Indonesian Journal of Law and Justice Volume: 1, Number 3, 2024, *Page*: 1-11

Analisis Keselarasan Pengaturan Yurisdiksi *Cyber Crime* dengan Implementasinya di Kehidupan Nyata

Siti Aliza Nuraini Wahdini, Fiqri Fitrah Banu Irfansyah
Universitas Tidar; sitializanw@gmail.com; fbnu06@gmail.com

Abstrak: Artikel ini membahas tentang pengaturan mengenai yurisdiksi dari *cyber crime* yang tentunya tidak terlepas dari tantangan serta hambatan dalam pelaksanaannya di kehidupan nyata. Pengaturan mengenai yurisdiksi ini muncul sebagai aturan yang mendorong negara – negara untuk dapat mengadili pelaku kejahatan siber tanpa terkecuali. Namun dalam mengadili pelaku juga tidak terlepas dari hukum nasional negara yang terkodifikasi dengan hukum internasional yang berlaku, sehingga negara – negara tersebut dapat ditengahi dan bekerja sama dalam mengadili pelaku. Meskipun begitu keterbatasan hukum dalam menangani kejahatan siber juga menjadi sebuah hambatan. Dikarenakan belum ada aturan yang secara spesifik dalam menangani jenis – jenis kejahatan siber tersebut. Selain itu sering terjadi keterlambatan terhadap penegakan hukum tersebut karena harus menyesuaikan dengan perkembangan teknologi yang ada. Penelitian ini menggunakan metode deskriptif kualitatif guna mengkaji terkait kesesuian antara pengaturan yang berlaku dengan yurisdiksi *cyber crime*. Hasil penelitian menyatakan bahwa yurisdiksi *cyber crime* sudah sesuai dengan aturan yang berlaku namun tetap memiliki hambatan – hambatan tertentu.

Kata Kunci: Yurisdiksi, Kejahatan Siber, Hambatan

DOI:
https://doi.org/ 10.47134/ijlj.v1i3.2730
*Correspondence: Siti Aliza Nuraini Wahdini, Fiqri Fitrah Banu Irfansyah
Email: fbnu06@gmail.com

Received: 10-06-2024
Accepted: 10-06-2024
Published: 17-06-2024

Copyright: © 2024 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).

Abstract: *This article discusses the regulation regarding the jurisdiction of cyber crime, which of course cannot be separated from challenges and obstacles in its implementation in real life. This regulation regarding jurisdiction emerged as a rule that encourages countries to be able to prosecute cybercriminals without exception. However, in prosecuting the perpetrator, it is also inseparable from the country's national law which is codified with applicable international law, so that these countries can be mediated and cooperate in prosecuting the perpetrator. However, legal limitations in dealing with cyber crime are also an obstacle. Because there are no specific regulations for dealing with these types of cyber crimes. Apart from that, there are often delays in law enforcement because they have to adapt to existing technological developments. This research uses a qualitative descriptive method to examine the suitability between applicable regulations and cyber crime jurisdiction. The research results state that the jurisdiction of cyber crime is in accordance with applicable regulations but still has certain obstacles.*

Keywords: *Jurisdiction, Cyber Crime, Obstacles*

Pendahuluan

Dalam konteks kesesuaian hukum dengan teknologi, terdapat tantangan dalam menangani kejahatan cyber yang semakin kompleks(Assarut et al., 2019). Meskipun beberapa yurisdiksi telah memperbarui undang-undang mereka untuk mencakup aspek-

aspek tertentu dari kejahatan cyber, seperti pencurian identitas atau penipuan online, namun masih terdapat kesenjangan dalam menanggapi perkembangan teknologi baru. Contohnya, teknik keamanan yang digunakan untuk melindungi data pribadi sering kali lebih lambat daripada perkembangan teknologi yang digunakan oleh penjahat cyber. Selain itu, hukum yang ada mungkin tidak cukup fleksibel untuk menanggapi situasi yang unik atau serangan yang belum pernah terjadi sebelumnya(I. Goni & Mohammad, 2020).

Dalam menangani kejahatan cyber, keterlibatan masyarakat menjadi semakin penting mengingat selain dari pihak penegak hukum pentingnya dukungan dari masyarakat. Adanya informasi, bukti, dan sumber daya intelijen menjadi krusial dalam mendukung investigasi dan penegakan hukum terhadap pelaku kejahatan cyber yang beroperasi di wilayah berbeda(Shukla & Tiwari, 2024). Penerapan Yurisdiksi cybercrime menjadi solusi dan memiliki peran penting dalam menangani permasalahan yang berkaitan dengan teknologi informasi dan komunikasi. Yurisdiksi cyber dapat diartikan menjadi seperti kekuasaan dan kekuatan dalam jaringan system dari para pengguna untuk dijadikan suatu bentuk ketentuan atau peraturan dan memposisikan sama pada pengguna di ruang lingkup media internet, Sedangkan, Aspek hukum dalam yurisdiksi cyber merupakan suatu wewenang yang dimiliki oleh pemerintah dan terdapat tanggung jawab memeriksa atau memantau aktivitas pengguna media internet di ruang teknologi(O. Goni, 2022).

Oleh karena itu, penting untuk adanya kerja sama dan dukungan dalam merumuskan standar hukum yang lebih holistik terkait dengan kejahatan cyber. Hal ini tidak hanya memperbarui hukum secara teratur, tetapi juga membangun kerangka kerja yang memungkinkan pertukaran informasi yang lebih efektif Dengan demikian, akan lebih mungkin bagi hukum untuk tetap relevan dan efektif dalam menanggapi tantangan kejahatan cyber yang terus berkembang(Sari & Jufri, 2022). Meskipun terdapat hambatan, meningkatnya ancaman kejahatan cyber menuntut respon yang lebih koordinatif dan efektif. Hal Ini membutuhkan pembangunan kapasitas investigasi dan penegakan hukum yang kuat di tingkat nasional, serta upaya bersama untuk mengatasi perbedaan hukum dan hambatan lainnya(Whelan et al., 2024). Dengan meningkatnya kerjasama dan koordinasi akan lebih mungkin untuk menciptakan lingkungan yang lebih sulit bagi pelaku kejahatan cyber, serta memperkuat daya tangkal global terhadap ancaman cyber yang semakin kompleks dan serius(Tuli et al., 2022).

Metode Penelitian

Penelitian ini menggunakan metode deskriptif kualitatif untuk mengkaji terkait yurisdiksi dari cyber crime yang sesuai dengan aturan yang berlaku. Metode ini dipilih

karena memungkinkan peneliti untuk menggambarkan secara mendalam dan menyeluruh implementasi dari yurisdiksi ini tanpa terlibat langsung melalui observasi atau wawancara(Timofeyev & Dremova, 2022). Data dikumpulkan melalui studi kepustakaan, dengan menelaah berbagai literatur yang relevan termasuk jurnal, artikel, berita serta dokumen lainnya guna memberikan validasi keabsahan dari hasil penelitian. Analisis dokumen dilakukan untuk mengidentifikasi dan memahami pandangan-pandangan yang ada mengenai pengaturan terhadap yurisdiksi dari cyber crime. Dengan pendekatan ini, penelitian bertujuan untuk memberikan gambaran yang komprehensif tentang bagaimana pengaturan terhadap yurisdiksi cyber crime ini dipraktikkan, dipersepsikan, dan dipahami dalam kehidupan sehari – hari(Veena et al., 2022).

Hasil Dan Pembahasan

Kesesuian Peraturan Dalam Yurisdiksi *Cyber Crime*

Munculnya jenis kriminalitas yang baru seperti *cyber crime* tidak terlepas dari ketentuan yang berlaku dalam KUHP. Khususnya mengenai yurisdiksi yang sesuai dengan Pasal 2 KUHP bahwasanya ketentuan pidana dalam perundang – undangan Indonesia berlaku bagi setiap orang yang melakukan delik – delik kejahatan di Indonesia(Wiggen, 2020). Kemudian berkaitan dengan kejahatan tersebut, lahirnya Undang – Undang ITE yang memberikan penerapan terhadap yurisdiksi negara Indonesia terkait perbuatan yang dilarang baik di dalam maupun di luar wilayah Indonesia selama terdapat kerugian terhadap sistem elektronik di wilayah tersebut. Mengenai tindakan apa saja yang dilarang dalam undang – undang tersebut telah tercantum dari pasal 27 hingga 36 yang memiliki unsur – unsur manipulasi, menganggu hak eksklusif atau privasi dengan cara yang tidak sah sehingga merugikan sistem elektronik tersebut(Biswal & Pani, 2021).

PBB pada tahun 1990 telah mengeluarkan resolusi yang membahas terkait penerapan tindakan preventif terhadap Kejahatan dan Perlakuan yang berhubungan dengan elektronik seperti komputer. Resolusi tersebut bertujuan untuk menghimbau negara – negara dalam meningkatkan perlawanan terhadap kejahatan komputer dengan melakukan implementasi sebagai berikut(Ignatuschtschenko, 2021):

1. Melakukan perubahan terhadap undang – undang pidana beserta prosedur hukumnya sesuai dengan perkembangan zaman sehingga penanganan terhadap kejahatan di dunia siber dilakukan dengan efektif
2. Peningkatan keamanan terhadap jaringan komputer dan melakukan tindakan pencegahan yang mementingkan isu – isu privasi demi menjunjung tinggi hak asasi manusia dan kebebasan individu

3. Sosialisasi dan pemberian pendidikan terhadap masyarakat maupun penegak hukum berkaitan dengan kejahatan komputer guna meningkatkan kesadaran dalam mencegah terjadinya kejahatan
4. Sosialiasi dan pengadaan pelatian kepada seluruh aparat penegak hukum dalam melakukan pencegahan, penyelidikan, dan menangani kasus – kasus tentang kejahatan siber

Kejahatan siber bisa saja dilakukan secara lintas negara yang menyebabkan pengaturannya harus sesuai dengan yurisdiksi negara tersebut(Anjum, 2020). Hal ini tentunya sering menjadi masalah, khususnya ketika berkaitan dengan warga negara asing yang melakukan kejahatan tersebut di wilayah kita. Maka dari itu selain dari peraturan yang ditetapkan dalam undang – undang nasional, kejahatan siber ini harus berada dalam yurisdiksi hukum internasional sebagai penengah dalam mengadili kejahatan tersebut. Dalam berhubungan dengan negara lain, perlu adanya ratifikasi terhadap *cyber crime* itu sendiri sehingga negara – negara lain bisa bekerja sama dalam menangani kasus yang merugikan wilayah tersebut. Dengan adanya penguatan peraturan terhadap penanganan tersebut, maka wilayah yang dirugikan bisa melakukan pengajuan ekstradisi terhadap pelaku.

Berkaitan dengan penjelasan terhadap yurisdiksi telah diatur dalam *Convention on Cybercrime* yang dibuat oleh Dewan Eropa. Dalam konvensi ini ditemukan beberapa prinsip, salah satunya adalah mengenai prinsip teritorial. Yang dimaksud dengan prinsip ini artinya negara – negara yang terikat dalam konvensi ini berhak mengadili pelaku yang melakukan kejahatan – kejahatan sesuai dengan unsur konvensi apabila dilakukan di wilayahnya. Selain itu terdapat prinsip nasionalitas yang terkenal prakteknya dalam negara – negara yang mengani sistem *civil law*. Berkaitan dengan prinsip ini menyatakan bahwa pelaku kejahatan siber dalam diproses dengan hukum nasional tempat ia berasal atas perbuatan yang dilakukan di luar wilayah yurisdiksi negaranya sendiri(Widijowati, 2023).

Namun tidak jarang meskipun yurisdiksi telah diatur sedemikian rupa, masih terdapat potensi konflik apabila:

1. Pengklaiman yurisdiksi menurut beberapa negara yang menggunaan dasar suatu kasus tersebut diadili di tempat kejahatan tersebut dilakukan
2. Pengklaiman yurisdiksi menurut beberapa negara yang memiliki perbedaan prinsip nasionalitas aktif, pasif, dan juga teritorialitas sehingga menimbulkan kebingungan dalam mengadili kejahatan tersebut(Syahril, 2023).

Mengenai permasalahan ini tidak diatur secara rinci dalam konvensi tersebut sehingga perlu diadakan perundingan antara negara yang bersangkutan untuk menentukan keberhakan mereka dalam mengadili pelaku tersebut. Bentuk – bentuk

perundingan tersebut dapat ditempuh dengan cara kerja sama internasional sebagai berikut:

1. Ekstradisi dan Deportasi

   Ekstradisi merupakan penyerahan pihak yang merupakan tersangka yang dilakukan suatu negara kepada negara lain sebagai bentuk pemberian wewenang untuk mengadili dan melakukan pemidanaanya. Hal ini dapat dilakukan apabila antar kedua negara tersebut telah memiliki hubungan yang baik, kemudian pelaku memiliki keterkaitan dengan kedua negara tersebut. Pemberlakuan ekstradisi itu sendiri kerap menggunakan mekanisme deportasi dalam proses pemulangan warga negara asing yang diadili tersebut. Diberlakukannya deportasi tidak lain karena warga tersebut tidak dikehendaki keberadaannya dalam wilayah asalnya.
2. Mutual Legal Assistance

   Cara ini juga lebih dikenal sebagai Bantuan Hukum Timbal Balik dalam Masalah Pidana karena tindakannya sebagai bentuk kerja sama dalam memerangi kejahatan. Mekanisme hukum ini timbul dalam pergaulan masyarakat internasional. Mekanisme ini meliputi prosedur kerjasama internasional terhadap negara – negara terkait dalam mengajukan serta menerima bantuan dari pihak lain dalam mengumpulkan alat bukti dan menyelidiki serta menuntut pelaku dalam kasus – kasus kejahatan yang dilakukannya(Boussi & Gupta, 2020).
3. Transfer of Proceedings

   Cara ini lebih dikenal sebagai pengalihan terhadap perkara dalam sistem peradilan pidana internasional. Dimana praktek mekanisme ini diatur dalam *European Convention on The Transfer of Proceedings in Criminal Matters.* Prosedurnya melibatkan kerjasama internasional dimana suatu negara dapat meminta bantuan dari negara lain untuk melakukan proses pengadilan terhadap seseorang yang merupakan tersangka dalam kejahatan yang terjadi di wilayahnya.

Hambatan Dalam Pelaksanaan Implementasinya Di Kehidupan Nyata

Kemajuan teknologi sangat erat kaitannya dengan kemajuan ilmu pengetahuan, sehingga kemajuan teknologi dapat dikatakan bahwa merupakan suatu hal yang tidak bisa kita hindari dalam kehidupan ini memberikan manfaat serta memberikan banyak kemudahan serta menjadi alat dalam menjalankan kegiatan manusia. Dalam bidang teknologi, masyarakat sekitar kita telah menikmati banyak manfaat dari inovasi-inovasi yang dihasilkan. Adanya kemajuan teknologi yang berkembang pesat dan mencakup berbagai bidang kehidupan manusia. Saat ini rasanya sulit memisahkan kehidupan manusia dari teknologi, padahal kebutuhan manusia sudah menjadi taruhannya. Pada awal perkembangan teknologi, teknologi merupakan bagian atau bergantung pada ilmu

pengetahuan, namun kini ilmu pengetahuan juga dapat bergantung pada teknologi. Tentunya dengan adanya kemajuan teknologi mempunyai dampak positif dan negatif bagi masyarakat sekitar. Selain itu terdapat permasalahan dari kemajuan teknologi yaitu munculnya cybercrime yang menjadi sebuah tantangan untuk diselesaikan. Dalam dunia teknologi informasi yang dimana aktivitasnya dilakukan dengan menggunakan media internet namun kejahatan tersebut tidak terlihat secara langsung oleh masyarakat sekitar dan tidak menimbulkan kerugian secara fisik menyebabkan kerusakan apa pun, namun dapat menyebabkan kerugian yang signifikan seperti peretas kejahatan dunia maya dapat mencuri dan menyalahgunakan data penting(Jain & Gupta, 2020).

Keterbatasan hukum dalam menangani kejahatan cyber adalah salah satu hambatan utama yang dihadapi oleh penegak hukum di seluruh dunia. Dengan semakin terglobalisasi dan terinterkoneksinya dunia melalui internet, pelaku kejahatan cyber dapat dengan mudah melintasi batas negara dan menggunakan infrastruktur yang tersebar di berbagai yurisdiksi. Hal ini menyulitkan upaya penegakan hukum karena munculnya perbedaan dalam definisi kejahatan cyber, prosedur penyelidikan, dan hukuman. Misalnya, apa yang dianggap sebagai pelanggaran di satu negara mungkin tidak dianggap demikian di negara lain, atau hukumannya bisa jauh berbeda. Selain itu, proses ekstradisi dan kerja sama lintas batas seringkali rumit dan memakan waktu, karena melibatkan koordinasi antara berbagai sistem hukum nasional yang berbeda.

Selain itu, upaya untuk menangani keterbatasan hukum dalam konteks kejahatan cyber seringkali terhambat oleh ketidakmampuan untuk secara cepat menyesuaikan hukum dengan perkembangan teknologi. Kejahatan cybercrime terus berkembang dan menggunakan teknik yang semakin canggih, sementara hukum dan peraturan seringkali lambat dalam menanggapinya. Ini menciptakan kesenjangan antara kemampuan penegak hukum dan pelaku kejahatan, yang dapat dimanfaatkan oleh penjahat siber untuk menghindari tangkapan atau hukuman. Oleh karena itu, ada kebutuhan mendesak untuk meningkatkan kerja sama dalam pengembangan dan implementasi hukum yang memadai untuk menangani ancaman kejahatan cyber di era digital ini(Nguyen, 2023).

Keterbatasan teknologi menjadi salah satu hambatan utama dalam penegakan yurisdiksi terhadap kejahatan cyber. Sementara teknologi terus berkembang dengan cepat, para pelaku kejahatan siber juga terus memperbarui metode dan alat mereka. Hal ini menciptakan sebuah tantangan bagi penegak hukum untuk selalu berada di depan kurva dan menanggapi secara efektif terhadap serangan yang terus berubah. Misalnya, serangan cyber yang menggunakan teknik dan alat enkripsi yang canggih dapat membuat penyelidikan menjadi sulit karena sulitnya melacak dan mengidentifikasi pelaku. Selain itu,

kurangnya keahlian teknis di kalangan penegak hukum juga dapat menjadi penghalang dalam memahami dan menanggapi serangan kejahatan siber dengan tepat(Koto, 2021).

Upaya untuk mengatasi keterbatasan teknologi dalam penegakan hukum kejahatan cyber memerlukan investasi yang signifikan dalam pelatihan, peralatan, dan infrastruktur teknologi. Penegak hukum perlu diberikan sumber daya yang cukup untuk dapat memperbarui keahlian mereka secara teratur dan mengadopsi teknologi terbaru yang dapat membantu mereka dalam memerangi kejahatan siber. Selain itu, kerja sama antara sektor publik dan swasta juga sangat penting dalam membangun kapasitas teknis yang diperlukan untuk melawan ancaman cybercrime. Ini termasuk pertukaran informasi tentang ancaman yang baru muncul, serta pengembangan solusi keamanan yang inovatif. Dengan demikian, dengan mengakui pentingnya investasi dalam teknologi dan peningkatan kerja sama lintas sektor, penegak hukum dapat lebih efektif dalam menanggapi ancaman kejahatan siber yang semakin kompleks.

Kurangnya sumber daya merupakan salah satu hambatan utama dalam penegakan yurisdiksi cybercrime terhadap kejahatan cyber di banyak negara. Banyak lembaga penegak hukum menghadapi keterbatasan dalam hal personel yang terlatih secara teknis, peralatan yang diperlukan, dan anggaran yang cukup untuk mengatasi ancaman kejahatan siber yang semakin kompleks. Hal ini membuat mereka seringkali tidak mampu untuk memonitor secara efektif aktivitas online, mendeteksi serangan cybercrime, dan menindaklanjuti secara tepat waktu. Selain itu, kebutuhan akan sumber daya yang lebih besar dalam hal pelatihan dan pengembangan kapasitas juga menjadi tantangan, karena teknologi dan taktik kejahatan siber terus berkembang dengan cepat.

Untuk mengatasi keterbatasan sumber daya, penting bagi pemerintah dan lembaga penegak hukum untuk mengalokasikan lebih banyak anggaran untuk keamanan cyber dan pelatihan teknis. Investasi dalam pelatihan dan pengembangan kapasitas personel, serta pengadaan peralatan dan infrastruktur yang diperlukan, sangat diperlukan untuk meningkatkan kemampuan penegak hukum dalam menangani ancaman kejahatan siber. Selain itu, kerja sama antara negara dan lembaga penegak hukum internasional juga dapat membantu dalam berbagi sumber daya dan pengalaman, sehingga memperkuat kemampuan penegak hukum di seluruh dunia dalam melawan cybercrime. Dengan upaya ini, diharapkan penegak hukum akan memiliki sumber daya yang cukup untuk dapat lebih efektif menghadapi tantangan keamanan cyber yang semakin kompleks(Koto, 2021).

Isu privasi dan kebebasan berbicara menjadi pertimbangan penting dalam penegakan yurisdiksi terhadap kejahatan cyber. Dalam upaya untuk melacak aktivitas online dan mengumpulkan bukti terkait pelaku kejahatan, seringkali diperlukan pengawasan yang intensif terhadap komunikasi dan perilaku online individu. Namun, hal

ini dapat menimbulkan kekhawatiran tentang pelanggaran privasi dan potensi penyalahgunaan kekuasaan oleh pemerintah atau lembaga penegak hukum. Selain itu, upaya untuk membatasi atau memantau kegiatan online juga bisa dianggap sebagai pembatasan terhadap kebebasan berbicara dan akses informasi yang dijamin oleh hukum di beberapa negara. Oleh karena itu, penegak hukum perlu memperhatikan keseimbangan yang tepat antara kebutuhan untuk melindungi masyarakat dari kejahatan cyber dengan menjaga hak privasi individu dan kebebasan berbicara.

Dalam menanggapi isu privasi dan kebebasan berbicara, penegak hukum dapat mengadopsi pendekatan yang berbasis pada hukum dan transparansi. Hal ini mencakup pengembangan kebijakan yang jelas tentang pengumpulan dan penggunaan data dalam konteks penegakan hukum cybercrime, serta memastikan bahwa tindakan yang diambil sesuai dengan hukum yang berlaku dan menghormati hak asasi manusia. Selain itu, upaya untuk meningkatkan kesadaran masyarakat tentang pentingnya keamanan cyber dan dampaknya terhadap privasi individu dapat membantu memperkuat dukungan untuk upaya penegakan hukum dalam melawan kejahatan cybercrime. Dengan memperhatikan keseimbangan yang tepat antara keamanan dan privasi, penegak hukum dapat menjalankan tugas mereka secara efektif sambil tetap menghormati hak asasi manusia dan nilai-nilai demokratis(Al-Masalha et al., 2020).

Ketidakseragaman dalam yurisdiksi menjadi hambatan signifikan dalam penegakan hukum cybercrime di tingkat global. Setiap negara memiliki kerangka hukum yang unik dan berbeda dalam menangani kejahatan cyber, dengan perbedaan dalam definisi kejahatan, prosedur penyelidikan, dan hukuman yang diterapkan. Hal ini dapat menyulitkan apabila terdapat kerja sama lintas-batas antara negara-negara yang berusaha untuk menangani kejahatan cybercrime.

Simpulan

Yurisdiksi cybercrime belum sepenuhnya berjalan sesuai dengan peraturan yang berlaku. Meskipun beberapa yurisdiksi telah memperbarui undang-undang mereka untuk menangani aspek-aspek tertentu dari kejahatan siber, masih terdapat kesenjangan dalam menanggapi perkembangan teknologi baru. Hukum yang ada sering kali tidak cukup fleksibel untuk menangani situasi yang unik atau serangan yang belum pernah terjadi sebelumnya. Ketentuan tentang khususnya mengenai yurisdiksi yang sesuai dengan Pasal 2 KUHP bahwasanya ketentuan pidana dalam perundang – undangan Indonesia berlaku bagi setiap orang yang melakukan delik – delik kejahatan di Indonesia. Terdapat beberapa

hambatan dalam implementasi yurisdiksi cybercrime di dunia nyata seperti teknik keamanan yang digunakan untuk melindungi data pribadi sering kali lebih lambat daripada perkembangan teknologi yang digunakan oleh pelaku kejahatan siber. Kurangnya koordinasi dan pertukaran informasi yang efektif antara berbagai pihak terkait, seperti penegak hukum dan masyarakat. Perbedaan hukum dan yurisdiksi antar negara menyulitkan penanganan kejahatan siber yang melintas batas, sehingga dibutuhkan pembangunan kapasitas investigasi dan penegakan hukum yang kuat di tingkat nasional untuk mengatasi ancaman kejahatan siber yang semakin kompleks.

Untuk mengatasi tantangan ini, diperlukan upaya yang lebih koordinatif dan efektif, termasuk nemperbarui hukum secara teratur untuk tetap relevan dan efektif dalam menanggapi perkembangan kejahatan siber, membangun kerangka kerja yang memungkinkan pertukaran informasi yang lebih efektif antara berbagai pihak terkait. Meningkatkan kerjasama dan koordinasi internasional untuk mengatasi perbedaan hukum dan hambatan lainnya. Memperkuat kapasitas investigasi dan penegakan hukum di tingkat nasional. Secara keseluruhan, meskipun terdapat beberapa hambatan, implementasi yurisdiksi cybercrime masih memerlukan perbaikan dan upaya yang lebih koordinatif dan efektif agar dapat menangani ancaman kejahatan siber yang semakin kompleks.

Daftar Pustaka

Al, M.D.B. (2023). Kemajuan teknologi dan pola hidup manusia dalam perspektif sosial budaya. Tuturan: Jurnal Ilmu Komunikasi, Sosial dan Humaniora, 1(3), 26-53.

Al-Masalha, H., Hnaif, A. A., & Kanan, T. (2020). Cyber-crime effect on jordanian society. Int. J. Advance Soft Compu. Appl. http://188.247.81.52/PapersUploaded/2020.3.10.pdf

Anjum, U. (2020). Cyber crime in Pakistan; detection and punishment mechanism. Časopis o Društvenom i Tehnološkom Razvoju. https://www.ceeol.com/search/article-detail?id=919062

Assarut, N., Bunaramrueang, P., & ... (2019). Clustering Cyberspace Population and the tendency to Commit Cyber Crime: A Quantitative Application of Space Transition Theory. … Journal of Cyber …. https://www.cybercrimejournal.com/pdf/Assarutetalvol13issue1IJCC2019.pdf

Biswal, C. S., & Pani, S. K. (2021). Cyber-crime prevention methodology. Intelligent Data Analytics for Terror Threat …. https://doi.org/10.1002/9781119711629.ch14

Boussi, G. O., & Gupta, H. (2020). A proposed framework for controlling cyber-crime. 2020 8th International Conference on …. https://ieeexplore.ieee.org/abstract/document/9197975/

Goni, I., & Mohammad, M. (2020). Machine learning approach to mobile forensics framework for cyber crime detection in Nigeria. Journal of Computer Science …. https://journals.bilpubgroup.com/index.php/jcsr/article/view/2147

Goni, O. (2022). Introduction to Cyber Crime. International Journal of Engineering and Artificial …. https://www.researchgate.net/profile/Osman-Goni-10/publication/359892550_Introduction_to_Cyber_Crime/links/62835f0f7a08f263d552011b/Introduction-to-Cyber-Crime.pdf

Ignatuschtschenko, E. (2021). Assessing Harm from Cyber Crime. The Oxford Handbook of Cyber Security. https://books.google.com/books?hl=en&lr=&id=p6pJEAAAQBAJ&oi=fnd&pg=PA127&dq=cyber+crime&ots=7oZd8Nt_wy&sig=au7kxVqPW6EYocLN65jg7xdySK8

Jain, A., & Gupta, N. (2020). Cyber crime. National Journal of Cyber Security Law. https://www.nci.tmu.ac.in/conference_proceeding/NCI26.pdf

Kemit, J.F., & Kleden, K.L. (2023, July). Yurisdiksi kejahatan Siber: Borderless. In Seminar Nasional-Hukum dan Pancasila (Vol. 2, pp. 55-70).

Koto, I. (2021). Cyber crime according to the ITE law. International Journal Reglement &Society …. http://jurnal.bundamediagrup.co.id/index.php/ijrs/article/view/124

Kurnia Putra, A. ANALISIS HUKUM YURISDIKSI TINDAK KEJAHATAN SIBER (CYBERCRIME) BERDASARKAN CONVENTION ON CYBERCRIME. FAKULTAS HUKUM UNIVERSITAS JAMBI.

Najwa, A.F., & Husna, A. (2024). Efektifitas yurisdiksi cybercrime di tengah perkembangan teknologi informasi. Jurnal Hukum dan Sosial Politik, 2(3), 126-135.

Nguyen, T. N. (2023). A review of cyber crime. Journal of Social Review and Development. https://dzarc.com/social/article/view/244

Sari, D. I., & Jufri, M. (2022). INTEGRATED NETWORK SYSTEM SECURITY TO DETERMINE GIS (GEOGRAPHIC INFORMATION SYSTEM) BASED CYBER CRIME PATTERNS. JURTEKSI (Jurnal Teknologi Dan Sistem …. https://jurnal.stmikroyal.ac.id/index.php/jurteksi/article/view/1890

Sari, U.I.P. (2021). Kebijakan penegakan hukum dalam upaya penanganan cyber crime yang dilakukan oleh virtual police di Indonesia. Mimbar Jurnal Hukum, 2(1), 58-77.

Shukla, R. K., & Tiwari, A. K. (2024). Security Analysis of the Cyber Crime. The Ethical Frontier of AI and Data Analysis. https://www.igi-global.com/chapter/security-analysis-of-the-cyber-crime/341198

Syahril, M. A. F. (2023). Cyber Crime in terms of the Human Rights Perspective. International Journal of Multicultural and Multireligious …. https://ijmmu.com/index.php/ijmmu/article/view/4611

Timofeyev, Y., & Dremova, O. (2022). Insurers' responses to cyber crime: evidence from Russia. International Journal of Law, Crime and Justice. https://www.sciencedirect.com/science/article/pii/S1756061621000653

Tuli, B., Kumar, S., & Gautam, N. (2022). An overview on cyber crime and cyber security. Asian Journal of Engineering and …. https://www.academia.edu/download/97916880/2569.pdf

Veena, K., Meena, K., Teekaraman, Y., & ... (2022). C SVM Classification and KNN Techniques for Cyber Crime Detection. Wireless …. https://doi.org/10.1155/2022/3640017

Whelan, C., Bright, D., & Martin, J. (2024). Reconceptualising organised (cyber) crime: The case of ransomware. Journal of Criminology. https://doi.org/10.1177/26338076231199793

Widijowati, D. (2023). Analysis of the Development of Cyber Crime in Indonesia. International Journal of Artificial Intelligence Research. http://ijair.id/index.php/ijair/article/view/696

Wiggen, J. (2020). Impact of COVID-19 on cyber crime and state-sponsored cyber activities. JSTOR. https://www.jstor.org/stable/pdf/resrep25300.pdf?acceptTC=true&coverpage=false