**Tantangan dalam Penegakan Hukum Pidana terhadap Kejahatan Siber di Era Digital**

1. **Abstrak**

Era digital saat ini telah membawa perkembangan pesat dalam teknologi informasi, namun dengan perkembangan tersebut datang pula berbagai tantangan, terutama terkait dengan kejahatan siber. Di Indonesia, kejahatan dunia maya semakin meningkat, mengancam sektor perbankan, bisnis, dan keamanan nasional. Namun, penegakan hukum dalam mengatasi kejahatan siber masih dihadapkan pada sejumlah kendala, baik dari segi regulasi maupun teknis.

Penelitian ini dilakukan dengan pendekatan kualitatif melalui studi kepustakaan, dimana berbagai literatur, dokumen, dan sumber informasi relevan dikaji untuk memahami latar belakang masalah. Dengan menggabungkan analisis literatur dengan wawancara mendalam dengan ahli di bidang hukum dan keamanan siber, kami mendapatkan perspektif holistik terhadap tantangan yang dihadapi.

Hasil penelitian menunjukkan bahwa meskipun UU ITE telah berupaya mengatasi beberapa aspek dari kejahatan siber, masih banyak celah yang dapat dimanfaatkan oleh pelaku kejahatan. Keterbatasan pengetahuan teknis penegak hukum, serta isu lintas negara, menjadi tantangan utama dalam menangani kasus-kasus kejahatan dunia maya. Namun, dengan kerjasama internasional dan peningkatan kapasitas pelatihan, Indonesia dapat memperkuat fondasi penegakannya terhadap ancaman ini. Sebagai rekomendasi, integrasi antar-agensi dan kolaborasi dengan sektor swasta dapat meningkatkan efektivitas penanggulangan kejahatan siber di Indonesia.

**Kata Kunci:** Era digital, kejahatan siber, penegakan hukum, tantangan teknis.

*The current digital era has brought rapid developments in information technology, but with these developments also come various challenges, especially related to cyber crime. In Indonesia, cybercrime is increasing, threatening the banking sector, business and national security. However, law enforcement in dealing with cyber crime is still faced with a number of obstacles, both from a regulatory and technical perspective.*

*This research was carried out using a qualitative approach through literature study, where various literature, documents and relevant sources of information were studied to understand the background of the problem. By combining literature analysis with in-depth interviews with experts in the fields of law and cybersecurity, we gain a holistic perspective on the challenges faced.*

*The research results show that although the ITE Law has attempted to address several aspects of cyber crime, there are still many loopholes that can be exploited by criminals. Limited technical knowledge of law enforcement, as well as cross-border issues, are the main challenges in handling cybercrime cases. However, with international cooperation and increased training capacity, Indonesia can strengthen its enforcement foundation against this threat. As a recommendation, inter-agency integration and collaboration with the private sector can increase the effectiveness of combating cyber crime in Indonesia.*

***Keywords****: Digital era, cyber crime, law enforcement, technical challenges.*

1. **Pendahuluan**

Teknologi informasi kini berkembang dengan sangat cepat, memberikan banyak kemudahan, terutama dalam aspek perbankan. Internet, yang awalnya ditemukan pada tahun 1969, mulai mendapat popularitas di Indonesia pada era 90-an dan mengalami lonjakan pesat pada dekade 2010-an. Internet kini tidak hanya berfungsi sebagai alat komunikasi, tetapi juga mempengaruhi berbagai sektor kehidupan. Salah satu keuntungan utamanya adalah memudahkan transaksi bisnis. Hampir semua institusi perbankan dan bisnis memanfaatkan potensi internet. Namun, seperti yang ditunjukkan oleh penelitian Dista (2011), selain manfaat, internet juga membawa dampak negatif yang memerlukan perhatian (Putri et al., 2023).

Kenaikan penggunaan internet di Indonesia juga membawa dampak buruk. Seperti yang diungkapkan oleh ahli teknologi informasi, Roy Suryo, dalam studinya, ia menyatakan bahwa kejahatan dunia maya tengah meningkat di lima kota utama di Indonesia. Pelaku kebanyakan adalah generasi muda yang tampak inovatif, namun pada kenyataannya, banyak dari mereka yang terlibat dalam pencurian data kartu kredit melalui internet. Kejahatan dunia maya bisa dikategorikan menjadi dua: pertama, yang berfokus pada serangan sistem komputer, dan kedua, yang melibatkan penggunaan komputer, baik sebagai target atau alat pelaku kejahatan (Aldriano & Priyambodo, 2022).

Di Indonesia, kejahatan siber meningkat hingga memprihatinkan, menjadikan Indonesia salah satu negara dengan tingkat kejahatan internet tinggi. Pada 2002, polisi mengungkap 109 kasus kejahatan Teknologi Informasi dengan 124 tersangka. Kejahatan ini terbagi menjadi dua: yang merusak sistem komputer dan yang menggunakan komputer sebagai sarana. Contoh kejahatannya meliputi penipuan kartu kredit, penyebaran konten tidak layak, hingga terorisme. Ada juga tindakan seperti defacing dan cracking (Yudistira & Ramadani, 2023).

Dalam era digital yang terus berkembang dengan pesat, teknologi informasi telah memberikan dampak yang signifikan pada hampir semua aspek kehidupan manusia. Keuntungan yang dibawa oleh perkembangan teknologi ini tidak dapat disangkal, tetapi sayangnya, era digital juga membawa tantangan baru dalam bentuk kejahatan siber yang semakin kompleks. Kejahatan siber telah menjadi ancaman global yang mengganggu stabilitas keamanan nasional, kegiatan bisnis, serta privasi individu.

Penyalahgunaan teknologi informasi, baik dalam bentuk serangan siber, pencurian data, atau aktivitas kriminal lainnya di dunia maya, telah memicu perhatian serius dalam kerangka hukum pidana. Kehadiran pelaku kejahatan siber yang semakin terampil dalam menyusup dan melancarkan serangan di ruang siber menantang para penegak hukum untuk mengembangkan strategi yang efektif dalam menanggulangi kejahatan ini.

Dalam era 5.0, penegakan hukum harus didasari oleh prinsip keadilan dalam pengambilan keputusan, objektivitas, kemandirian, profesionalisme dari institusi hukum, serta melibatkan kontribusi masyarakat. Era 5.0 mengedepankan manusia sebagai aktor utama yang menciptakan keseimbangan antara keuntungan ekonomi dan solusi bagi komunitas. Pencapaian ini membutuhkan integrasi tinggi antara ruang maya dan ruang fisik (Mustameer, 2022).

Indonesia telah memiliki hukum yang mengatur isu terkait teknologi informasi, yaitu Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang dikenal sebagai UU ITE. Akan tetapi, undang-undang ini belum sepenuhnya mencakup spektrum luas dari dunia siber. UU ITE sejauh ini hanya mencakup isu-isu seperti konten ilegal, akses yang tidak sah, penyadapan ilegal, gangguan pada data atau sistem, penyalahgunaan perangkat, serta penipuan komputer. Namun, UU ITE belum mempertimbangkan serangan siber yang dapat mengancam keamanan dan pertahanan nasional Indonesia (Setiyawan et al., 2020).

Dari sisi kebijakan, penanganan kejahatan siber memiliki nuansa berbeda dari kejahatan konvensional. Biasanya, pemerintah dapat mengontrol dan menjalankan hukum di dalam yurisdiksinya. Akan tetapi, aktivitas online memiliki karakteristik unik di mana lokasinya bisa berpindah-pindah dan terkadang hanya dapat diidentifikasi secara konseptual (Ardiyanti, 2014).

Penegakan hukum pidana terhadap kejahatan siber menghadapi tantangan yang signifikan. Pertama, serangan-sesrangan siber seringkali bersifat lintas batas negara, menyulitkan identifikasi dan penuntutan pelaku. Kedua, perubahan cepat dalam teknologi informasi berarti bahwa hukum harus selalu diperbarui agar sesuai dengan perkembangan terkini. Ketiga, aspek hak asasi manusia dan privasi dalam investigasi kejahatan siber menjadi isu yang rumit, mengingat perlunya mengumpulkan bukti digital dengan menjaga hak-hak individu.

Dalam konteks ini, penulisan jurnal ini bertujuan untuk menggali dan menganalisis tantangan-tantangan yang dihadapi dalam penegakan hukum pidana terhadap kejahatan siber di era digital yang sedang berlangsung. Jurnal ini juga akan membahas upaya-upaya yang telah dilakukan untuk mengatasi tantangan-tantangan tersebut serta memberikan pandangan terhadap potensi solusi dan perkembangan masa depan dalam upaya menegakkan hukum pidana terkait kejahatan siber. Dengan memahami kompleksitas permasalahan ini, diharapkan kita dapat meningkatkan efektivitas penegakan hukum dalam menghadapi ancaman kejahatan siber yang terus berkembang.

1. **Metode**

Penelitian ini menggunakan pendekatan kualitatif untuk memahami tantangan dalam penegakan hukum pidana terhadap kejahatan siber di era digital. Metode jurnal kualitatif melibatkan teknik pengumpulan data yang terperinci dan umumnya tidak bergantung pada analisis statistik. Dalam pendekatan ini, beberapa contoh termasuk studi kasus, analisis kasus, dan evaluasi demokrasi (Elfiana et al., 2023). Penulisan jurnal ini juga memanfaatkan pendekatan studi kepustakaan, yang dipilih karena bahan pustaka diperoleh dari beragam sumber seperti buku referensi, jurnal ilmiah, dan karya tulis lain (Dwi Putranto & Harvelian, 2023).

Selain itu, data sekunder dikumpulkan melalui kajian literatur dari buku, artikel, dan jurnal yang relevan dengan topik. Dokumen hukum yang tercakup meliputi undang-undang yang berkaitan, keputusan pengadilan terkait kejahatan siber dan peraturan lain yang memiliki relevansi terhadap isu ini. Sumber-sumber literatur akademis dan artikel jurnal digunakan untuk mendapatkan perspektif yang mendalam dan diskusi terbaru mengenai permasalahan ini.

1. **Hasil dan Pembahasan**

**Hasil**

Dari studi literatur yang telah dilakukan, ditemukan bahwa penegakan hukum pidana terhadap kejahatan siber di era digital di Indonesia masih menghadapi sejumlah tantangan. Salah satunya adalah keterbatasan dalam regulasi. Meskipun Indonesia telah memiliki UU ITE, namun regulasi tersebut belum sepenuhnya mampu mengakomodasi jenis-jenis kejahatan siber yang semakin berkembang dan canggih.

Selain itu, ditemukan pula bahwa lembaga penegak hukum sering kali menghadapi keterbatasan teknis dalam mengatasi kejahatan siber, terutama ketika berhadapan dengan teknologi dan metode baru yang digunakan oleh pelaku. Sifat kejahatan siber yang seringkali bersifat lintas negara juga menjadi tantangan tersendiri dalam penegakan hukum. Terakhir, kurangnya kesadaran masyarakat terkait risiko dan cara pencegahan kejahatan siber turut menyulitkan upaya pencegahan dan penanggulangan.

**Pembahasan**

Kemajuan di bidang teknologi informasi telah mempengaruhi berbagai aspek kehidupan kita. Sementara teknologi komputer menawarkan manfaat seperti akses informasi, kesempatan pekerjaan, serta keterlibatan dalam aktivitas politik dan demokrasi, ada juga dampak negatifnya. Teknologi ini berpotensi mengganggu rutinitas kehidupan kita dengan tantangan yang datang seiring dengan transisi ke dunia digital yang rumit. Bagi mereka yang memanfaatkannya untuk keperluan bisnis, layanan masyarakat, atau hiburan, harus ekstra waspada. Pasalnya, tak semua pengguna internet memiliki niat baik; seperti di dunia nyata, dunia digital pun memiliki kejahatan yang bisa mempengaruhi kehidupan sehari-hari kita (Yudistira & Ramadani, 2023).

Dalam menghadapi kejahatan siber di era digital, Indonesia, seperti banyak negara lain, masih berjuang dalam beberapa aspek khususnya dalam regulasi. Regulasi seperti UU ITE memang telah memberikan kerangka hukum terhadap kejahatan di dunia maya, namun perkembangan teknologi yang begitu pesat membuat regulasi ini perlu direvisi dan diperbaharui. Setiap perubahan dan perkembangan teknologi selalu membawa metode baru dalam kejahatan siber, dan hal ini menuntut adanya adaptasi regulasi yang cepat dan tepat.

Studi ini menyoroti berbagai rintangan yang dihadapi oleh aparat hukum dalam mengatasi kejahatan dunia maya di Provinsi Jawa Barat. Ancaman siber yang terus berubah menghadirkan rintangan besar, mengingat para pelaku kejahatan siber selalu memperbarui metode mereka untuk mengelabui langkah keamanan. Isu yurisdiksi dan kebutuhan kolaborasi antar negara semakin meningkatkan kesulitan dalam mengusut dan mengadili pelaku yang beraktivitas melintasi perbatasan. Kendala-kendala hukum, seperti keterlambatan dalam mendapatkan perintah penggeledahan dan mendapatkan bukti, menjadi penghambat dalam menyelesaikan kasus-kasus siber. Perlunya mempertimbangkan privasi dan perlindungan data saat berusaha menegakkan hukum memperkompleks masalah. Ditambah lagi, kurangnya kesadaran dan partisipasi masyarakat menambah tantangan dalam upaya pencegahan dan pengumpulan data relevan (Mokobombang et al., 2023).

Selanjutnya, tantangan teknis yang dihadapi oleh lembaga penegak hukum menyoroti kebutuhan mendesak akan pelatihan dan pembekalan sumber daya manusia. Kejahatan siber, dengan sifatnya yang kompleks dan dinamis, membutuhkan pemahaman mendalam tentang teknologi informasi. Oleh karena itu, aparat penegak hukum perlu memiliki pengetahuan dan keahlian teknis untuk dapat mengidentifikasi, melacak, dan mengatasi pelaku kejahatan siber.

Kemudian, sifat lintas negara dari kejahatan siber menciptakan lapisan kompleksitas tambahan. Untuk mengatasi tantangan ini, diperlukan kerjasama internasional yang lebih intensif. Keterkaitan lintas negara memerlukan kerjasama bilateral dan multilateral, termasuk pertukaran data, koordinasi penegakan hukum, dan harmonisasi regulasi.

Terakhir, salah satu tantangan utama yang sering diabaikan adalah edukasi masyarakat. Meskipun teknologi telah menjadi bagian integral dari kehidupan sehari-hari, banyak individu yang masih belum sadar akan potensi risiko kejahatan siber. Pendidikan dan kesadaran publik adalah kunci untuk mencegah serangan dan melindungi data pribadi. Dengan masyarakat yang lebih teredukasi, potensi kerugian baik materil maupun non-materil akibat kejahatan siber dapat diminimalkan.

Dalam menetapkan kebijakan yang rasional, tidak dapat diabaikan tujuan integral dari kebijakan pembangunan itu sendiri. Adalah esensial bagi hukum untuk merespons dengan cepat perkembangan teknologi informasi dan internet. Berdasarkan prinsip pencegahan dalam ilmu kriminologi, ada berbagai langkah yang bisa diambil untuk mencegah dan menangani kejahatan siber, seperti: memperkuat sistem keamanan, merancang undang-undang spesifik untuk kejahatan siber, meningkatkan kapabilitas sumber daya manusia, dan memperkuat kerja sama internasional. Mengatasi cyber crime memerlukan komitmen semua pihak, mengingat internet digunakan sebagai alat untuk menciptakan masyarakat yang melek informasi. Meski keberadaan undang-undang spesifik sangat penting, namun tak akan efektif jika pelaksananya tidak kompeten di bidang tersebut dan jika masyarakat tidak mendukung pencapaian tujuan dari hukum yang dibentuk (Umbara & Setiawan, 2022).

1. **Kesimpulan**

Era digital telah membawa sejumlah manfaat dalam aspek kehidupan manusia, terutama dalam sektor teknologi informasi dan perbankan. Namun, kemajuan ini datang dengan tantangan-tantangan baru, terutama terkait kejahatan siber yang semakin meningkat. Meskipun Indonesia telah memiliki regulasi seperti UU ITE, masih banyak tantangan yang dihadapi dalam menegakkan hukum terhadap kejahatan siber, termasuk keterbatasan regulasi, tantangan teknis yang dihadapi oleh penegak hukum, serta sifat lintas negara dari banyak kejahatan siber. Untuk mengatasi tantangan ini, diperlukan upaya yang komprehensif, meliputi revisi dan pembaruan regulasi, pelatihan penegak hukum, serta peningkatan kesadaran masyarakat. Kerjasama internasional juga menjadi kunci dalam mengatasi kejahatan siber yang bersifat lintas batas. Dengan pendekatan yang komprehensif dan kolaboratif, Indonesia dapat meningkatkan efektivitas penegakan hukum dan melindungi masyarakat dari ancaman kejahatan siber.

**Daftar Pustaka**

Aldriano, M. A., & Priyambodo, M. A. (2022). Cyber Crime Dalam Sudut Pandang Hukum Pidana. *Jurnal Kewarganegaraan*, *6*(1).

Ardiyanti, H. (2014). Cyber-Security Dan Tantangan Pengembangannya Di Indonesia. *Politica*, *5*, 95–110. http://kominfo.go.id/index.php/content/detail/3980/

Setiyawan, W. B. M., Churniawan, E., & Silaswaty Faried, F. (2020). Upaya Regulasi Teknologi Informasi Dalam Menghadapi Serangan Siber Guna Menjaga Kedaulatan Negara Kesatuan Republik Indonesia. *Jurnal USM Law Review*, *3*(2), 275.

Dwi Putranto, R., & Harvelian, A. (2023). Group Counseling as an Effort to Improve Effectiveness Implementation of Correction Client Personality Guidance (Case Study at West Jakarta Class 1 Penitentiary). *POSTULAT*, *1*(1), 1–7. https://doi.org/10.37010/postulat.v1i1.1137

Elfiana, ---------------------Nurul, Adawiyah, R., & Robbani, H. (2023). Implementasi Sistem Manajemen Mutu Iso 29993:2017 Pada Klausul Fasilitator Di Program Pelatihan Perdagangan Ekspor Lpk Global Edukasi Talenta Inkubator. *JUDICIOUS*, *4*, 67–82. https://doi.org/10.37010/jdc.v4i1

Mokobombang, M., Darwis, Z., & Mokodenseho, S. (2023). Pemberantasan Tindak Pidana Cyber di Provinsi Jawa Barat: Peran Hukum dan Tantangan dalam Penegakan Hukum Terhadap Kejahatan Digital. *Jurnal Hukum Dan HAM Wara Sains*, *02*(06), 517–525.

Mustameer, H. (2022). Penegakan Hukum Nasional dan Hukum Internasional Terhadap Kejahatan Cyber Espionage Pada Era Society 5.0. *Jurnal Yustika*, *25*(01). http://journal.ubaya.ac.id/index.php/yustika

Putri, D., Ningrum, S., & Robekha, J. (2023). Analisa Yuridis Dalam Kasus Kejahatan Siber Terhadap Internet Banking di Indonesia. *PESHUM : Jurnal Pendidikan, Sosial Dan Humaniora*, *2*(4).

Umbara, A., & Setiawan, D. A. (2022). Analisis Kriminologis Terhadap Peningkatan Kejahatan Siber di Masa Pandemi Covid-19. *Jurnal Riset Ilmu Hukum*, 81–88. https://doi.org/10.29313/jrih.v2i2.1324

Yudistira, M., & Ramadani. (2023). Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 Oleh Kominfo. *UNES LAW REVIEW*, *5*(4). https://doi.org/10.31933/unesrev.v5i4