodologi Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan metode deskriptif analitis. Data dikumpulkan melalui studi pustaka terhadap regulasi, dokumen hukum, artikel ilmiah, serta studi kasus yang berkaitan dengan kejahatan hacking di Indonesia. Pendekatan yuridis normatif digunakan untuk menganalisis norma hukum yang berlaku, sedangkan pendekatan empiris digunakan untuk melihat penerapannya di lapangan (Umbara & Setiawan, 2022).

Hasil dan Diskusi

1. Implementasi UU ITE terhadap Kejahatan Hacking

Sejak disahkannya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), Indonesia telah memiliki dasar hukum yang cukup kuat dalam menindak kejahatan siber, khususnya tindak pidana hacking. UU ini memuat secara eksplisit larangan terhadap akses ilegal ke dalam sistem elektronik milik pihak lain. Dalam praktiknya, Pasal 30 dan Pasal 46 UU ITE sering dijadikan dasar hukum untuk menjerat pelaku hacking (Chintia et al., 2019).

Beberapa kasus telah membuktikan efektivitas hukum ini dalam menindak kejahatan. Salah satu kasus yang cukup menyita perhatian publik adalah kasus peretasan terhadap sistem Komisi Pemilihan Umum (KPU) pada tahun 2019. Dalam kasus tersebut,

pelaku terbukti melakukan akses tanpa hak terhadap data server milik pemerintah yang menyimpan data penting pemilu. Berdasarkan hasil penyidikan, pelaku dijatuhi hukuman pidana sebagaimana diatur dalam UU ITE. Hal ini menunjukkan bahwa secara normatif, regulasi yang ada telah dapat dijalankan untuk menangani kejahatan siber (Farhan et al., 2023).

Namun, keberhasilan normatif ini belum sepenuhnya tercermin dalam statistik penegakan hukum secara kuantitatif. Banyak laporan masyarakat terkait kasus hacking yang tidak bisa ditindaklanjuti. Salah satu penyebab utamanya adalah kesulitan dalam melacak pelaku. Tidak jarang, pelaku menggunakan identitas palsu, menyembunyikan jejak melalui server luar negeri, atau menerapkan teknik masking tingkat tinggi yang menyulitkan identifikasi oleh apparat (Delvyan Putri Surya Ningrum & Jamiatur Robekha, 2023).

Di samping itu, sebagian pelaku berasal dari luar negeri, sehingga proses penegakan hukum harus melalui jalur diplomatik atau kerja sama antarnegara, yang memerlukan waktu dan prosedur panjang. Hal ini berdampak pada rendahnya angka penyelesaian kasus hacking yang dilaporkan, dibandingkan dengan jumlah kejadian sebenarnya di lapangan (Rahmawati, 2017a).

2. Hambatan Penegakan Hukum

Dalam realitasnya, penegakan hukum terhadap kejahatan hacking masih menghadapi banyak tantangan serius. Hambatan-hambatan ini tidak hanya bersifat teknis, tetapi juga struktural dan kultural. Beberapa hambatan utama yang ditemukan dalam proses penegakan hukum antara lain:

a. Keterbatasan Sumber Daya Manusia (SDM)

Banyak aparat penegak hukum, baik di kepolisian, kejaksaan, maupun pengadilan, belum memiliki keahlian teknis dalam bidang teknologi informasi dan digital forensik. Hal ini menyebabkan proses penyelidikan dan pembuktian terhadap tindak pidana hacking sering kali tidak berjalan efektif. Di beberapa daerah, masih banyak penyidik yang belum familiar dengan perangkat analisis jaringan atau metode pelacakan

jejak digital. Akibatnya, potensi bukti digital sering kali tidak dapat dimanfaatkan secara maksimal dalam proses persidangan (Fediro & Tata Sutabri, 2023).

b. Kurangnya Infrastruktur Teknologi

Fasilitas teknologi merupakan faktor kunci dalam memberantas kejahatan siber. Namun, kenyataannya, perangkat pendukung seperti software pelacak IP address, perangkat *packet analyzer*, alat *digital forensic*, dan *cyber forensic lab* belum tersedia secara merata di seluruh wilayah Indonesia. Hanya pusat-pusat tertentu, seperti di Mabes Polri atau Pusat Laboratorium Forensik, yang memiliki kelengkapan fasilitas tersebut. Sementara itu, aparat penegak hukum di tingkat daerah masih sangat bergantung pada pelaporan manual dan metode konvensional (Laksana & Mulyani, 2024).

c. Tantangan Pembuktian dalam Proses Peradilan

Kejahatan siber memiliki karakteristik unik, yakni dilakukan dalam dunia maya yang tidak berbatas, dengan metode penyamaran digital yang rumit. Pelaku biasanya menggunakan teknik seperti *IP spoofing*, *VPN*, *proxy chaining*, atau bahkan *dark web* untuk menghindari pelacakan. Ini menyebabkan proses pembuktian hukum menjadi jauh lebih kompleks dibandingkan tindak pidana konvensional. Selain itu, tidak semua hakim memiliki pemahaman yang cukup dalam hal teknologi informasi, yang pada gilirannya dapat mempengaruhi kualitas pertimbangan hukum dalam vonis (Ma'rufah et al., 2020).

d. Minimnya Kesadaran Hukum Masyarakat

Kesadaran hukum masyarakat terhadap kejahatan siber, termasuk hacking, masih relatif rendah. Banyak masyarakat yang tidak menyadari bahwa tindakan seperti membobol akun media sosial orang lain, mencoba masuk ke sistem instansi, atau bermain-main dengan situs pemerintah merupakan pelanggaran hukum serius. Tidak jarang pelaku menganggap perbuatan tersebut hanya sebagai bentuk iseng atau uji kemampuan teknis belaka. Rendahnya literasi digital ini menyebabkan banyak kejahatan siber terjadi tanpa adanya pelaporan atau tindakan hukum (Butarbutar, 2023).

3. Upaya Perbaikan dan Rekomendasi

Melihat berbagai hambatan tersebut, diperlukan langkah-langkah perbaikan yang sistematis dan berkesinambungan untuk meningkatkan efektivitas penegakan hukum terhadap kejahatan hacking. Beberapa rekomendasi berikut dapat dipertimbangkan oleh pemerintah dan pihak terkait:

a. Peningkatan Kapasitas SDM Penegak Hukum

Pemerintah perlu secara aktif menyelenggarakan pelatihan intensif dan sertifikasi bagi aparat penegak hukum dalam bidang keamanan siber dan digital forensik. Pendidikan formal dan non-formal harus mengakomodasi kebutuhan akan penyidik, jaksa, dan hakim yang memiliki keahlian di bidang teknologi informasi. Selain itu, perekrutan tenaga ahli IT ke dalam institusi penegak hukum juga harus diperluas, agar dapat mendukung proses investigasi yang bersifat teknis (Rompi & Muaja, 2021).

b. Penguatan Infrastruktur dan Teknologi Pendukung

Pembangunan laboratorium digital forensik di tingkat provinsi maupun kabupaten/kota sangat penting untuk mempercepat proses penanganan kasus kejahatan siber. Pemerintah harus berinvestasi dalam pengadaan perangkat lunak dan perangkat keras yang memadai untuk mendeteksi dan melacak aktivitas hacking. Anggaran penguatan cybercrime unit di kepolisian juga harus ditingkatkan agar dapat merespons dengan cepat terhadap laporan masyarakat (Setiawan, 2020).

c. Penguatan Kerja Sama Internasional

Karena sifat kejahatan hacking yang berskala global, kerja sama antarnegara sangat penting. Indonesia harus menjalin kerja sama yang lebih erat dengan organisasi internasional seperti INTERPOL, ASEANAPOL, dan lembaga-lembaga keamanan dunia maya lainnya. Perjanjian ekstradisi dan mekanisme *mutual legal assistance* harus dioptimalkan agar proses penegakan hukum terhadap pelaku lintas negara bisa berjalan lebih efektif (Frianto et al., 2020).

d. Revisi dan Penyesuaian UU ITE

UU ITE perlu terus diperbaharui agar tetap relevan dengan perkembangan teknologi. Perubahan tersebut tidak hanya pada aspek substansi, tetapi juga pada

ketentuan teknis, seperti pengaturan jenis bukti elektronik, prosedur forensik digital, dan perlindungan terhadap saksi serta pelapor kejahatan siber. Regulasi turunan dalam bentuk Peraturan Pemerintah dan Peraturan Kapolri juga harus disesuaikan agar dapat mengakomodasi perkembangan modus kejahatan yang semakin canggih (Aulia & Adriani, 2020).

e. Sosialisasi dan Literasi Hukum Digital

Edukasi publik mengenai kejahatan siber perlu diperluas, baik melalui pendidikan formal maupun kampanye sosial. Sekolah-sekolah, kampus, dan lembaga masyarakat harus dilibatkan dalam memberikan pemahaman tentang pentingnya etika digital dan hukum teknologi. Pemerintah juga bisa bekerja sama dengan influencer digital, media massa, dan komunitas IT untuk menyebarluaskan informasi terkait keamanan digital dan dampak hukum dari tindakan hacking (Bano et al., 2020).

Kesimpulan

Penegakan hukum terhadap kejahatan siber jenis hacking di Indonesia sudah memiliki dasar hukum yang memadai melalui UU ITE. Namun, dalam praktiknya masih terdapat berbagai kendala yang menghambat efektivitasnya, mulai dari aspek SDM, infrastruktur, hingga tantangan teknis di lapangan. Diperlukan pembenahan struktural dan sinergi antar-lembaga untuk menciptakan sistem hukum yang adaptif terhadap ancaman dunia digital. Selain itu, peningkatan kesadaran hukum masyarakat menjadi bagian penting dalam menciptakan ekosistem digital yang aman dan berkeadilan.

Referensi

Aulia, A. R., & Adriani, Y. (2020). Pengaruh Sense Of Humor Dan Religiusitas Terhadap Kebahagiaan Pada Lansia. *Tazkiya: Journal Of Psychology*, *8*(2). Https://Doi.Org/10.15408/Tazkiya.V8i2.17689

Bano, R. Parenta., Ramadhani, K. D., & Synthesa, Putricia. (2020). Perbedaan Minat Baca Antara Mahasiswa Bermigrasi Dan Tidak Bermigrasi. *Magistra : Jurnal Keguruan Dan Ilmu Pendidikan*, *7*(2).

Budiman, M. Arif. (2022). Penggunaan Agen Berbasis Intelijen Untuk Menangani Kejahatan Siber. *Journal Of Innovation Research And Knowledge*, *1*(8).

Butarbutar, R. (2023). Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya. *Jurnal Hukum & Pembangunan*, *2*(2). Https://Doi.Org/10.21143/Telj.Vol2.No2.1043

Chintia, E., Nadiah, R., Ramadhani, H. N., Haedar, Z. F., Febriansyah, A., & Rakhmawati S.Kom., M.Sc.Eng, N. A. (2019). Kasus Kejahatan Siber Yang Paling Banyak Terjadi Di Indonesia Dan Penanganannya. *Journal Of Information Engineering And Educational Technology*, *2*(2). Https://Doi.Org/10.26740/Jieet.V2n2.P65-69

Delvyan Putri Surya Ningrum, & Jamiatur Robekha. (2023). Analisa Yuridis Dalam Kasus Kejahatan Siber Terhadap Internet Banking Di Indonesia. *Peshum : Jurnal Pendidikan, Sosial Dan Humaniora*, *2*(4). Https://Doi.Org/10.56799/Peshum.V2i4.2115

Djanggih, H. (2018). Konsepsi Perlindungan Hukum Bagi Anak Sebagai Korban Kejahatan Siber Melalui Pendekatan Penal Dan Non Penal. *Mimbar Hukum - Fakultas Hukum Universitas Gadjah Mada*, *30*(2). Https://Doi.Org/10.22146/Jmh.32017

Djanggih, H., & Qamar, N. (2018). Penerapan Teori-Teori Kriminologi Dalam Penanggulangan Kejahatan Siber [Implementation Of Criminological Theories In Cyber Crime Prevention]. *Pandecta: Research Law Journal*, *13*(1).

Farhan, M., Syaefunaldi, R., Hidayat, D. R. D., & Hosnah, A. U. (2023). Penerapan Hukum Dalam Menanggulangi Kejahatan Siber Penegakan Hukum Terhadap Tindak Pidana Siber. *Kultura: Jurnal Ilmu Hukum, Sosial, Dan Humaniora*, *1*(6).

Fediro, B., & Tata Sutabri. (2023). Rancang Bangun Sistem Pelaporan Insiden Kejahatan Siber. *Jurnal Informatika Teknologi Dan Sains*, *5*(1). Https://Doi.Org/10.51401/Jinteks.V5i1.2210

Frianto, D., Ashari, A. D., & Amal, S. (2020). Pengaruh Faktor Sikap Terhadap Penerimaan Vaksin Hpv Pada Orang Tua Murid Sekolah Dasar Di Kecamatan Teluk Jambe Timur Dan Tegalwaru. *Pharma Xplore : Jurnal Ilmiah Farmasi*, *5*(2). Https://Doi.Org/10.36805/Farmasi.V5i2.1192

Kasim, F. M., Daud, M., Mursalin, M., & Ali, M. (2022). Pembinaan Masyarakat Melalui Edukasi Bahaya Pinjaman Online Untuk Menghindari Bahaya Kejahatan Siber Di Gampong Cot Keumuneng Kecamatan Sawang Kabupaten Aceh Utara. *Jurnal Solusi Masyarakat Dikara*, *2*(3).

Laksana, T. G. (2024). Perlindungan Hukum Konsumen E-Commerce Pada Produk Kesehatan: Pembelajaran Pada Kejahatan Siber. *Indo Green Journal*, *2*(1). Https://Doi.Org/10.31004/Green.V2i1.45

Laksana, T. G., & Mulyani, S. (2024). Pengetahuan Dasar Identifikasi Dini Deteksi Serangan Kejahatan Siber Untuk Mencegah Pembobolan Data Perusahaan. *Jurnal Ilmiah Multidisiplin*, *3*(01). Https://Doi.Org/10.56127/Jukim.V3i01.1143

Mahira Dewantoro, N., & Dian Alan Setiawan S.H., M.H. (2023). Penegakan Hukum Kejahatan Siber Berbasis Phising Dalam Bentuk Application Package Kit (Apk) Berdasarkan Undang-Undang Informasi Dan Transaksi Elektronik. *Bandung Conference Series: Law Studies*, *3*(2). Https://Doi.Org/10.29313/Bcsls.V3i2.7247

Ma'rufah, N., Khairul, R. H., & Kerta, W. D. K. (2020). Degradasi Moral Sebagai Dampak Kejahatan Siber Pada Generasi Millenial Di Indonesia. *Tahun*, *7*(1).

Meirisah, F., & Sutabri, T. (2023). Analisa Kasus Kejahatan Siber Dengan Menggunakan Visualisasi Data. *Jurnal Informatika Teknologi Dan Sains …*.

Purwani, M. S. F. (2023). Analisis Peran Dan Penanggulangan Kejahatan Siber: Studi Kasus Spearphishing. *Restorative : Journal Of Indonesian Probation And Parole System*, *1*(1). Https://Doi.Org/10.61682/Restorative.V1i1.5

Putri, A. W. O. K., Aditya, A. R. M., Musthofa, D. L., & Widodo, P. (2022). Serangan Hacking Tools Sebagai Ancaman Siber Dalam Sistem Pertahanan Negara (Studi Kasus: Predator). *Global Political Studies Journal*, *6*(1). Https://Doi.Org/10.34010/Gpsjournal.V6i1.6698

Rahmawati, I. (2017a). Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Peningkatan Cyber Defense. *Jurnal Pertahanan & Bela Negara*, *7*(2). Https://Doi.Org/10.33172/Jpbh.V7i2.179

Rahmawati, I. (2017b). The Analysis Ofcyber Crime Threat Risk Management To Increase Cyber Defense. *Jurnal Pertahanan & Bela Negara*, *7*(2). Https://Doi.Org/10.33172/Jpbh.V7i2.193

Rompi, T., & Muaja, H. S. (2021). Tindak Kejahatan Siber Di Sektor Jasa Keuangan Dan Perbankan. *Lex Privatum*, *9*(4).

Setiawan, E. (2020). Pengaruh Atribut Hotel Dan Karakteristik Sosial Demografi Wisatawan Pada Pemilihan Hotel Di Bali. *Media Mahardhika*, *18*(2). Https://Doi.Org/10.29062/Mahardika.V18i2.209

Sudiyawati, N. P. L., & Mertha, I. K. (2022). Kejahatan Siber (Cybercrime) Dalam Konteks Kekerasan Seksual Berbasis Gender Online Di Indonesia. *Kertha Semaya : Journal Ilmu Hukum*, *10*(4). Https://Doi.Org/10.24843/Ks.2022.V10.I04.P11

Syah, R. (2023). Strategi Kepolisian Dalam Pencegahan Kejahatan Phising Melalui Media Sosial Di Ruang Siber. *Jurnal Impresi Indonesia*, *2*(9). Https://Doi.Org/10.58344/Jii.V2i9.3594

Umbara, A., & Setiawan, D. A. (2022). Analisis Kriminologis Terhadap Peningkatan Kejahatan Siber Di Masa Pandemi Covid-19. *Jurnal Riset Ilmu Hukum*. Https://Doi.Org/10.29313/Jrih.V2i2.1324

Vadila, N., & Pratama, A. R. (2021). Analisis Kesadaran Keamanan Terhadap Ancaman Phishing. *Automata*, *2*(2).

Wijaya, T. H. D. (2022). Penerapan Sanksi Sosial Sebagai Alternatif Pemidanaan Terhadap Pelaku Tindak Pidana Kejahatan Siber (Cyber Crime). *Al-Qisth Law Review*, *5*(2). Https://Doi.Org/10.24853/Al-Qisth.5.2.371-404

Yudistira, M. (2023). Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No . 27 Tahun 2022 Oleh Kominfo. *Unes Law Review*, *5*(4).

Yuswanto, A., & Wibowo, B. (2021). Pembangunan Pusat Pengendalian Operasional Keamanan Informasi (Pusdalops Kami) Guna Meningkatkan Pelayanan E-Gov Dari Ancaman Kejahatan Siber. *Format : Jurnal Ilmiah Teknik Informatika*, *9*(2). Https://Doi.Org/10.22441/Format.2020.V9.I2.003