P-ISSN : 2654-4946
E-ISSN :2654-7538 https://doi.org/10.37817/ikraith-humaniora.v9i2

Kajian Teoritis Implikasi *The United Nations Convention Against Cybercrime* Terhadap Pengaturan Tindak Pidana Siber Indonesia

[1]Andi Rania Risya Zamayya, [2]Devito Imanda Wagiyanto, [3]Paolo Gibran Joesoef, [4] Richie Evanno Salim, [5]Tiffany Thendean
[1]Fakultas Hukum, Universitas Pelita Harapan, Tangerang
[2]Fakultas Hukum, Universitas Pelita Harapan, Tangerang
[3]Fakultas Hukum, Universitas Pelita Harapan, Tangerang
[4]Fakultas Hukum, Universitas Pelita Harapan, Tangerang
[5]Fakultas Hukum, Universitas Pelita Harapan, Tangerang

E-mail: [1]01051220166@student.uph.edu, [2]01051220155@student.uph.edu, [3]01051220204@student.uph.edu, [4]01051220131@student.uph.edu, [5]01051220193@student.uph.edu

ABSTRAK

Perkembangan teknologi digital telah mendorong kemunculan berbagai bentuk kejahatan siber yang kompleks dan bersifat lintas negara. Untuk menjawab tantangan ini, Perserikatan Bangsa-Bangsa menginisiasi *The United Nations Convention Against Cybercrime* sebagai upaya global dalam harmonisasi kebijakan hukum dan peningkatan kerja sama internasional. Artikel ini bertujuan untuk mengkaji implikasi teoritis dari konvensi tersebut terhadap kerangka hukum pidana siber di Indonesia, khususnya Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan KUHP. Penelitian ini menggunakan metode yuridis normatif dengan pendekatan perundang-undangan, analisis isi, dan komparasi hukum. Hasil analisis menunjukkan bahwa konvensi ini memberikan landasan untuk memperkuat pengaturan tindak pidana siber melalui harmonisasi definisi, prosedur penegakan hukum, kerja sama lintas negara, serta perlindungan hak asasi manusia. Namun demikian, tantangan berupa perbedaan kepentingan politik, keterbatasan sumber daya, dan resistensi terhadap perubahan hukum juga menjadi hambatan. Oleh karena itu, diperlukan strategi nasional yang komprehensif untuk mengadopsi konvensi ini secara efektif guna memperkuat posisi Indonesia dalam menangani kejahatan siber secara global

Kata kunci : ***The United Nations Convention Against Cybercrime, Hukum Pidana Siber Indonesia, UU ITE, harmonisasi hukum internasional, kerja sama penegakkan hukum, privasi.***

ABSTRACT

The rapid advancement of digital technology has led to the emergence of complex and transnational forms of cybercrime. In response to these challenges, the United Nations initiated The United Nations Convention Against Cybercrime as a global effort to harmonize legal policies and enhance international cooperation. This article aims to examine the theoretical implications of the convention on Indonesia's cybercrime legal framework, particularly the Electronic Information and Transactions Law (UU ITE) and the Indonesian Penal Code (KUHP). This study employs a normative juridicial method using a statutory, content analysis, and comparative law

https://doi.org/10.37817/ikraith-humaniora.v9i2
P-ISSN : 2654-4946
E-ISSN :2654-7538

approach. The findings indicate that the convention provides a foundation for strengthening the regulation of cybercrime through harmonization of definitions, law enforcement procedures, cross-border cooperation, and the protection of human rights. Nevertheless, challenges such as differing political interests, limited resources, and resistance to legal changes may hinder implementation. Therefore, a comprehensive national strategy is required to effectively adopt the convention and strengthen Indonesia's position in addressing global cybercrime threats.

Keyword : ***The United Nations Convention Against Cybercrime*, *Hukum Pidana Siber Indonesia, UU ITE, harmonisasi hukum internasional, kerja sama penegakkan hukum, privasi.***

1. PENDAHULUAN

Perkembangan teknologi digital yang begitu cepat telah membawa perubahan besar pada tatanan global, memfasilitasi pertumbuhan ekonomi, inovasi, dan konektivitas. Namun, transformasi ini juga telah memunculkan lonjakan kejahatan siber, yang menghadirkan tantangan besar bagi keamanan nasional dan internasional. Menurut Andi Hamzah (1989) *cybercrime* adalah kejahatan dibidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal. Mulai dari penipuan keuangan dan pencurian identitas hingga terorisme siber dan pelanggaran data, semakin canggih dan bersifat transnasional, sehingga membutuhkan kerangka kerja peraturan yang kuat dan kooperatif.

Konvensi Perserikatan Bangsa-Bangsa (PBB) melawan Kejahatan Dunia Maya, atau *The United Nations Convention against Cybercrime*, merupakan upaya global untuk mengatasi tantangan-tantangan ini. Hal tersebut diadopsi untuk mendorong kerja sama internasional dalam memerangi kejahatan siber, konvensi ini bertujuan untuk menyelaraskan standar hukum, meningkatkan kolaborasi penegakan hukum, dan mendorong pengembangan kapasitas di negara-negara anggota. Ketentuan-ketentuannya membahas bidang-bidang penting seperti kriminalisasi pelanggaran dunia maya, mekanisme prosedural untuk pengumpulan bukti, dan kerjasama lintas negara dalam penyelidikan.

Indonesia, sebagai salah satu negara dengan pertumbuhan ekonomi digital tercepat di Asia Tenggara, menghadapi tantangan unik dalam mengatur kejahatan siber. Indonesia telah menyaksikan peningkatan eksponensial dalam penggunaan internet dan transaksi digital, yang disertai dengan peningkatan ancaman siber. Meskipun telah diberlakukannya peraturan domestik seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), masih terdapat kesenjangan dalam menangani kompleksitas kejahatan siber transnasional dan memastikan keselarasan yang memadai dengan standar internasional.

Makalah penelitian ini akan mengeksplorasi implikasi teoritis dari Konvensi PBB Menentang Kejahatan Siber terhadap kerangka peraturan Indonesia untuk kejahatan siber. Dengan menganalisis ketentuan-ketentuan dalam konvensi tersebut dan mengevaluasi relevansinya dengan lanskap hukum dan kelembagaan Indonesia, penelitian ini bertujuan untuk memberikan wawasan tentang bagaimana kerangka kerja internasional

P-ISSN : 2654-4946
E-ISSN :2654-7538 https://doi.org/10.37817/ikraith-humaniora.v9i2

dapat mempengaruhi dan meningkatkan peraturan kejahatan siber nasional. Studi ini juga mengkaji potensi tantangan dan peluang dalam menyelaraskan kebijakan Indonesia dengan konvensi tersebut, dengan mempertimbangkan konteks sosial-politik, perkembangan teknologi, dan mekanisme hukum yang ada.

Hingga penyusunan jurnal ini, informasi resmi mengenai waktu pelaksanaan upacara penandatanganan konvensi tersebut belum tersedia. Berdasarkan informasi yang dilansir dari situs resmi UNODC, jadwal upacara tersebut masih akan dikonfirmasi lebih lanjut. Penetapan waktu yang belum pasti ini menunjukkan adanya proses diplomasi dan koordinasi yang masih berlangsung di antara negara-negara anggota PBB. Negara-negara yang berminat untuk menjadi pihak dalam konvensi tersebut diperkirakan memiliki kesempatan untuk menandatangani dokumen hingga sekitar Mei 2025. Hal ini memberikan waktu memadai bagi pemerintah masing-masing negara untuk mempertimbangkan signifikansi konvensi itu sendiri.

2. LANDASAN TEORI

Landasan teori dalam kajian ini berfokus pada tiga aspek utama yang relevan dengan implikasi *The United Nations Convention Against Cybercrime* teradap pengaturan tindak pidana siber di Indonesia, yaitu teori hukum internasional, teori harmonisasi hukum, dan teori kejahatan siber.

a. Teori Hukum Internasional

Teori hukum internasional menjelaskan bagaimana hukum internasional dihasilkan, diterapkan, dan diakui di berbagai negara. Indonesia adalah negara penganut aliran monisme. Aliran monisme menganggap hukum internasional berlaku pula (terinkorporasi) di lingkungan hukum nasional, setaraf dengan hukum nasional dengan mempertahankan sifat hukum internasional tersebut tanpa mengubahnya sejauh isinya cocok untuk diterapkan pada hubungan-hubungan hukum nasional. Konvensi PBB melawan kejahatan dunia maya berfungsi sebagai instrumen hukum yang mengatur kerjasama internasional dalam menghadapi tantangan kejahatan siber yang semakin kompleks dan transnasional. Dengan adanya konvensi ini, negara-negara anggota diharapkan dapat mengadopsi standar hukum yang seragam, sehingga penegakan hukum terhadap kejahatan siber dapat dilakukan secara lebih efektif dan efisien di tingkat global. Teori ini menekankan pentingnya pengakuan dan penerapan norma-norma internasional dalam sistem hukum nasional, yang menjadi landasan bagi upaya kolaborasi internasional dalam memerangi kejahatan di dunia maya.

b. Teori Harmonisasi Hukum

Selanjutnya, teori harmonisasi hukum berfokus pada proses penyesuaian dan penyelarasan norma hukum antara hukum internasional dan hukum nasional. Dalam konteks Indonesia, harmonisasi hukum menjadi krusial untuk mengintegrasikan ketentuan-ketentuan dalam Konvensi PBB ke dalam sistem hukum domestik. Proses ini melibatkan identifikasi kesenjangan antara hukum yang berlaku di Indonesia, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), dengan ketentuan yang ditetapkan dalam konvensi. Teori ini menggarisbawahi pentingnya upaya untuk menyelaraskan kebijakan dan praktik hukum nasional agar sesuai dengan standar internasional, sehingga Indonesia dapat berperan aktif dalam kerjasama internasional dalam penanganan kejahatan siber.

c. Teori Kejahatan Siber

P-ISSN : 2654-4946
https://doi.org/10.37817/ikraith-humaniora.v9i2 E-ISSN :2654-7538

Terakhir, teori kejahatan siber memberikan perspektif tentang karakteristik, penyebab, dan dampak dari kejahatan yang dilakukan melalui teknologi informasi dan komunikasi. Kejahatan siber sering kali bersifat transnasional dan dapat melibatkan berbagai jenis tindakan kriminal, seperti penipuan, pencurian identitas, dan serangan siber. Teori ini menekankan bahwa untuk menangani kejahatan siber secara efektif, diperlukan pendekatan yang komprehensif dan kolaboratif antara negara. Konvensi PBB mencakup berbagai jenis kejahatan siber, yang menunjukkan perlunya pengaturan yang tepat dalam konteks hukum untuk menghadapi ancaman yang terus berkembang.

Secara keseluruhan, ketiga teori ini saling terkait dan memberikan kerangka kerja untuk menganalisis implikasi Konvensi PBB terhadap pengaturan tindak pidana siber di Indonesia. Pemahaman yang mendalam mengenai hukum internasional, harmonisasi hukum, dan kejahatan siber sangat penting untuk mengevaluasi bagaimana kerangka hukum internasional dapat mempengaruhi kebijakan dan praktik hukum di tingkat nasional. Dengan demikian, penelitian ini diharapkan dapat memberikan wawasan yang lebih luas mengenai tantangan dan peluang dalam menyelaraskan hukum nasional dengan standar internasional dalam menghadapi kejahatan siber.

3. METODOLOGI

Penelitian ini menggunakan metode penelitian yuridis normatif, yang berfokus pada analisis terhadap norma-norma hukum yang terkait dengan pengaturan tindak pidana siber di Indonesia serta implikasi dari *The United Nations Convention Against Cybercrime*. Jenis penelitian ini bersifat deskriptif dan analitis dengan pendekatan kualitatif. Sumber data yang digunakan terdiri dari bahan hukum primer, sekunder, dan tersier. Bahan hukum primer meliputi konvensi internasional seperti *The United Nations Convention Against Cybercrime* dan peraturan perundang-undangan Indonesia terkait tindak pidana siber, seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) serta Kitab Undang-Undang Hukum Pidana (KUHP). Bahan hukum sekunder mencakup buku, artikel jurnal, dan literatur hukum yang membahas kejahatan siber, konvensi internasional, dan harmonisasi hukum. Sementara itu, bahan hukum tersier meliputi kamus hukum, ensiklopedia, dan sumber referensi umum lainnya. Hal ini dilakukan karena penelitian hukum normatif yang menggunakan pendekatan perundang-undangan (*statute approach*), analisis hukum yang dihasilkannya akan lebih akurat bila dibantu oleh satu atau lebih pendekatan lain yang cocok guna memperkaya pertimbangan-pertimbangan hukum yang tepat untuk menghadapi problem hukum yang dihadapi.

Teknik pengumpulan data dilakukan melalui studi dokumen dan kajian literatur. Studi dokumen melibatkan analisis terhadap dokumen-dokumen hukum seperti konvensi internasional, peraturan perundang-undangan, dan putusan pengadilan yang relevan. Kajian literatur dilakukan dengan mengumpulkan dan menganalisis literatur sekunder seperti buku, jurnal, dan artikel ilmiah terkait topik penelitian. Analisis data dilakukan dengan menggunakan metode analisis isi (*content analysis*), komparasi hukum, dan interpretasi hukum. Analisis isi digunakan untuk menganalisis ketentuan-ketentuan yang ada di dalam *The United Nations Convention Against Cybercrime* dan membandingkannya dengan peraturan

P-ISSN : 2654-4946
E-ISSN :2654-7538 https://doi.org/10.37817/ikraith-humaniora.v9i2

hukum pidana siber di Indonesia. Komparasi hukum dilakukan untuk membandingkan prinsip-prinsip dan ketentuan dalam konvensi internasional dengan hukum nasional guna mengidentifikasi kesenjangan atau harmonisasi. Interpretasi hukum digunakan untuk menafsirkan norma-norma hukum yang terkait dengan kejahatan siber.

Kerangka teori yang digunakan dalam penelitian ini meliputi teori hukum internasional, teori harmonisasi hukum, dan teori kejahatan siber. Teori hukum internasional digunakan untuk memahami posisi konvensi internasional dalam sistem hukum global. Teori harmonisasi hukum digunakan untuk menganalisis upaya harmonisasi antara hukum internasional dan hukum nasional. Sementara itu, teori kejahatan siber digunakan untuk memahami karakteristik dan pengaturan tindak pidana siber. Tahapan penelitian dimulai dengan identifikasi masalah, pengumpulan data, analisis data, penyimpulan, dan rekomendasi. Output daripada penelitian ini diharapkan dapat memberikan kesimpulan mengenai implikasi *The United Nations Convention Against Cybercrime* terhadap pengaturan tindak pidana siber di Indonesia serta rekomendasi untuk memperbaiki atau menyelaraskan hukum nasional dengan standar internasional.

Dengan metode penelitian yuridis normatif ini, diharapkan dapat diperoleh pemahaman yang mendalam tentang implikasi konvensi internasional terhadap sistem hukum Indonesia, khususnya dalam pengaturan tindak pidana siber.

4. HASIL DAN PEMBAHASAN

United Nations Convention Against Cybercrime atau disingkat UNODC lahir dari kekhawatiran masyarakat global terhadap kejahatan yang kian terus beradaptasi dengan teknologi. Konvensi ini diadopsi di New York oleh Majelis Umum PBB pada tanggal 24 Desember 2024 lalu melalui Resolusi 79/24, yang terdiri atas 9 Bab dan 71 Pasal. Konvensi ini merupakan perjanjian global pertama yang komprehensif dan memberikan negara-negara berbagai langkah yang harus dilakukan untuk mencegah dan memerangi kejahatan dunia maya.

Kerangka Kerja The United Nations Convention Against Cybercrime

Konvensi ini dirancang untuk memberikan standar internasional dalam pencegahan, penyidikan, dan penuntutan kejahatan siber dengan mengklasifikasikan berbagai bentuk kejahatan, seperti akses ilegal ke sistem komputer, gangguan data, penyalahgunaan perangkat, dan kejahatan berbasis konten. Standarisasi definisi ini penting agar negara-negara memiliki pemahaman yang sama dalam penanganannya. Selain itu, konvensi mendorong negara anggota untuk menyelaraskan undang-undang domestik mereka dengan standar internasional. Harmonisasi ini memungkinkan adanya pendekatan hukum yang seragam dan memperlancar kerjasama lintas negara. Konvensi juga menyediakan pedoman untuk teknik penyidikan digital, termasuk pengumpulan dan pelestarian bukti elektronik, yang penting karena kejahatan siber tidak jarang untuk melibatkan data yang mudah dimanipulasi atau dihapus.

Kerjasama internasional merupakan pilar utama dalam kerangka kerja konvensi ini. Mengingat kejahatan siber tidak mengenal batas geografis, kolaborasi antara negara menjadi kunci utama. Negara anggota didorong untuk berbagi informasi intelijen terkait ancaman siber secara real-time guna

P-ISSN : 2654-4946
https://doi.org/10.37817/ikraith-humaniora.v9i2 E-ISSN :2654-7538

mempercepat respons terhadap insiden siber dan mengidentifikasi pola serangan. Bantuan hukum timbal balik (Mutual Legal Assistance/MLA) juga difasilitasi dalam penyidikan lintas batas, termasuk ekstradisi pelaku dan penyitaan aset digital. Selain itu, konvensi mendorong pembentukan pusat respons dan koordinasi di tingkat regional dan global untuk mengatasi serangan siber secara kolektif.

Namun, terdapat berbagai tantangan dalam implementasi konvensi ini. Perbedaan kepentingan politik dan hukum di antara negara-negara, terutama terkait isu privasi, sensor, dan hak asasi manusia, menjadi kendala utama. Tidak semua negara memiliki infrastruktur teknologi dan sumber daya manusia yang memadai untuk menerapkan standar konvensi. Di samping itu, perkembangan teknologi yang pesat membuat ancaman siber terus berubah, sehingga konvensi harus bersifat fleksibel dan adaptif terhadap dinamika ini.

Tinjauan Tindak Pidana Siber Dalam Hukum Pidana Indonesia

Tahap kebijakan legislatif merupakan tahap yang paling strategis dilihat dari mengoperasionalkan sanksi pidana. Pada tahap ini dirumuskan garis kebijaksanaan sistem pidana dan pemidanaan yang sekaligus sebagai landasan legislatif bagi tahap-tahap berikutnya, yaitu tahap penerapan pidana oleh badan pengadilan dan tahap pelaksanaan pidana dan oleh aparat pelaksana pidana. Kebijakan legislatif dalam perumusan sistem pidana juga berperan penting dalam pengaturan tindak pidana siber di Indonesia. Hal ini karena pengaturan tindak pidana siber, baik dalam arti luas maupun sempit, harus disusun secara komprehensif agar selaras dengan sistem pemidanaan yang telah ditetapkan serta dapat diimplementasikan secara efektif pada tahap peradilan dan pelaksanaan pidana.

Pengaturan tindak pidana siber di Indonesia secara materil memiliki dua pengertian, yaitu dalam arti luas dan sempit. Dalam arti luas, tindak pidana siber mencakup semua tindak pidana yang melibatkan sarana atau sistem elektronik, termasuk tindak pidana konvensional dalam KUHP seperti pembunuhan atau perdagangan orang, selama menggunakan bantuan sistem elektronik. Selain itu, pengaturan ini juga mencakup tindak pidana yang diatur dalam Undang-Undang No. 3 Tahun 2011 Tentang Transfer Dana, Undang-Undang Perbankan, dan Undang-Undang No. 8 Tahun 2010 Tentang Tindak Pidana Pencucian Uang.

Dalam arti sempit, tindak pidana siber diatur melalui Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang telah diubah oleh Undang-Undang No. 19 Tahun 2016. Meskipun tidak memberikan definisi langsung tentang tindak pidana siber, UU ITE mengacu pada pembagian dalam *Convention on Cybercrimes*, yaitu tindak pidana yang melibatkan aktivitas ilegal seperti penyebaran konten tidak sah, perjudian, penghinaan, pemerasan, berita bohong, dan penyebaran kebencian berdasarkan SARA. Selain itu, UU ITE juga mencakup tindak pidana gangguan data dan sistem elektronik, pemalsuan dokumen elektronik, serta tindak pidana tambahan seperti pemberatan ancaman pidana.

UU ITE juga mengatur tindak pidana siber formil, khususnya dalam proses penyidikan. Berdasarkan Pasal 42 UU ITE, penyidikan dilakukan sesuai dengan ketentuan KUHAP dan UU ITE, dengan keunikan tertentu seperti pelibatan penyidik dari Kepolisian RI atau PPNS Kementerian Komunikasi dan Informatika. Penyidikan harus memperhatikan perlindungan privasi, kerahasiaan, dan kelancaran layanan

P-ISSN : 2654-4946
E-ISSN :2654-7538
https://doi.org/10.37817/ikraith-humaniora.v9i2

publik, termasuk aturan khusus dalam penggeledahan atau penyitaan sistem elektronik.

Proses penyidikan dan penuntutan tindak pidana siber melibatkan pelaporan korban kepada penyidik, yang kemudian melanjutkan kasus ke penuntut umum untuk dibawa ke pengadilan. Jika penyidik berasal dari PPNS, hasil penyidikan disampaikan melalui penyidik POLRI. Proses ini berlaku baik untuk tindak pidana siber dalam arti luas maupun sempit, seperti pada kasus perpajakan atau perbankan.

Selain UU ITE, dasar hukum penanganan tindak pidana siber di Indonesia juga mencakup peraturan pelaksana UU ITE, KUHAP, dan berbagai aturan teknis di masing-masing instansi penyidik. Pengaturan ini memastikan kelancaran proses hukum sambil tetap menjaga kepentingan publik dan keutuhan sistem elektronik.

Salah satu pendekatan dalam memahami tindak pidana siber adalah pembagian yang dilakukan oleh Sussan Brenner (2011). Ia mengelompokkan tindak pidana siber ke dalam tiga kategori utama:

1. Kejahatan di mana komputer menjadi target dari aktivitas kriminal.
2. Kejahatan di mana komputer digunakan sebagai alat untuk melakukan tindak pidana.
3. Kejahatan di mana penggunaan komputer merupakan aspek tambahan dalam pelaksanaan tindak pidana.

Dalam hukum pidana, suatu tindakan dapat dianggap sebagai kejahatan jika telah dirumuskan sebagai delik atau tindak pidana, yang berarti dapat dikenakan sanksi berdasarkan aturan hukum yang berlaku. Istilah "tindak pidana" atau *strafbaar feit* dalam hukum Belanda memiliki arti "dapat dihukum" (*strafbaar*) dan "kenyataan" (*feit*). Menurut ahli hukum seperti Moeljatno, *strafbaar feit* harus memenuhi unsur-unsur tertentu, termasuk larangan atau kewajiban yang diatur undang-undang, sifat melawan hukum, dan tanggung jawab pelaku atas perbuatannya. Menurutnya, perbuatan pidana adalah tindakan yang dilarang oleh peraturan hukum, di mana larangan tersebut disertai ancaman atau sanksi berupa hukuman pidana tertentu bagi siapa saja yang melanggarnya. Dengan demikian, tindak pidana dapat dianggap sebagai dasar utama untuk menjatuhkan hukuman kepada orang yang melakukan perbuatan tersebut.

Kejahatan siber dianggap sebagai bentuk kejahatan baru dalam ranah hukum pidana. Berbagai pasal dalam KUHP (misalnya Pasal 362 tentang pencurian, Pasal 378 tentang penipuan, Pasal 406 tentang *hacking*) sering digunakan untuk menjerat pelaku kejahatan siber. Namun, tantangan utama adalah bahwa KUHP belum dirancang untuk mencakup kejahatan yang bersifat lintas batas negara atau melibatkan teknologi digital, sehingga penegakan hukum seringkali membutuhkan penafsiran hukum yang luas.

Kejahatan siber di Indonesia diklasifikasikan menjadi beberapa bentuk, seperti pelanggaran kerahasiaan data, penipuan berbasis komputer, pelanggaran hak cipta, dan penyebaran konten ilegal (misalnya pornografi anak). Namun, banyak pasal dalam KUHP memuat sanksi yang ringan dan kurang relevan untuk menjerat kejahatan siber modern. Selain itu, penegakan hukum sering terhambat oleh asas legalitas yang ketat, yang hanya menerima interpretasi hukum berdasarkan undang-undang yang telah ada.

Implikasi terhadap UU Tindak Pidana di Indonesia

Indonesia telah memiliki beberapa peraturan perundang-undangan yang mengatur kejahatan dunia maya, terutama UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang telah diubah dengan UU Nomor 19 Tahun 2016. Namun, dengan adanya *The United Nations Convention Against*

https://doi.org/10.37817/ikraith-humaniora.v9i2
P-ISSN : 2654-4946
E-ISSN :2654-7538

Cybercrime, terdapat beberapa implikasi yang perlu dipertimbangkan untuk memperkuat kerangka hukum domestik. Yaitu, Melakukan harmonisasi definisi dan ruang lingkup kejahatan siber. Konvensi PBB menetapkan definisi dan ruang lingkup kejahatan siber yang lebih komprehensif. Hal ini memerlukan penyelarasan dalam UU ITE dan peraturan terkait lainnya untuk memastikan bahwa semua bentuk kejahatan siber yang diatur dalam konvensi juga tercakup dalam hukum domestik. Misalnya, kejahatan seperti pencurian data, serangan ransomware, dan penyalahgunaan teknologi kecerdasan buatan perlu diatur secara lebih spesifik.

Konvensi ini menuntut negara anggota untuk menyelaraskan hukum domestik mereka dengan standar internasional yang diatur dalam perjanjian tersebut. Dalam konteks Indonesia, UU ITE telah menjadi dasar hukum utama dalam menangani kejahatan dunia maya, seperti akses ilegal (*illegal access*), penyadapan ilegal (*illegal interception*), dan penyebaran konten pornografi anak. Namun, beberapa aspek dalam konvensi, seperti kerja sama lintas negara dalam pengumpulan bukti elektronik dan ekstradisi pelaku kejahatan siber, memerlukan penyesuaian lebih lanjut pada UU ITE maupun regulasi terkait lainnya. Sebagai contoh, konvensi ini mengatur bahwa negara anggota harus dapat meminta data elektronik dari penyedia layanan internet di negara lain selama penyelidikan terhadap kejahatan serius. Hal ini membutuhkan pembaruan mekanisme hukum di Indonesia agar sesuai dengan prosedur internasional yang cepat dan terpercaya.

Dan salah satu prinsip utama konvensi adalah kerja sama internasional dalam penegakan hukum. Indonesia perlu memperkuat mekanisme kerja sama kerja sama dalam hal ini perihal ekstradisi dengan negara lain, bantuan hukum timbal balik, dan pertukaran informasi intelijen. Namun hal tersebut memerlukan revisi terhadap UU yang sudah ada ataupun pembentukan UU baru yang mengatur kerja sama internasional dalam penanganan kejahatan siber. Konvensi ini juga menekankan pentingnya menjaga keseimbangan antara penegakan hukum dan perlindungan HAM, termasuk hak atas privasi. Indonesia perlu memastikan bahwa UU tindak pidana domestik tidak hanya efektif dalam memerangi kejahatan siber, tetapi juga menghormati hak-hak dasar warga negara. Hal ini dapat dilakukan dengan memperkuat pengawasan terhadap penggunaan data pribadi dan mencegah penyalahgunaan wewenang oleh aparat penegak hukum.

Implikasi lain dari konvensi ini adalah kebutuhan untuk meningkatkan kapasitas aparat penegak hukum, termasuk kepolisian, kejaksaan, dan lembaga peradilan, dalam menangani kasus-kasus kejahatan siber. Pelatihan dan pembaharuan kurikulum pendidikan hukum perlu dilakukan agar aparat penegak hukum dapat memahami kompleksitas kejahatan siber dan menerapkan hukum secara efektif. Konvensi PBB juga menyarankan agar sanksi untuk kejahatan siber bersifat proporsional dan efektif. Indonesia perlu meninjau kembali sanksi yang diatur dalam UU ITE dan peraturan terkait lainnya untuk memastikan bahwa sanksi tersebut dapat memberikan efek jera tanpa mengabaikan prinsip keadilan. Selain itu, mekanisme pemulihan bagi korban kejahatan siber juga perlu diperkuat.

Implementasi *The United Nations Convention Against Cybercrime* dalam hukum domestik Indonesia tidak lepas dari tantangan. Salah satunya adalah resistensi dari berbagai pihak yang mungkin menganggap bahwa harmonisasi hukum akan mengurangi kedaulatan nasional. Selain itu, keterbatasan

P-ISSN : 2654-4946
E-ISSN :2654-7538
https://doi.org/10.37817/ikraith-humaniora.v9i2

sumber daya, baik finansial maupun manusia, juga menjadi kendala dalam memperbarui sistem hukum dan meningkatkan kapasitas penegak hukum. Namun, di balik tantangan tersebut, terdapat peluang besar bagi Indonesia untuk memperkuat sistem hukumnya dan meningkatkan posisinya di mata internasional. Dengan mengadopsi standar global yang diatur dalam konvensi, Indonesia dapat membangun kepercayaan internasional, menarik investasi asing, dan melindungi warganya dari ancaman kejahatan siber yang semakin canggih.

The United Nations Convention Against Cybercrime tentunya akan memberikan dampak yang besar terhadap pengaturan tindak pidana siber di Indonesia. Konvensi ini bertujuan untuk mendorong harmonisasi hukum internasional, memperkuat kerjasama lintas negara, dan meningkatkan kapasitas kelembagaan negara anggota dalam menghadapi kejahatan siber yang kian kompleks dan bersifat transnasional. Bagi Indonesia, harmonisasi hukum nasional dengan standar internasional menjadi langkah penting. Konvensi ini mendorong penyesuaian peraturan domestik, khususnya Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Kitab Undang-Undang Hukum Pidana (KUHP), sehingga dapat menciptakan kerangka hukum yang relevan dan efektif dalam mengatasi kejahatan siber. Harmonisasi ini akan memastikan keseragaman standar hukum yang mendukung penegakan hukum yang lebih efisien.

Selain itu, penguatan kerjasama internasional merupakan aspek krusial dari konvensi ini. Indonesia dapat memperkuat hubungan dengan lembaga penegak hukum di negara lain untuk berbagi informasi, melakukan ekstradisi pelaku, serta mengadakan penyelidikan lintas yurisdiksi. Kerjasama semacam ini akan meningkatkan kemampuan Indonesia dalam menangani kejahatan siber yang melibatkan pelaku dan korban dari berbagai negara. Dalam konteks ini, penyesuaian prosedur penyidikan dan penuntutan juga menjadi hal yang esensial. Konvensi memberikan pedoman mengenai pengumpulan bukti digital dan perlindungan privasi yang harus diadopsi Indonesia. Penyesuaian ini mencakup revisi prosedur penggeledahan dan penyitaan sistem elektronik agar lebih sejalan dengan standar internasional dan mempercepat proses hukum.

Selanjutnya, klasifikasi dan definisi tindak pidana siber di Indonesia juga perlu diperjelas. Konvensi mengidentifikasi berbagai aktivitas ilegal seperti penipuan, pencurian identitas, dan serangan siber. Dengan mengadopsi klasifikasi ini, Indonesia akan memiliki landasan hukum yang lebih kokoh untuk menghadapi ancaman siber modern. Di sisi kelembagaan, peningkatan kapasitas institusi seperti BSSN dan PPATK harus dilakukan melalui pelatihan teknis dan pembangunan infrastruktur keamanan siber yang memadai.

Selanjutnya, klasifikasi dan definisi tindak pidana siber di Indonesia juga perlu diperjelas. Konvensi mengidentifikasi berbagai aktivitas ilegal seperti penipuan, pencurian identitas, dan serangan siber. Dengan mengadopsi klasifikasi ini, Indonesia akan memiliki landasan hukum yang lebih kokoh untuk menghadapi ancaman siber modern. Di sisi kelembagaan, peningkatan kapasitas institusi seperti BSSN dan PPATK harus dilakukan melalui pelatihan teknis dan pembangunan infrastruktur keamanan siber yang memadai.

Namun, implementasi konvensi ini tidak terlepas dari tantangan. Kesenjangan regulasi, keterbatasan kapasitas teknis,

P-ISSN : 2654-4946
https://doi.org/10.37817/ikraith-humaniora.v9i2 E-ISSN :2654-7538

dan perbedaan kepentingan sosial-politik dapat menghambat proses harmonisasi hukum. Oleh karena itu, Indonesia perlu merumuskan strategi holistik untuk mengatasi tantangan tersebut. Beberapa rekomendasi yang dapat dipertimbangkan antara lain adalah revisi UU ITE untuk mengakomodasi ketentuan konvensi, pelaksanaan program pendidikan dan pelatihan bagi aparat penegak hukum, serta penguatan kerjasama dengan sektor swasta dalam membangun infrastruktur pertahanan siber.

Secara keseluruhan, The United Nations Convention Against Cybercrime berpotensi memperkuat kerangka hukum Indonesia dalam menangani tindak pidana siber. Harmonisasi hukum nasional dengan standar internasional, penguatan kerjasama lintas negara, serta peningkatan kapasitas kelembagaan merupakan langkah-langkah penting yang harus dilakukan. Dengan pendekatan yang komprehensif dan berkelanjutan, Indonesia dapat mengadopsi strategi yang lebih efektif dalam menghadapi dinamika kejahatan siber di era digital saat ini

5. KESIMPULAN

Sebagaimana Konvensi *The United Nations Convention Against Cybercrime* telah memberikan kerangka hukum internasional yang komprehensif untuk menangani kejahatan siber, sehingga konvensi ini membawa implikasi penting bagi Indonesia, khususnya dalam harmonisasi hukum nasional seperti UU ITE dan KUHP agar dapat sesuai dengan standar Internasional. Harmonisasi ini dapat dianggap krusial untuk memastikan penegakan hukum yang efektif dan mengurangi kesenjangan regulasi. Selain itu, kerjasama internasional menjadi pilar utama dalam menghadapi kejahatan siber. Indonesia perlu memperkuat hubungan dengan lembaga penegak hukum internasional melalui mekanisme ekstradisi, pertukaran informasi intelijen, dan penyelidikan lintas yurisdiksi. Penguatan kapasitas kelembagaan, seperti BSSN dan PPATK, menjadi hal penting yang harus dilakukan, baik melalui peningkatan infrastruktur maupun pelatihan teknis. Namun, implementasi konvensi ini tidak terlepas dari tantangan, seperti kesenjangan regulasi, keterbatasan teknis, dan perbedaan kepentingan sosial-politik. Oleh karena itu, strategi holistik diperlukan untuk mengatasi hambatan-hambatan tersebut.

Untuk menghadapi tantangan tersebut, beberapa saran dapat dipertimbangkan. Pertama, dengan melakukan revisi terhadap UU ITE dan peraturan terkait lainnya diperlukan agar mengakomodasi definisi dan ruang lingkup kejahatan siber yang diatur dalam Konvensi PBB, termasuk pengaturan mengenai pencurian data, serangan ransomware, dan penyalahgunaan teknologi kecerdasan buatan. Kedua, penguatan mekanisme kerjasama internasional perlu dibangun, seperti perjanjian ekstradisi dan bantuan hukum timbal balik, untuk mempercepat proses penegakan hukum terhadap kejahatan siber lintas negara. Ketiga, perlindungan hak asasi manusia, khususnya hak atas privasi, harus dipastikan dengan memperkuat regulasi terkait perlindungan data pribadi dan mencegah penyalahgunaan wewenang oleh aparat penegak hukum. Keempat, peningkatan kapasitas aparat penegak hukum melalui pelatihan dan pembaharuan kurikulum pendidikan hukum sangat penting agar mereka dapat memahami dan menangani kasus kejahatan siber yang kompleks. Kelima, keterlibatan sektor swasta dalam membangun infrastruktur pertahanan siber serta peningkatan kesadaran

masyarakat terhadap kejahatan siber juga harus didorong untuk menciptakan ekosistem keamanan siber yang tangguh. Terakhir, penyesuaian sanksi terhadap kejahatan siber harus proporsional dan memberikan efek jera, sementara mekanisme pemulihan bagi korban kejahatan siber perlu diperkuat untuk memastikan keadilan dan perlindungan bagi masyarakat. Dengan mengimplementasikan saran-saran tersebut, Indonesia diharapkan dapat memperkuat kerangka hukum dan kelembagaan dalam menghadapi tantangan kejahatan siber di era digital, sekaligus memperkuat posisinya di kancah internasional.

6. UCAPAN TERIMA KASIH

Kami, segenap penulis, mengucapkan terima kasih yang sebesar-besarnya kepada Bapak Prof. Dr. Agus Budianto, S.H., M.H. dan Bapak Pietro Grassio, S.H., M.Krim. atas bimbingan dan ilmu yang telah diberikan selama perkuliahan Kejahatan Dunia Maya berlangsung. Artikel jurnal ini merupakan salah satu bentuk konkret dari hasil pembelajaran yang kami peroleh selama satu semester. Kami berharap, ilmu dan nilai-nilai yang telah Bapak tanamkan dapat kami terapkan dalam kehidupan nyata dan kontribusikan bagi pengembangan ilmu hukum di masa mendatang.

DAFTAR PUSTAKA

Anshori. (2021). Cyber crime in a criminology perspective. *International Journal of Sociology, Policy and Law*, 2(3).

Arief, B. N. (1996). *Kebijakan legislatif dalam penanggulangan kejahatan dengan pidana penjara*. Badan Penerbit Universitas Diponegoro.

Brenner, S. W. (2001). Defining cybercrime: A review of state and federal law. In *Cybercrime: The investigation, prosecution and defense of a computer-related crime.*

Efendi, J., & Rijadi, P. (2016). *Metode penelitian hukum normatif dan empiris* (Edisi Kedua). Kencana.

Ketaren, E. (2016). Cybercrime, cyber space, dan cyber law. *Jurnal Hukum STMIK TIME*, *5*, 36.

Putra, A. K. (2014). Harmonisasi konvensi cybercrime dalam hukum nasional. https://media.neliti.com/media/publications/43297-ID-harmonisasi-konvensi-cyber-crime-dalam-hukum-nasional.pdf

Marita, L. S. (2015). Cyber crime dan penerapan cyber law dalam pemberantasan cyber law di Indonesia. https://ejournal.bsi.ac.id/ejurnal/index.php/cakrawala/article/view/4901/2845

Moeljatno. (2002). *Asas-asas hukum pidana* (Buku 7). Rineka Cipta.

Mukhsin, F. R., Suci, A. T., Nandrini, F. T., Rofiq, A., & Khoirurozy, O. (n.d.). The review of cybercrime case handling based on Indonesian jurisdiction and international law. *International Journal of Law and Legal Ethics*, *12*, 23–36.

Sefriani. (2022). *Hukum internasional: Suatu pengantar*. Rajawali Pers.

Putri, D., Ningrum, S., & Robekha, J. (2023). Analisa yuridis dalam kasus kejahatan siber terhadap internet banking di Indonesia. *PESHUM: Jurnal Pendidikan, Sosial dan Humaniora*, *2*(4).

Rais, M. A., & Songkarn, P. (2022). Hacker and the threat for national security: Challenges in law

enforcement. *Indonesian Journal of Counter Terrorism and National Security*, *1*(1), 45–66. https://doi.org/10.15294/ijctns.v1i1.56728

Sitompul, J. (2012). *Cyberspace, cybercrimes, cyberlaw: Tinjauan aspek hukum pidana*. PT Tatanusa.

Widayanti, P. W. (2022). Tindak pidana pencurian data nasabah dalam bidang perbankan sebagai cyber crime. *Legacy: Jurnal Hukum dan Perundang-Undangan*, *2*(2).