SCIENTIA JOURNAL Jurnal Ilmiah Mahasiswa
E-issn:2714-593X

PERKEMBANGAN HUKUM DI DUNIA DIGITAL: EVOLUSI HUKUM KEJAHATAN DUNIA MAYA

Dina Melina [1], **Diki Zukriadi**[2]
[1]**Mahasiswa Program Studi Ilmu Hukum, Universitas Putera Batam**
[2]**Dosen Program Studi Ilmu Hukum,Universitas Putera Batam**
Email : Pb200710019upbatatam.ac.id

ABSTRACT

Penelitian ini mengeksplorasi evolusi hukum cybercrime dalam menghadapi perkembangan teknologi informasi dan komunikasi (TIK) selama beberapa dekade terakhir. Perkembangan teknologi digital telah memberikan manfaat yang tak terhitung jumlahnya, namun juga memunculkan ancaman yang semakin kompleks dalam bentuk serangan siber dan cybercrime. Tujuan penelitian ini adalah untuk menyelidiki bagaimana hukum cybercrime telah berkembang dalam menanggapi perubahan TIK dan bagaimana perkembangan ini telah memengaruhi efektivitas penegakan hukum cybercrime. Penelitian ini juga menganalisis peran kerja sama lintas batas dalam penegakan hukum cybercrime dan bagaimana perkembangan dalam hukum internasional telah memengaruhi kemampuan negara-negara untuk menangani ancaman cybercrime yang bersifat global. Hasil penelitian menunjukkan bahwa evolusi hukum cybercrime mencakup pembentukan undang-undang cybercrime yang lebih spesifik dan perlindungan data pribadi yang lebih kuat. Kerja sama lintas batas memainkan peran penting dalam penegakan hukum cybercrime, termasuk pertukaran informasi, penuntutan bersama, pembekuan aset, dan ekstradisi. Perkembangan dalam hukum internasional, seperti Konvensi Budapest dan Regulasi Umum Perlindungan Data (GDPR), telah memberikan dasar hukum yang diperlukan untuk kerja sama lintas batas yang lebih efektif. Namun, tantangan tetap ada, termasuk perbedaan hukum dan yurisdiksi antarnegara yang seringkali menghambat upaya penegakan hukum. Oleh karena itu, peningkatan kerja sama internasional dan upaya untuk mengatasi hambatan ini menjadi sangat penting dalam menjaga keamanan dan privasi di era digital yang terus berkembang.

Keywords**:** Hukum Cybercrime, Teknologi Informasi dan Komunikasi, Kerja Sama Lintas Batas, Perlindungan Data, Penegakan Hukum, Ancaman Cybercrime.

PENDAHULUAN

Dunia digital telah mengalami perkembangan yang pesat selama beberapa dekade terakhir. Revolusi teknologi informasi dan komunikasi (TIK) telah membentuk cara kita berkomunikasi, bekerja, berbelanja, dan bahkan bermain. Sementara itu, keuntungan dan inovasi yang tak terhitung jumlahnya yang ditawarkan oleh teknologi digital juga membawa tantangan serius dalam bentuk kejahatan dunia maya atau yang lebih dikenal sebagai cybercrime. Kejahatan seperti pencurian data, peretasan, penipuan online, penyebaran malware, dan pelanggaran privasi telah menjadi ancaman yang semakin meresahkan.

Perkembangan yang sangat pesat ini telah memaksa sistem hukum di seluruh dunia untuk beradaptasi dengan kebutuhan baru dalam melindungi masyarakat dari ancaman cybercrime yang semakin canggih. Oleh karena itu, studi mengenai evolusi

hukum cybercrime dalam perkembangan hukum dalam dunia digital sangat relevan dan penting.

Pada awalnya, undang-undang yang berkaitan dengan kejahatan di dunia maya cenderung terbatas dan tidak memadai. Hukum yang ada pada saat itu seringkali tidak dapat menangani kejahatan-kejahatan yang memanfaatkan karakteristik khusus dari teknologi digital, seperti anonimitas dan cakupan global. Oleh karena itu, hukum cybercrime pertama kali dihadirkan sebagai respons terhadap perkembangan teknologi.

Evolusi hukum cybercrime mencakup berbagai aspek yang harus dipahami. Salah satunya adalah perubahan dalam pendekatan hukum terhadap kejahatan dunia maya. Awalnya, undang-undang cenderung berfokus pada penegakan hukum yang lebih konvensional. Namun, dengan meningkatnya frekuensi dan kerumitan serangan cyber, hukum beradaptasi untuk memberikan alat dan wewenang yang lebih kuat bagi penegak hukum dan kebijakan keamanan siber. Selain itu, perlindungan hak individu dan privasi juga menjadi isu kunci dalam evolusi hukum cybercrime. Dalam upaya untuk melindungi warga dari penyebaran data pribadi yang tidak sah dan penyalahgunaan informasi pribadi, hukum telah berkembang untuk menciptakan kerangka kerja perlindungan data yang lebih kuat. Ini termasuk undang-undang perlindungan data, aturan tentang pengungkapan pelanggaran data, dan pedoman pengelolaan data.

Perkembangan lain yang relevan dalam evolusi hukum cybercrime adalah kerja sama lintas batas. Kejahatan cyber sering kali menyeberang negara dan yurisdiksi. Oleh karena itu, ada kebutuhan untuk kerja sama internasional dalam menangani kejahatan tersebut. Beberapa perjanjian dan konvensi internasional telah dibuat untuk memfasilitasi kerja sama antar negara dalam penegakan hukum cybercrime.

Sementara hukum terus berkembang untuk mengatasi kejahatan dunia maya, tantangan yang dihadapi hukum cybercrime tidak pernah berhenti. Serangan siber yang semakin kompleks dan perubahan konstan dalam teknologi memaksa hukum untuk tetap up-to-date dan relevan. Oleh karena itu, penelitian yang mendalam tentang evolusi hukum cybercrime dalam perkembangan hukum dalam dunia digital menjadi sangat penting untuk memahami bagaimana hukum dapat terus melindungi masyarakat di era digital ini.

KAJIAN TEORI

Hukum Cyber

Hukum Cyber merujuk pada seperangkat aturan yang mengatur perilaku individu, perusahaan, dan pemerintah dalam konteks internet, komputer, dan teknologi informasi lainnya. Hukum ini mencakup berbagai aspek seperti privasi data, keamanan informasi, kejahatan cyber, hak kekayaan intelektual, serta regulasi bisnis online. Hukum Cyber sering kali merupakan gabungan dari hukum nasional dan internasional yang berlaku di wilayah tertentu, dengan tujuan untuk mengatur tindakan yang terjadi dalam dunia maya dan memastikan perlindungan serta keadilan bagi semua pihak yang terlibat.

Dunia Digital

Dunia digital merujuk pada lingkungan yang dibentuk oleh teknologi informasi dan komunikasi di mana informasi disampaikan, diproses, dan dibagikan melalui jaringan internet dan sistem komputer. Dunia digital mencakup berbagai platform seperti situs web, media sosial, aplikasi seluler, dan infrastruktur teknologi lainnya. Dalam dunia digital, individu dapat berinteraksi, berkomunikasi, berbelanja, serta mengakses berbagai layanan dan informasi dengan cepat dan mudah. Namun, dunia digital juga menimbulkan tantangan baru

terkait privasi, keamanan, dan ketersediaan informasi yang memerlukan regulasi dan perlindungan hukum yang sesuai.

METODE PENELITIAN

Dalam penelitian kualitatif mengenai evolusi hukum cybercrime dalam perkembangan hukum dalam dunia digital, pendekatan ini akan memfokuskan pada analisis mendalam terhadap perubahan-perubahan dalam regulasi dan praktik hukum terkait kejahatan cyber. Metode ini melibatkan pengumpulan data melalui berbagai sumber, termasuk dokumen hukum, laporan kasus, dan penelitian sebelumnya tentang hukum cybercrime. Selain itu, penelitian ini akan melibatkan wawancara dengan para ahli hukum, penegak hukum, dan pemangku kepentingan lainnya untuk memahami pandangan mereka tentang perkembangan hukum dalam menanggapi tantangan kejahatan cyber di era digital. Analisis kualitatif akan dilakukan untuk mengidentifikasi tren, pola, dan perubahan dalam hukum cybercrime dari waktu ke waktu, serta memahami dampaknya terhadap penegakan hukum dan keamanan digital secara keseluruhan. Dengan pendekatan ini, diharapkan dapat memberikan wawasan yang mendalam tentang bagaimana hukum cybercrime berevolusi seiring dengan perkembangan dunia digital dan teknologi informasi.

HASIL DAN PEMBAHASAN

Perkembangan Hukum Cybercrime Dalam Menanggapi Perkembangan Teknologi Informasi

Selama beberapa dekade terakhir, perkembangan teknologi informasi dan komunikasi (TIK) telah mengubah lanskap hukum cybercrime secara signifikan. Sejarah evolusi hukum dalam menanggapi perkembangan ini mencerminkan perubahan yang mencolok dalam tindakan hukum, peraturan, dan pendekatan penegakan hukum cybercrime. Tantangan terbesar yang dihadapi adalah bagaimana hukum dapat terus mempertahankan relevansinya dalam menghadapi serangan siber yang semakin kompleks. Pertanyaan utama adalah sejauh mana perkembangan hukum ini telah mempengaruhi efektivitas penegakan hukum cybercrime.

Pada awal era digital, hukum cybercrime cenderung terbatas dan tidak mampu menangani serangan siber yang semakin cerdik. Undang-undang klasik yang berfokus pada kejahatan konvensional seringkali tidak mampu menyelidiki atau menuntut pelaku cybercrime. Sebagai tanggapan, legislator dan pengambil kebijakan di seluruh dunia mulai mengkaji ulang kerangka kerja hukum mereka.

Salah satu perubahan paling signifikan adalah pembentukan undang-undang cybercrime yang lebih spesifik. Undang-undang ini dirancang untuk mengatasi kejahatan di dunia maya dengan memberikan wewenang lebih kepada penegak hukum. Mereka mencakup berbagai tindak pidana seperti peretasan, pencurian data, penipuan online, dan penyebaran malware. Seiring waktu, undang-undang semacam ini telah diadopsi di banyak negara, memberikan alat yang lebih efektif bagi penegak hukum untuk menangani serangan siber. Hukum perlindungan data pribadi juga telah mengalami perkembangan penting. Dalam upaya melindungi privasi individu, banyak negara telah memperkenalkan undang-undang perlindungan data yang ketat. Sebagai contoh, Regulasi Umum Perlindungan Data (GDPR) di Uni Eropa telah menjadi tonggak dalam perlindungan data pribadi dan memberikan konsekuensi serius bagi pelanggarannya. Ini menciptakan insentif bagi perusahaan dan entitas yang memproses data untuk lebih berhati-hati dalam pengelolaan data pribadi.

Sementara hukum terus berkembang, hukum cybercrime juga harus menghadapi tantangan dalam menjalankan penegakan

hukum yang efektif. Serangan siber yang semakin cerdik dan kompleks memaksa penegak hukum untuk terus memperbarui keterampilan mereka. Kejahatan dunia maya yang bersifat internasional juga menimbulkan pertanyaan tentang kerja sama lintas batas dan ekstradisi pelaku cybercrime.

Kerja sama lintas batas menjadi kunci dalam penegakan hukum cybercrime. Ini melibatkan perjanjian antarnegara, pertukaran informasi, dan upaya bersama dalam menangani serangan siber. Namun, kerja sama ini seringkali rumit oleh perbedaan yurisdiksi dan peraturan negara. Bagaimana hukum internasional telah memengaruhi kemampuan negara-negara untuk menangani ancaman cybercrime yang bersifat global adalah pertanyaan yang perlu dijawab. Dalam kesimpulan, evolusi hukum cybercrime dalam perkembangan TIK telah menghasilkan perubahan yang signifikan dalam kerangka kerja hukum yang digunakan untuk melindungi masyarakat dari serangan siber. Meskipun hukum telah berkembang untuk mengatasi tantangan ini, penegakan hukum cybercrime tetap menjadi tantangan yang kompleks dan berkelanjutan yang memerlukan upaya terus-menerus untuk mempertahankan keamanan dan privasi di era digital.

Peran Kerja Sama Lintas Batas Dalam Upaya Penegakan Hukum Cybercrime

Kerja sama lintas batas memainkan peran krusial dalam upaya penegakan hukum cybercrime dan penanggulangan ancaman siber yang bersifat global. Dalam era digital yang semakin terinterkoneksi, serangan siber tidak lagi terbatas pada batas nasional, dan kerja sama internasional menjadi suatu keharusan. Perkembangan dalam hukum internasional telah memengaruhi kemampuan negara-negara dalam menangani ancaman cybercrime yang bersifat global dengan berbagai cara.

Peran kerja sama lintas batas dalam penegakan hukum cybercrime sangat penting karena serangan siber sering kali melibatkan pelaku dari negara yang berbeda. Penyelidikan serangan ini seringkali memerlukan kolaborasi antarpenegak hukum dari berbagai negara, pertukaran informasi, dan bantuan hukum saling melengkapi. Beberapa peran kerja sama lintas batas dalam penegakan hukum cybercrime adalah:

1. Pertukaran Informasi: Negara-negara dapat berbagi data dan informasi terkait serangan siber, pelaku, atau alat yang digunakan. Ini memungkinkan penegak hukum untuk memahami taktik pelaku dengan lebih baik.
2. Penuntutan Bersama: Dalam beberapa kasus, serangan siber melibatkan pelaku dari beberapa yurisdiksi. Kerja sama lintas batas memungkinkan penegak hukum untuk melakukan penuntutan bersama yang efisien.
3. Pembekuan Aset: Kerja sama internasional memungkinkan pembekuan aset pelaku yang terlibat dalam kejahatan siber. Ini dapat berdampak besar pada motivasi pelaku dan mencegah kejahatan lebih lanjut.
4. Ekstradisi: Dalam situasi yang lebih serius, ekstradisi pelaku ke negara yang bersangkutan dapat diterapkan melalui perjanjian ekstradisi yang ada antarnegara.

Perkembangan dalam hukum internasional juga telah memberikan landasan hukum bagi kerja sama lintas batas yang lebih efektif dalam menangani ancaman cybercrime yang bersifat global. Beberapa perkembangan penting dalam hukum internasional yang berdampak pada penegakan hukum cybercrime meliputi:

1. Konvensi Budapest tentang Kejahatan Siber: Konvensi Budapest adalah perjanjian internasional yang dirancang untuk memerangi kejahatan siber. Ini memberikan dasar hukum untuk kerja sama lintas batas dalam penyelidikan, penuntutan, dan ekstradisi pelaku

cybercrime.

2. Regulasi Umum Perlindungan Data (GDPR): GDPR adalah peraturan Uni Eropa yang mengatur perlindungan data pribadi. Ini memengaruhi perusahaan di seluruh dunia yang berurusan dengan data warga Uni Eropa dan memperkuat hak individu dalam hal perlindungan data. GDPR mengharuskan kerja sama lintas batas dalam perlindungan data dan penanganan pelanggaran data.
3. Kerja Sama Regional: Beberapa kawasan seperti Uni Eropa dan ASEAN telah mengembangkan kerangka kerja hukum dan mekanisme kerja sama regional untuk menghadapi ancaman siber bersama-sama.

Namun, meskipun ada perkembangan positif dalam hukum internasional dan kerja sama lintas batas, masih ada beberapa tantangan yang perlu diatasi. Perbedaan hukum dan yurisdiksi antarnegara seringkali menghambat upaya penegakan hukum. Juga, negara-negara yang kurang memadai dalam hal kapasitas dan sumber daya mungkin menghadapi kesulitan dalam berpartisipasi dalam kerja sama lintas batas yang efektif.

Dalam konteks yang semakin kompleks ini, peran kerja sama lintas batas dan perkembangan dalam hukum internasional menjadi kunci dalam menangani ancaman cybercrime yang bersifat global. Upaya terus-menerus dalam meningkatkan kerja sama dan menyesuaikan hukum dengan perkembangan teknologi sangat penting untuk menjaga keamanan dan stabilitas di dunia digital yang terus berkembang.

KESIMPULAN

Evolusi hukum cybercrime dalam menanggapi perkembangan teknologi informasi dan komunikasi telah menghasilkan perubahan signifikan dalam kerangka hukum yang mengatur kejahatan siber. Upaya ini mencakup pembentukan undang-undang cybercrime yang lebih spesifik, perlindungan data pribadi yang lebih kuat, dan peningkatan kerja sama lintas batas. Namun, serangan siber yang semakin cerdik dan kompleks menantang efektivitas penegakan hukum cybercrime.

Kerja sama lintas batas memainkan peran krusial dalam penegakan hukum cybercrime. Pertukaran informasi, penuntutan bersama, pembekuan aset, dan ekstradisi adalah beberapa aspek penting dalam kerja sama ini. Perkembangan dalam hukum internasional, seperti Konvensi Budapest dan Regulasi Umum Perlindungan Data (GDPR), telah memberikan landasan hukum yang diperlukan untuk kerja sama lintas batas yang lebih efektif.

Namun, masih ada beberapa tantangan yang harus diatasi. Perbedaan hukum dan yurisdiksi antarnegara seringkali memperlambat upaya penegakan hukum. Negara-negara dengan sumber daya terbatas mungkin mengalami kesulitan dalam berpartisipasi dalam kerja sama lintas batas yang efektif. Oleh karena itu, upaya lebih lanjut dalam memperkuat kerja sama internasional dan mengatasi hambatan ini sangat penting.

DAFTAR PUSTAKA

Alexandrou, A. (2021). *Cybercrime and information technology: The computer network infrastructure and computer security, cybersecurity laws, Internet of Things (IoT), and mobile devices*. CRC Press.

Alghamdi, M. I. (2020). A descriptive study on the impact of cybercrime and possible measures to curtail its spread worldwide. *International Journal of Engineering Research and Technology*, *9*, 731-5.

Almazkyzy, K., & Esteusizov, Y. N. (2018). The essence and content of cybercrime in modern times. *Journal of Advanced Research in Law and Economics*, *9*(3 (33)), 834-841.

Babanina, V., Tkachenko, I., Matiushenko, O., & Krutevych, M. (2021). Cybercrime: History of formation, current state and ways of counteraction. *Amazonia Investiga*, *10*(38), 113-122.

Bunga, D. (2019). Legal response to cybercrime in global and national dimensions. *PADJADJARAN Jurnal Ilmu Hukum (Journal of Law)*, *6*(1), 69-89.

Choi, K. S., Lee, C. S., & Louderback, E. R. (2020). Historical evolutions of cybercrime: From computer crime to cybercrime. *The Palgrave handbook of international cybercrime and cyberdeviance*, 27-43.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2022). *Cybercrime and digital forensics: An introduction*. Routledge.

Jayasekara, S. D., & Abeysekara, I. (2019). Digital forensics and evolving cyber law: case of BIMSTEC countries. *Journal of Money Laundering Control*, *22*(4), 744-752.

Khan, S., Saleh, T., Dorasamy, M., Khan, N., Tan Swee Leng, O., & Gale Vergara, R. (2022). A systematic literature review on cybercrime legislation. *F1000Research*, *11*, 971.

Kovacs, A. M. (2022). Here there be Dragons: Evolution, Potentials and Mitigation Opportunities of Cybercrime in Nigeria: A Review, Analysis, and Evaluation. *Journal of Central and Eastern European African Studies*, *2*(1).

Losavio, M. M., Pastukov, P., Polyakova, S., Zhang, X., Chow, K. P., Koltay, A., ... & Ortiz, M. E. (2019). The juridical spheres for digital forensics and electronic evidence in the insecure electronic world. *Wiley Interdisciplinary Reviews: Forensic Science*, *1*(5), e1337.

Malik, J. K., & Choudhury, S. (2019). A Brief review on Cyber Crime-Growth and Evolution. *Pramana Research Journal*, *9*(3), 242.

Marion, N. E., & Twede, J. (2020). *Cybercrime: An encyclopedia of digital crime*. Bloomsbury Publishing USA.

Payne, B. K. (2020). Defining cybercrime. *The Palgrave handbook of international cybercrime and cyberdeviance*, 3-25.

Rakha, N. A. (2023). Cyber Law: Safeguarding Digital Spaces in Uzbekistan. *International Journal of Cyber Law*, *1*(5).

Schjolberg, S. (2020). *The History of Cybercrime* (Vol. 13). BoD–Books on Demand.

Świątkowska, J. (2020). Tackling cybercrime to unleash developing countries' digital potential. *Pathways for Prosperity Commission Background Paper Series*, *33*, 2020-01.

Widijowati, D. (2022). Legal Complexity in Dealing with Cyber Crime in Indonesia. *Research Horizon*, *2*(6), 597-606.

Younies, H., & Al-Tawil, T. N. E. (2020). Effect of cybercrime laws on protecting citizens and businesses in the United Arab Emirates (UAE). *Journal of Financial Crime*, *27*(4), 1089-1105.