JOURNAL IURIS SCIENTIA
Volume 2 | Nomor 2 | July 2024
ISSN Print 2985-5950
ISSN Online 2985-8836
Penerbit : **Yayasan Merassa Indonesia Publikasi**
https://journal.merassa.id/index.php/JIS
This article is published in a peer-reviewed section of Journal IURIS SCIENTIA

ANALISIS IMPLEMENTASI KEBIJAKAN HUKUM TERHADAP PENANGANAN KEJAHATAN SIBER DI ERA DIGITAL

Afifah Rizqy Widianingrum[a]

[a] *Magister Hukum, Fakultas Hukum, Universitas 17 Agustus 1945 Semarang. Email : afifahningrum9@gmail.com.*

Article

Kata Kunci:
Kejahatan Siber; Kebijakan Hukum; UU ITE;Penegakan Hukum.

Riwayat Artikel
Received: June 7, 2024;
Reviewed: July 1, 2024;
Accepted: July 15, 2024;
Published: July 27, 2024

DOI: 10.62263/jis.v2i2.40

Abstract

Kejahatan siber mencakup berbagai aktivitas kriminal yang dilakukan melalui jaringan komputer dan internet, termasuk penipuan online, pencurian identitas, serangan malware, peretasan, dan eksploitasi data pribadi. Dengan pesatnya perkembangan teknologi informasi dan komunikasi, kejahatan siber menjadi semakin kompleks dan tersebar luas, menimbulkan dampak merugikan terhadap ekonomi, keamanan, dan privasi individu. Tantangan terbesar dalam penanganan kejahatan siber adalah menyesuaikan peraturan yang ada dengan dinamika kejahatan yang terus berkembang. Tulisan ini bertujuan untuk menganalisis implementasi kebijakan penanganan kejahatan siber di Indonesia melalui pendekatan sosiologi hukum. Implementasi kebijakan penanganan kejahatan siber di Indonesia, terutama melalui Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), melibatkan koordinasi antara berbagai lembaga penegak hukum dan kolaborasi dengan sektor swasta. Studi kasus pencurian data pribadi oleh komplotan peretas pada tahun 2022 menunjukkan proses penegakan hukum yang kompleks, mulai dari pelaporan kasus, investigasi forensik digital, penangkapan pelaku, hingga proses pengadilan. Faktor-faktor sosial, ekonomi, dan teknologi, termasuk literasi digital yang rendah, perkembangan teknologi yang cepat, dan kapasitas teknis aparat penegak hukum, mempengaruhi efektivitas kebijakan ini. Penelitian ini menyimpulkan bahwa peningkatan edukasi dan literasi digital, peningkatan kapasitas teknis dan kerjasama lintas lembaga, serta revisi regulasi yang responsif terhadap dinamika kejahatan siber, adalah langkah-langkah penting untuk meningkatkan efektivitas kebijakan penanganan kejahatan siber di Indonesia.

Cybercrime encompasses a wide range of criminal activities committed through computer networks and the internet, including online fraud, identity theft, malware attacks, hacking, and exploitation of personal data. With the rapid development of information and communication technology, cybercrime has become increasingly complex and widespread, causing adverse impacts on the economy, security, and privacy of individuals. The biggest challenge in handling cybercrime is adapting existing regulations to the evolving dynamics of crime. This paper aims to analyze the implementation of cybercrime handling policies in Indonesia through a sociology of law approach. The implementation of cybercrime policy in Indonesia, especially through the Electronic Information and Transaction Law (UU ITE), involves coordination between various law enforcement agencies and collaboration with the private sector. The case study of personal data theft by a hacker gang in 2022 shows a complex law enforcement process, ranging from case reporting, digital forensic investigation, arrest of perpetrators, to court proceedings. Social, economic, and technological factors, including low digital literacy, rapid

technological development, and the technical capacity of law enforcement officers, affect the effectiveness of these policies. This study concludes that improving digital education and literacy, increasing technical capacity and cross-agency cooperation, as well as revising regulations that are responsive to the dynamics of cybercrime, are important steps to improve the effectiveness of cybercrime handling policies in Indonesia.

PENDAHULUAN

Kejahatan siber atau *cybercrime* mengacu pada berbagai aktivitas kriminal yang dilakukan melalui jaringan komputer dan internet. Bentuk-bentuk kejahatan ini meliputi penipuan online, pencurian identitas, serangan malware, peretasan, dan eksploitasi data pribadi. Dengan pesatnya perkembangan teknologi informasi dan komunikasi, kejahatan siber menjadi semakin kompleks dan tersebar luas, mempengaruhi individu, organisasi, dan negara[1]. Era digital telah membawa kemajuan signifikan dalam berbagai aspek kehidupan, termasuk ekonomi, pendidikan, dan kesehatan. Di sisi lain, era ini juga membuka celah bagi pelaku kejahatan untuk mengeksploitasi teknologi demi keuntungan ilegal[2].

Penanganan kejahatan siber menjadi sangat krusial mengingat dampak merugikannya terhadap ekonomi, keamanan, dan privasi individu. Kejahatan siber tidak hanya menyebabkan kerugian finansial yang besar, tetapi juga dapat merusak reputasi, menciptakan ketidakamanan, dan menimbulkan ketakutan di kalangan masyarakat[3]. Dalam konteks hukum, tantangan terbesar adalah menyesuaikan peraturan yang ada dengan dinamika kejahatan siber yang terus berkembang. Hukum harus mampu melindungi hak-hak korban, mengejar pelaku kejahatan, dan mencegah kejahatan serupa di masa depan[4].

Proses hukum yang efektif memerlukan adaptasi yang cepat dan regulasi yang tepat untuk menghadapi perubahan teknologi yang pesat. Dalam konteks masyarakat, peningkatan kesadaran akan risiko kejahatan siber dan cara pencegahannya sangat penting untuk menciptakan lingkungan digital yang aman dan terpercaya. Masyarakat perlu dibekali dengan pengetahuan tentang bagaimana melindungi diri dari ancaman siber dan memahami pentingnya praktik keamanan digital[5].

Indonesia telah mengadopsi berbagai kebijakan untuk menangani kejahatan siber, termasuk undang-undang dan regulasi yang mengatur aktivitas di dunia maya. Salah satu regulasi utama adalah Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang mencakup

[1] Rian Dwi Hapsari and Kuncoro Galih Pambayun, "ANCAMAN CYBERCRIME DI INDONESIA: Sebuah Tinjauan Pustaka Sistematis," *Jurnal Konstituen* 5, no. 1 (2023): 1–17.
[2] Miftakhur Rokhman Habibi and Isnatul Liviani, "Kejahatan Teknologi Informasi (Cyber Crime) Dan Penanggulangannya Dalam Sistem Hukum Indonesia," *Al-Qanun: Jurnal Pemikiran dan Pembaharuan Hukum Islam* 23, no. 2 (2020): 400–426.
[3] Tri Ginanjar Laksana and Sri Mulyani, "Pengetahuan Dasar Identifikasi Dini Deteksi Serangan Kejahatan Siber Untuk Mencegah Pembobolan Data Perusahaan," *Jurnal Ilmiah Multidisiplin* 3, no. 01 (2024): 109–122.
[4] Utin Indah Permata Sari, "Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia," *Jurnal Studia Legalia* 2, no. 01 (2022): 58–77.
[5] R. E. Purba et al., "Peranan Hukum Positif Dalam Mengatur Cyberspace Untuk Menghadapi Tantangan Dan Peluang Di Era Digital," *Mandub: Jurnal Politik, Sosial, Hukum dan Humaniora* 2, no. 2 (2024): 167–176.

berbagai aspek kejahatan siber. UU ITE bertujuan untuk memberikan dasar hukum yang kuat dalam menghadapi berbagai bentuk kejahatan siber, serta memberikan perlindungan bagi pengguna teknologi informasi[6]. Selain itu, pemerintah Indonesia juga telah membentuk lembaga dan unit khusus untuk menangani dan menginvestigasi kasus kejahatan siber, seperti Badan Siber dan Sandi Negara (BSSN). Lembaga ini bertugas mengawasi dan mengamankan infrastruktur siber nasional, serta melakukan koordinasi dengan berbagai pihak untuk meningkatkan keamanan siber di Indonesia[7]. Kebijakan-kebijakan ini bertujuan untuk memberikan perlindungan hukum yang memadai bagi masyarakat, serta memastikan bahwa pelaku kejahatan siber dapat diadili dan dihukum sesuai dengan ketentuan yang berlaku. Selain itu, kebijakan ini juga berfungsi untuk mendorong kesadaran dan literasi digital di kalangan masyarakat, sehingga mereka dapat lebih proaktif dalam melindungi diri dari ancaman kejahatan siber[8].

PERMASALAHAN

Berdasarkan penjabaran latar belakang di atas, maka dapat di rumuskan pertanyaan penelitian sebagai berikut :" Bagaimana praktik - praktik hukum dalam implementasi kebijakan penanganan kejahatan siber di Indonesia, serta faktor-faktor sosial, teknologi, dan sebab-sebab yang mempengaruhi efektivitas kebijakan tersebut?"

METODE PENELITIAN

Dalam penulisan karya ilmiah ini, pendekatan yang digunakan merupakan pendekatan sosiologi hukum, yaitu mempelajari bagaimana hukum diterapkan dan berfungsi dalam masyarakat. Sifat dari penulisan ini adalah deskriptif analitis dengan mengkaji implementasi kebijakan hukum dalam menangani kejahatan siber di Indonesia. Metode penelitian ini menggunakan pendekatan yuridis normatif, yang mencakup studi pustaka sebagai sumber data utama. Data primer diperoleh dari literatur hukum, jurnal ilmiah, artikel, laporan penelitian, dan regulasi terkait, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Penelitian ini juga melibatkan analisis dokumen dari lembaga penegak hukum seperti Badan Siber dan Sandi Negara (BSSN). Pendekatan ini bertujuan untuk mengidentifikasi hambatan dan tantangan dalam penegakan hukum terkait kejahatan siber, serta mengeksplorasi faktor-faktor sosial, ekonomi, dan teknologi yang mempengaruhi efektivitas kebijakan tersebut. Dengan menggunakan metode ini, penelitian dapat memberikan gambaran yang komprehensif tentang bagaimana kebijakan penanganan kejahatan siber diterapkan dalam praktik dan memberikan rekomendasi untuk meningkatkan efektivitasnya.

ANALISIS DAN PEMBAHASAN

A. Konteks Sosial dan Teknologi yang Melatarbelakangi Kejahatan Siber dan Kebijakan Penanganannya

Kejahatan siber atau *cybercrime* telah menjadi tantangan serius di era digital ini. Permasalahan utama yang muncul dalam konteks ini meliputi beberapa aspek penting.

[6] Miftakhur Rokhman Habibi and Isnatul Liviani.
[7]BSSN, "Lanskap Keamanan Siber Indonesia," (2023), https://www.bssn.go.id/wp-content/uploads/2024/03/Lanskap-Keamanan-Siber-Indonesia-2023.pdf
[8] Utin Indah Permata Sari.

Pertama, kerugian ekonomi akibat kejahatan siber sangat signifikan. Banyak kasus penipuan online yang merugikan individu dan perusahaan secara finansial, seperti phishing, pencurian identitas, dan penipuan kartu kredit yang sering kali melibatkan skema rumit dan sulit dilacak. Selain itu, serangan siber yang menggunakan malware atau teknik peretasan dapat menyebabkan kerugian besar bagi perusahaan, termasuk pencurian data, perusakan sistem, dan gangguan operasional yang memerlukan biaya besar untuk pemulihan. Kedua, masalah keamanan dan privasi menjadi perhatian utama. Banyaknya pelanggaran data pribadi dan perusahaan menyebabkan informasi sensitif jatuh ke tangan yang salah, yang mengakibatkan risiko terhadap privasi individu dan keamanan perusahaan. Selain itu, serangan siber terhadap infrastruktur kritikal seperti sistem perbankan, energi, dan komunikasi dapat mengancam keamanan nasional dan stabilitas sosial. Ketiga, kompleksitas hukum dan regulasi menjadi tantangan tersendiri. Hukum yang ada sering kali tidak dapat mengikuti perkembangan teknologi yang cepat, menyebabkan kesenjangan dalam regulasi dan penegakan hukum terhadap kejahatan siber. Penanganan kejahatan siber juga memerlukan koordinasi yang efektif antara berbagai lembaga penegak hukum, baik di tingkat nasional maupun internasional, dan kurangnya koordinasi dapat menghambat upaya penegakan hukum yang efektif. Keempat, kesadaran dan literasi digital di masyarakat masih rendah. Banyak masyarakat yang belum menyadari sepenuhnya risiko kejahatan siber dan cara melindungi diri, membuat mereka rentan terhadap serangan siber. Literasi digital yang rendah juga menghambat kemampuan individu dan organisasi untuk mengambil langkah-langkah pencegahan yang efektif terhadap ancaman siber. Kelima, terdapat hambatan teknis dalam penanganan kejahatan siber. Teknologi keamanan siber yang ada sering kali tidak mampu mengimbangi metode serangan siber yang semakin canggih, menciptakan celah yang dapat dieksploitasi oleh pelaku kejahatan. Selain itu, kurangnya sumber daya manusia yang terlatih dalam bidang keamanan siber dan teknologi informasi menjadi hambatan dalam penanganan kejahatan siber. Terakhir, tantangan penegakan hukum terkait kejahatan siber cukup besar. Identifikasi dan penangkapan pelaku kejahatan siber sering kali sulit karena mereka dapat beroperasi dari lokasi yang berbeda-beda dan menggunakan teknik yang menyulitkan pelacakan. Proses hukum yang lambat dan birokrasi yang berbelit-belit juga dapat menghambat penanganan kasus kejahatan siber, mengurangi efektivitas penegakan hukum. Permasalahan-permasalahan ini menunjukkan kompleksitas dan urgensi dalam penanganan kejahatan siber yang memerlukan pendekatan komprehensif dan kolaboratif dari berbagai pihak.

perubahan sosial yang cepat, seperti urbanisasi dan globalisasi, serta penetrasi internet yang tinggi, menciptakan ekosistem di mana kejahatan siber dapat berkembang[9]. Teknologi yang semakin terhubung juga memperbesar risiko kebocoran data dan serangan siber. Masyarakat yang semakin bergantung pada teknologi informasi dan komunikasi

[9] N P S Meinarni, "Tinjauan Yuridis Cyber Bullying Dalam Ranah Hukum Indonesia," *Jurnal Ilmu Sosial Dan Humaniora* 5 (2019): 577–593, http://jayapanguspress.penerbit.org/index.php/ganaya/article/view/225.

menghadapi risiko keamanan yang meningkat, terutama karena banyaknya data pribadi yang tersimpan secara digital[10].

Kebijakan penanganan kejahatan siber di Indonesia harus mempertimbangkan konteks sosial dan teknologi ini. Regulasi yang ada harus mampu mengakomodasi perubahan cepat dalam teknologi dan perilaku sosial. Selain itu, pemerintah juga perlu menggalakkan program literasi digital untuk meningkatkan kesadaran masyarakat tentang risiko kejahatan siber dan cara menghadapinya[11].

Adapun dampak perubahan sosial dan perkembangan teknologi terhadap kejahatan siber serta penanganannya, antara lain[12]:

a. Dalam perubahan sosial terdapat urbanisasi dan meningkatnya penggunaan teknologi oleh masyarakat yang meningkatkan eksposur terhadap risiko kejahatan siber. Banyak orang yang pindah ke kota besar membawa serta kebiasaan mereka yang kurang melek teknologi, sehingga menjadi target empuk bagi pelaku kejahatan siber. Selain itu, mobilitas sosial yang tinggi juga membuat data pribadi lebih mudah disalahgunakan.
b. Sementara teknologi memberikan alat yang lebih baik untuk penegakan hukum, perkembangan teknologi juga memberikan pelaku kejahatan alat baru untuk melakukan kejahatan. Misalnya, perkembangan kecerdasan buatan dapat digunakan untuk mengotomatisasi serangan siber, membuatnya lebih sulit dideteksi dan dicegah. Kebijakan penanganan kejahatan siber harus selalu diperbarui untuk menghadapi ancaman baru yang muncul dari perkembangan teknologi ini.

Dengan memahami konteks sosial dan teknologi yang melatarbelakangi kejahatan siber, kebijakan yang dibuat dapat lebih efektif dan relevan. Penegak hukum perlu terus memperbarui pengetahuan dan keterampilan mereka, sementara masyarakat perlu lebih sadar akan risiko dan cara melindungi diri dari kejahatan siber. Kolaborasi antara pemerintah, masyarakat, dan sektor swasta juga sangat penting untuk menciptakan ekosistem digital yang aman dan terpercaya[13].

B. Salah Satu Bentuk Kejahatan Siber Yang Terjadi Di Indonesia

Perjudian sudah lama ada di Indonesia, sehingga sudah menjadi hal yang umum di tengah-tengah masyarakat. Perkembangan teknologi dan informasi juga mempengaruhi perkembangan perjudian. Perjudian yang awalnya dilakukan sacara tatap muka sekarang bisa dilakukan secara online, sehingga pemain tidak harus bertemu langsung satu sama lain. Berbeda dengan judi konvesional, judi online berkamuflase dalam bentuk aplikasiatau sebuah game sehingga sangat mudah menjangkau seluruh kalangan masyarakat secara luas.

[10] Eko Budi, Dwi Wira, and Ardian Infantono, "Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional Di Era Society 5.0," *Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia (SENASTINDO)* 3, no. November (2021): 223–234.
[11] Edy Soesanto et al., "Analisis Dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman Dan Solusi Dalam Lingkungan Digital Untuk Mengamankan Objek Vital Dan File," *SAMMAJIVA : Jurnal Penelitian Bisnisdan Manajemen* 1, no. 2 (2023): 186.
[12] Raodia, "Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (Cybercrime)," *Jurisprudentie : Jurusan Ilmu Hukum Fakultas Syariah dan Hukum* 6, no. 2 (2019): 39.
[13] Utin Indah Permata Sari.

Adanya perjudian online membuat orang semakin tertarik untuk melakukan perjudian, sebab banyak fitur-fitur atau jenis permainan yang ditawarkan oleh situs judi online. Perjudian online memudahkan seseorang dalam bermain judi, sebab pemain tidak harus pergi ke tempat judi, cukup dilakukan di mana saja yang terpenting ada akses internetnya serta memiliki saldo deposit buat bahan taruhan. Perjudian online merupakan tindak pidana yang perbuatannya melibatkan media internet. Perjudian online bisa dilakukan kapan saja dan di mana saja yang terpenting tersambung oleh jaringan internet. Dengan kemudahan yang diberikan dalam bermain judi, judi online semakin diminati banyak orang karena syarat yang tidak rumit dan mudah serta keuntungan besar yang dijanjikan[14].

Dalam hal pengaturan tindak pidana judi online ini tidak dapat dilepaskan dari pengaturan tindak pidana judi (konvensional) yang sudah lebih dahulu dikenal di masyarakat, untuk itu peranan dari peraturan- peraturan yang telah ada sebelumnya sangat dibutuhkan, seperti pengaturan tindak pidana di dalam Pasal 303 dan 303 bis Kitab Undang-Undang Hukum Pidana, Untuk mengatasi tindak pidana perjudian yang dilakukan melalui sistem elektronik atau internet yang terjadi saat ini, Pemerintah Indonesia telah membuat Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik (Undang-Undang ITE) yang di dalamnya mengatur berbagai kegiatan yang dilakukan di dunia maya *Cyberspace*, termasuk beberapa perbuatan yang dilarang karena melanggar hukum dan mengandung unsur pidana. Walaupun tindak pidana di dunia maya (*Cybercrime*) belum diatur secara khusus dalam suatu peraturan perundang-undangan tertentu, namun telah diatur dalam Undang-Undang Nomor 19 Tahun 2016 Pasal 27 Ayat (2) menyatakan:

"Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan perjudian."

Ancaman pidana Pasal 27 Ayat (2) juncto Pasal 45 Ayat (1), menyatakan:

"Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 Ayat (1), Ayat (2), Ayat (3), atau Ayat (4) dipidana dengan penjara paling lama 6 (Enam) tahun dan/atau denda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah)."

Sedangkan dalam pengaturan KUHP Pasal 303 ayat (1) menyatakan

"Diancam dengan pidana penjara paling lama sepuluh tahun atau pidana denda paling banyak Rp. 25.000.000,00 (Dua puluh lima juta rupiah)."

Hukuman Para Pelaku Perjudian masih dianggap rendah sehingga para pelaku tidak mendapatkan efek jera dengan perbuatannya, maka dengan hal itu perlu adanya revisi Undang-Undang Informasi dan Transaksi Elektronik Nomor 19 Tahun 2016 tentang penjatuhan hukuman dan denda untuk para pelaku Perjudian online.

C. Kebijakan Penanganan Kejahatan Siber Diterapkan dalam Praktik Hukum

Kebijakan penanganan kejahatan siber di Indonesia diimplementasikan melalui berbagai instrumen hukum utama, terutama Undang-Undang Informasi dan Transaksi

[14] Muhammad Yanuar Vernanda Saputra and Edi Pranoto, "Pencegahan Tindak Pidana Perjudian Online," *PLEDOI (Jurnal Hukum dan Keadilan)* 2, no. 1 (2023): 20–30.

Elektronik (UU ITE). UU ITE dirancang untuk mengatur berbagai aktivitas di dunia maya dan memberikan landasan hukum bagi penindakan terhadap kejahatan siber[15]. Implementasi kebijakan ini melibatkan koordinasi antara berbagai lembaga penegak hukum seperti Kepolisian Republik Indonesia (Polri), Badan Siber dan Sandi Negara (BSSN), serta kejaksaan[16].

Proses penegakan hukum dimulai dari pelaporan kasus oleh masyarakat atau deteksi oleh lembaga terkait. Setelah laporan diterima, lembaga penegak hukum melakukan investigasi awal yang mencakup pengumpulan bukti digital, analisis forensik komputer, dan identifikasi pelaku. Langkah-langkah ini sering kali memerlukan keahlian teknis yang mendalam serta peralatan canggih untuk mengatasi berbagai tantangan teknis yang ada dalam investigasi kejahatan siber[17].

Selain itu, aparat penegak hukum juga sering kali bekerja sama dengan pihak swasta seperti penyedia layanan internet dan perusahaan teknologi untuk mendapatkan informasi tambahan dan memfasilitasi investigasi. Penyedia layanan internet, misalnya, dapat membantu dalam melacak alamat IP yang digunakan oleh pelaku kejahatan[18].

Dalam implementasi kebijakan penanganan kejahatan siber di Indonesia, praktik-praktik hukum melibatkan serangkaian langkah yang kompleks dan melibatkan berbagai lembaga penegak hukum. Kasus pencurian data pribadi oleh komplotan peretas yang berhasil diungkap oleh Kepolisian Republik Indonesia pada tahun 2022 menjadi salah satu contoh konkret bagaimana kebijakan ini diterapkan dalam praktik hukum[19].

Proses penegakan hukum dalam kasus ini dimulai dengan penerimaan laporan dari beberapa korban yang merasa identitas mereka telah dicuri dan digunakan secara ilegal[20]. Langkah awal ini menandakan pentingnya partisipasi masyarakat dalam memberikan informasi kepada pihak berwenang, sehingga tindakan penegakan hukum dapat diambil. Kolaborasi antara masyarakat dan lembaga penegak hukum adalah kunci utama dalam menangani kejahatan siber, karena sering kali pelaku tidak mudah terdeteksi tanpa adanya laporan dari korban atau pihak yang terkena dampak.

Setelah menerima laporan, Badan Siber dan Sandi Negara (BSSN) bersama Kepolisian Republik Indonesia melakukan penyelidikan intensif. Proses penyelidikan ini melibatkan analisis forensik digital untuk melacak jejak elektronik para pelaku. Analisis forensik digital menjadi salah satu alat penting dalam investigasi kejahatan siber karena membantu mengumpulkan bukti elektronik yang dapat digunakan dalam proses pengadilan. Keterampilan teknis yang tinggi diperlukan dalam melakukan analisis forensik digital ini, sehingga memerlukan kerjasama antara aparat penegak hukum dan ahli teknologi informasi[21].

---

[15] Utin Indah Permata Sari.
[16] Yustika Citra Mahendra and Ni Komang Desy Setiawati Arya Pinatih, "Strategi Penanganan Keamanan Siber (Cyber Security) Di Indonesia," *Jurnal Review Pendidikan dan Pengajaran (JRPP)* 6, no. 4 (2023): 1941–1949, http://journal.universitaspahlawan.ac.id/index.php/jrpp/article/view/20659.
[17] Fakhri Awaluddin, Amsori, and Momon Mulyana, "Tantangan Dan Peran Digital Forensik Dalam Penegakan Hukum Terhadap Kejahatan Di Ranah Digital," *Humaniorum* 2, no. 1 (2024): 14–19.
[18] *Ibid*.
[19] Utin Indah Permata Sari.
[20] Rona Suroya Zain, "DATA MELALUI FILE YANG MEMUAT HASIL RETASAN" 01 (2016): 161–170.
[21] Utin Indah Permata Sari.

Investigasi mengungkap bahwa para peretas menggunakan teknik *phishing* untuk memperoleh data pribadi dari korban mereka. *Phishing* merupakan salah satu bentuk serangan siber yang umum dilakukan oleh pelaku kejahatan untuk mendapatkan informasi sensitif seperti kata sandi, nomor kartu kredit, atau informasi identitas pribadi lainnya dengan menyamar sebagai entitas yang tepercaya. Teknik ini seringkali berhasil karena memanfaatkan kurangnya kesadaran dan literasi digital di kalangan masyarakat.

Setelah mengumpulkan cukup bukti, dilakukan penangkapan dan penggerebekan di beberapa lokasi. Proses penangkapan ini menunjukkan komitmen aparat penegak hukum dalam menindaklanjuti hasil penyelidikan dan mengambil tindakan tegas terhadap pelaku kejahatan siber. Penangkapan tersebut juga menjadi salah satu langkah penting dalam memberikan kepastian hukum bagi korban, serta memberikan sinyal bahwa tindakan kejahatan siber tidak akan ditoleransi oleh negara.

Para pelaku akhirnya diadili berdasarkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan dijatuhi hukuman penjara serta denda. Dalam proses persidangan, pengadilan akan menilai bukti yang diajukan oleh penuntut dan pembela. Hakim akan mempertimbangkan semua bukti yang ada dan memutuskan apakah terdakwa bersalah atau tidak. Dalam kasus pencurian data pribadi ini, terdakwa dinyatakan bersalah berdasarkan bukti digital yang kuat dan saksi ahli yang memberikan kesaksian mengenai cara kerja pelaku dalam mencuri data[22]. Proses peradilan ini menunjukkan bahwa kejahatan siber dianggap serius oleh hukum Indonesia dan bahwa pelaku akan dihukum sesuai dengan ketentuan yang berlaku. Selain itu, hukuman yang diberikan juga bertujuan sebagai efek jera bagi pelaku kejahatan siber lainnya.

Kasus ini menunjukkan betapa pentingnya kolaborasi antara berbagai lembaga, seperti BSSN dan Kepolisian, dalam menangani kejahatan siber. Tanpa kerjasama yang baik antara lembaga penegak hukum dan teknologi informasi, sulit untuk mengungkap dan menindak pelaku kejahatan siber dengan efektif[23]. Selain itu, kasus ini juga menekankan pentingnya partisipasi masyarakat dalam memberikan informasi dan mendukung upaya penegakan hukum. Kesadaran akan risiko kejahatan siber dan pentingnya melaporkan tindakan mencurigakan menjadi kunci dalam memerangi kejahatan siber di Indonesia.

D. Faktor-Faktor yang Menyebabkan Terjadinya Kejahatan Siber

Kejahatan siber terjadi karena berbagai alasan yang kompleks dan saling terkait. Salah satu motif utama adalah keuntungan finansial, di mana pelaku kejahatan mencari cara untuk mendapatkan uang dengan cepat melalui aktivitas ilegal di internet. Misalnya, penipuan online dan pencurian identitas sering kali dilakukan untuk mencuri uang dari rekening bank korban atau menjual informasi pribadi di pasar gelap.

Selain motif finansial, ada juga kejahatan siber yang dilakukan karena motif ideologis, politik, atau balas dendam pribadi. Serangan siber terhadap infrastruktur kritis, misalnya, bisa dilakukan oleh kelompok yang ingin menyampaikan pesan politik atau

[22] Mahendra and Pinatih, "Strategi Penanganan Keamanan Siber (Cyber Security) Di Indonesia."
[23] Raodia.

merusak reputasi suatu negara atau perusahaan. Adapun faktor-faktor sosial, ekonomi, dan teknologi yang mendasari munculnya kejahatan siber antara lain:

a. Sosial
   Minimnya literasi digital di kalangan masyarakat membuat banyak orang tidak sadar akan pentingnya menjaga data pribadi dan praktik keamanan *online*. Kurangnya edukasi tentang keamanan siber juga menyebabkan banyak orang mudah tertipu oleh taktik *phishing* atau penipuan *online* lainnya[24].
b. Ekonomi
   Kesenjangan ekonomi menciptakan tekanan bagi sebagian orang untuk mencari sumber pendapatan alternatif, termasuk melalui aktivitas ilegal. Di beberapa negara berkembang, keterbatasan kesempatan kerja dan kemiskinan menjadi faktor pendorong orang-orang untuk terlibat dalam kejahatan siber[25].
c. Teknologi
   Pesatnya perkembangan teknologi informasi menciptakan celah keamanan yang dapat dieksploitasi oleh penjahat siber. Teknologi juga memberikan anonimitas yang membuat pelaku sulit dilacak dan ditangkap. Selain itu, teknologi yang terus berkembang sering kali lebih cepat daripada perkembangan regulasi dan kebijakan keamanan siber, menciptakan celah yang bisa dimanfaatkan oleh pelaku kejahatan[26].

Upaya preventif dan represif yang digunakan dalam menanggulangi tindak pidana perjudian online dianggap belum cukup karena terbukti kasus perjudian online yang meningkat setiap tahunnya, selain itu, terdapat beberapa faktor yang menghambat proses penganggulangan tindak pidana perjudian online, diantaranya[27]:

1. Faktor Ekonomi
   Perjudian online sangat rentan terjadi kepada seseorang dengan kondisi ekonomi menengah ke bawah karena tidak dapat memenuhi kebutuhan hidup sehari-sehari sehingga mencari solusi untuk dapat memenuhi kebutuhannya secara instan. Sepintas nampak bahwa dengan berjudi, seseorang dapat meningkatkan perekonomiannya dengan cepat melalui judi karena modal yang dikeluarkan sedikit namun mendapatkan hasil yang berlipat-lipat, sehingga lebih mudah menghasilan uang yang banyak.
2. Faktor Kemenangan
   Para pelaku perjudian selalu memiliki persepsi pikiran dalam hal kemenangan apabila mereka bermain judi. Para pelaku perjudian yang sulit meninggalkan perjudian biasanya cenderung memiliki persepsi yang keliru tentang kemungkinan untuk menang. Pelaku perjudian pada umumnya merasa sangat yakin akan kemenangan yang akan diperolehnya, meski pada kenyataannya peluang tersebut amatlah kecil karena keyakinan yang ada hanyalah suatu ilusi yang diperoleh dari

[24] Soesanto et al., "Analisis Dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman Dan Solusi Dalam Lingkungan Digital Untuk Mengamankan Objek Vital Dan File."
[25] Raodia.
[26] Utin Indah Permata Sari.
[27] F Fahrul, "Penegakan Hukum Terhadap Pelaku Tindak Pidana Judi Online (Studi Kasus Proses Tindak Pidana Kasus Judi Online Di Wilayah Hukum Kepolisian Daerah Jawa Timur)," *Angewandte Chemie International Edition, 6(11), 951–952.* 10, no. 6 (2024): 298–308.

evaluasi peluang berdasarkan suatu situasi atau kejadian yang tidak menentu dan sangat subyektif.

3. Faktor Belajar
   Keingintahuan terhadap sesuatu merupakan hal manusiawi, namun apabila hal tersebut dilakukan dengan cara yang salah, maka hanya efek buruk yang akan diterima oleh pelakunya, seperti perjudian online, kekurangan pendidikan dan pengetahuan dapat mengakibatkan seseorang tidak berfikir panjang dalam perbuatannya termasuk bermain judi online.
4. Faktor Ketidakpatuhan Masyarakat Terhadap Hukum
   Pemerintah membuat peraturan bertujuan sebagai payung hukum untuk menjaga keamanan dan keadilan bagi masyarakat sebagaimana penegakan hukum yang sesungguhnya, akan tetapi di dalam praktiknya masyarakat ada yang patuh dengan suatu kebijakan peraturan dan ada juga yang tidak patuh dengan peraturan tersebut.

E. Faktor-Faktor yang Mempengaruhi Efektivitas Kebijakan Penanganan Kejahatan Siber

Efektivitas kebijakan penanganan kejahatan siber dipengaruhi oleh berbagai faktor, termasuk kapasitas dan kompetensi aparat penegak hukum, kesadaran dan partisipasi masyarakat, serta kemajuan teknologi yang digunakan untuk penegakan hukum. Faktor-faktor ini saling berkaitan dan mempengaruhi seberapa efektif kebijakan dapat diterapkan di lapangan. Pembentukan peraturan perundang-undangan yang terarah melalui prolegnas diharapkan dapat mengarahkan pembangunan hukum dan mewujudkan konsistensi peraturan perundang-undangan[28].

1. Kapasitas dan Kompetensi Aparat Penegak Hukum

   Aparat penegak hukum perlu memiliki keahlian teknis yang mendalam untuk mengatasi kejahatan siber yang kompleks. Pelatihan khusus dan peningkatan kapasitas teknologi bagi aparat penegak hukum terus dilakukan untuk menghadapi tantangan teknis dan taktis dalam menghadapi kejahatan siber. Namun, pelatihan ini harus kontinu dan adaptif terhadap perkembangan teknologi yang cepat[29].

   Dalam hal ini kepolisian dan BSSN memiliki peran kunci dalam investigasi dan penindakan terhadap kejahatan siber. Mereka bertanggung jawab untuk menangani laporan kejahatan, melakukan investigasi, dan mengadili pelaku. Selain itu, mereka juga harus terus memperbarui pengetahuan dan keterampilan mereka untuk mengikuti perkembangan teknologi dan taktik kejahatan siber[30].
2. Kesadaran dan Partisipasi Masyarakat

   Kesadaran dan partisipasi masyarakat juga merupakan aspek penting dalam mencegah kejahatan siber. Edukasi tentang risiko kejahatan siber dan cara pencegahannya harus ditingkatkan melalui berbagai program sosialisasi.

[28] Mahendra and Pinatih.
[29] Aisyah Putri Nabila, Nathania Aurell Manabung, and Aquilla Cinta Ramadhansha, "Peran Hukum Internasional Dalam Menanggulangi Cyber Crime Pada Kejahatan Transnasional," *Indonesian Journal of Law* 1, no. 1 (2024): 26–37.
[30] BSSN, "Lanskap Keamanan Siber Indonesia."

Masyarakat perlu dibekali dengan pengetahuan tentang bagaimana melindungi diri dari ancaman siber dan memahami pentingnya praktik keamanan digital[31].

3. Kemajuan Teknologi

Penggunaan teknologi canggih, seperti analisis *big data* dan kecerdasan buatan, dapat membantu dalam deteksi dini dan investigasi kejahatan siber. Namun, teknologi juga harus terus ditingkatkan untuk mengimbangi taktik yang semakin canggih dari pelaku kejahatan. Inovasi teknologi harus didukung oleh regulasi yang tepat agar dapat digunakan secara efektif dalam penegakan hukum[32].

Sarana dan prasarana termasuk fasilitas yang digunakan oleh penegak hukum untuk membantu proses berjalannya tugas dengan sebaik-baiknya sesuai perundang-undangan yang berlaku. Fasilitas untuk menjalankan proses penegakan hukum harus memadai agar hasil yang diperoleh juga baik, maka dibutuhkan fasilitas seperti alat-alat yang modern dan anggaran operasional. Fasilitas alat-alat yang modern yang dibutuhkan seperti kendaraan, sarana komunikasi, jaringan internet yang kuat dan perangkat teknologi IT untuk mendeteksi perjudian online. Fasilitas anggaran dapat digunakan untuk menjalankan operasional yang dibutuhkan alat-alat modern seperti pembelian bahan bakar dan pendukung perangkat teknologi (jaringan wifi). Apabila fasilitas sudah mendukung semua, maka pencegahan dan penegakan hukum perjudian online akan berjalan lebih baik. Sumber daya manusia dari personal kepolisian juga berperan penting dalam pemberantasan perjudian online. Perjudian online sulit untuk diberantas disebabkan karena terbatasnya anggota personal kepolisian dalam memperlancar proses penegakan hukum. Hal ini disebabkan karena hanya sedikit personal kepolisian yang memahami tentang teknologi informasi (IT). Tidak bisa dipungkiri, batas pendidikan formal untuk bisa menjadi anggota kepolisian cukup hanya sampai lulusan sekolah menengah atas (SMA). Padahal, untuk bisa memberantas kasus *cybercrime*, seseorang harus mempunyai pengalaman dan pendidikan dalam memahami tentang teknologi informasi (IT)[33].

KESIMPULAN

Melalui pendekatan sosiologi hukum terhadap implementasi kebijakan penanganan kejahatan siber di Indonesia, dapat disimpulkan bahwa kolaborasi antara lembaga penegak hukum, masyarakat, dan sektor swasta memainkan peran penting dalam mengatasi ancaman kejahatan siber. Kasus pencurian data pribadi oleh komplotan peretas pada tahun 2022 menjadi contoh konkret bagaimana kebijakan ini diterapkan dalam praktik hukum. Proses penegakan hukum dimulai dengan penerimaan laporan dari korban, diikuti dengan penyelidikan intensif yang melibatkan analisis forensik digital, penangkapan pelaku, dan proses pengadilan.

Meskipun implementasi kebijakan penanganan kejahatan siber telah menunjukkan kemajuan yang signifikan, masih terdapat tantangan dalam menjaga keamanan *cyber* di

[31] Supanto et al., "Pencegahan Dan Penanggulangan Kejahatan Teknologi Informasi Di Wilayah Pdm Kabupaten Klaten Melalui Metode Sosialisasi Interaktif," *Jurnal Gema Keadilan* 10, no. 3 (2023): 170–182.
[32] Utin Indah Permata Sari.
[33] Kadek Setiawan, I Wayan Landrawan, and Ketut Sudiatmaka, "Upaya Kepolisian Dalam Penegakan Hukum Terhadap Pelaku Tindak Pidana Perjudian Online Di Buleleng," *Jurnal Ilmu Hukum Sui Generis* 03, no. 04 (2023): 194–198.

Indonesia. Faktor-faktor seperti kurangnya literasi digital di kalangan masyarakat, perkembangan teknologi yang cepat, dan kebutuhan akan kerjasama lintas lembaga masih menjadi hambatan dalam upaya menangani kejahatan siber secara efektif. Oleh karena itu, pendekatan yang mengintegrasikan aspek hukum dan sosial perlu diperkuat untuk mengatasi permasalahan tersebut.Maka dari itu, untuk meningkatkan efektivitas kebijakan penanganan kejahatan siber, perlu dilakukan beberapa langkah perbaikan, antara lain:

1. Penguatan edukasi dan literasi digital di kalangan masyarakat untuk meningkatkan kesadaran akan risiko kejahatan siber.
2. Peningkatan kapasitas teknis dan kerjasama antara lembaga penegak hukum dan sektor swasta dalam menghadapi ancaman kejahatan siber.
3. Revisi dan pembaruan regulasi yang lebih responsif terhadap perkembangan teknologi dan dinamika kejahatan siber.

Temuan ini memberikan pemahaman yang lebih dalam tentang kompleksitas fenomena kejahatan siber dan menyoroti pentingnya pendekatan yang holistik dalam penanganannya. Implikasi temuan ini dapat menjadi dasar untuk penyusunan kebijakan yang lebih efektif dan responsif terhadap dinamika kejahatan siber di masa depan. Pentingnya sinergi antara hukum dan aspek sosial juga menjadi poin penting yang perlu diperhatikan dalam merancang kebijakan penanganan kejahatan siber yang holistik dan berkelanjutan.

DAFTAR PUSTAKA/REFERENSI

Awaluddin, Fakhri, Amsori, and Momon Mulyana. "Tantangan Dan Peran Digital Forensik Dalam Penegakan Hukum Terhadap Kejahatan Di Ranah Digital." *Humaniorum* 2, no. 1 (2024): 14–19.

BSSN. "Lanskap Keamanan Siber Indonesia," no. 70 (2024).

Budi, Eko, Dwi Wira, and Ardian Infantono. "Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional Di Era Society 5.0." *Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia (SENASTINDO)* 3, no. November (2021): 223–234.

Fahrul, F. "Penegakan Hukum Terhadap Pelaku Tindak Pidana Judi Online (Studi Kasus Proses Tindak Pidana Kasus Judi Online Di Wilayah Hukum Kepolisian Daerah Jawa Timur)." *Angewandte Chemie International Edition, 6(11), 951–952.* 10, no. 6 (2024): 298–308.

Habibi, Miftakhur Rokhman, and Isnatul Liviani. "Kejahatan Teknologi Informasi (Cyber Crime) Dan Penanggulangannya Dalam Sistem Hukum Indonesia." *Al-Qanun: Jurnal Pemikiran dan Pembaharuan Hukum Islam* 23, no. 2 (2020): 400–426.

Hapsari, Rian Dwi, and Kuncoro Galih Pambayun. "ANCAMAN CYBERCRIME DI INDONESIA: Sebuah Tinjauan Pustaka Sistematis." *Jurnal Konstituen* 5, no. 1 (2023): 1–17.

Laksana, Tri Ginanjar, and Sri Mulyani. "Pengetahuan Dasar Identifikasi Dini Deteksi Serangan Kejahatan Siber Untuk Mencegah Pembobolan Data Perusahaan." *Jurnal Ilmiah Multidisiplin* 3, no. 01 (2024): 109–122.

Mahendra, Yustika Citra, and Ni Komang Desy Setiawati Arya Pinatih. "Strategi Penanganan Keamanan Siber (Cyber Security) Di Indonesia." *Jurnal Review Pendidikan dan Pengajaran (JRPP)* 6, no. 4 (2023): 1941–1949.

http://journal.universitaspahlawan.ac.id/index.php/jrpp/article/view/20659.

Meinarni, N P S. "Tinjauan Yuridis Cyber Bullying Dalam Ranah Hukum Indonesia." *... : Jurnal Ilmu Sosial Dan Humaniora* 5 (2019): 577–593. http://jayapanguspress.penerbit.org/index.php/ganaya/article/view/225.

Nabila, Aisyah Putri, Nathania Aurell Manabung, and Aquilla Cinta Ramadhansha. "Peran Hukum Internasional Dalam Menanggulangi Cyber Crime Pada Kejahatan Transnasional." *Indonesian Journal of Law* 1, no. 1 (2024): 26–37.

Purba, R. E., D. Maharani, M. A. A. BMY, and R. Z. Al Zahra. "Peranan Hukum Positif Dalam Mengatur Cyberspace Untuk Menghadapi Tantangan Dan Peluang Di Era Digital." *Mandub: Jurnal Politik, Sosial, Hukum dan Humaniora* 2, no. 2 (2024): 167–176.

Raodia, Raodia. "Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (Cybercrime)." *Jurisprudentie : Jurusan Ilmu Hukum Fakultas Syariah dan Hukum* 6, no. 2 (2019): 39.

Setiawan, Kadek, I Wayan Landrawan, and Ketut Sudiatmaka. "Upaya Kepolisian Dalam Penegakan Hukum Terhadap Pelaku Tindak Pidana Perjudian Online Di Buleleng." *Jurnal Ilmu Hukum Sui Generis* 03, no. 04 (2023): 194–198.

Soesanto, Edy, Achmad Romadhon, Bima Dwi Mardika, and Moch Fahmi Setiawan. "Analisis Dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman Dan Solusi Dalam Lingkungan Digital Untuk Mengamankan Objek Vital Dan File." *SAMMAJIVA : Jurnal Penelitian Bisnisdan Manajemen* 1, no. 2 (2023): 186.

Supanto, Ismunarno, Tika Andarasni Parwitasari, and Winarno Budyatmojo. "Pencegahan Dan Penanggulangan Kejahatan Teknologi Informasi Di Wilayah Pdm Kabupaten Klaten Melalui Metode Sosialisasi Interaktif." *Jurnal Gema Keadilan* 10, no. 3 (2023): 170–182.

Utin Indah Permata Sari. "Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia." *Jurnal Studia Legalia* 2, no. 01 (2022): 58–77.

Yanuar Vernanda Saputra, Muhammad, and Edi Pranoto. "Pencegahan Tindak Pidana Perjudian Online." *PLEDOI (Jurnal Hukum dan Keadilan)* 2, no. 1 (2023): 20–30.

Zain, Rona Suroya. "DATA MELALUI FILE YANG MEMUAT HASIL RETASAN" 01 (2016): 161–170.