Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.6. No.1 (2025)
Tema/Edisi : Hukum Internasional dan Perbandingan Hukum (Bulan Kesatu)
https://jhlg.rewangrencang.com/

KEBIJAKAN HUKUM PIDANA TERHADAP KEJAHATAN *CYBER* STUDI PERBANDINGAN ANTARA INDONESIA DAN THAILAND DALAM PERSPEKTIF HUKUM INTERNASIONAL

CRIMINAL LAW POLICY ON CYBERCRIME: A COMPARATIVE STUDY BETWEEN INDONESIA AND THAILAND IN THE PERSPECTIVE OF INTERNATIONAL LAW

Aulia Mawaddah Matondang dan Andryan

Universitas Muhammadiyah Sumatera Utara

Korespondensi Penulis: aulwaddah27@gmail.com

Citation Structure Recommendation :

Matondang, Aulia Mawaddah dan Andryan. *Kebijakan Hukum Pidana terhadap Kejahatan Cyber Studi Perbandingan Antara Indonesia dan Thailand dalam Perspektif Hukum Internasional*. Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.6. No.1 (2025).

ABSTRAK

Penelitian ini membahas perbandingan peraturan hukum pidana terhadap kejahatan siber di Thailand dan Indonesia, serta tantangan yang dihadapi dalam penegakannya. Penelitian normatif ini menggunakan pendekatan perundang-undangan untuk mengevaluasi efektivitas kerangka hukum kedua negara dalam mencegah dan menangani kejahatan siber. Thailand mengandalkan Computer Crime Act (CCA) yang berfokus pada berbagai jenis kejahatan siber, sementara Indonesia memiliki Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang mengatur lebih luas aspek transaksi digital dan penyebaran informasi. Penelitian ini menemukan bahwa meskipun kerangka hukum di kedua negara cukup komprehensif, keterbatasan sumber daya manusia dan keterampilan teknis adalah tantangan besar dalam penegakan hukum terhadap kejahatan siber. Penegakan hukum siber memerlukan keterampilan teknis yang sangat tinggi, dan banyak lembaga penegak hukum di kedua negara masih kekurangan personel yang memiliki kompetensi dalam teknologi informasi dan keamanan siber.Aspek lain yang penting dalam penelitian ini adalah kerjasama internasional yang menjadi kunci dalam penanggulangan kejahatan siber lintas batas. Thailand dan Indonesia, seperti negara-negara lainnya, berhadapan dengan kejahatan siber yang sering melibatkan pelaku dan korban di berbagai negara. Dalam hal ini, konvensi internasional seperti Budapest Convention on Cybercrime berperan penting. Konvensi ini menyediakan dasar hukum internasional untuk kerjasama dalam memerangi kejahatan siber, termasuk prosedur untuk meminta bantuan hukum dan ekstradisi. Selain itu, organisasi internasional seperti Interpol juga memainkan peran penting dalam koordinasi dan pertukaran informasi antara negara-negara untuk menangani kejahatan siber. Hasil penelitian ini menunjukkan bahwa upaya lebih lanjut diperlukan dalam hal koordinasi antar lembaga, pelatihan penegak hukum, dan edukasi publik untuk meningkatkan perlindungan terhadap kejahatan siber di Thailand dan Indonesia. Kolaborasi internasional yang lebih erat, baik melalui forum bilateral maupun multilateral, juga menjadi hal yang sangat penting untuk meningkatkan efektivitas penegakan hukum siber.

Kata Kunci: Kejahatan Siber, Perbandingan Hukum, Thailand dan Indonesia

ABSTRACT

This study discusses a comparison of criminal law regulations against cybercrime in Thailand and Indonesia, as well as the challenges faced in their enforcement. This normative research uses a legislative approach to evaluate the effectiveness of the legal frameworks of both countries in preventing and dealing with cybercrime. Thailand relies on the Computer Crime Act (CCA) which focuses on various types of cybercrime, while Indonesia has the Information and Electronic Transactions Law (ITE Law) which regulates more broadly aspects of digital transactions and information dissemination. The study found that although the legal framework in both countries is quite comprehensive, limited human resources and technical skills are major challenges in law enforcement against cybercrime. Cyber law enforcement requires very high technical skills, and many law enforcement agencies in both countries still lack personnel who have competence in information technology and cybersecurity. Another important aspect of this study is international cooperation which is key in tackling cross-border cybercrime. Thailand and Indonesia, like other countries, deal with cybercrime that often involves perpetrators and victims in various countries. In this regard, international conventions such as the Budapest Convention on Cybercrime play an important role. The Convention provides an international legal basis for cooperation in combating cybercrime, including procedures for requesting legal assistance and extradition. In addition, international organizations such as Interpol also play an important role in the coordination and exchange of information between countries to deal with cybercrime. The results of this study show that further efforts are needed in terms of inter-agency coordination, law enforcement training, and public education to improve protection against cybercrime in Thailand and Indonesia. Closer international collaboration, both through bilateral and multilateral forums, is also very important to increase the effectiveness of cyber law enforcement.

Keywords: Cybercrime, Legal Comparison, Thailand and Indonesia

A. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan signifikan dalam berbagai aspek kehidupan, termasuk dalam munculnya kejahatan siber (cybercrime). Kejahatan ini tidak hanya terjadi dalam lingkup domestik, tetapi juga bersifat transnasional, melibatkan pelaku dan korban dari berbagai negara. Fenomena ini menuntut adanya kebijakan hukum pidana yang efektif untuk menangani dan mencegah tindak kejahatan siber. Indonesia dan Thailand, sebagai negara di kawasan Asia Tenggara dengan perkembangan digital yang pesat, menghadapi tantangan serupa dalam menangani *cybercrime.* Akan tetapi, kebijakan hukum pidana yang diterapkan di kedua negara tersebut memiliki perbedaan dalam aspek regulasi, penerapan sanksi, serta mekanisme penegakan hukum.

Perkembangan teknologi juga membawa tantangan baru, terutama dalam hal keamanan digital. Kejahatan siber (*cybercrime*) telah muncul sebagai salah satu ancaman serius di era digital. Kejahatan ini mencakup berbagai aktivitas ilegal yang dilakukan melalui atau terhadap sistem komputer dan jaringan, seperti pencurian data, penipuan online, peretasan, dan penyebaran malware. Dampak dari kejahatan siber tidak hanya merugikan individu, tetapi juga dapat mengancam keamanan nasional dan ekonomi suatu negara.

Kejahatan siber mencakup berbagai bentuk, seperti pencurian identitas, peretasan, penipuan online, dan penyebaran malware, yang dapat merugikan individu, perusahaan, bahkan pemerintah. Dampak dari kejahatan siber dapat berupa kerugian finansial, kerusakan reputasi, serta ancaman terhadap keamanan nasional dan stabilitas ekonomi.

Beberapa jenis kejahatan siber yang umum terjadi adalah sebagai berikut:

1. *Phishing:* Kejahatan ini melibatkan penipuan yang dilakukan dengan cara mengelabui korban untuk memberikan informasi pribadi seperti kata sandi, nomor kartu kredit, atau data sensitif lainnya. Pelaku *phishing* biasanya menyamar sebagai entitas yang tepercaya, seperti bank atau lembaga pemerintah, dan menggunakan email atau situs web palsu untuk mengumpulkan informasi tersebut.
2. *Hacking: Hacking* adalah tindakan membobol atau meretas sistem komputer tanpa izin, dengan tujuan mencuri data, merusak sistem, atau mendapatkan akses yang tidak sah ke dalam jaringan komputer. Hacker dapat melakukan aksi ini untuk berbagai alasan, termasuk pencurian data pribadi, serangan terhadap infrastruktur penting, atau bahkan untuk tujuan politik.
3. *Cyberbullying:* Ini adalah bentuk intimidasi atau kekerasan yang terjadi di dunia maya, di mana pelaku menggunakan media sosial, pesan instan, atau platform online lainnya untuk menyebarkan kebencian, fitnah, atau ancaman terhadap korban. *Cyberbullying* sering kali menargetkan individu atau kelompok tertentu, terutama di kalangan remaja, dan dapat memiliki dampak psikologis yang serius bagi korban.

4. *Malware: Malware* adalah perangkat lunak berbahaya yang dirancang untuk merusak sistem komputer atau mencuri informasi. Jenis malware yang umum termasuk *virus, trojan*, dan *ransomware*. *Ransomware*, misalnya, mengenkripsi data korban dan meminta tebusan untuk membuka kunci data tersebut.
5. *Identity Theft*: Kejahatan ini melibatkan pencurian identitas seseorang dengan cara mendapatkan akses ilegal ke data pribadi dan menggunakannya untuk keuntungan pribadi, seperti pembukaan rekening bank atau pinjaman dengan nama korban.

Kejahatan siber telah menjadi masalah global yang memengaruhi banyak negara, termasuk Thailand dan Indonesia. Di Thailand, *Computer Crime Act 2007* menjadi dasar hukum utama dalam mengatur kejahatan siber. Sementara itu, di Indonesia, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) menjadi landasan hukum dalam menangani kasus-kasus terkait siber. (Handoyo, B., Husamuddin, M. Z., & Rahma, I. (2024). Negara thailand sendiri, berdasarkan laporan dari Thailand *Computer Crime Investigation Bureau* (CCIB), terjadi lonjakan jumlah kejahatan siber dalam beberapa tahun terakhir. Pada tahun 2021, lebih dari 6.000 kasus kejahatan siber dilaporkan, yang sebagian besar terkait dengan penipuan online dan peretasan data pribadi.

Selain peraturan hukum domestik, prinsip-prinsip hukum internasional juga memainkan peran penting dalam penanggulangan kejahatan siber. Dalam konteks ini, *Budapest Convention on Cybercrime* yang diadopsi oleh Dewan Eropa pada tahun 2001, menjadi acuan internasional untuk kerjasama antarnegara dalam menangani kejahatan siber, termasuk pengaturan prosedur permintaan bantuan hukum, ekstradisi, dan pertukaran data antarnegara. Thailand dan Indonesia, meskipun bukan negara anggota penuh konvensi tersebut, aktif berpartisipasi dalam forum internasional yang membahas isu kejahatan siber, seperti melalui Interpol dan ASEAN *Cybersecurity Cooperation*. Posisi kedua negara dalam forum global ini menunjukkan komitmen mereka untuk memperkuat kerjasama internasional dalam menangani kejahatan siber yang bersifat lintas batas, meskipun terdapat tantangan dalam penerapan hukum domestik yang selaras dengan norma internasional.

Di Indonesia, kejahatan siber juga mengalami peningkatan yang signifikan. Berdasarkan data dari Kementerian Komunikasi dan Informatika Indonesia (Kominfo), pada tahun 2020 terdapat lebih dari 1 juta laporan terkait kejahatan siber yang diterima, dengan jenis kejahatan terbesar adalah penipuan online dan penyebaran konten negatif melalui internet. (Yudistira, M., & Ramadani, R. (2023) Penelitian ini bertujuan mengeksplorasi persamaan dan perbedaan dalam peraturan hukum pidana terkait kejahatan siber di Thailand dan Indonesia, serta menilai efektivitas penegakan hukum tersebut. Dengan memahami pendekatan yang diambil oleh kedua negara, diharapkan dapat memberikan wawasan bagi pengembangan kebijakan hukum pidana yang lebih baik di masa depan, khususnya dalam menghadapi ancaman kejahatan siber yang terus berkembang.

B. PEMBAHASAN

1. Kebijakan Hukum Pidana di Indonesia dan Thailand dalam Mengatur Serta Menanggulangi Kejahatan Cyber

Kejahatan cyber merupakan salah satu bentuk tindak pidana yang semakin berkembang seiring dengan pesatnya kemajuan teknologi informasi. Indonesia dan Thailand sebagai negara di kawasan Asia Tenggara menghadapi tantangan besar dalam menangani kejahatan ini. Oleh karena itu, kedua negara telah menerapkan berbagai kebijakan hukum pidana guna mengatur dan menanggulangi kejahatan cyber. Meskipun memiliki dasar hukum yang berbeda, baik Indonesia maupun Thailand memiliki tujuan yang sama, yaitu melindungi masyarakat dari dampak negatif kejahatan siber. (Fricticarani, A., Hayati, A., Ramdani, R., Hoirunisa, I., & Rosdalina, G. M. (2023)

Dalam konteks kejahatan siber lintas batas, hukum internasional memberi landasan penting bagi kerjasama antarnegara dalam penegakan hukum. Salah satu instrumen utama adalah kewajiban negara untuk melakukan ekstradisi pelaku kejahatan siber yang melarikan diri ke negara lain, dengan dasar hukum yang sering kali dipertegas dalam perjanjian ekstradisi bilateral atau multilateral. Selain itu, pembentukan *Mutual Legal Assistance Treaties* (MLAT) antara negara-negara tersebut menjadi sarana vital untuk memfasilitasi pertukaran informasi dan bukti yang dibutuhkan dalam penyelidikan kasus kejahatan siber,

mengingat kejahatan ini sering kali melibatkan data yang terdistribusi di berbagai yurisdiksi. Prinsip *universal jurisdiction* juga semakin relevan, di mana negara dapat mengejar pelaku kejahatan siber yang terjadi di luar wilayahnya, terutama bila kejahatan tersebut berdampak serius pada kepentingan nasional atau internasional. Oleh karena itu, kerjasama internasional yang mencakup ekstradisi, MLAT, dan penerapan prinsip universal jurisdiction sangat penting dalam menanggulangi kejahatan siber yang bersifat transnasional.

Di Indonesia, regulasi terkait kejahatan cyber diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang kemudian mengalami beberapa perubahan, dengan yang terbaru melalui Undang-Undang Nomor 1 Tahun 2024. UU ITE mengatur berbagai jenis kejahatan cyber, seperti akses ilegal ke sistem elektronik, penyebaran informasi bohong, pencemaran nama baik, serta tindakan peretasan dan penyalahgunaan data pribadi. Selain itu, Indonesia juga memiliki Kitab Undang-Undang Hukum Pidana (KUHP) baru yang mulai berlaku pada 2026 dan mengakomodasi beberapa ketentuan terkait kejahatan cyber.

Sementara itu, Thailand memiliki Computer-Related Crime Act (CCA) B.E. 2550 (2007) yang merupakan regulasi utama dalam menangani kejahatan cyber. Undang-undang ini mencakup berbagai aspek kejahatan digital, seperti akses ilegal ke sistem komputer, pemalsuan data elektronik, serta penyebaran informasi palsu yang dapat merugikan individu atau negara. Thailand juga mengadopsi beberapa perubahan melalui CCA Amendment Act (2017) untuk memperkuat ketentuan hukum terhadap pelaku kejahatan siber dan meningkatkan kapasitas penegakan hukum di bidang ini.

UU ITE di Indonesia lebih menekankan pada aspek transaksi elektronik dan perlindungan terhadap penyalahgunaan teknologi informasi, sedangkan CCA Thailand lebih fokus pada aspek teknis dari kejahatan komputer. Misalnya, dalam kasus akses ilegal ke sistem komputer, CCA Thailand secara khusus mengatur sanksi yang lebih berat terhadap pelaku yang menyebabkan kerugian finansial atau operasional yang signifikan. Sementara itu, UU ITE Indonesia lebih banyak mengatur aspek sosial, seperti ujaran kebencian dan penyebaran berita bohong. (Putri, A., & Wijaya, S. (2021)

Dalam hal pnegakan hukum, Indonesia memiliki Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri yang bertugas menangani berbagai kasus kejahatan cyber. Selain itu, Indonesia juga bekerja sama dengan berbagai lembaga internasional, seperti INTERPOL dan ASEAN Cybersecurity Forum, untuk memperkuat kapasitas dalam menghadapi ancaman cyber. Thailand, di sisi lain, memiliki Cyber Crime Investigation Bureau (CCIB) di bawah kepolisian Thailand, yang memiliki peran utama dalam menyelidiki dan menindak pelaku kejahatan siber, terutama dalam kasus yang melibatkan kejahatan lintas negara.

Dalam aspek kerja sama internasional, Thailand telah bergabung dalam beberapa inisiatif global untuk menangani kejahatan cyber, seperti Budapest Convention on Cybercrime, yang menjadi standar internasional dalam menangani kejahatan siber lintas negara. Indonesia sendiri hingga saat ini belum meratifikasi konvensi tersebut, meskipun telah menjalin berbagai kerja sama bilateral dengan negara lain untuk meningkatkan kapasitas dalam menanggulangi kejahatan siber.

Efektivitas kebijakan hukum pidana terhadap kejahatan cyber di kedua negara juga dipengaruhi oleh tantangan dalam implementasi regulasi. Di Indonesia, UU ITE sering kali dikritik karena memiliki pasal karet yang berpotensi disalahgunakan untuk membungkam kebebasan berekspresi. Sebaliknya, di Thailand, CCA 2007 juga menuai kontroversi karena dianggap memberikan wewenang berlebihan kepada pemerintah dalam melakukan pemantauan dan penyensoran terhadap aktivitas online masyarakat. (Rahman, A., & Kusuma, P. (2023)

Baik Indonesia maupun Thailand terus melakukan pembaruan dalam kebijakan hukum pidana untuk menyesuaikan dengan perkembangan teknologi dan modus operandi kejahatan cyber. Indonesia misalnya, telah membentuk Badan Siber dan Sandi Negara (BSSN) yang berperan dalam meningkatkan ketahanan cyber nasional. Sementara itu, Thailand memiliki Thailand Computer Emergency Response Team (ThaiCERT) yang bertanggung jawab atas respons cepat terhadap insiden keamanan siber.

2. Perbandingan Peraturan Hukum Pidana Mengenai Kejahatan Siber yang Diterapkan di Thailand dan Indonesia

Perbandingan peraturan kejahatan siber antara Thailand dan Indonesia mencerminkan pendekatan yang berbeda meskipun kedua negara menghadapi tantangan serupa dalam menangani kejahatan siber. Masing-masing negara memiliki kerangka hukum yang dirancang untuk mengatasi kejahatan yang terjadi di dunia maya, dengan perbedaan dalam definisi, struktur hukum, dan penerapan sanksi terhadap pelaku. (Rahman, A., & Kusuma, P. (2023)

Indonesia memiliki UU ITE yang mulai diberlakukan pada tahun 2008. UU ini mencakup berbagai jenis kejahatan siber, seperti pencemaran nama baik, penyebaran informasi pribadi tanpa izin, hingga penipuan online. Selain itu, Indonesia juga memiliki KUHP yang mengatur tindak pidana umum yang bisa diterapkan dalam konteks kejahatan siber, seperti pencurian data atau hacking. UU ITE ini memberikan dasar hukum yang kuat bagi penegakan hukum terkait kejahatan di dunia maya, meskipun sering mendapat kritik terkait dengan penerapan yang bisa melanggar kebebasan berekspresi.

Thailand, di sisi lain, memiliki kerangka hukum yang lebih kompleks dalam menangani kejahatan siber. Selain memiliki Undang-Undang Keamanan Informasi Nasional (National Cybersecurity Act 2019), Thailand juga menerapkan hukum pidana yang lebih spesifik untuk mengatur kejahatan siber. Salah satu regulasi utama di Thailand adalah Computer Crime Act (CCA), yang pertama kali diberlakukan pada tahun 2007 dan telah diperbarui beberapa kali. CCA mencakup berbagai bentuk kejahatan, termasuk akses ilegal, pencurian data, dan penyebaran konten ilegal. Thailand juga mengatur kejahatan siber dalam konteks ancaman terhadap keamanan negara dan infrastruktur kritis.

Salah satu perbedaan mencolok antara Indonesia dan Thailand adalah pendekatan terhadap kebebasan berbicara. Indonesia, meskipun telah merevisi UU ITE pada tahun 2016, masih sering menggunakan UU ITE untuk menindak ujaran kebencian atau pencemaran nama baik melalui media sosial. Di Thailand, CCA lebih berfokus pada tindakan yang merugikan keamanan nasional, seperti penyebaran informasi yang dapat mengancam stabilitas sosial dan politik, yang kadang-kadang menimbulkan kritik terhadap pembatasan kebebasan berekspresi.

Dari sisi penegakan hukum, kedua negara memiliki lembaga yang berwenang menangani kejahatan siber, namun dengan pendekatan yang sedikit berbeda. Di Indonesia, Badan Reserse Kriminal Polri memiliki unit khusus yang menangani kejahatan dunia maya, sedangkan di Thailand, penegakan hukum lebih terpusat pada Komisi Keamanan Siber Nasional dan departemen kepolisian yang fokus pada kejahatan siber. Meskipun demikian, kedua negara menghadapi tantangan dalam hal sumber daya manusia yang terlatih dan keterbatasan teknis dalam mengatasi kejahatan siber yang semakin canggih.

Perbedaan lainnya adalah dalam hal sanksi dan hukuman. Indonesia menerapkan sanksi pidana yang relatif berat terhadap pelanggaran yang tercantum dalam UU ITE, yang bisa berupa denda hingga penjara, terutama untuk kasus yang melibatkan pencemaran nama baik atau penyebaran informasi palsu. Di Thailand, hukuman yang diterapkan melalui CCA juga dapat mencakup denda dan penjara, namun dengan tambahan sanksi yang lebih terkait dengan ancaman terhadap negara, seperti hukuman yang lebih berat bagi mereka yang terlibat dalam aktivitas hacking yang mengancam keamanan nasional. (Putri, A., & Wijaya, S. (2021)

Keamanan dan perlindungan data pribadi menjadi salah satu isu penting dalam kejahatan siber. Indonesia mengatur perlindungan data pribadi dalam UU ITE, meskipun hukum ini belum sepenuhnya mencakup aspek perlindungan data yang lebih modern seperti yang terdapat dalam undang-undang perlindungan data pribadi yang baru-baru ini diberlakukan di negara-negara lain. Thailand, sementara itu, mengadopsi Personal Data Protection Act (PDPA) yang mulai berlaku pada tahun 2022, yang lebih sejalan dengan Regulasi Perlindungan Data Umum (GDPR) Uni Eropa. Hal ini memberikan tingkat perlindungan yang lebih tinggi terhadap data pribadi warganya dibandingkan dengan Indonesia.

Meskipun terdapat perbedaan dalam kerangka hukum, kedua negara juga memiliki kesamaan dalam hal kerjasama internasional. Baik Indonesia maupun Thailand terlibat dalam berbagai perjanjian internasional terkait dengan keamanan siber, seperti kerja sama dengan Interpol dan ASEAN. Ini penting untuk memperkuat penegakan hukum di tingkat global, mengingat kejahatan siber seringkali melibatkan pelaku yang beroperasi lintas batas negara.

Secara keseluruhan, meskipun Indonesia dan Thailand memiliki pendekatan hukum yang berbeda dalam mengatasi kejahatan siber, keduanya semakin memperkuat regulasi mereka untuk menghadapi tantangan yang terus berkembang di dunia maya. Penerapan undang-undang ini harus seimbang antara memberikan perlindungan terhadap masyarakat dan mencegah penyalahgunaan hukum yang dapat mengekang kebebasan sipil.

3. Tantangan yang Dihadapi oleh Thailand dan Indonesia dalam Penegakan Hukum Terhadap Kejahatan Siber

Penegakan hukum terhadap kejahatan siber di Thailand dan Indonesia menghadapi sejumlah tantangan yang signifikan, meskipun kedua negara telah mengembangkan kerangka hukum untuk menanggulangi permasalahan ini. Salah satu tantangan utama yang dihadapi oleh kedua negara adalah kecepatan dan perkembangan teknologi yang sangat pesat. Kejahatan siber sering kali lebih cepat berkembang daripada kemampuan lembaga penegak hukum untuk menangani dan menyesuaikan diri dengan teknologi baru. Misalnya, dengan munculnya teknologi seperti blockchain, kripto, dan kecerdasan buatan, pelaku kejahatan siber dapat menggunakan alat-alat canggih ini untuk melakukan tindakan ilegal yang lebih sulit dideteksi dan diberantas. (Maulana, R., & Dewi, S. (2022)

Keterbatasan sumber daya manusia dan keterampilan teknis adalah tantangan lain yang dihadapi oleh Thailand dan Indonesia dalam penegakan hukum terhadap kejahatan siber. Penegakan hukum siber memerlukan keterampilan teknis yang sangat tinggi, dan banyak lembaga penegak hukum di kedua negara masih kekurangan personel yang memiliki kompetensi dalam teknologi informasi dan keamanan siber. Keterbatasan ini memperburuk kemampuan mereka untuk melakukan investigasi yang mendalam, mengidentifikasi pelaku kejahatan siber yang tersembunyi di balik teknologi canggih, serta menangani kejahatan siber yang melibatkan data besar atau serangan dunia maya yang kompleks.

Tantangan lain yang dihadapi oleh kedua negara adalah masalah kerjasama internasional dalam menangani kejahatan siber yang bersifat lintas negara.

Kejahatan siber seringkali melibatkan pelaku yang beroperasi di berbagai negara, sehingga koordinasi antarnegara sangat penting. Meskipun Thailand dan Indonesia terlibat dalam kerjasama internasional seperti dengan Interpol dan ASEAN, namun perbedaan peraturan hukum, sistem yudisial, serta kendala komunikasi antar lembaga internasional seringkali memperlambat penindakan terhadap pelaku kejahatan siber yang berada di luar wilayah hukum suatu negara. (Handoyo, B., Husamuddin, M. Z., & Rahma, I. (2024).

Salah satu tantangan utama dalam penegakan hukum terhadap pelaku kejahatan siber adalah penentuan lokasi dan yurisdiksi yang tepat. Kejahatan siber sering kali dilakukan secara anonim dan tanpa batasan geografis, sehingga membuat sulit untuk menentukan lokasi pelaku atau di mana pelanggaran hukum terjadi. Di Indonesia dan Thailand, hal ini menyulitkan pihak berwenang dalam menentukan undang-undang yang berlaku, apakah itu hukum nasional atau hukum internasional, serta di mana proses hukum harus dilakukan.

Keterbatasan infrastruktur dan teknologi penegakan hukum juga menjadi hambatan yang signifikan di kedua negara. Meskipun Indonesia dan Thailand semakin memperbarui sistem teknologi mereka untuk menangani kejahatan siber, infrastruktur yang tidak memadai masih menjadi masalah. Kurangnya alat dan perangkat keras untuk memantau dan menganalisis serangan siber secara real-time membuat kedua negara kesulitan untuk merespons insiden siber secara cepat. Selain itu, banyak lembaga penegak hukum yang belum sepenuhnya mengimplementasikan teknologi canggih dalam sistem penyelidikan mereka, yang memperlambat proses penegakan hukum.

Perlindungan terhadap saksi dan korban juga merupakan tantangan besar dalam penegakan hukum terkait kejahatan siber. Banyak korban kejahatan siber, seperti penipuan online atau peretasan, enggan untuk melapor ke pihak berwajib karena khawatir akan risiko keamanan, kebocoran data pribadi, atau stigma sosial. Selain itu, saksi dalam kasus kejahatan siber seringkali dihadapkan pada ancaman atau intimidasi dari pelaku yang memiliki kemampuan teknis untuk mengakses data pribadi dan lokasi mereka. Dalam hal ini, Thailand dan Indonesia perlu meningkatkan upaya untuk melindungi saksi dan korban, dengan menyediakan mekanisme perlindungan yang lebih kuat.

Tantangan terkait regulasi yang terlalu luas atau ambigu juga mempengaruhi efektivitas penegakan hukum. Di Indonesia, misalnya, UU ITE sering dikritik karena penggunaan pasal-pasal yang dapat disalahgunakan untuk menindak kebebasan berekspresi atau ujaran publik, yang berisiko menimbulkan efek chilling bagi masyarakat. Begitu juga di Thailand, meskipun CCA memberikan dasar hukum yang kuat untuk menangani kejahatan siber, ketidakjelasan dalam penerapan hukum atau definisi yang luas tentang "ancaman terhadap keamanan negara" dapat menyebabkan pelaksanaan hukum yang tidak konsisten. Hal ini menciptakan ketidakpastian hukum yang bisa merugikan pihak yang tidak bersalah. (Fricticarani, A., Hayati, A., Ramdani, R., Hoirunisa, I., & Rosdalina, G. M. (2023)

Kendala budaya dan persepsi masyarakat juga memainkan peran penting dalam penegakan hukum terhadap kejahatan siber di Thailand dan Indonesia. Banyak masyarakat yang masih kurang menyadari potensi ancaman kejahatan siber, dan mereka cenderung menganggap hal tersebut sebagai masalah teknis yang hanya melibatkan pihak berwenang. Dalam hal ini, kesadaran dan pendidikan masyarakat tentang pentingnya keamanan siber masih sangat diperlukan. Tanpa kesadaran yang cukup, banyak korban yang tidak melaporkan kejahatan atau tidak melindungi data pribadi mereka dengan baik, yang membuat mereka lebih rentan terhadap kejahatan siber.

Secara keseluruhan, Thailand dan Indonesia menghadapi banyak tantangan dalam penegakan hukum terhadap kejahatan siber. Dari keterbatasan teknis dan infrastruktur, masalah kerjasama internasional, hingga kesulitan dalam melindungi korban dan saksi, keduanya perlu terus beradaptasi dan memperbarui sistem hukum serta meningkatkan kapasitas lembaga penegak hukum mereka untuk menanggulangi ancaman yang terus berkembang di dunia maya.

C. PENUTUP

Thailand dan Indonesia memiliki kerangka hukum yang dirancang untuk mengatasi kejahatan siber, tapi terdapat perbedaan signifikan di pendekatannya. Thailand mengandalkan Computer Crime Act (CCA) yang mencakup kejahatan seperti akses ilegal, penyebaran informasi palsu, dan terkait perusakan data.

CCA dirancang dengan revisi untuk menyesuaikan dengan perkembangan teknologi. Sementara itu, Indonesia menggunakan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), yang mengatur berbagai aspek kejahatan siber seperti perlindungan data pribadi dan penyebaran berita hoaks. Kedua undang-undang tersebut memiliki kesamaan dalam hal pengaturan umum tentang kejahatan siber, namun Indonesia lebih fokus pada aspek transaksi elektronik dan penyebaran informasi digital.

Beberapa masalah utama yang dihadapi oleh kedua negara meliputi kurangnya sumber daya teknis dan manusia, kurangnya koordinasi antar lembaga penegak hukum, serta rendahnya kesadaran masyarakat tentang pentingnya keamanan siber. Untuk meningkatkan efektivitas hukum pidana dalam menangani kejahatan siber, kedua negara perlu fokus pada reformasi kebijakan yang mencakup pelatihan dan peningkatan keterampilan aparat penegak hukum, penguatan koordinasi antara lembaga terkait, serta edukasi publik yang lebih luas mengenai ancaman siber dan cara melindungi diri.

dalam konteks kerja sama hukum internasional, Thailand dan Indonesia harus memperkuat keterlibatan mereka dalam forum internasional, seperti *Budapest Convention on Cybercrime*, serta meningkatkan penggunaan *Mutual Legal Assistance Treaties* (MLAT) dan prinsip *universal jurisdiction* untuk menangani kejahatan siber lintas batas. Penguatan mekanisme hukum regional dan global juga perlu dilakukan, dengan membangun kerjasama yang lebih erat di dalam ASEAN atau dengan negara-negara lain yang menjadi mitra dalam penanggulangan kejahatan siber. Dengan demikian, tidak hanya kerangka hukum domestik yang diperkuat, tetapi juga kolaborasi internasional yang lebih solid untuk menghadapi ancaman siber yang semakin berkembang.

DAFTAR PUSTAKA

Publikasi

Balaka, K. I., A. R. Hakim dan F. D. Sulistyany. *Pencurian Informasi Nasabah di Sektor Perbankan: Ancaman Serius di Era Digital*. Yustitiabelen. Vol.10. No.2 (2024).

Butarbutar, R.. *Kejahatan Siber Terhadap Individu: Jenis, Analisis, dan Perkembangannya*. Technology and Economics Law Journal. Vol.2. No.2 (2023).

Fricticarani, A., A. Hayati, I. Ramdani, Hoirunisa dan G. M. Rosdalina. *Strategi Pendidikan untuk Sukses di Era Teknologi 5.0*. Jurnal Inovasi Pendidikan dan Teknologi Informasi (JIPTI). Vol.4. No.1 (2023).

Handoyo, B., M. Z. Husamuddin dan I. Rahma, *Tinjauan Yuridis Penegakan Hukum Kejahatan Cyber Crime Studi Implementasi Undang-Undang Nomor 11 Tahun 2008*. MAQASIDI: Jurnal Syariah dan Hukum. Vol.4. No.1 (2024).

Kusuma, R. dan D. Hartanto. *Harmonisasi Sistem Hukum Pidana dalam Penanganan Kejahatan Siber di ASEAN*. Jurnal Penelitian Hukum De Jure. Vol.20. No.3 (2020).

Maulana, R. dan S. Dewi. *Sistem Pembuktian Digital dalam Peradilan Pidana: Studi Komparatif Indonesia-Thailand*. Jurnal Hukum IUS QUIA IUSTUM. Vol.29. No.2 (2022).

Putri, A. dan S. Wijaya. *Efektivitas Penegakan Hukum Siber dalam Sistem Peradilan Pidana Indonesia*. Padjadjaran Journal of Law. Vol.8. No.2 (2021).

Rahman, A., dan P. Kusuma. *Tantangan Modernisasi Sistem Peradilan Pidana di Era Digital*. Jurnal Konstitusi. Vol.20. No.1 (2023).

Sari, N. W. *Kejahatan Cyber dalam Perkembangan Teknologi Informasi Berbasis Komputer*. Jurnal Surya Kencana Dua: Dinamika Masalah Hukum Dan Keadilan. Vol.5. No.2 (2018).

Supriyadi, W. dan F. Rahman. *Perbandingan Sistem Peradilan Pidana Indonesia dan Thailand dalam Penanganan Cybercrime*. Jurnal Hukum & Pembangunan. Vol.49. No.2 (2019).

Yudistira, M. dan Ramadani. *Tinjauan Yuridis terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 oleh KOMINFO*. UNES Law Review. Vol. 5 No.4 (2023).

Sumber Hukum

Kitab Undang-Undang Hukum Pidana (KUHP).

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Thailand Computer-Related Crime Act (CCA) 2007.

Thailand National Cybersecurity Act 2019.