

CYBERCRIME LINTAS NEGARA ASEAN: STUDI KASUS PERJUDIAN ONLINE DALAM ANCAMAN KEAMANAN NASIONAL DI INDONESIA

**Cybercrime Across ASEAN Borders: A Case Study Of Online Gaming In
The Context Of National Security Threats In Indonesia**

St. Fatimah Azzahra Zalia

Universitas Hasanuddin

**Jl. Perintis Kemerdekaan No.KM.10, Tamalanrea Indah, Kec. Tamalanrea, Kota Makassar,
Sulawesi Selatan 90245**

st.fatimah100405@gmail.com

Abstract

Online gambling has emerged as a significant transnational cybercrime threat in Southeast Asia, particularly affecting Indonesia's national security. This study explores how illegal online gambling networks exploit jurisdictional gaps, digital payment systems, and weak regional law enforcement coordination to operate across borders. The research focuses on three key areas: the evolving tactics of cross-border gambling operations, their economic and social impacts on Indonesian society, and the institutional challenges faced by ASEAN countries in addressing this issue. Using a mixed-methods approach that combines legal analysis, case studies, and policy evaluation, the study reveals that these criminal networks increasingly rely on cryptocurrency, offshore servers, and local affiliates to sustain their activities. Findings also show strong links between online gambling and other forms of transnational crime such as money laundering and organized crime. Moreover, it highlights how these activities undermine Indonesia's digital sovereignty, drain billions of rupiah annually from the national economy, and contribute to rising social instability. The study concludes that effective countermeasures require stronger regional cooperation, including harmonized cybercrime laws, improved intelligence sharing, and enhanced technical capacities among ASEAN member states.

Keywords: *Online gambling, cybercrime, national security, transnational crime, ASEAN*

Abstrak

Perjudian online telah muncul sebagai ancaman cybercrime lintas negara yang signifikan di kawasan Asia Tenggara, terutama berdampak pada keamanan nasional Indonesia. Penelitian ini mengeksplorasi bagaimana jaringan perjudian online ilegal memanfaatkan celah yurisdiksi, sistem pembayaran digital, dan lemahnya koordinasi penegakan hukum regional untuk beroperasi lintas batas. Penelitian ini fokus pada tiga area utama: taktik operasional perjudian lintas batas yang terus berkembang, dampak ekonomi dan sosialnya terhadap masyarakat Indonesia, serta tantangan institusional yang dihadapi negara-negara ASEAN dalam mengatasi masalah ini. Dengan menggunakan pendekatan metode campuran yang menggabungkan analisis hukum, studi kasus, dan evaluasi kebijakan, penelitian ini mengungkapkan bahwa jaringan kriminal semakin bergantung pada mata uang

kripto, server offshore, dan afiliasi lokal untuk mempertahankan aktivitas mereka. Hasil penelitian juga menunjukkan hubungan kuat antara perjudian online dengan bentuk kejahatan transnasional lainnya seperti pencucian uang dan kejahatan terorganisir. Selain itu, penelitian ini menyoroti bagaimana aktivitas tersebut merusak kedaulatan digital Indonesia, menguras miliaran rupiah dari perekonomian nasional setiap tahun, serta berkontribusi pada meningkatnya ketidakstabilan sosial. Studi ini menyimpulkan bahwa langkah-langkah antisipatif yang efektif membutuhkan kerja sama regional yang lebih kuat, termasuk harmonisasi undang-undang cybercrime, peningkatan berbagi informasi intelijen, dan peningkatan kapasitas teknis di antara negara anggota ASEAN.

Kata Kunci: Perjudian online, cybercrime, keamanan nasional, kejahatan transnasional, ASEAN

PENDAHULUAN

Pesatnya evolusi teknologi di tengah globalisasi membuat akses terhadap teknologi dan informasi menjadi lebih mudah bagi masyarakat. Perkembangan teknologi saat ini ibarat dua sisi koin yang memiliki dampak positif dan negatif bagi masyarakat. Salah satu dampak negatifnya adalah kejahatan siber, yaitu tindakan ilegal yang dilakukan melalui komputer atau jaringan, biasanya secara online (Budi Suhariyanto, 2013). Kejahatan siber ini pun dapat menimpa siapa saja dan dapat menyebabkan kerugian yang besar. Bahkan, dampaknya bisa dirasakan pada kesehatan mental serta kerugian finansial. Tindak pidana yang terjadi di dunia maya atau cybercrime memiliki hubungan yang kuat dengan penggunaan internet. Internet, yang berfungsi sebagai ruang baru dalam kehidupan masyarakat, dikenal sebagai cyberspace. Keberadaan internet membuat kehidupan yang sebelumnya dibatasi oleh waktu dan jarak menjadi tidak terbatas. Pelanggaran yang dilakukan dengan memanfaatkan cyberspace ini disebut sebagai kejahatan siber atau cybercrime (Ketaren, E. 2016).

Perkembangan teknologi digital telah membawa dampak signifikan terhadap berbagai aspek kehidupan, termasuk dalam hal kejahatan. Di kawasan Asia Tenggara, fenomena cybercrime khususnya perjudian online ilegal, telah menjadi perhatian serius bagi banyak negara, termasuk Indonesia. Menurut laporan dari United Nations Office on Drugs and Crime (UNODC) tahun 2023, kawasan ini telah menjadi pusat pertumbuhan industri perjudian online ilegal dengan nilai transaksi yang diperkirakan mencapai lebih dari USD 7 miliar per tahun. Aktivitas ini tidak hanya merugikan ekonomi, tetapi juga mengancam stabilitas keamanan nasional dan regional (UNODC, 2023).

Indonesia sebagai negara dengan populasi digital terbesar di Asia Tenggara, menghadapi tantangan yang kompleks dalam menangani perjudian online. Data dari Kementerian Komunikasi dan Informatika Republik Indonesia menunjukkan bahwa selama periode 2022-2023, lebih dari 45.000 situs judi online ilegal telah diblokir. Namun, mayoritas situs tersebut beroperasi dari luar negeri, dengan Kamboja dan Filipina sebagai sumber utama (Kominfo, 2023). Hal ini menunjukkan adanya celah hukum yang dimanfaatkan oleh pelaku kejahatan, serta tantangan dalam penegakan hukum yang efektif. Lebih lanjut, laporan dari Interpol (2022) mengungkapkan bahwa perjudian online ilegal sering kali terkait dengan berbagai bentuk kejahatan transnasional lainnya, seperti pencucian uang dan perdagangan manusia. Keterkaitan ini menciptakan jaringan kriminal yang semakin sulit untuk diberantas, terutama ketika melibatkan berbagai negara dengan

regulasi yang berbeda-beda. Dalam konteks ini, kerjasama antar negara menjadi sangat penting untuk mengatasi masalah yang bersifat lintas batas ini (ASEAN Secretariat, 2021).

Tantangan yang dihadapi Indonesia dalam penegakan hukum terhadap perjudian online ilegal juga dipengaruhi oleh faktor internal, seperti rendahnya literasi digital di kalangan masyarakat dan keterbatasan sumber daya di tubuh penegak hukum. Menurut Badan Siber dan Sandi Negara (BSSN) tahun 2023, banyak masyarakat yang masih kurang memahami risiko dan dampak dari perjudian online, sehingga mereka menjadi lebih rentan terhadap penipuan dan eksploitasi. Selain itu, keterbatasan sumber daya manusia yang terlatih dalam bidang keamanan siber juga menjadi kendala dalam upaya penegakan hukum yang efektif. Korupsi di kalangan aparat penegak hukum juga menjadi masalah serius yang menghambat upaya pemberantasan perjudian online. Dalam banyak kasus, pelaku kejahatan dapat dengan mudah menyuap petugas untuk menghindari penegakan hukum. Hal ini menciptakan lingkungan yang kondusif bagi berkembangnya perjudian online ilegal dan kejahatan siber lainnya (BSSN, 2023). Oleh karena itu, penting untuk memahami dinamika perjudian online ilegal dan dampaknya terhadap keamanan nasional, serta mencari solusi yang efektif untuk mengatasi masalah ini. Dampak perjudian online ilegal tidak hanya terbatas pada aspek ekonomi, tetapi juga mencakup dampak sosial yang lebih luas. Penelitian menunjukkan bahwa perjudian online dapat menyebabkan masalah kecanduan yang serius, yang pada gilirannya dapat memicu masalah sosial seperti kekerasan dalam rumah tangga, pengabaian tanggung jawab, dan peningkatan angka kriminalitas (Holt & Bossler, 2016). Selain itu, perjudian online juga dapat mengakibatkan kerugian finansial yang signifikan bagi individu dan keluarga, yang dapat memperburuk kondisi sosial-ekonomi masyarakat.

Dalam konteks regional, kegagalan dalam mengatasi masalah perjudian online ilegal dapat membawa konsekuensi serius bagi stabilitas politik dan keamanan di Asia Tenggara. Integrasi ekonomi kawasan bisa terganggu, dan kepercayaan terhadap institusi regional akan menurun. Hal ini dapat menghambat upaya pembangunan sosial-ekonomi di kawasan yang sedang berkembang pesat (Leukfeldt & Yar, 2016). Oleh karena itu, diperlukan pendekatan komprehensif dan terintegrasi yang melibatkan berbagai pemangku kepentingan di tingkat nasional maupun regional. Kerjasama antar negara di kawasan Asia Tenggara menjadi sangat penting dalam menghadapi tantangan perjudian online ilegal. Melalui kerjasama ini, negara-negara dapat berbagi informasi, sumber daya, dan teknologi untuk memperkuat kapasitas penegakan hukum. Selain itu, kerjasama ini juga dapat menciptakan standar regulasi yang lebih baik untuk mengatasi perjudian online lintas batas (ASEAN Secretariat, 2021). Dengan demikian, upaya pemberantasan perjudian online ilegal dapat dilakukan secara lebih efektif dan berkelanjutan.

Berdasarkan penelitian yang dilakukan oleh Sari (2024), penelitian tersebut secara komprehensif mengkaji perjudian online sebagai ancaman keamanan nasional di Indonesia, menyoroti karakteristiknya yang lintas batas, modus operandi yang canggih, serta dampak ekonomi dan sosial yang ditimbulkannya. Sari (2024) juga menganalisis tantangan dalam penanganan perjudian online di Indonesia, termasuk keragaman regulasi di antara negara-negara ASEAN, keterbatasan perjanjian ekstradisi, dan perbedaan kapasitas teknis antarnegara anggota. Meskipun demikian, penelitian tersebut belum secara spesifik mengelaborasi lebih dalam mengenai keterkaitan antara jaringan perjudian online dengan potensi pendanaan terorisme atau kejahatan siber yang lebih kompleks, serta belum mengusulkan model kerja sama regional yang terintegrasi untuk mengatasi celah hukum dan teknis yang ada.

Penelitian lain yang dilakukan oleh Ramadhan (2022), menganalisis perjudian online sebagai ancaman serius terhadap keamanan nasional Indonesia, khususnya dari perspektif ekonomi dan sosial. Ramadhan (2022) menguraikan bagaimana aktivitas ilegal ini menyebabkan kerugian finansial negara, memicu praktik pencucian uang, serta menimbulkan dampak negatif pada stabilitas sosial melalui peningkatan kriminalitas dan masalah keluarga. Meskipun demikian, penelitian ini cenderung berfokus pada dampak internal di Indonesia dan belum secara mendalam membahas dinamika kerja sama regional ASEAN dalam menghadapi tantangan lintas batas perjudian online, termasuk hambatan harmonisasi hukum dan efektivitas mekanisme ekstradisi antarnegara anggota.

Meskipun penelitian-penelitian sebelumnya telah memberikan pemahaman yang kuat mengenai ancaman perjudian online terhadap keamanan nasional Indonesia, serta mengidentifikasi beberapa tantangan dalam penanganannya, masih terdapat celah yang perlu dieksplorasi lebih dalam. Studi-studi yang ada cenderung berfokus pada dampak internal atau belum secara komprehensif mengurai kompleksitas modus operandi lintas batas yang terus berevolusi, termasuk keterkaitannya dengan kejahatan siber yang lebih canggih dan potensi pendanaan aktivitas terlarang lainnya. Selain itu, dinamika kerja sama regional ASEAN dalam menghadapi kejahatan siber lintas negara, khususnya perjudian online, masih memerlukan analisis yang lebih mendalam terkait hambatan harmonisasi hukum dan efektivitas mekanisme penegakan hukum. Oleh karena itu, penelitian ini hadir untuk mengisi kekosongan tersebut, dengan menawarkan analisis yang lebih terperinci mengenai bagaimana jaringan perjudian online lintas batas beroperasi, dampak multidimensionalnya terhadap keamanan nasional Indonesia, serta merumuskan rekomendasi strategis untuk memperkuat kerangka kerja sama regional ASEAN dalam memberantas ancaman cybercrime ini secara lebih efektif dan berkelanjutan.

Sejalan dengan identifikasi celah tersebut, penelitian ini secara spesifik bertujuan untuk menganalisis secara mendalam modus operandi perjudian online lintas batas yang terus berevolusi, termasuk keterkaitannya dengan kejahatan siber yang lebih kompleks dan potensi pendanaan aktivitas terlarang lainnya. Selain itu, penelitian ini juga berupaya mengidentifikasi dan mengevaluasi dampak multidimensional perjudian online terhadap keamanan nasional Indonesia, mencakup aspek ekonomi, sosial, dan kedaulatan digital. Terakhir, penelitian ini akan menganalisis tantangan yang dihadapi oleh pemerintah Indonesia dalam penegakan hukum terhadap perjudian online lintas batas, khususnya dalam konteks kerja sama regional ASEAN. Diharapkan hasil penelitian ini tidak hanya memberikan pemahaman yang lebih komprehensif mengenai dinamika dan tantangan perjudian online ilegal, tetapi juga dapat memberikan kontribusi nyata dalam merumuskan rekomendasi kebijakan yang tepat sasaran dan efektif. Lebih jauh, penelitian ini diharapkan dapat memperkuat kerangka kerja sama regional ASEAN dalam menghadapi ancaman cybercrime yang bersifat lintas batas secara lebih terintegrasi dan berkelanjutan.

METODOLOGI

Penelitian ini dilakukan dengan menggunakan metode studi pustaka (library research). Pendekatan ini dipilih karena peneliti ingin mendalami isu cybercrime lintas negara ASEAN, khususnya dalam bentuk perjudian online ilegal, melalui analisis teoretis dan normatif terhadap literatur, dokumen, serta regulasi yang tersedia. Metode ini sangat relevan digunakan dalam penelitian yang menitikberatkan pada eksplorasi konsep, teori, kebijakan, dan isu-isu hukum atau keamanan nasional seperti yang dibahas dalam topik ini.

Data yang digunakan dalam penelitian ini sepenuhnya bersifat sekunder. Sumber data meliputi dokumen-dokumen resmi dari organisasi regional seperti ASEAN, khususnya terkait kerja sama dalam penanganan cybercrime. Selain itu, peneliti juga mengacu pada peraturan perundang-undangan di Indonesia, seperti UU Informasi dan Transaksi Elektronik (UU ITE) dan Kitab Undang-Undang Hukum Pidana (KUHP), yang menjadi dasar larangan aktivitas perjudian online ilegal. Sumber lain yang digunakan termasuk jurnal ilmiah, artikel media, laporan penelitian, buku teks, serta hasil studi terdahulu yang relevan dengan tema cybercrime lintas batas dan ancaman keamanan non-tradisional.

HASIL DAN PEMBAHASAN

1. Cybercrime Lintas Batas dalam Konteks Perjudian Online Ilegal

Perkembangan teknologi digital telah membawa berbagai perubahan dalam kehidupan masyarakat modern, termasuk dalam bidang ekonomi dan hiburan. Salah satu bentuk aktivitas ilegal yang semakin marak di tengah keterbukaan akses internet adalah perjudian online. Fenomena ini tidak hanya menjadi masalah nasional bagi banyak negara, tetapi juga sebuah tantangan regional, terutama di kawasan ASEAN, karena sifatnya yang lintas batas dan sulit dilacak (Sari, 2024). Kondisi geografis dan konektivitas antarnegara ASEAN membuat wilayah ini menjadi medan subur bagi berkembangnya cybercrime, termasuk perjudian daring ilegal. Banyak platform perjudian online memilih untuk beroperasi dari negara-negara dengan regulasi yang longgar atau minim pengawasan, seperti Filipina, Kamboja, dan Myanmar, namun menargetkan pengguna dari negara-negara yang melarang keras praktik perjudian, salah satunya Indonesia (Ramadhan, 2022). Hal ini tentu saja menciptakan kompleksitas tersendiri dalam upaya pemberantasan kejahatan tersebut.

Modus operandi pelaku perjudian online ilegal pun semakin canggih. Mereka kerap menggunakan server luar negeri sebagai tempat penyimpanan data dan operasional situs mereka, sehingga sulit dilacak oleh otoritas setempat. Selain itu, penggunaan Virtual Private Network (VPN) menjadi strategi umum untuk menyamarkan lokasi asli server maupun para pelaku. Transaksi keuangan yang dilakukan juga sering kali memanfaatkan mata uang kripto, seperti Bitcoin atau Ethereum, agar lebih sulit dilacak oleh lembaga keuangan dan sistem perbankan konvensional (Abdurrohm, 2022). Pendekatan ini sangat efektif untuk menghindari deteksi serta pemblokiran dana dari pihak otoritas. Selain itu, jaringan afiliasi pemasaran (*affiliate marketing*) turut memperluas jangkauan operasi perjudian online ilegal ini. Para pelaku merekrut agen lokal melalui media sosial dan aplikasi pesan instan seperti WhatsApp, Telegram, atau LINE untuk mempromosikan situs-situs judi kepada calon pemain. Strategi pemasaran ini sangat efektif karena memanfaatkan kepercayaan masyarakat terhadap individu-individu di sekitar mereka, serta memanfaatkan kecenderungan orang untuk mengakses informasi melalui saluran digital (Smith, 2020).

Dampak dari fenomena ini cukup signifikan, baik secara ekonomi maupun sosial. Dari sisi ekonomi, aliran dana besar-besaran keluar negeri akibat aktivitas perjudian online ilegal tidak tercatat dalam sistem keuangan nasional, sehingga mengurangi potensi pendapatan pajak negara. Selain itu, praktik pencucian uang (*money laundering*) juga sering kali terjadi dalam skema ini, karena transaksi yang menggunakan cryptocurrency sulit dilacak dan dapat dimanfaatkan untuk tujuan

kriminal lainnya (Pushpanathan, 2022). Dari sisi sosial, maraknya perjudian online ilegal juga berdampak pada meningkatnya kerawanan sosial, seperti utang piutang, kekerasan rumah tangga, hingga gangguan mental akibat ketergantungan judi.

Penanganan terhadap cybercrime lintas batas seperti perjudian online ilegal ini menjadi sangat kompleks karena adanya perbedaan regulasi antarnegara anggota ASEAN. Sementara beberapa negara seperti Singapura memiliki kerangka hukum yang mengatur perjudian secara terbatas dan ketat, negara lain seperti Indonesia memberlakukan larangan total terhadap segala bentuk perjudian (De Leon, 2024). Ketidaksamaan ini menciptakan celah hukum yang dimanfaatkan oleh sindikat kejahatan untuk beroperasi di negara dengan regulasi yang lebih longgar, sementara menargetkan pengguna dari negara yang melarang aktivitas tersebut. Upaya kolaborasi regional melalui mekanisme seperti ASEAN Cybercrime Operations Desk (ACOD) telah diinisiasi sebagai langkah awal dalam mengatasi isu ini. Namun, implementasinya masih menghadapi banyak kendala, terutama terkait kurangnya harmonisasi hukum antarnegara serta belum optimalnya mekanisme ekstradisi dan pertukaran informasi intelijen (Sari, 2024). Tanpa koordinasi yang kuat dan kesepakatan bersama tentang definisi serta penanganan cybercrime, maka upaya pemberantasan terhadap sindikat perjudian online ilegal akan terus menemui jalan buntu (Ramadhan, 2022).

Untuk mengatasi tantangan ini, dibutuhkan pendekatan multilateral yang lebih intensif. Negara-negara ASEAN perlu melakukan harmonisasi regulasi, minimal dalam hal definisi cybercrime dan standar minimum penindakan. Selain itu, perlunya sistem intelijen bersama dan kapasitas teknis yang merata di seluruh negara anggota menjadi kunci penting dalam membangun daya tangkal terhadap ancaman cybercrime lintas batas. Pelatihan bersama, pertukaran informasi real-time, serta penguatan kerja sama penegakan hukum harus terus ditingkatkan agar tidak ada ruang bagi pelaku kejahatan untuk bersembunyi di balik perbedaan yurisdiksi. Dengan semakin cepatnya perkembangan teknologi dan meningkatnya ketergantungan masyarakat pada dunia digital, ancaman cybercrime seperti perjudian online ilegal akan terus berkembang. Oleh karena itu, negara-negara ASEAN harus menunjukkan komitmen politik yang kuat untuk bekerja sama dalam menangani isu ini, bukan hanya sebagai bagian dari keamanan nasional, tetapi juga demi menjaga stabilitas ekonomi dan sosial di kawasan.

1.1 Karakteristik Perjudian Online di Kawasan Asia Tenggara

Perjudian online di kawasan ASEAN telah berkembang menjadi salah satu bentuk cybercrime paling kompleks di era digital saat ini. Keberadaannya tidak hanya menimbulkan dampak ekonomi, tetapi juga tantangan serius bagi sistem hukum dan keamanan nasional di negara-negara anggota ASEAN, terutama Indonesia. Fenomena ini memiliki karakteristik unik yang memanfaatkan keragaman regulasi antarnegara serta kemajuan teknologi digital (Sari, 2024). Salah satu tren utama yang mencirikan perjudian online ilegal di kawasan ini adalah penggunaan platform berbasis server luar negeri. Banyak situs judi daring beroperasi dari negara seperti Filipina, Kamboja, dan Myanmar, wilayah yang memiliki regulasi yang jauh lebih longgar atau bahkan melegalkan operasional perjudian online. Negara-negara tersebut secara aktif memberikan lisensi kepada operator perjudian internasional, sehingga menjadikannya sebagai pusat bisnis judi

digital global. Di sisi lain, Indonesia secara tegas melarang segala bentuk perjudian sesuai dengan Kitab Undang-Undang Hukum Pidana (KUHP) Pasal 303, membuat praktik ini menjadi ilegal dan dikenai sanksi hukum (Ramadhan, 2022). Namun, pelaku bisnis ilegal ini memanfaatkan celah yurisdiksi dengan mendirikan server dan basis operasional mereka di luar wilayah Indonesia, namun tetap menyasar masyarakat Indonesia sebagai target pasar utama. Strategi pemasaran agresif dilakukan melalui media sosial, iklan digital, hingga promosi langsung melalui aplikasi pesan instan seperti WhatsApp dan Telegram. Hal ini membuktikan bahwa pelaku sangat memahami perilaku digital masyarakat modern dan memanfaatkannya untuk memperluas jaringan mereka.

Modus operandi yang digunakan oleh sindikat perjudian online semakin canggih dan dirancang untuk menghindari deteksi otoritas keamanan dan keuangan. Salah satunya adalah penggunaan proxy dan Virtual Private Network (VPN) untuk menyamarkan lokasi geografis pemilik situs maupun pengguna layanan. Dengan demikian, pelacakan IP address dan server menjadi sangat sulit dilakukan oleh aparat penegak hukum lokal. Selain itu, transaksi finansial dalam skema perjudian online ini sering kali dilakukan melalui mata uang kripto seperti Bitcoin, Ethereum, dan Tether (USDT), yang memberikan lapisan anonimitas tinggi dan menyulitkan lembaga keuangan dalam melacak aliran dana (De Leon, 2024). Jaringan afiliasi pemasaran (affiliate marketing) juga menjadi tulang punggung dalam ekspansi bisnis ilegal ini. Operator besar merekrut agen-agen lokal yang bertugas mempromosikan situs judi melalui jejaring pertemanan, grup komunitas, atau media sosial. Para agen ini biasanya dibayar dengan komisi berdasarkan jumlah pemain baru yang bergabung atau volume taruhan yang terjadi. Ini menjadikan model bisnis ini sangat efektif karena memanfaatkan kepercayaan sosial dan kedekatan relasi personal untuk menarik korban (Novitasari, 2018).

Dampak ekonomi dari praktik perjudian online ilegal ini sangat signifikan. Pertama, terjadi aliran dana besar-besaran keluar negeri. Menurut data Bank Indonesia (2023), meskipun belum ada angka pasti, banyak analisis menunjukkan bahwa puluhan triliun rupiah setiap tahun dialirkan ke platform judi online asing melalui transaksi cryptocurrency dan rekening bank offshore. Dana ini tidak masuk ke dalam sistem keuangan domestik, sehingga tidak memberikan kontribusi apa pun bagi perekonomian nasional. Kedua, aktivitas perjudian online sering kali dikaitkan dengan praktik pencucian uang (*money laundering*). Cara ini sulit dideteksi karena sistem perjudian online tidak selalu menyimpan riwayat transaksi yang transparan. Ketiga, negara mengalami kerugian pajak yang signifikan. Karena semua transaksi dilakukan secara ilegal dan tidak tercatat dalam sistem keuangan resmi, maka tidak ada pajak yang dipungut atas pendapatan yang dihasilkan dari aktivitas perjudian ini. Padahal, jika legal dan diatur dengan baik, sektor ini bisa menjadi sumber pendapatan negara melalui pajak dan retribusi (Pushpanathan, 2022). Tanpa upaya sistematis dan koordinasi lintas batas yang kuat, perjudian online ilegal akan terus menjadi ancaman serius bagi stabilitas ekonomi, keamanan nasional, dan ketertiban sosial. Diperlukan langkah-langkah konkret seperti harmonisasi regulasi antarnegara ASEAN, peningkatan kapasitas intelijen digital, serta edukasi publik untuk mencegah masyarakat menjadi korban perjudian daring ilegal.

1.2 Kerjasama ASEAN dan Tantangan Penanganannya

Upaya penanganan cybercrime lintas batas seperti perjudian online ilegal di kawasan Asia Tenggara membutuhkan pendekatan yang bersifat regional. Keberadaan internet sebagai media bebas tanpa batas negara membuat pelaku kejahatan digital bisa beroperasi dari satu wilayah sementara menargetkan korban di wilayah lain. Oleh karena itu, kerja sama antarnegara anggota ASEAN menjadi sangat penting. ASEAN Cybercrime Operations Desk (ACOD) merupakan salah satu inisiatif yang dirancang untuk menjembatani kesenjangan ini. Lembaga ini berfungsi sebagai pusat koordinasi untuk memfasilitasi pertukaran informasi, kapasitas teknis, serta sinergi dalam penegakan hukum cybercrime di kawasan (Ramadhan, 2022). Namun, meskipun sudah ada upaya kolaboratif, efektivitasnya masih terbatas oleh beberapa faktor struktural dan regulatif.

Salah satu tantangan utama dalam penanganan perjudian online di tingkat regional adalah kurangnya harmonisasi kerangka hukum antarnegara ASEAN (Abdurrohm, 2022). Setiap negara memiliki pandangan, definisi, dan prioritas yang berbeda terhadap kejahatan siber secara umum, termasuk perjudian daring. Di satu sisi, Indonesia menerapkan larangan total terhadap segala bentuk perjudian sesuai Kitab Undang-Undang Hukum Pidana (KUHP), sedangkan di sisi lain, Singapura tidak hanya melegalkan tetapi juga mengatur industri kasino dan perjudian daring dengan sistem lisensi ketat dan pengawasan pemerintah (Pushpanathan, 2022). Perbedaan ini menciptakan ruang bagi para pelaku kejahatan untuk memanfaatkan yurisdiksi yang lebih longgar guna melindungi operasi mereka. Selain perbedaan normatif, masalah ekstradisi menjadi kendala serius dalam proses penuntasan kasus perjudian online lintas negara. Meskipun beberapa negara ASEAN telah memiliki perjanjian bilateral terkait ekstradisi, banyak dari perjanjian tersebut belum mencakup ranah cybercrime secara spesifik (De Leon, 2024). Hal ini menyebabkan banyak kasus tidak dapat dilanjutkan hanya karena tersangka berada di negara yang tidak memiliki kerja sama hukum yang memadai dengan Indonesia. Bahkan jika tersangka berhasil diidentifikasi, proses hukum bisa terhambat oleh ketidakjelasan aturan antarnegara (Novitasari, 2018). Selain itu, adanya disparitas kapasitas teknis antarnegara anggota ASEAN semakin memperlebar kesenjangan dalam penanganan cybercrime. Negara seperti Singapura dan Malaysia memiliki infrastruktur keamanan siber yang relatif maju, lengkap dengan unit investigasi digital, laboratorium forensik, dan tim ahli yang mumpuni (Ramadhan, 2022). Sebaliknya, beberapa negara ASEAN lainnya masih menghadapi keterbatasan sumber daya manusia dan teknologi dalam menghadapi ancaman digital yang semakin canggih. Ketimpangan ini menyebabkan koordinasi penindakan menjadi tidak proporsional dan sering kali gagal dalam tataran implementasi.

Minimnya mekanisme pembagian bukti digital secara real-time juga menjadi isu kritis. Dalam dunia cybercrime, waktu adalah elemen krusial. Bukti digital seperti log aktivitas server, riwayat transaksi, atau data pengguna bisa hilang atau dihapus dalam hitungan jam. Sayangnya, sistem pertukaran informasi antar lembaga penegak hukum di ASEAN belum cukup responsif untuk mendukung penyelidikan yang cepat dan efektif (Abdurrohm, 2022). Akibatnya, banyak kasus menjadi sulit dibuktikan saat sampai pada tahap penyelidikan formal. Untuk mengatasi berbagai tantangan ini, diperlukan langkah-langkah konkret yang bersifat jangka panjang. Salah satunya adalah penguatan kerangka hukum regional yang bisa menjadi acuan bersama bagi seluruh negara anggota ASEAN dalam

menangani cybercrime, termasuk perjudian online. Ini bisa dimulai dengan penyusunan protokol tambahan dalam kerja sama ASEAN yang secara khusus mengatur definisi, klasifikasi, dan mekanisme penanganan cybercrime lintas negara (Sari, 2024). Selain itu, peningkatan kapasitas institusi keamanan siber nasional harus didukung dengan program pelatihan bersama, pertukaran intelijen, dan investasi dalam infrastruktur digital yang aman dan andal. Program ASEAN Cybersecurity Capacity Building Programme (ASEAN CCBP) bisa menjadi model yang dikembangkan lebih lanjut untuk meningkatkan kesetaraan kemampuan di antara negara-negara anggota. Tanpa solusi kolektif yang komprehensif, upaya penindakan terhadap sindikat perjudian online akan terus menghadapi jalan buntu (Pushpanathan, 2022). Keterbatasan koordinasi, perbedaan regulasi, serta ketidakseimbangan kapasitas teknis akan terus menjadi celah yang dimanfaatkan oleh pelaku kejahatan digital.

2. Ancaman Terhadap Keamanan Nasional Indonesia

Perjudian online lintas negara telah berkembang menjadi ancaman serius bagi keamanan nasional Indonesia dari berbagai dimensi, baik itu ekonomi, siber, hingga sosial (Sari, 2024). Dalam era digital saat ini, kejahatan tidak lagi dibatasi oleh garis geografis, dan perjudian daring ilegal menjadi salah satu contoh nyata betapa rentannya suatu negara terhadap fenomena cybercrime transnasional. Di Indonesia, di mana praktik perjudian dilarang keras baik secara hukum maupun normatif, maraknya platform judi online yang beroperasi dari luar negeri justru semakin mengkhawatirkan karena dampaknya yang luas dan kompleks.

Pada tingkat makro, aktivitas ilegal ini berpotensi melemahkan kedaulatan ekonomi negara melalui aliran dana besar-besaran ke luar negeri yang tidak terkontrol. Menurut data Bank Indonesia (2023), meskipun belum ada angka pasti, analisis intelijen keuangan menyebut bahwa puluhan triliun rupiah setiap tahun dialirkan ke platform perjudian online asing melalui transaksi cryptocurrency dan rekening bank offshore. Dana-dana ini keluar dari sistem keuangan domestik tanpa tercatat dalam neraca pembayaran, sehingga mengurangi potensi pendapatan negara baik dari pajak maupun devisa. Selain itu, praktik pencucian uang (*money laundering*) yang kerap menyertai operasi perjudian online dapat mengganggu stabilitas sistem keuangan nasional. Pelaku kejahatan dapat memanfaatkan transaksi judi sebagai cara untuk menyamarkan asal-usul dana ilegal. Misalnya, uang hasil korupsi, narkoba, atau kejahatan lainnya dicuci dengan cara “bertaruh” dan kemudian menarik kemenangan sebagai dana bersih. Proses ini sulit dideteksi karena sistem perjudian online tidak selalu menyimpan riwayat transaksi yang transparan dan mudah diakses oleh otoritas keuangan seperti PPATK (Pusat Pelaporan dan Analisis Transaksi Keuangan) (Pushpanathan, 2022).

Dari aspek keamanan siber, jaringan perjudian online juga menjadi pintu masuk bagi ancaman digital lebih lanjut. Banyak situs judi ilegal tidak memiliki standar keamanan yang memadai, sehingga rentan diretas. Akibatnya, data pribadi pengguna, seperti nama lengkap, nomor KTP, nomor telepon, hingga rekening bank bisa bocor dan digunakan untuk kejahatan identitas, pemerasan, atau bahkan penipuan berbasis data pribadi (Abdurrohim, 2022). Hal ini tentu saja membahayakan hak privasi warga negara dan meningkatkan risiko kejahatan digital yang lebih luas.

Pada tingkat sosial, dampak perjudian online menciptakan kerentanan baru dengan meningkatnya kasus utang piutang, kriminalitas terkait, hingga disintegrasi keluarga. Berdasarkan data Bareskrim Polri (2023), sebagian besar kasus bunuh diri dan percobaan bunuh diri yang terjadi di masyarakat awalnya dipicu oleh utang judi online. Selain itu, banyak kasus KDRT (kekerasan dalam rumah tangga) dan konflik sosial juga terkait erat dengan kecanduan judi daring. Fenomena ini pada akhirnya dapat menggerakkan ketidakstabilan sosial yang berpotensi memicu gesekan horizontal dalam masyarakat. Yang lebih mengkhawatirkan adalah potensi keterkaitan antara jaringan perjudian online dengan kelompok kriminal terorganisir lintas negara, termasuk kemungkinan pendanaan kegiatan teroris melalui mekanisme pencucian uang yang sulit dilacak (De Leon, 2024). Meski belum ada bukti konkret, beberapa investigasi intelijen menunjukkan adanya pola transaksi mencurigakan yang menghubungkan rekening agen judi online dengan entitas non-profit atau organisasi yang diduga terafiliasi dengan kelompok radikal.

Ancaman ini diperparah oleh sifat operasi digital yang tanpa batas, di mana pelaku dapat dengan mudah memindahkan basis operasi mereka ke yurisdiksi lain ketika ditekan (Novitasari, 2018). Misalnya, jika sebuah situs judi diblokir di Indonesia, operator cukup memindahkan server ke negara tetangga atau menggunakan domain baru untuk kembali beroperasi. Mereka juga memanfaatkan enkripsi dan teknologi blockchain untuk menghindari penyadapan dan mempercepat proses transaksi lintas negara. Kelemahan dalam sistem pengawasan transaksi digital dan keterbatasan kapasitas penegakan hukum siber membuat Indonesia khususnya rentan terhadap ancaman ini (Sari, 2024). Badan Siber dan Sandi Negara (BSSN) serta lembaga penegak hukum seperti POLRI dan KOMINFO terus berupaya meningkatkan kemampuan deteksi dan respons, namun tantangan koordinasi antarinstansi masih menjadi kendala besar.

Selain itu, rendahnya kesadaran masyarakat tentang risiko perjudian online turut memperburuk situasi. Banyak masyarakat, terutama generasi muda, tertarik bergabung dengan platform tersebut karena promosi yang menarik, iming-iming hadiah besar, serta minimnya edukasi tentang efek buruk jangka panjang. Survei Lembaga Perlindungan Konsumen Digital (LPKD) pada tahun 2023 menemukan bahwa lebih dari 60% remaja di Jabodetabek pernah mencoba bermain judi online, meskipun sebagian besar tidak menyadari risiko hukum dan finansial yang menyertainya. Untuk itu, diperlukan pendekatan komprehensif yang menggabungkan aspek hukum, teknologi, dan kerja sama internasional agar upaya penindakan efektif (Ramadhan, 2022). Strategi terpadu harus tidak hanya menindak pelaku, tetapi juga memperkuat ketahanan digital nasional, meningkatkan kesadaran masyarakat terhadap risiko, serta melakukan edukasi preventif kepada generasi muda tentang bahaya perjudian online (Abdurrohm, 2022). Penguatan regulasi pun sangat penting. Saat ini, RUU Anti Pornografi dan Pornoaksi (RUU PPE) sedang dalam pembahasan di DPR, yang salah satunya akan mengatur lebih ketat soal konten perjudian online. Selain itu, kolaborasi regional seperti ASEAN Cybercrime Operations Desk (ACOD) perlu diperkuat untuk menutup celah hukum dan meningkatkan koordinasi penegakan hukum lintas negara. Tanpa langkah-langkah strategis dan kolaboratif tersebut, perjudian online akan terus berkembang sebagai tantangan multidimensi bagi keamanan nasional Indonesia.

2.1 Aspek Keamanan Siber dan Kedaulatan Digital

Perjudian online ilegal bukan hanya sekadar masalah hukum pidana biasa, tetapi juga ancaman serius terhadap keamanan siber dan kedaulatan digital Indonesia. Platform perjudian ilegal kerap mengumpulkan data pribadi pengguna secara massal, termasuk nama lengkap, nomor identitas, alamat email, riwayat transaksi, hingga informasi rekening bank (Sari, 2024). Data-data ini tidak hanya berisiko disalahgunakan oleh pelaku kejahatan, tetapi juga rentan bocor karena minimnya standar proteksi di server-server ilegal tersebut. Banyak platform judi daring tidak memiliki sistem enkripsi yang memadai, sehingga ketika diretas, seluruh basis data bisa dengan mudah diakses oleh aktor jahat (Ramadhan, 2022).

Fakta mengejutkan muncul pada tahun 2023 ketika sebuah forum gelap (*dark web*) menjual basis data lebih dari 8 juta warga Indonesia yang diduga terlibat dalam aktivitas perjudian online (Abdurrohim, 2022). Informasi yang diperjualbelikan mencakup data sensitif seperti foto e-KTP, nomor HP, hingga riwayat taruhan. Dengan data ini, pelaku kejahatan dapat melakukan berbagai bentuk penipuan, pemerasan, hingga pencucian uang digital. Kasus ini membuktikan bahwa risiko perjudian online tidak berhenti pada ranah ekonomi atau moral, tetapi telah merambah ke ranah keamanan nasional melalui potensi pelanggaran privasi skala besar. Selain itu, banyak platform ilegal ini tidak tunduk pada regulasi perlindungan data yang berlaku di Indonesia, seperti UU No. 27 Tahun 2022 tentang Pengelolaan Data Pribadi (UU PDP), karena beroperasi di luar yurisdiksi nasional (Pushpanathan, 2022). Hal ini membuat negara kesulitan untuk menuntut tanggung jawab operator situs terkait pelanggaran hak-hak digital warganya. Padahal, dalam konteks kedaulatan digital, negara harus memiliki kontrol atas data warganya, baik dalam hal penyimpanan, penggunaan, maupun perlindungan dari risiko eksternal.

Dari sisi infrastruktur digital, sindikat perjudian online ternyata tidak hanya fokus pada bisnis taruhan, tetapi juga memanfaatkan jaringan mereka untuk kegiatan ilegal lain yang lebih kompleks (De Leon, 2024). Laporan dari Badan Siber dan Sandi Negara (BSSN) menyebutkan bahwa beberapa server yang digunakan oleh platform perjudian daring ilegal juga diamati sebagai titik awal serangan siber terhadap institusi strategis di Indonesia. Salah satunya adalah kasus Distributed Denial of Service (DDoS) yang menargetkan lembaga keuangan swasta pada kuartal pertama 2023, di mana salah satu IP yang digunakan berasal dari domain judi online yang sudah diblokir (Novitasari, 2018). Yang lebih mengkhawatirkan, beberapa jaringan ini diduga bekerja sama dengan kelompok kejahatan siber internasional, mengubah platform judi mereka menjadi ujung tombak serangan yang lebih luas. Contohnya, ada indikasi kolaborasi antara sindikat judi online di Asia Tenggara dengan kelompok ransomware berbasis Rusia dan China, yang memanfaatkan infrastruktur TI perjudian sebagai sarana untuk menyembunyikan aktivitas cybercrime mereka (Sari, 2024). Ini membuktikan bahwa kejahatan perjudian online tidak lagi bersifat konvensional, tetapi telah berevolusi menjadi ancaman multidimensi yang menggerogoti kedaulatan digital Indonesia.

Ancaman ini semakin nyata ketika kita melihat bagaimana server ilegal ini sering kali tidak hanya digunakan untuk operasional judi, tetapi juga sebagai *command and control* (C2) server bagi malware yang menyebar di jaringan

domestik. Dalam beberapa investigasi, server yang awalnya digunakan untuk transaksi judi ternyata juga digunakan untuk mendistribusikan *malware banking*, spyware, dan *crypto-miner* yang secara diam-diam menguras sumber daya perangkat pengguna (Ramadhan, 2022). Serangan jenis ini sulit dilacak karena seringkali dilakukan secara bertahap dan tanpa sepengetahuan korban. Tanpa penguatan sistem deteksi dini dan peningkatan kapasitas respons insiden siber, kerentanan ini akan terus dimanfaatkan oleh jaringan kejahatan transnasional. Menurut laporan APJII (Asosiasi Penyelenggara Jasa Internet Indonesia) tahun 2023, jumlah serangan siber yang berasal dari domain judi online meningkat 40% dibandingkan tahun sebelumnya, menunjukkan tren yang terus berkembang dan semakin mengkhawatirkan (Abdurrohm, 2022).

Untuk itu, diperlukan langkah-langkah proaktif dari pemerintah, baik dalam hal regulasi, penegakan hukum, maupun peningkatan kesadaran masyarakat. Regulasi harus diperketat agar semua platform digital, termasuk yang beroperasi dari luar negeri, wajib mematuhi aturan perlindungan data Indonesia jika ingin menjangkau pengguna dalam negeri. Selain itu, koordinasi antara KOMINFO, POLRI, BSSN, dan lembaga intelijen harus ditingkatkan untuk membangun sistem early warning yang efektif dan respon cepat terhadap serangan siber yang berasal dari ekosistem perjudian online. Kedaulatan digital Indonesia tidak boleh dikompromikan hanya karena kelemahan dalam menghadapi fenomena cybercrime lintas batas. Dengan pendekatan holistik yang melibatkan regulasi kuat, teknologi canggih, dan edukasi publik, ancaman perjudian online dapat diminimalkan, sehingga keamanan siber dan kedaulatan digital bangsa tetap terjaga.

2.2 Dampak Sosial dan Stabilitas Nasional

Perjudian online telah menimbulkan dampak sosial yang mengkhawatirkan sekaligus mengancam stabilitas nasional Indonesia melalui berbagai mekanisme yang saling berkaitan (Sari, 2024). Di tengah tingginya penetrasi internet dan penggunaan perangkat digital di masyarakat, maraknya platform judi daring ilegal membawa konsekuensi serius pada struktur sosial dan ketertiban umum. Salah satu dampak paling nyata adalah meningkatnya angka kriminalitas terkait aktivitas perjudian, mulai dari kasus penagihan utang dengan cara intimidasi, pemerasan terhadap pemain yang kalah besar, hingga praktik *cyberbullying* terhadap korban yang tidak mampu melunasi hutang (Ramadhan, 2022).

Banyak pelaku judi online yang terjatuh utang besar kemudian beralih ke tindakan kriminal seperti pencurian, penipuan, atau bahkan pemerkosaan demi menutupi kerugian finansial mereka (Abdurrohm, 2022). Data Bareskrim Polri (2023) mencatat bahwa lebih dari 60% kasus kriminalitas ekonomi di wilayah Jabodetabek selama tahun tersebut memiliki keterkaitan langsung dengan utang judi online. Fenomena ini tidak hanya merusak tatanan sosial, tetapi juga membebani aparat penegak hukum yang harus menangani efek domino dari maraknya perjudian online (Pushpanathan, 2022). Yang lebih mengkhawatirkan adalah potensi penyalahgunaan jaringan perjudian online untuk kegiatan yang lebih berbahaya, termasuk pendanaan aksi terorisme (De Leon, 2024). Modus operandi "*follow the money*" menunjukkan bagaimana aliran dana dari perjudian online dapat dialihkan untuk mendukung jaringan radikal melalui mekanisme

pencucian uang yang rumit (Novitasari, 2018). Transaksi menggunakan *cryptocurrency* dan sistem pembayaran digital yang tidak terpantau memudahkan pelaku untuk menyamarkan aliran dana ilegal ini (Sari, 2024).

Beberapa laporan intelijen dari BNPT (Badan Nasional Penanggulangan Terorisme) pada awal 2023 menyebut adanya pola transaksi mencurigakan yang menghubungkan rekening agen judi online dengan beberapa organisasi yang masuk dalam daftar terlarang oleh pemerintah (Ramadhan, 2022). Meskipun belum ada bukti kuat tentang hubungan langsung, temuan ini menunjukkan potensi ancaman laten yang perlu diwaspadai secara serius. Selain itu, dampak sosial lainnya yang sering diabaikan adalah gangguan terhadap keharmonisan keluarga dan meningkatnya masalah kesehatan mental (Abdurrohim, 2022). Banyak kasus menunjukkan bagaimana kecanduan judi online merusak hubungan keluarga, memicu perceraian, bahkan mendorong tindakan putus asa seperti bunuh diri (Pushpanathan, 2022). Berdasarkan survei Lembaga Perlindungan Konsumen Digital (LPKD) pada 2023, lebih dari 40% responden yang mengaku kecanduan judi online mengalami gejala depresi berat dan kecemasan tinggi akibat tekanan utang dan stigma sosial.

Secara kolektif, masalah-masalah ini jika tidak dikendalikan dapat menggerogoti ketahanan sosial bangsa dan menjadi pemicu ketidakstabilan yang lebih luas. Pemerintah menghadapi tantangan besar untuk menangani tidak hanya aspek hukumnya, tetapi juga dampak sosial yang sudah menyebar ke berbagai lapisan masyarakat (De Leon, 2024). Upaya pencegahan harus mencakup edukasi masyarakat tentang bahaya judi online, penguatan sistem pelaporan transaksi mencurigakan, serta rehabilitasi bagi korban kecanduan judi, sambil terus memperketat pengawasan terhadap potensi penyalahgunaan jaringan ini untuk kegiatan yang mengancam keamanan nasional (Novitasari, 2018). Salah satu langkah konkret yang telah diambil adalah penyuluhan digital yang dilakukan oleh Kementerian Komunikasi dan Informatika bekerja sama dengan lembaga swadaya masyarakat dan tokoh agama. Program ini bertujuan untuk memberikan edukasi kepada remaja dan orang tua tentang risiko *cybercrime*, termasuk perjudian online. Namun, skalabilitas program masih terbatas karena minimnya anggaran dan koordinasi lintas instansi.

Peningkatan kapasitas lembaga seperti PPATK (Pusat Pelaporan dan Analisis Transaksi Keuangan) juga diperlukan untuk memastikan setiap aliran dana mencurigakan dari transaksi digital bisa terdeteksi lebih cepat. Selain itu, kolaborasi dengan penyedia layanan pembayaran digital dan bank (Budianto & Azarkasyi, 2024) akan sangat penting untuk membangun sistem *early warning* terhadap transaksi ilegal. Masalah perjudian online tidak bisa lagi dipandang sebagai isu individu semata, tetapi harus dianggap sebagai ancaman multidimensi yang berpotensi mengganggu harmoni sosial dan stabilitas negara. Tanpa intervensi yang komprehensif dan berkelanjutan, dampak buruknya akan terus menjalar, merusak generasi muda, mengganggu ketertiban umum, dan membahayakan keamanan nasional.

KESIMPULAN

Penelitian ini menunjukkan bahwa perjudian online ilegal telah menjadi bentuk *cybercrime* lintas batas yang kompleks dan membawa dampak multidimensional terhadap

keamanan nasional Indonesia. Fenomena ini tidak hanya merugikan secara ekonomi melalui aliran dana besar keluar negeri setiap tahun, tetapi juga mengancam aspek keamanan siber, stabilitas sosial, serta kedaulatan digital Indonesia. Jaringan perjudian daring memanfaatkan server luar negeri, transaksi mata uang kripto, serta celah yurisdiksi antarnegara ASEAN untuk terus berkembang meskipun di bawah tekanan regulasi nasional. Selain itu, keterkaitannya dengan kejahatan transnasional lain seperti pencucian uang semakin memperparah tingkat ancamannya.

Hasil penelitian menunjukkan bahwa modus operandi pelaku semakin canggih dan sulit dilacak. Mereka memanfaatkan teknologi enkripsi, proxy, dan sistem pembayaran anonim untuk menghindari deteksi otoritas keamanan. Di tingkat regional, perbedaan kerangka hukum, keterbatasan mekanisme ekstradisi, serta disparitas kapasitas teknis antarnegara anggota ASEAN turut memperbesar tantangan dalam pemberantasan kejahatan ini. Pada tingkat domestik, rendahnya literasi digital masyarakat dan kurangnya sinergi antarlembaga penegak hukum membuat upaya penindakan menjadi kurang efektif.

Salah satu kelebihan penelitian ini adalah pendekatan multidimensi yang digunakan melalui kombinasi analisis hukum, studi kasus, dan evaluasi kebijakan. Pendekatan ini memberikan pemahaman yang lebih utuh tentang dinamika cybercrime lintas negara, terutama dalam konteks perjudian online. Namun, penelitian ini memiliki beberapa keterbatasan. Pertama, akses terhadap data primer yang bersifat sensitif sangat terbatas karena keterbukaan informasi publik yang belum memadai. Kedua, investigasi lapangan tidak dapat dilakukan secara mendalam akibat keterbatasan waktu, biaya, dan akses ke sumber terpercaya. Ketiga, hubungan antara jaringan perjudian online dan potensi pendanaan aktivitas radikal masih memerlukan bukti empiris yang lebih kuat dan analisis lebih lanjut.

Sebagai langkah pengembangan selanjutnya, dibutuhkan penelitian empiris yang lebih fokus pada pola transaksi keuangan ilegal, terutama yang melibatkan mata uang kripto. Studi yang lebih dalam mengenai kerja sama intelijen antarnegara ASEAN dalam konteks cybercrime akan sangat penting untuk mengevaluasi efektivitas mekanisme pertukaran informasi dan respons cepat terhadap ancaman digital. Selain itu, penelitian yang mengkaji aspek psikologis dan perilaku korban kecanduan judi online juga perlu dilakukan guna melengkapi pemahaman tentang dampak sosial dari fenomena ini.

Dengan adanya penelitian lanjutan yang lebih spesifik dan kolaboratif, diharapkan dapat dirancang strategi kebijakan yang lebih tepat sasaran dan efektif baik di tingkat nasional maupun regional. Upaya penguatan harmonisasi hukum cybercrime, pembangunan sistem early warning digital, serta peningkatan kapasitas teknis dan institusional di kawasan ASEAN menjadi prioritas utama dalam menghadapi ancaman cybercrime lintas batas yang terus berkembang. Tanpa koordinasi yang kuat dan komitmen politik bersama, ancaman perjudian online ilegal akan terus menjadi masalah serius bagi stabilitas keamanan, ekonomi, dan sosial di Indonesia dan kawasan Asia Tenggara.

DAFTAR PUSTAKA

Abdurrohim, M. "ASEAN Digital Masterplan: Responding Cyber Security Dilemma in the Post-Covid Era." *Global Focus* 2, no. 1 (2022): 17–26. <https://doi.org/https://doi.org/10.21776/ub.jgf.2022.002.01.2>

ASEAN Secretariat. *ASEAN Cybersecurity Cooperation Strategy*. 2021.

Badan Siber dan Sandi Negara (BSSN). *Laporan Ancaman Keamanan Siber Nasional 2022-2023*. 2023.

Budi Suhariyanto. *Tindak Pidana Teknologi Informasi (Cybercrime)*. Jakarta: Rajawali Pers, 2013.

De Leon, A. "Cutting Losses: Southeast Asia's Crackdown on Online Gambling." *New Perspectives on Asia | CSIS*, 2024. <https://www.csis.org/blogs/new-perspectives-asia/cutting-losses-southeast-asias-crackdown-online-gambling>

Holt, Thomas J., and Adam M. Bossler. *Cybercrime and Digital Forensics: An Introduction*. New York: Routledge, 2016.

Interpol. *Cybercrime in Southeast Asia: A Threat Assessment*. 2022.

Kementerian Komunikasi dan Informatika Republik Indonesia. *Laporan Tahunan Pemblokiran Konten Ilegal 2022-2023*. 2023.

Ketaren, E. "Cybercrime, Cyber Space, dan Cyber Law." *Jurnal Times* 5, no. 2 (2016): 37–39. <https://doi.org/10.51351/jtm.5.2.2016556>

Budianto, K., & Azarkasyi, B. (2024). Community Outreach Gaps in Drafting Regional Regulations: A Call for Enhanced Government Socialization. *Nurani: Jurnal Kajian Syari'ah Dan Masyarakat*, 24(1), 103–118.

Leukfeldt, Erwin R., and Majid Yar, eds. *The Routledge Handbook of Cybercrime*. New York: Routledge, 2016.

Novitasari, I. "Babak Baru Regim Keamanan Siber di Asia Tenggara Menyongsong ASEAN Connectivity 2025." *Jurnal Asia Pacific Studies* 1, no. 2 (2018): 220. <https://doi.org/10.33541/japs.v1i2.624>.

Pushpanathan, S. "ASEAN Cooperation to Combat Transnational Crime: Progress, Perils, and Prospects." *Journal of Southeast Asian Economies* 39, no. 1 (2022).
<https://doi.org/10.3389/fpos.2024.1304828>

Ramadhan, I. "ASEAN Consensus and Forming Cybersecurity Regulation in Southeast Asia." In *Proceedings of the 1st International Conference on Contemporary Risk Studies, ICONIC-RS* 2022. 2022.
<https://journal.unpar.ac.id/index.php/Sentris/article/download/9088/4666/31085>

Sari, M. N. "Cybercrime in Association of Southeast Asian Nations: Regional Effort and Its Effectiveness." *Journal of Information Policy* 14 (2024).
<https://doi.org/10.5325/jinfopoli.14.2024.0016>

Smith, R. B. "Cybercrime in ASEAN: Anti-Child Pornography Legislation." *Journal of Indonesian Legal Studies* 5, no. 2 (2020): 277–294.
<https://doi.org/10.15294/jils.v5i2.37931>

United Nations Office on Drugs and Crime (UNODC). *World Drug Report 2023: Transnational Organized Crime in Southeast Asia*. 2023.