YURISDIKSI KEJAHATAN SIBER: *BORDERLESS*

Jhos Franklin Kemit (1312100154)

Universitas 17 Agustus 1945 Surabaya, Jfranklink11@gmail.com

Vanya Agatha H (1312100207)

Universitas 17 Agustus 1945 Surabaya, Vanyaagatha11@gmail.com

Kristoforus Laga Kleden

Universitas 17 Agustus 1945 Surabaya, kleden@untag-sby.ac.id

Abstract

Cybercrime has become a rapidly growing global threat in the current digital era. In this context, the jurisdiction of cybercrime has become an increasingly complex and challenging issue. This article aims to explore the concept of jurisdiction in cybercrime cases and the challenges faced by international law in addressing them. In the cyberspace, which lacks clear physical boundaries, fundamental questions of jurisdiction arise. When and how can a country prosecute cybercriminals operating from foreign territories? How does international law regulate the handling of cybercrime cases involving actors from various jurisdictions? This article employs a literature-based research method with a normative juridical research approach, involving the search, selection, and analysis of relevant literature to gain an understanding of the researched topic. The article illustrates that cybercrime often transcends national borders, thereby challenging legal systems based on traditional territorial jurisdiction. This phenomenon is referred to as "borderless crimes," where perpetrators can easily slip through legal loopholes and carry out attacks from relatively safe havens. This makes law enforcement difficult, as national laws often prove insufficient in addressing cybercrimes that cross borders.

The article also highlights international efforts to address the challenges of cybercrime jurisdiction. Some countries have adopted laws that expand their jurisdiction to include cybercriminal activities beyond their territories. International organizations, such as Interpol, also play a crucial role in facilitating intergovernmental cooperation in cybercrime investigation and prosecution. However, despite efforts to enhance international cooperation, challenges in addressing cybercrime jurisdiction remain significant. Differences in national laws, complex extradition processes, and human rights issues further complicate global law enforcement in cybercrime cases. The article concludes that an effective resolution to the problem of cybercrime jurisdiction requires stronger intergovernmental cooperation, harmonization of national laws, and the development of a comprehensive international legal framework. Additionally, it is important to enhance the expertise and capacity of law enforcement agencies in the field of cybercrime to effectively handle cross-border cases.

Keywords: Jurisdiction, Cybercrime, Borderless, International Law, International Cooperation.

Abstrak

Kejahatan siber telah menjadi ancaman global yang berkembang pesat di era digital saat ini. Dalam konteks ini, yurisdiksi kejahatan siber menjadi isu yang semakin kompleks dan menantang. Artikel ini bertujuan untuk mengeksplorasi konsep yurisdiksi dalam kasus kejahatan siber dan tantangan yang dihadapi oleh hukum internasional dalam menghadapinya. Dalam lingkungan siber yang tidak memiliki batas fisik yang jelas, pertanyaan mendasar tentang yurisdiksi muncul. Kapan dan bagaimana sebuah negara dapat menuntut pelaku kejahatan siber yang beroperasi dari wilayah asing? Bagaimana hukum internasional mengatur penanganan kasus kejahatan siber yang melibatkan aktor dari berbagai yurisdiksi?. Artikel ini menggunakan metode penelitian berbasis kajian pustaka

dengan metode penelitian yuridis normatif yang melibatkan pencarian, pemilihan dan analisis litereratur terkait yang relevan untuk mendapatkan pemahaman terkait topik yang diteliti. Artikel ini menggambarkan bahwa kejahatan siber seringkali melintasi batas-batas negara, sehingga menantang sistem hukum yang berbasis pada yurisdiksi teritorial tradisional. Fenomena ini disebut sebagai "borderless crimes", di mana pelaku dapat dengan mudah menyelinap melalui celah hukum dan menjalankan serangan dari tempat yang relatif aman. Hal ini membuat penegakan hukum menjadi sulit, karena hukum nasional sering kali tidak cukup untuk menangani kejahatan siber yang melintasi batas.

Artikel ini juga menyoroti upaya internasional dalam mengatasi tantangan yurisdiksi kejahatan siber. Beberapa negara telah mengadopsi undang-undang yang memperluas yurisdiksi mereka untuk melibatkan tindakan kejahatan siber di luar wilayah mereka. Organisasi internasional, seperti Interpol, juga berperan penting dalam kerja sama antarnegara dalam penyelidikan dan penuntutan kejahatan siber. Namun, meskipun ada upaya untuk meningkatkan kerja sama internasional, tantangan dalam menangani yurisdiksi kejahatan siber tetap signifikan. Perbedaan dalam undang-undang nasional, proses ekstradisi yang kompleks, dan masalah hukum hak asasi manusia semakin mempersulit penegakan hukum global dalam kasus kejahatan siber. Artikel ini menyimpulkan bahwa penyelesaian efektif untuk masalah yurisdiksi kejahatan siber memerlukan kerja sama yang lebih kuat antarnegara, harmonisasi hukum nasional, dan pengembangan kerangka hukum internasional yang komprehensif. Selain itu, penting untuk mengembangkan keahlian dan kapasitas penegak hukum dalam bidang kejahatan siber agar dapat secara efektif menangani kasus-kasus yang melintasi batas.

Kata Kunci: *Yurisdiksi, Kejahatan Siber, Borderless, Hukum Internasional, Kerja Sama Internasional.*

Pendahuluan

Dampak *Covid-19* pada saat ini masih terasa hingga sekarang yang dimana masyarakat yang dihimbau untuk tidak kontak fisik atau bertemu langsung untuk menghindari penyebaran virus *Covid-19* yang banyak memakan korban jiwa. Masyarakat yang membutuhkan biaya dalam penghidupan dirinya atau keluarganya banyak beralih beraktifitas secara daring atau online melalui jaringan internet dan juga masyarakat banyak yang beralih berselancar didalam internet untuk mencari hiburan. Dari peralihan aktifitas tersebut aktifitas dunia dapat disebut dengan "*Web of the world*" pada saat komunikasi antarmanusia menggunakan komunikasi bergerak atau benda bergerak seperti smartphone, laptop, komputer yang terkoneksi dengan internet yang dapat menghubungkan dunia fisik kedalam suatu jaringan.[1]

"*Web of the world*" merupakan metafora untuk menggambarkan dua sisi yang berbeda, selain memberikan kontribusi pada peningkatan kesejahteraan, kemajuan, dan peradaban manusia, internet menjadi sarana yang berpengaruh melanggar hukum. Akses yang mudah dilakukan dari berbagai tempat di seluruh dunia menyebabkan kerugian dapat dialami oleh siapa saja, termasuk pihak yang tidak memiliki hubungan langsung. Sebagai contoh, pencurian dana kartu kredit melalui pembelanjaan online. Selain itu, masalah pembuktian menjadi faktor penting karena data elektronik dapat dipalsukan, disadap, dan rentan diubah, kemudian dikirim ke

[1] Ahmad Ramli, "*Teknologi Informasi, Eksistensi Hak Kekayaan Intlektual, dan Urgensi Hukum Siber (Cyber Law) dalam Sistem Hukum Nasional.*" PT Refika Aditama, Bandung, 2010.,hlm. 1-3.

seluruh dunia dalam hitungan detik. Dampaknya terjadi dengan cepat dan bisa sangat merusak.[2]

Kegiatan dunia maya atau lebih dikenal sebagai kegiatan siber, dapat dianggap sebagai tindakan hukum yang nyata, meskipun dilakukan secara virtual. Dalam konteks hukum, ruang siber tidak lagi memperhatikan ukuran dan kualifikasi hukum konvensional dalam mengkategorikan sesuatu sebagai objek perbuatan. Jika pendekatan tersebut diambil, akan timbul banyak ketidakpastian dalam hukum. Siber merupakan kegiatan virtual yang memiliki dampak yang sangat berwujud, walaupun buktinya bersifat elektronik. Oleh karena itu pelaku kegiatan siber juga harus dikategorikan sebagai manusia yang secara nyata melakukan perbuatan hukum.

Metode Penelitian

Penulisan artikel ini, kami menerapkan metode yang mendeskripsikan tentang kenyataan menggunakan pendekatan *yuridis normatif*. Pendekatan ini didukung oleh data bahan primer, sekunder, dan tersier yang terdiri dari peraturan perundang-undangan, literatur hukum, dan buku-buku terkait. Untuk mengumpulkan data, kami menggunakan teknik studi kepustakaan yang fokus pada hukum siber dan hukum internasional.

Hasil dan Pembahasan

I. Kejahatan Siber

Di era yang semakin modern ini ditandai dengan maraknya penggunaan terkonolgi informasi dalam menunjang setiap aspek untuk meningkatkan produktifitas dan efisiensi sebagai pensupport setiap individu untuk kesejahteraan diri, keluarga dan negaranya. Disamping itu hal tersebut juga memiliki dampak negatif yang dapat berimbas pada siapa jasa dan dimana saja.

Dibandingkan dengan kejahatan konvensional, teknologi informasi merupakan jenis interaksi virtual yang memiliki kemungkinan akan banyak hal baru untuk dapat dipahami baik dalam hal ini tindak kejahatannya. **Ronni R. Nitibaskara** berpendapat bahwa interaksi sosial yang sering terjadi dalam bentuk virtual atau dunia maya, tanpa melibatkan interaksi fisik langsung, adalah salah satu karakteristik revolusi teknologi informasi. Oleh karena itu, penyimpangan dari interaksi virtual ini dalam bentuk kejahatan siber akan beradaptasi dengan karakteristik baru tersebut.[3]

Pada rentang waktu antara 1983 dan 1988, *Organisasi Kerjasama Ekonomi dan Pembangunan (OECD)* melakukan upaya internasional pertama dalam memerangi

[2] Maman Budiman, "*Kejahatan Korporasi Indonesia*", Setara Press, Malang, 2020. Hlm. 8-15.
[3] Admad M. Ramli, *"Perkembangan Cyber Law Global dan Implikasinya Bagi Indonesia"* , Telematika Indonesia, Jakarta, 2004, Hlm. 5-6

tindak pidana kejahatan siber. Beberapa tindakan yang diusulkan dan telah terkodifikasi dalam hukum pidana khusus nasional Indonesia pada pasal 37 UU ITE dapat menerapkan yurisdiksi negara Indonesia sehubungan dengan melakukan perbuatan yang dilarang baik itu di luar negara Indonesia selama kerugian sistem elektronik tersebut berada diwilayah yurisdiksi Indonesia.

Secara garis besar dapat dipahami bahwa tindakan yang dilarang dari pasal 27 sampai 36 UU ITE merupakan perbuatan yang berupa unsur-unsur terjadinya manipulasi, pelanggaran serhadap hak eksklusif atau privasi atau akses yang tidak sah yang merugikan sistem elektronik yang berada di wilayah Indonesia.

Tahun 1990, *Perserikatan Bangsa-Bangsa (PBB)* mengeluarkan Resolusi dalam Kongres PBB ke-8 mengenai tindakaan preventif terhadap Kejahatan dan Perlakuan yang menyuarakan pentingnya pemantauan terhadap kejahatan terkait komputer. Resolusi tersebut mendorong negara-negara untuk meningkatkan upaya mereka dalam melawan kejahatan terkait komputer dengan mengimplementasikan tindakan-tindakan berikut ini:

1. Mengubah undang-undang pidana dan prosedur hukum pidana nasional agar sesuai dengan perkembangan zaman dan memastikan bahwa mereka efektif dalam menangani kejahatan siber.
2. Meningkatkan langkah-langkah keamanan komputer dan tindakan pencegahan, sambil mempertimbangkan isu-isu terkait privasi, penghormatan terhadap hak asasi manusia, kebebasan individu, dan mengatur penggunaan serta pemanfaatan komputer.
3. Memberikan pendidikan kepada masyarakat dan aparat penegak hukum mengenai permasalahan kejahatan terkait komputer serta kesadaran akan pentingnya pencegahan kejahatan tersebut.
4. Menyelenggarakan pelatihan yang memadai bagi hakim, aparat penegak hukum, dan pejabat yang bertanggung jawab dalam usaha pencegahan, penyelidikan, penuntutan, dan pengadilan kasus-kasus kejahatan siber.
5. Membangun kemitraan dengan organisasi-organisasi terkait untuk mengintegrasikan nilai-nilai etika dalam pengajaran dan pelatihan di bidang informatika sebagai bagian yang tidak terpisahkan dari kurikulum dan etika profesional.

G-delapan, yang terdiri dari *Amerika Serikat, Jerman, Prancis, Kanada, Jepang, Britania Raya, Rusia, dan Italia,* merupakan sebuah kelompok negara-negara industri. G-delapan mencapai kesepakatan mengenai sepuluh prinsip dalam upaya melawan kejahatan teknologi tinggi, di antaranya adalah:

1) Tidak ada tempat perlindungan bagi individu yang menyelewengkan teknologi informasi.

2) Proses Peradilan terhadap pelaku kejahatan siber tanpa batas suatu negara harus dilakukan dengan koordinasi antar negara yang berkepentigan, dengan tidak memperhatikan yurisdiksi dimana kerugian terjadi.

3) Aparat yang bewewenang dalam penegakan hukum harus menerima pelatihan yang memadai dalam menangani kejahatan siber.

4) Kepastian hukum oleh sistem hukum yang melindungi setiap domain atau privasi, integritas, dan menjamin dapat dipulihkannya data yang rusak akibat kejahatan siber, serta menjamin adanyasanksi administratif, perdata,dan pidana terhadap tindakan tersebut.

5) Dalam investigasi kejahatan hal yang penting adalah sistem memberikan perlindungan data dan akses data yang cepat.

6) Kolaborasi antar negara untuk memperoleh data atau bantuan timbal balik untuk menangani kasus siber internasional

7) Tidak perlunya izin akses yang dapat di akses oleh publik oleh aparat penegak hukum.

8) Pengembangan standar forensik dalam penetapan data elektronik agar mempercepat daripada proses penyelidikan dan penuntutan atau efisiensi.

9) Sistem informasi dan telekomunikasi pemerintah harus lebih canggih daripada pelaku kejahatan siber dan untuk membantu mencegah dan mengidentifikasi penyalahgunaan teknologi informasi.

10) Kegiatan dalam bidang ini harus dikoordinasikan dengan forum internasional lain yang relevan untuk menghindari tumpang tindih.

Pada tahun 2001, *Dewan Eropa (CoE)* mengusulkan kesepakatan tentang kejahatan siber yang didorong oleh Uni Eropa. Kesepakatan tentang Kejahatan Siber 2001 adalah peraturan internasional pertama mengatur tindak pidana siber dan acuan dalam pengaturan tindak pidana siber hukum nasional.

Menarik cakupan dari bukunya **Jonathan Rosenoer** tentang *"hukum siber"*, dapat di lihat kejahatan-kejahatan hukum siber sebagai berikut:

• Hak Cipta • Merek Dagang • Pencemaran nama baik • Ujaran kebencian • Hacking, viruses, illegal	• Tanggung Jawab Pidana • Procedural Issues (Jurisdiction, investigation, evidence, etc) • Kontrak Elektronik • Pornografi • Pencurian Data

access • Regulasi Sumber daya Internet • Privasi • Kewajiban Keberatan	• Perlindungan Konsumen • E-Commerce, E-Goverment

Jenis-jenis Kejahatan Siber meliputi:
1. Akses Tanpa Izin
2. Konten Ilegal
3. Penyebaran Virus
4. Hacking dan Cracker
5. Penculikan Data

Saat ini, istilah kejahatan siber merujuk pada tindak kejahatan yang dilakukan melalui jaringan internet atau dunia virtual dengan menggunakan perangkat seperti komputer, smartphone, laptop, dan teknologi lainnya. Kejahatan siber adalah bentuk kejahatan baru dan canggih yang bersifat lintas negara dan tidak terbatas oleh batas yurisdiksi suatu negara. Hal ini mendorong komunitas internasional untuk bekerja sama dalam upaya pencegahan kejahatan siber dan mengadopsi langkah-langkah preventif.

Dewasa ini kasus kejahatan siber salah satunya adalah pelecehan seksual atau kekerasan seksual yang dilakukan secara verbal melalui media internet marak terjadi, dan dapat terjadi tanpa mengenal batas ruang dan waktu. Kekerasan seksual melalui media internet dapat berupa merendahkan orang lain di media komunikasi umum dengan menyebarkan privasi seksual korban tersebut atau dengan merendahkan martabat atau bentuk fisik korban tersebut.[4]

Maraknya *fintech* atau finansial teknologi yang memudahkan masyarakat dalam melakukan transaksi keuangan juga memiliki dampak negatif salah satunya adalah *fintech* illegal yang pelaku kejahatan transaksi elektronik tersebut dapat berada di mana saja dan dapat melakukan kejahatannya melalui antar-negara, *fintech* illegal merupakan salah satu kejahatan siber, dan oleh karena itu dibutuhkan peran penegak hukum untuk melindungi korban, memberikan kepastian hukum dan keadilan bagi masyarakat. [5]

II. Yurisdiksi

[4] Ilhami, Maulana Daffa, and Wiwik Afifah. "MENGUKUR SIFAT ASAS UNUS TESTIS NULLUS TESTIS TERHADAP PEMBUKTIAN TINDAK PIDANA KEKERASAN SEKSUAL." Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance 3.2 (2023): 1625-1637.

[5] Simangunsong, Frans, and Wiwik Afifah. "SOSIALISASI PINJAMAN ONLINE ILEGAL." PSHPM: Prosiding Seminar Hasil Kegiatan Pengabdian Masyarakat. Vol. 1. No. 1. 2022.

Jurisdiction atau *yurisdiksi*, yang berasal dari bahasa Latin "*yurisdictio*", memiliki makna sebagai berikut:

a. *Yurisdiksi* adalah kontrol fundamental oleh hukum.
b. *Yurisdiksi* adalah hak yang didasarkan pada hukum.
c. *Yurisdiksi* adalah kedaulatan yang ditentukan oleh hukum.
d. *Yurisdiksi* adalah kewenangan yang berdasarkan pada hukum.

Yurisdiksi merupakan *asas fundamental* negara yang berdaulat. Negara yang diakui berdaulat dengan memiliki yurisdiksinya sendiri. Pendapat **Hans Kelsen**, adagium "*Par in Parem Non Habet Imperium*" menyatakan bahwa suatu negara hanya berhak menjalankan yurisdiksi pengadilannya sendiri terhadap negaranya sediri, dan jika antar negara yang sama-sama memiliki kepentingan dapat meminta persetujuan dari negara lain untuk melaksanakan yurisdiksi pengadilannya. Disampaikan diatas bahwa suatu perjanjian Internasional antar negara tidak dapat mengadili tindakan negara yang tidak ikut berpartisipasi dalam perjanjian internasional tersebut, dan setiap negara masing- masing memiliki legitimasi yang harus dihormati oleh negara lainnya.

Mengklasifikasikan Yurisdiksi

1. Yurisdiksi Teritorial

Penerapan undang-undang pidana suatu negara sesuai dengan Pasal 2 KUHP mencakup *Prinsip Teritorial*, yang berarti bahwa tindak pidana yang dilakukan di wilayah Indonesia dapat dikenakan hukuman. Berdasarkan prinsip ini, negara memiliki wewenang terhadap subjek hukum yaitu warga negara asli atau asing dan badan hukum dari dalam bentuk korporasi atau yang bukan yang berbadan hukum, sebagaimana diatur dalam Pasal 3 KUHP. Pendapat **Hakim Lord Macmillan** mengenai *Prinsip Teritorial* menyatakan bahwa negara berhak menetapkan yurisdiksi bagi setiap individu, objek, serta perkara pidana atau perdata dalam batas wilayahnya, yang menjadi simbol kedaulatan negara.

2. Yurisdiksi Individual

Pada pasal 3 dan 5 KUHP yang dipahami sebagai norma nasional aktif merupakan suatu negara bisa mengadili atau memberikan perlindungan dipromatik untuk warga negaranya yang melakukan kejahatan diluar negaranya.

3. Yurisdiksi Perlindungan

Berdasarkan pada Pasal 4 KUHP dipahami bahwa peraturan hukum pidana atau yurisdiksi peradilan Indonesia berlaku untuk kejahatan yang merugikan kepentingan hukum negara Indonesia. Berdasarkan ketentuan dan, beberapa contoh berdasarkan pasal tersebut kejahatan yang merugikan kepentingan hukum negara Indonesia adalah sebagai berikut:

1. Tindak kejahatan yang melanggar keamanan, integritas, atau reputasi Presiden dan Wakil Presiden RI.
2. Tindak kejahatan yang melibatkan pemalsuan mata uang dan materai yang digunakan oleh pemerintah Indonesia.
3. Tindak kejahatan yang melibatkan penggandaan surat dan serifikat yang diterbitkan oleh pemerintah Indonesia.
4. Tindak kejahatan yang melibatkan perompakan kapal laut dan pesawat udara yang merupakan milik Indonesia.

4. Yurisdiksi Universal

Dalam upaya menjaga keamanan dan ketertiban dunia, setiap negara memiliki tanggung jawab bersama untuk ikut serta. Prinsip ini juga diterapkan dalam perundangan hukum pidana Indonesia, sebagaimana diatur dalam Pasal 438 dan 444 KUHP, yang mengancamkan pidana berat terhadap tindakan perompakan kapal..

Terdapat Pasal 4 ayat (2) dan (4) KUHP juga terdapat ketentuan mengenai yurisdiksi universal, yaitu ketika suatu kejahatan mengancam kepentingan dan keselamatan warga sipil Indonesia serta melibatkan keperluan negara lain yang dilindungi oleh ketentuan pidana tersebut. Dalam konteks internasional, terdapat tiga jenis yurisdiksi yang diakui, yaitu: yurisdiksi untuk menetapkan perundangan, yurisdiksi untuk penegakan hukum, dan yurisdiksi untuk menuntut. Terkait juga pemutusan hukum, berdasar pada prinsip umum yang digunakan.

1. *Prinsip territorialitas subjektif* adalah ketentuan bahwa berlakunya hukum ditentukan oleh lokasi di mana tindakan dikenakan, dan penanganan tindak pidana dapat diproses di negara yang berbeda.
2. *Prinsip territorialitas objektif* menerangkan bahwasannya hukum yang berlaku yaitu hukum di negara, yang di mana akibat utamanya tindakan tersebut dapat terjadi.
3. *Asas kewarganegaraan* yaitu prinsip bahwa hukum yang didasarkan pada kewarganegaraan pelaku.
4. *Asas kewarganegaraan pasif* yaitu prinsip yang sebenarnya berlaku pada kewarganegaraan korban.
5. *Asas perlindungan* yaitu prinsip bahwa hukum berlaku ditentukan oleh kemauan negara untuk menjaga kepentingan negaranya dari kejahatan yang dilakukan di luar wilayahnya.
6. *Asas universalitas* yaitu prinsip bahwa kejahatan antar negara yang diperlakukan sangat serius, semacam perompakan dan preman (kejahatan terhadap kemanusiaan), patuh kepada yurisdiksi semua negara.

Yurisdiksi Kejahatan Siber

Banyaknya masalah hukum yang timbul dalam pengungkapan kejahatan di ruang siber oleh aparat penegak hukum, terutama masalah kasus kejahatan siber

yang melibatkan unsur tidak biasa, menimbulkan kompleksitas terkait yurisdiksi atau kewenangan suatu negara dalam mengambil, menghentikan, memohon, dan memeriksa pelaku kejahatan tersebut. Kejadian ini dapat mengganggu kepentingan beberapa negara yang terlibat dalam kasus tersebut.

Yurisdiksi memiliki peran yang sangat penting dalam pengungkapan kejahatan siber yang berkarakter internasional. Dengan keadaan kejelasan mengenai yurisdiksi, suatu negara dapat dikenal memiliki kedaulatan penuh. Kekuasaan ini juga harus dihormati oleh negara lain sebagaimana mereka menghormati kekuasaan atau kedaulatan negara lain.

Yurisdiksi mencakup kekuasaan pengadilan, yaitu lingkup kekuasaan kehakiman dalam hal peradilan, hak dan kewajiban, serta tanggung jawab di suatu negara/wilayah, serta kewenangan hukum secara umum. Yurisdiksi melibatkan kompetensi hukum terhadap subjek hukum, termasuk individu, benda, atau peristiwa hukum di negara yang merdeka, termasuk wilayah darat, laut, dan udara.

Yurisdiksi konvensional suatu negara diakui oleh hukum internasional dengan batasan geografis tertentu. Namun, teknologi informasi dan transaksi elektronik bersifat internasional dan tanpa batas, sehingga belum ada kejelasan mengenai yurisdiksi suatu negara terkait tindakan preventif dan represif terhadap kejahatan siber yang bersifat tanpa batas.

Perundangan No. 19 Tahun 2016 tentang " *Perubahan Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik* " mengatur bahwa pemerintah Indonesia memiliki yurisdiksi untuk menutup akses atau sistem informasi yang melanggar undang-undang. Selain itu, penyidik memiliki kewenangan dalam melakukan penyelidikan dan penyitaan terhadap instrumen yang diduga terlibat dalam kejahatan siber, yang telah diatur dalam Pasal 43 ayat (3), (4), (5) huruf h, dan (7a).

Menurut Masaki Harmano ada tiga jenis yaitu yurisdiksi tradisional sebagai landasan analisa tentang permasalahan dalam yurisdiksi kejahatan siber.[6]

1. Yurisdiksi Legislatif

Yurisdiksi legislatif yaitu kewenangan suatu negara dalam menciptakan undang-undang untuk kepentingan masyarakat, dengan memperhatikan kepastian hukum dan perkembangan yang terjadi di dalam masyarakat saat ini. Dalam konteks kejahatan siber yang melintasi batas negara, sering kali terjadi kebingungan mengenai negara mana yang memiliki wewenang terhadap aktivitas yang dilakukan oleh individu di dunia maya, sehingga muncul masalah seperti "pilihan hukum ".

[6] Masaki Harmano, "*Comparative Study in The Approach to Jurisdiction In Cyberspac*" Chapter: The Principle of Juridiction,, hal.I. lihat dalam Barda Nawawi Arief, *Tindak Pidana Mayantara,* Raja Grafindo Persada, Jakarta, 2006.,hal.27-28.

2. Yurisdiksi Untuk Memperhitungkan

Diartikan sebagai tanggung jawab negara untuk melaksanakan prosedur pemeriksaan acara pada seseorang pang patut diduga sebagai orang yang melakukan kejahatan siber. Pada yurisdiksi ini, masalah yang muncul adalah pilihan hukum.

3. Yurisdiksi Untuk Melakukan

Tanggung jawab wewenang negara yang melaksanakan eksekusi akan pelaku kejahatan mendapatkan hukuman, baik memalui pengadilan atau pengenaan sanksi adnistratif atau tuntutan untuk membayar ganti rugi.

Masaki harmano membedakan pengertian yurisdiksi siber dari aspek dunia virtual (maya) dan aspek hukum. Dari aspek maya, yurisdiksi siber dapat diartikan menjadi (Kekuasaan sistem operator dan para user atau pemakai untuk ketentuan aturan dan menyamakan pada komunitas pengguna (users) di ruang virtual. Sedangkan, aspek hukum yurisdiksi siber yaitu kewenangan secara jasmani oleh pemerintah dan tanggung jawab memeriksa kepada pengguna internet atau aktivitas mereka di ruang siber.

Menurut kutipan **Masaki Harmano** yang disebutkan oleh **Barda Nawawi Arief**, terdapat tiga wilayah yurisdiksi yang terkait dengan pengaturan dan pelaksanaan pengawasan di dunia maya atau ruang siber. Ketiga kategori yurisdiksi tersebut meliputi *yurisdiksi legislatif, yurisdiksi yudisial, dan yurisdiksi eksekutif*. Dalam konteks ini, negara memiliki kekuasaan untuk membuat undang-undang yang berkaitan dengan ruang siber, menjalankan sistem peradilan untuk menyelesaikan sengketa yang muncul, dan melaksanakan tindakan eksekutif untuk mengawasi dan menegakkan hukum terkait dengan peristiwa, objek, dan individu yang berada di ruang siber.[7]

Berdasarkan tiga yurisdiksi oleh **Masaki Harmano** tersebut, bahwa perbuatan yang bertentangan dengan perundangan ITE ketika warganegara Indonesia memenuhi tindak pidana diluar Indonesia *(Asas Nasioanlitas aktif)* tanpa akibat yang dirasakan di Indonesia. Masalah yang dibahas dalam kutipan tersebut terkait dengan *yurisdiksi yudisial* dan *yurisdiksi eksekutif* dalam konteks ruang siber. *Yurisdiksi yudisial* mencakup kekuasaan untuk mengadili dan menetapkan hukum, sedangkan *yurisdiksi eksekutif* melibatkan pelaksanaan putusan dan tindakan terkait. Kedua yurisdiksi ini sangat berhubungan dengan kekuasaan wilayah dan hukum di masing negara. Setiap negara memiliki kebebasan dalam menentukan konstitusi dan sistem hukumnya sendiri, dan tidak dapat memaksakan hukumnya terhadap negara lain yang berhadapan dengan kedaulatan juga konstitusi negara tersebut. Maka, aturan hukum hanya berdasar di negara yang berkepentingan. Dalam mengatasi kejahatan

[7] Barda Nawawi Arief, *Kapita Selekta Hukum Pidana,* PT. Citra Aditya Bakti, Bandung 2003, Hal 253.

siber, penting adanya perjanjian internasional dan kerjasama antar negara untuk menangani kejahatan siber.

Dalam tulisannya yang berjudul "*Jurisdiction in Cyberspace: A Theory of International Spaces*,"[8] **Darrel Menthe** menjelaskan tentang keberadaan wilayah teritorial yang tunduk pada hukum internasional yang disebut "*ruang internasional*" atau "*international spaces*". Sekarang, ada tiga jenis ruang internasional dapat disebutkan, yaitu luar angkasa, dan lautan luas. Pada konteks dunia maya atau ruang siber, yurisdiksi menghadapi tantangan dalam hal konsep pengadilan dalam negeri dan pengadilan luar negeri yang semacamnya. Berbeda dengan yurisdiksi tradisional bisa melibatkan dua atau tiga yurisdiksi dan saling bertentangan, dalam kasus kejahatan siber, hukum yang berlaku cenderung bersifat universal dan tidak terbatas pada wilayah tertentu.

Pengakuan **Darrel Menthe** terhadap pembedaan 3 jenis Yurisdiksi yang diakui secara internasional, yaitu: *yurisdiksi legislatif, yurisdiksi yudikatif, dan yurisdiksi eksekutif*.[9]

Di dunia maya, **Darrel Menthe** mengatakan bahwasannya yurisdiksi di dunia maya memerlukan prinsip jelas dari hukum internasional, dan cuma melalui prinsip yurisdiksi dalam hukum internasional ini negara dapat menghimbau untuk memperoleh penanggulangan yang sama terhadap pertanyaan mengenai yurisdiksi internet.

Beberapa teori **Darrel Menthe** yang berdasar di Amerika Serikat tentang dunia maya.

1. **Teori pengunggah dan pengunduh.**
   Dalam teori ini penguna daripada jaringan internet dalam dunia maya bisa diartikan ada dua hal utama yang dilakukan untuk saling berinteraksi yaitu *Pengunggah* sebagai bagian yang membagikan informasi kedalam dunia maya dan *Pengunduh* yaitu bagian yang memakai informasi, atau pengguna melakukan keduanya dalam interaksinya dalam dunia maya. Suatu negara dapat membatasi atau melarang terhadap kegiatan *Pengunggah* dan *Pengunduh* jika menggangu atau bertentangan dengan kepentingan negara.
2. **Teori hukum server.**

[8] Darrel Menthe, *Jurisdiction in Cyberspaces : A Theory of International Spaces,* diakses di http://www.mttlr.org/vlogfour/menthe.html, hlm. 2. Cf. Walker, Clive, Andrew Ashworth, *the criminal law review,* special Edition, Sweet and Maxwell, 1998, hlm. 51 dst. Cf. Koop, Bert-Jaap,(ed.), *ICT Law and Internationalisation, A Survey Of Government Views, Kluwer Law International,* 2000, hlm. 40-dst.

[9] Darrel Menthe, *Jurisdiction in Cyberspaces : A Theory of International Spaces,* diakses di http://www.mttlr.org/vlogfour/menthe.html

Teori ini, semacam halaman web yang dihosting oleh server di *Stanford University* dianggap berada di lokasi fisik dan patuh pada hukum California. Tetapi, penerapan teori ini menjadi berat karena seringkali pengguna yang mengunggah konten berada di yurisdiksi asing atau mentransmisikan data secara anonim, sehingga lokasinya sulit untuk diketahui.

3. **Teori ruang internasional.**
   Hukum dalam dunia maya dinyatakan sebagai lingkungan hukum yang terbagi dan independen dari hukum konvensional. Setiap negara memiliki kebesaran yang sama di dalamnya. Teori ini, **Darrel Menthe** mengusulkan bahwa dunia maya harus diakui sebagai "*Ruang Keempat*". Terhadap hukum internasional, ada pemahaman tentang ruang luas luar angkasa sebagai "*ruang dimensi keempat* ", di mana kegiatan yang terjadi di sana dibuat secara kolektif oleh negara-negara. Analogi ini diterapkan pada kegiatan di dunia maya, di mana semua kegiatan di dalamnya diatur secara bersama oleh negara.

David R. Jhonson dan **David G. Post** dalam artikelnya berjudul "*And How Should the Internet Be Governet"?* memberikan 4 kriteria yaitu:[10]

1. Badan-badan pengadilan atau pejabat yang berwewenang sebagai pelaksana kontrol.
2. Pejabat Nasional melakukan perjanjian internasional.
3. Pembuatan suatu organisasi internasional baru yang secara khusus menangani masalah di dunia internet.
4. Pemerintah/ pengaturan tersendiri oleh para pemakai internet.

Jhonson dan **Post** beranggapan bahwasannya ruang siber harus dibedakan dengan prinsip tradisional, yang jika dipersamakan akan mengacaukan apabila diterapkan. Dengan perkembangan jaman hukum konvensional menjadi tidak dapat mengikuti untuk memberklakukan peraturan konvensional yang oleh karena hal itu dibutuhkan peraturan penyimpangan atau hukum khusus. Ruang siber harus diberlakukan secara tersendiri dari dunia nyata dengan mempergunakan hukum yang bertentangan untuk ruang siber.

Cristoper Doran beranggapan sebenarnya tatapan **Jhonson** dan **Post** tidak dapat ditetapkannya yurisdiksi perorangan terhadap para terduga internet, mustahil pandangan yang berpengaruh. Begitu dengan **Masaki harmano** berpendapat bahwa konsep **Jhonson** dan **Post** tidak terbentuk dalam kebenaran. Menurut **Masaki Harmano**, meskipun banyak masalah hukum yang mengenai dengan dunia siber, Tapi pengadilan di Amerika serikat sudah membolehkan pendekatan tradisional terhadap sengkata yurisdiksi ruang siber daripada membuat aturan baru mengenai hukum siber.

[10] David R. Jhonson and David Post, "*Law And Borders: The Rise Of Law In Cyberspace", 481 Standford law Review* 1996, hlm. 1367.

Penyelesaian masalah yurisdiksi dalam dunia maya menjadi sulit karena tidak adanya satu negara pun yang memiliki wewenang tunggal untuk menetapkan yurisdiksi di ruang siber. Hal ini disebabkan oleh kesulitan dalam menentukan lokasi geografis yang jelas dari wilayah ruang siber itu sendiri.

Menanggapi masalah yurisdiksi yang ada di dunia maya, dengan mengamati ketentuan dalam *konvensi kejahatan dunia maya,* **Barda Nawawi** memgemukakan prinsip universal dan Ubikuitas, menerangkan sebetulnya tindak pidana dapat dilaksanakan di beberapa wilayah negara dan melibatkan bagian dari wilayah teritorial negara lain harus dapat diperlakukan di bawah yurisdiksi setiap negara yang terlibat. Prinsip Ubikuitas tersebut pernah dinyatakan dalam *" Pertemuan Internasional para Ahli Penggunaan Pasal Pidana dalam Perlindungan Lingkungan, Internasional, Domestik, dan Regional "* Di Portland, Oregon, Amerika Serikat tanggan 19 samapai 23 maret 1994.

Pandangan **Soedarto**, untuk memohon seorang di depan pengadilan keadaan tindak pidana, hingga harus pasti untuk tempat dan waktu kejadian tindak pidana. Keputusan untuk waktu dibutuhkan untuk, apakah perundangan yang terkait bisa di tetapkan tentang tindak pidana itu. Sedangkan ketentuan atas tempat diperlukan untuk menentukan daripada prinsip yurisdiksi Indonesia dan kompetensi relatif tentang pengadilan yang berkuasa untuk mengadili tindak pidana tersebut.[11]

Locus Delicti yaitu tempat teradinya peristiwa pidana, yang ilmu hukum pidana dan yurisprudensi menduga mengememukakan beberapa teori, yaitu:

1. **Teori Perbuatan Materiil.**

Berdasarkan teori diatas yaitu tempat dimana terdakwa melakukan tindak pidana atau delik. Ada juga pengertian lain yaitu tempat tindakan terjadi agar delik dapat dilancarkan oleh pembuat atau tersangka/terdakwa. Waktu dan tempat pelaku dalam melakukan tindak pidana haruslah sama ketika perbuatan materiil diselenggarakan dapat menjadi waktu delik.

2. **Teori Instrumen Atau Alat Yang Digunakan.**

Teori perbuatan materiil dianggap kurang bisa menyelesaikan kesulitan-kesulitan yang timbul, dengan teori instrumen ini unsur-unsur daripada delik dapat menyelesaikan daripada proses penyidikan dan penuntutan pada persidangan atau sebagai alat bukti dalam persidangan.

3. **Teori Akibat.**

Dalam hal menentukan menyelesaikan masalah, dimana *locus Delicti* itu dilakukan. Untuk memenuhi daripada unsur-unsur tindak pidana teori terakhir

[11] Soedarto, *Hukum Pidana I,* Yayasan Sudarto, Semarang, 1991, hlm. 26-37.

adalah teori akibat yang dimana dengan adanya waktu dan tempat, alat untuk memenuhi tindak pidana dan dampak dari tindak pidana tersebut.

Acuan untuk menentukan yurisdiksi sampai saat ini belum ada kepastian berdasarkan teori-teori yang diungkapkan diatas sebagai acuan untuk menentukan yurisdiksi mana kejahatan siber tersebut untuk diadili, karena kejahatan siber memang bersifat transnasional sehingga setiap negara yang memiliki kepintingan berhak mengadili menurut yurisdiksinya. Kejahatan siber juga harus memperhatikan dampak dan seberapa besar kerugian yang ditimbulkannya. Penting untuk memperhatikan dampak dan tingkat kerugian yang ditimbulkan oleh kejahatan siber. Kejahatan siber yang memiliki dampak yang luas, termasuk yang terkait dengan masalah kedaulatan negara, keamanan, dan kemanusiaan, menjadi sangat penting. Oleh karena itu, kerjasama antarnegara dan kerjasama internasional sangat penting dalam menangani kejahatan siber tersebut. Dalam konteks ini, pendapat beberapa ahli hukum dapat menjadi acuan dalam menentukan yurisdiksi mana yang berwenang untuk mengadili kejahatan siber tersebut.

Menurut asas *au dedere au judicare,* dapat di jadikan dasar pemikiran untuk menanggulangi tindak pidana internasional. dapat dimengerti bahwa berdasarkan prinsip tersebut *"bahwa setiap negara berkewajiban untuk berkolaborasi dengan negara lain untuk dapat menuntut serta mengadili setiap orang yang layak pendapat sudah memenuhi suatu tindak pidana internasional"*. Prinsip tersebut dapat digunakan untuk masalah yurisdiksi siber.

Kesimpulan

Perkembangan teknologi dan internet telah menciptakan tantangan baru dalam penegakan hukum terkait kejahatan siber. Kejahatan siber tidak mengenal batas negara dan sering kali dilakukan oleh pelaku yang beroperasi di wilayah yang berbeda. Hal ini menciptakan kesulitan dalam menentukan yurisdiksi yang bertanggungjawab untuk menangani kasus-kasus tersebut. Ketika terjadi kejahatan siber, hukum yang berlaku di wilayah satu tidak selalu bisa diterapkan di wilayah lain. Proses penyidikan dan penuntutan menjadi rumit karena perbendaan hukum antarnegara. Selain itu, pelaku kejahatan sering menggunakan teknologi dan alat-alat untuk menyembunyikan identitas mereka yang membut proses penangkapan dan penuntutan menjadi lebih sulit.

Untuk mengatasi tantangan tersebut kerjasama internasional menjadi sangat penting. Negara-negara harus bekerjasama untuk meningkatkan pertukaran informasi, hukum yang berlaku, dan standar keamanan siber. Perlunya upaya kolaboratif antara lembaga penegak hukum, pemerintah, dan sektor swasta untuk memerangi kejahatan siber, dan perlunya upaya pemerintah untuk mengembangkan kerangka hukum yang lebih efektif dalam menangani kejahatan siber yang melintasi batas negara. Hal ini termasuk menyusun perjanjian bilateral atau multilateral yang memfasilitasi ekstradisi dan penuntutan pelaku kejahatan siber. Berdasarkan konteks tersebut peran lembaga internasional seperti interpol dan forum-forum internasional

yang berkaitan dengan kejahatan siber menjadi krusial. Mereka dapat menjadi platform untuk membagi informasi, koordinasi tindakan, dan pengembangan kerangka kerja hukum yang lebih kokoh. Secara keseluruhan, menghadapi kejahatan siber yang tidak mengenali batas negara membutuhkan pendekatan yang terkoordinasi dan kolabolatif dari berbagai pihak. Hanya dari kerjasama yang kuat dan kerangka hukum yang efektif kita dapat meningkatkan kemampuan untuk mengatasi ancaman kejahatan siber di era yang semakin terhubung ini (*Web Of The World*).

Ucapan Terimakasih

Kami sangat berterima kasih kepada Universitas 17 Agustus 1945 Surabaya, pemberi data, informan, dan responden atas dukungan dan kontribusinya yang berharga dalam penulisan artikel ini. Terimakasih atas waktu, pengetahuan, dan data yang telah diberikan. Kami menghargai upaya dan kerjasama yang telah diberikan, yang telah memungkinkan kami untuk menyusun artikel ini dengan baik. Ucapan terimakasih yang ikhlas kami bagikan kepada semua partisipan yang telah berperan terus penelitian ini.

DAFTAR PUSTAKA

Ahmad M. Ramli, *Cyber Law dan HAKI Dalam Sistem Hukum Indonesia.* Edisi ketiga,Bandung: PT Refika Aditama.2010.

Bu, Qingxiu (2018) *Extraterritirial jurisdiction vis-a-vis sovereignty in tracking transnasional counterfeits: between a rock and a hard place*. Sussex Search Online. Available: http://sro.sussex.ac.uk/id/eprint/76457/

Borka Jerman-Blazic, Tomaz Klobucar, "A New Legal Framework for Cross-Border Data Collection In Crime Investigation amongst Selected European Counties,"*Internasional Crimonal Journal of Cyber Criminology*. Vol. 13(2): 270-289. July-December, 2019.

Xiaobing Li, Yongfeng Quin (2018) *Research on Criminal Jurisdiction of Computer Cyber Crime*. Elsevier Ltd. Available: https://creativecommons.org/licenses/by-nc-nd/4.0

Nehaluddin Ahmad, Norulaziemah Zulkiffle, "Jurisdiction Issues in Cyberspace: An Overview in Respect of Brunei and Malaysia Compared to the United States System." *Journal of Southeast Asian Research.* Vol. 2022(2022), Article ID 384427.

Alexandra Perloff-Giles, "Transnasional Cyber Offenses: Overcoming Jurisdictional Challenges," *The Yale Journal of International Law.* Vol. 43:191.2017.

Yuxuan Li, "The Legal Dilemma of Criminal Jurisdiction of Cybercrime in China And The Way to improve it," *A Holl et al. (Eds.)*: ICHESS 2022, ASSEHR 720, PP. 3-15, 2022.

Yuliana Surya Galih, "Yurisdiksi Hukum Pidana Dalam Dunia Maya," Vol. 7, No.1-Maret,2019.

Dudi Badruzaman, "Kajian Hukum Tentang Internet Mobile Dalam Upaya Pencegahan D ampak Negatif Teknologi Informasi dan Komunikasi Indonesia," *Ajidikasi: Jurnal Ilmu Hukum,* Vol. 3, No.2.- Desember,2019.

Yulia P., Hanna P., Iryana B., "Jurisdictional Issues In The Digital Age," *Revista de Derecho,* Vol. 10 (I) 2021.-April, 2021

Cristos Velasco, "Cybercrime Jurisdiction: Past, Present and Future," *ERA Forum*, DOI10.1007/s12027-015-0379-y. June, 2015.

Ni Luh Ketut Dewi Yani Putri, " Konstruksi Hukum dalam Pembuktian Terhadap Kejahatan Mayaantara," *Jurnal Kertha Semaya,*Vol. 8, No. 8, E-ISSN: No 2303-0569, 2020.

Andysah Putera Utama S., "Pelanggaran Cybercrime dan Kekuatan Yurisdiksi di Indonesia," *Jurnal Teknik dan Informatika,* Vo.5, No.1-Januari, 2018.

Prasetiyo, Mukhtar Zuhdy, "Penegakan Hukum Oleh Aparat penyidik Cyber Crime dalam Kejahatan Dunia Maya (Cybercrime) di Wilayah Hukum Polda DIY," *Indonesian Journal of Criminal Law and Criminology,* Vol. 1, No.2-Juli 2020.

Daffa Ilhami, M., & Afifah, W. (n.d.). MENGUKUR SIFAT ASAS UNUS TESTIS NULLUS TESTIS TERHADAP PEMBUKTIAN TINDAK PIDANA KEKERASAN SEKSUAL. *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance*, *3*(2), 2023. https://doi.org/10.53363/bureau.v3i2.269

Penelitian, L., Pengabdian, D., Masyarakat, K., Simangunsong, F., & Afifah, W. (n.d.). *PROSIDING SEMINAR HASIL PENGABDIAN KEPADA MASYARAKAT*.