

CYBER SOVEREIGNTY AND CYBERCRIME REGULATION: A COMPARATIVE STUDY OF INDONESIA'S ITE LAW AND MALAYSIA'S COMPUTER CRIMES ACT

A.HAIDAR MUHAMMAD BAGIR

Universitas Prima Nusantara Bukittinggi

Abstract: *Based on a comparative analysis of the development of cybercrime regulations in Indonesia and Malaysia, it can be concluded that both countries recognize the urgency of strengthening cyber sovereignty as part of protecting national interests in the digital era. However, the normative and philosophical approaches used show quite fundamental differences. Indonesia, through the 2008 Electronic Information and Transactions (ITE) Law, its 2016 revision, and the second amendment in 2024 (Law No. 1 of 2024), developed a broad and comprehensive regulatory model. These regulations not only regulate technical acts of cybercrime such as illegal access and data manipulation, but also encompass dimensions of digital content, including insults, hate speech, and the distribution of prohibited information. The 2024 revision demonstrates the country's efforts to clarify norms, align with the new Criminal Code, and respond to developments in digital technology. However, the main challenges remain: consistent law enforcement, the potential for multiple interpretations of norms, and the need to improve the capacity of law enforcement officers. In contrast, Malaysia, through the Computer Crimes Act 1997 (Act 563), initially adopted a more technical and limited approach, focusing on illegal access and misuse of computer systems. However, recent developments through the Cyber Security Act 2024 indicate a paradigm shift toward a more structural and risk-management-based approach, particularly in protecting the nation's critical information infrastructure. These reforms demonstrate Malaysia's focus on strengthening cybersecurity systems and risk governance, rather than solely criminalizing digital content.*

Keywords: *Cybercrime, Indonesia, Malaysia.*

Abstrak: Berdasarkan analisis komparatif terhadap perkembangan regulasi cybercrime di Indonesia dan Malaysia, dapat disimpulkan bahwa kedua negara sama-sama mengakui urgensi penguatan kedaulatan siber (cyber sovereignty) sebagai bagian dari perlindungan kepentingan nasional di era digital. Namun, pendekatan normatif dan filosofis yang digunakan menunjukkan perbedaan yang cukup mendasar. Indonesia melalui UU ITE 2008, revisi 2016, dan perubahan kedua tahun 2024 (UU No. 1 Tahun 2024) mengembangkan model regulasi yang bersifat luas dan komprehensif. Regulasi tersebut tidak hanya mengatur tindakan teknis kejahatan siber seperti akses ilegal dan manipulasi data, tetapi juga mencakup dimensi konten digital, termasuk penghinaan, ujaran kebencian, dan distribusi informasi terlarang. Revisi 2024 menunjukkan upaya negara untuk memperjelas norma, menyesuaikan dengan KUHP baru, serta merespons perkembangan teknologi digital. Meskipun demikian, tantangan utama tetap terletak pada konsistensi penegakan hukum, potensi multitafsir norma, dan kebutuhan peningkatan kapasitas aparat penegak hukum. Sebaliknya, Malaysia melalui Computer Crimes Act 1997 (Akta 563) pada awalnya mengadopsi pendekatan yang lebih teknis dan terbatas, dengan fokus pada akses ilegal dan penyalahgunaan sistem komputer. Namun, perkembangan terbaru melalui Cyber Security Act 2024 menunjukkan pergeseran paradigma menuju pendekatan yang lebih struktural dan berbasis manajemen risiko, terutama dalam perlindungan infrastruktur informasi kritical nasional. Reformasi ini memperlihatkan orientasi Malaysia pada penguatan sistem keamanan siber dan tata kelola risiko, bukan semata-mata pada kriminalisasi konten digital.

Kata Kunci: Cybercrime, Indonesia, Malaysia.

A. Pendahuluan

Perkembangan teknologi informasi dan komunikasi telah membawa revolusi besar dalam interaksi sosial, ekonomi, serta politik di berbagai negara. Internet sebagai ruang siber yang bersifat *borderless* (tanpa batas negara secara fisik) menghadirkan tantangan baru terhadap konsep kedaulatan negara (*state sovereignty*) yang selama ini berbasis wilayah teritorial. Dalam konteks ini, muncul konsep *cyber sovereignty*, yaitu hak dan kewenangan suatu negara untuk mengatur serta mengendalikan ruang digital di wilayah yurisdiksinya guna melindungi kepentingan nasional dan keamanan digitalnya dalam menghadapi ancaman siber yang semakin kompleks.

Indonesia dan Malaysia adalah dua negara berkembang di Asia Tenggara dengan penetrasi internet dan penggunaan digital yang tinggi. Di Indonesia, regulasi utama dalam mengatur aktivitas siber adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Undang-undang ITE) yang telah mengalami beberapa perubahan untuk memperluas ruang lingkup penanganan kejahatan siber. Regulasi ini mencakup bukan hanya akses ilegal dan gangguan terhadap sistem, tetapi juga pengaturan konten digital dan ekspresi publik.

Sementara itu, Malaysia menerapkan *Computer Crimes Act* 1997 sebagai instrumen hukum utama untuk menangani cybercrime, yang menitikberatkan pada tindak pidana berkaitan dengan penyalahgunaan komputer seperti akses ilegal, peretasan, dan perusakan data. Meskipun undang-undang ini relatif lebih tua, kajian akademik menunjukkan bahwa struktur hukum ini masih dipakai sebagai payung hukum untuk mengatur berbagai kejahatan berbasis teknologi di Malaysia.

Pertumbuhan tajam kejahatan siber seperti *phishing*, penipuan digital, dan serangan *ransomware* menuntut respons hukum yang efektif di kedua negara. Studi perbandingan hukum siber di ASEAN menunjukkan bahwa Indonesia memiliki ruang lingkup regulasi yang lebih luas dibandingkan negara tetangga dalam beberapa aspek tata kelola perlindungan digital, namun juga berpotensi menimbulkan tafsir yang beragam dalam praktik penegakan hukum.

Perbedaan pendekatan antara Undang-undang ITE dan *Computer Crimes Act* Malaysia mencerminkan variasi dalam pengimplementasian konsep *cyber sovereignty* di masing-masing yurisdiksi. Perbandingan semacam ini diperlukan untuk memahami kekuatan dan kelemahan masing-masing sistem regulasi serta implikasinya dalam konteks penegakan hukum dan perlindungan hak dasar warga negara di ruang siber. Studi ini juga relevan dalam upaya harmonisasi hukum siber di kawasan ASEAN, menyusul meningkatnya kebutuhan untuk kerja sama lintas negara dalam menghadapi kejahatan siber yang bersifat transnasional. Untuk kepentingan inilah kertas kerja ini dibuat.

B. Metodologi Penelitian

Penelitian ini merupakan penelitian hukum normatif dengan fokus pada kajian norma, aturan, dan sistem hukum yang berlaku dalam pengaturan kejahatan siber (*cybercrime*) dan konsep *cyber sovereignty* di Indonesia dan Malaysia. Pendekatan normatif dipilih karena penelitian menitikberatkan pada penelaahan terhadap sumber hukum tertulis serta literatur ilmiah bidang hukum siber. Penelitian semacam ini umum digunakan dalam kajian hukum komparatif antarnegara di bidang teknologi dan keamanan informasi. Penelitian ini menggunakan beberapa pendekatan, yaitu: Pendekatan Yuridis-Normatif, digunakan untuk menganalisis ketentuan peraturan perundang-undangan terkait cybercrime dan *cyber sovereignty* di kedua negara serta untuk mengidentifikasi asas hukum yang mendasari pembentukannya. Pendekatan Komparatif, mengkaji dan membandingkan regulasi serta implementasi hukum di Indonesia dan Malaysia, khususnya mengidentifikasi persamaan, perbedaan, dan implikasi hukum dari masing-masing sistem.

Pendekatan Literatur dan Studi Kepustakaan, menelaah artikel ilmiah, buku, serta sumber akademik lainnya yang relevan dengan hukum siber dan penegakan cybercrime, termasuk laporan studi kasus dan analisis akademik dalam lima tahun terakhir. Pendekatan campuran ini memungkinkan penelitian memahami fenomena hukum secara holistik serta memberikan gambaran perbandingan yang komprehensif.

C. Hasil dan Pembahasan

Perkembangan Regulasi Cybercrime di Indonesia

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik merupakan dasar hukum awal Indonesia dalam mengatur aktivitas elektronik dan tindakan yang melibatkan teknologi informasi, termasuk berbagai bentuk kejahatan siber. Di tingkat awal, Undang-undang ini sering dikritik karena sejumlah pasal multitafsir yang berpotensi digunakan untuk kriminalisasi yang luas terhadap aktivitas online masyarakat.

Revisi Undang-Undang Nomor 19 Tahun 2016 memperbaiki beberapa pasal Undang-undang ITE 2008, namun masih meninggalkan ruang interpretasi luas pada pasal-pasal seperti penghinaan melalui media elektronik yang menciptakan kontroversi dalam praktik penegakan hukum.

Pemerintah kemudian mengesahkan Undang-undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Undang-undang Nomor 11 Tahun 2008, yang fokus pada pembaruan struktur pidana, penyesuaian ketentuan dengan KUHP baru, serta pengaturan lain terkait penyelenggaraan sistem elektronik guna menanggapi teknologi dan modus kejahatan siber yang berkembang.

- 1) Ruang lingkup diperluas untuk mencakup cyber-dependent dan cyber-enabled offenses.
- 2) Berupaya menyeimbangkan perlindungan terhadap kebebasan berekspresi dan penanggulangan kejahatan siber.
- 3) Penelitian terbaru menunjukkan meskipun regulasi ini telah memperjelas beberapa ketentuan dan menurunkan beberapa jenis cybercrime seperti phishing, tantangan tetap signifikan dalam implementasi.

Perkembangan Regulasi Cybercrime di Malaysia

Computer Crimes Act 1997 (Akta 563). Malaysia menggunakan Akta 563 sebagai dasar pidana untuk kejahatan yang berkaitan dengan komputer dan sistem informasi. Akta ini mengatur tindakan seperti akses tidak sah dan pengubahan data dalam komputer, namun dianggap tidak relevan terhadap ancaman siber modern.

Cyber Security Act 2024 (Act 854). Malaysia memberlakukan Cyber Security Act 2024, fokus pada perlindungan infrastruktur kritis dan kewajiban audit keamanan siber bagi penyelenggara layanan, sekaligus memperluas tindakan kriminal yang berkaitan dengan ancaman siber.

Cybercrime Bill 2026 (Proposal). Rancangan undang-undang ini diharapkan menggantikan Computer Crimes Act 1997, menangani kejahatan siber modern termasuk deepfakes, penipuan online, dan kejahatan berbasis teknologi baru.

Perbandingan Substantif : Indonesia vs Malaysia

Dimensi Regulasi	Indonesia (UU ITE 2024)	Malaysia (Akta 563 & Cyber Security Act2024 / Cybercrime Bill)
Ruang Lingkup	Komprehensif (konten & tindakan)	Lebih teknis pada tindakan komputer; Cyber Security Act fokus pada infrastruktur

Kejahatan Siber		& mitigasi risiko
Pembaruan Legislasi	Telah direvisi 2024 untuk relevansi teknologi & KUHP baru	Sedang mengalami transisi dari Akta 563 ke Cybercrime Bill
Pendekatan Penegakan	Menyasar baik perbuatan siber maupun konten	Campuran penanganan risiko siber dan tindakan kriminal berbasis teknologi

Temuan Utama

- 1) Kedua negara mengakui ancaman kejahatan siber sebagai masalah hukum nasional, namun dengan pendekatan berbeda.
- 2) Undang-undang ITE 2024 memperjelas aturan pidana siber di Indonesia, namun tantangan implementasi masih signifikan.
- 3) Malaysia mengarah pada pembentukan kerangka hukum modern melalui Cyber Security Act 2024 dan Cybercrime Bill.

Cyber Sovereignty dalam Regulasi Nasional

Cyber sovereignty menjadi konsep penting di era digital karena kedaulatan negara di ruang siber mencerminkan kontrol atas data, warga negara, teknologi, dan nilai-nilai hukum nasional. Di Indonesia, konsep ini terlihat melalui perluasan ruang lingkup pengaturan aktivitas digital dalam Undang-undang ITE, yang tidak hanya menangani kejahatan teknis tetapi juga aspek konten online seperti ujaran kebencian dan penyebaran informasi yang dilarang.

Indonesia memperluas ruang lingkup regulasi dari Undang-undang ITE 2008 melalui Undang-undang ITE 2016 dan revisi kedua tahun 2024 (*Undang-undang No. 1/2024*) yang memasukkan pasal-pasal baru terkait layanan elektronik modern dan memperjelas batasan hukum dalam ranah siber, termasuk pasal yang menyentuh isu kebebasan berekspresi serta pidana atas penggunaan teknologi digital tertentu. Sementara itu, Malaysia dengan Computer Crimes Act 1997 (Akta 563) awalnya hanya menargetkan *misuse of computers* (akses ilegal, manipulasi data) tanpa mengatur dimensi konten secara sosial atau nilai seperti kebebasan berekspresi secara eksplisit.

Namun perkembangan regulasi Malaysia melalui Cyber Security Act 2024 menunjukkan pergeseran fokus negara itu dari sekadar kriminalisasi tindakan teknis ke pendekatan yang lebih komprehensif terhadap kerentanan dan ancaman infrastruktur elektronik negara. Act ini menempatkan Cyber Security sebagai landasan untuk melindungi sistem kritikal dan memperkenalkan pendekatan mitigasi risiko serta kewajiban pelaporan insiden siber demi menjaga keutuhan sistem digital nasional. Analisis akademik menunjukkan bahwa pergeseran ini mencerminkan upaya Malaysia untuk menyeimbangkan kebutuhan kedaulatan siber dengan kerangka hukum yang lebih bersifat teknis dan struktural daripada sekadar pidana konten.

Efektivitas Penegakan dan Kompleksitas Hukum

Tantangan penegakan hukum dalam konteks cybercrime sering muncul karena sifat siber yang lintas batas dan cepat berubah. Di Indonesia, sejumlah studi menunjukkan kompleksitas hukum dalam menangani kejahatan siber karena cakupan UU ITE yang luas dan beberapa pasal yang masih multitafsir, sehingga menimbulkan tantangan implementasi praktis untuk aparat penegak hukum. Kajian norma dan legislasi juga menyatakan bahwa keterbatasan sumber daya manusia dan kapasitas teknis di Indonesia berpengaruh pada efektivitas penegakan hukum siber.

Malaysia, dengan Computer Crimes Act 1997, menghadapi kritik karena undang-undang ini *tidak berkembang secara signifikan* sejak pengesahannya dan tidak

sepenuhnya mampu menangani modus siber modern; namun langkah pembaharuan melalui Cyber Security Act 2024 dianggap langkah maju untuk merespon dinamika ancaman siber kontemporer, meskipun masih perlu waktu untuk melihat dampaknya terhadap efektivitas penegakan hukum pidana siber secara menyeluruh. Studi banding menunjukkan bahwa sistem hukum yang terlalu fokus pada pidana tradisional dapat kurang responsif terhadap ancaman siber kontemporer yang seringkali memerlukan pendekatan teknis, koordinasi lembaga, dan respon cepat.

Perbedaan filosofi antara kedua sistem hukum ini terlihat jelas dari substansi regulasi: Pendekatan Indonesia: 1) Konten & Tindakan: Regulasi cybercrime di Indonesia mencakup baik aspek konten (mis. ujaran kebencian) maupun tindakan (mis. akses ilegal); 2) Pidana & Kontrol sosial: UU ITE 2024 menggabungkan aspek pidana dengan kontrol sosial di ruang digital; dan 3) Pengaturan luas: Menangani transaksi elektronik, perlindungan data, serta penyalahgunaan teknologi dalam satu kerangka hukum. Pendekatan Malaysia: 1) Fokus Sistem & Infrastruktur: Cyber Security Act 2024 menitikberatkan perlindungan terhadap National Critical Information Infrastructure dan mitigasi risiko siber struktural, 2) Teknis & Manajemen Risiko: Menata kewajiban pelaporan insiden siber dan pengelolaan keamanan siber secara administrasi teknis, dan 3) Perkembangan legislatif bertahap: Transisi dari Computer Crimes Act 1997 ke kerangka hukum yang lebih modern menunjukkan evolusi bertahap dalam peraturan siber. Dari sisi teoritis, perbedaan ini merupakan refleksi pilihan politik hukum masing-masing negara dalam memadukan keamanan nasional dan hak individu dalam ruang siber.

Mengingat ASEAN merupakan kawasan dengan tingkat penetrasi internet yang terus meningkat dan kejahatan siber lintas batas yang serius, perbedaan dalam filosofi hukum dan substansi regulasi seperti di Indonesia dan Malaysia menimbulkan tantangan dalam harmonisasi regional. Penelitian normatif menunjukkan bahwa meskipun Indonesia telah memiliki kerangka hukum yang kuat melalui UU ITE, masih terdapat kelemahan dalam penegakan hukum, harmonisasi regulasi, dan perlindungan data pribadi jika dibandingkan dengan praktik terbaik di kawasan ASEAN. Isu harmonisasi hukum ini penting dalam konteks cyber sovereignty regional, karena kejahatan siber seringkali tidak menghormati batas negara.

D. Penutup

Berdasarkan analisis komparatif terhadap perkembangan regulasi cybercrime di Indonesia dan Malaysia, dapat disimpulkan bahwa kedua negara sama-sama mengakui urgensi penguatan kedaulatan siber (cyber sovereignty) sebagai bagian dari perlindungan kepentingan nasional di era digital. Namun, pendekatan normatif dan filosofis yang digunakan menunjukkan perbedaan yang cukup mendasar. Indonesia melalui UU ITE 2008, revisi 2016, dan perubahan kedua tahun 2024 (UU No. 1 Tahun 2024) mengembangkan model regulasi yang bersifat luas dan komprehensif. Regulasi tersebut tidak hanya mengatur tindakan teknis kejahatan siber seperti akses ilegal dan manipulasi data, tetapi juga mencakup dimensi konten digital, termasuk penghinaan, ujaran kebencian, dan distribusi informasi terlarang. Revisi 2024 menunjukkan upaya negara untuk memperjelas norma, menyesuaikan dengan KUHP baru, serta merespons perkembangan teknologi digital. Meskipun demikian, tantangan utama tetap terletak pada konsistensi penegakan hukum, potensi multitafsir norma, dan kebutuhan peningkatan kapasitas aparat penegak hukum. Sebaliknya, Malaysia melalui Computer Crimes Act 1997 (Akta 563) pada awalnya mengadopsi pendekatan yang lebih teknis dan terbatas, dengan fokus pada akses ilegal dan penyalahgunaan sistem komputer. Namun, perkembangan terbaru melalui Cyber Security Act 2024 menunjukkan pergeseran paradigma menuju pendekatan yang lebih struktural dan berbasis manajemen risiko, terutama dalam perlindungan infrastruktur

informasi kritikal nasional. Reformasi ini memperlihatkan orientasi Malaysia pada penguatan sistem keamanan siber dan tata kelola risiko, bukan semata-mata pada kriminalisasi konten digital.

Daftar Pustaka

- N. Rahmawati & A. W. Sanjaya, *Comparative Law Between Indonesia and Malaysia in the Resolution of Cyberbullying Crimes, Supremasi Hukum*
- Adnasohn Aqilla Respati, “Reformulasi Undang-Undang ITE terhadap Artificial Intelligence Dibandingkan dengan Uni Eropa dan China AI Act Regulation”. *Jurnal USM Law Review Vol 7 No 3 Tahun*
- Andi Cakra Cindrapole & Arianty Anggraeny Mangarengi, *Dilema Yurisdiksi di Ruang Siber: Tantangan dan Strategi Penegakan Keamanan Lintas Negara, Judicatum: Jurnal Dimensi Catra Hukum* 3, no. 1
- Between Regulation and Reality: Reflections on State Responsibility and the Effectiveness of Criminal Law in Dealing with Cybercrime in Indonesia*, Al-Risalah Jurnal Ilmu Syariah dan Hukum (2025).
- Clara Ignatia Tobing et al., *Globalisasi Digital dan Cybercrime: Tantangan Hukum dalam Menghadapi Kejahatan Siber Lintas Batas, Jurnal Hukum Sasana* 10, no. 2
- Gapenas Bureaucracy Journal, “Undang-undang ITE 2016 dan Kontroversi Pasal-Pasal Multitafsir”
- Harian Metro, “Computer Crimes Act 1997: Tantangan Menghadapi Ancaman Siber Modern”
- idho Duha, *Punishment for Cybercrime: A Major Challenge in Modern Legal Systems, Verdict: Journal of Law Science*
- Kompas.com, “UU ITE 2024: Revisi Kedua Memperjelas Cybercrime”, 5 Januari 2024,
- L. Sulastris & R. Cartin-Pecson, *Dynamics of the Electronic Transaction Information Law in Tackling Cybercrime in Indonesia, Hermeneutika : Jurnal Ilmu Hukum*
- Lusia Sulastris & Rowela Cartin-Pecson, *Dynamics of the Electronic Transaction Information Law in Tackling Cybercrime in Indonesia, Hermeneutika: Jurnal Ilmu Hukum*
- M. T. Rusydi, *Perbandingan Hukum Siber Indonesia dengan Negara ASEAN, Jurnal Kolaboratif Sains*
- Maudy A. Djibu, *Transformasi Digital dan Keamanan Siber: Upaya Penanggulangan Kejahatan di Era Teknologi di Indonesia, Judge: Jurnal Hukum* 6, no. 1
- Mohammad Daud, *Issues and Challenges in Addressing Cybercrime in Malaysia*
- Muh. Chaerul Anwar, Andi Dewi Pratiwi, Muh. Arfhani Ichsan. “Efektivitas Hukum Uu Nomor 1 Tahun 2024 Dalam Penanggulangan Kejahatan Cybercrime Di Indonesia”. Vol 18
- Muhammad Taufik Rusydi, *Perbandingan Hukum Siber Indonesia dengan Negara ASEAN: Suatu Kajian Normatif, Jurnal Kolaboratif Sains* 8, no. 1
- Muhammad Taufik Rusydi, *Perbandingan Hukum Siber Indonesia dengan Negara ASEAN*
- Munir, “Kajian Pasal 27 A UU No. 1 Tahun 2024”, *Jurnal Hukum Perubahan Kedua UU No. 11 Tahun 2008 tentang ITE, JDIH Kemenkoinfra*
- PwC Malaysia, “Cyber Security Act 2024: Overview and Implications”,
- Rusydi, “Perbandingan Hukum Siber Indonesia dengan Negara ASEAN”
- The Salient Features of the Cyber Security Act 2024, Malaysian Bar Journal*
- The Sun Malaysia, “New Cybercrime Bill to Replace Outdated Computer Crimes Act”