LEX LECTIO LAW JOURNAL

Lex Lectio : *Jurnal Kajian Hukum*
Volume 03 No. 01. Tahun 2024
E-ISSN: 3025-3276

Analisis Yurisdiksi Kriminal Penanganan Tindak Pidana Siber di Wilayah Hukum Kepolisian Daerah Bali

Komang Aldi Saskara
Universitas Mahendradatta
komangaldi234@gmail.com

Abstract *This cyber crime is also categorized as a transnational crime, because this crime does not recognize borders (borderless) and the time of the incident because the victim and perpetrator are often in different countries. This research will examine the concept and regulation of state criminal jurisdiction for dealing with cyber crimes and whether the concept for dealing with cyber crimes by the police at the Bali Regional Police is ideal. This research uses a type of empirical legal research using several types of approaches including a statutory approach, a conceptual approach and a legal psychology approach. The data sources used in this research are primary data sources and secondary data. The jurisdictional principles that form the basis for the application of criminal law in Indonesia to cyber crimes include the territorial principle and the protection principle. Meanwhile, the current concept of dealing with cyber crime is seen from the jurisdictional aspect, of course to ensnare the perpetrators takes quite a long time and is considered not ideal. It is hoped that the government will ratify the Budapest Convention on cybercrime so that the results of this ratification will become an instrument for Indonesia to collaborate with other countries in applying extraterritorial jurisdiction. The government provides the public with an understanding of ethics and responsibility in interacting in the cyber world by increasing public literacy awareness regarding cyber security. Apart from that, the police need to establish various forms of sustainable partnerships to support the quality of human resources in the IT sector, in addition to getting educated and trained human resources who can support cyber crime investigations.*

Keywords: Criminal Jurisdiction, Cyber, Bali Regional Police.

Abstrak *SeKejahatan siber ini juga dikategorikan sebagai kejahatan yang bersifat transnasional, oleh karena kejahatan ini tidak mengenal adanya batas wilayah (borderless) serta waktu*

Submitted: 10-02-2024 Accepted: 30-10-2024 Published: 30-10-2024

kejadian karena korban dan pelaku sering berada di negara yang berbeda. Penelitian ini akan mengkaji tentang konsep dan pengaturan yurisdiksi kriminal negara terhadap penanggulangan tindak pidana siber serta apakah konsep terhadap penanggulangan tindak pidana siber oleh kepolisian di Polda Bali telah ideal. Penelitian ini menggunakan jenis penelitian hukum empiris dengan menggunakan beberapa jenis pendekatan yang meliputi pendekatan perundang-undangan, pendekatan konseptual serta pendekatan psikologi hukum. Sumber data yang digunakan dalam penelitian ini adalah sumber data primer dan data sekunder. Prinsip yurisdiksi yang menjadi dasar berlakunya hukum pidana di Indonesia terhadap tindak pidana siber meliputi, prinsip teritorial dan prinsip perlindungan. Sedangkan konsep penanggulangan tindak pidana siber saat ini di lihat dari aspek yurisdiksinya tentu untuk menjerat para pelaku membutuhkan waktu yang cukup lama dan dianggap belum ideal. Kiranya pemerintah meratifikasi Konvensi Budapest tentang cybercrime agar hasil dari ratifikasi tersebut menjadi instrument bagi Indonesia menjalin kerja sama dengan negara lain dalam mengaplikasikan yurisdiksi ekstrateritorial. Pemerintah memberi pemahaman kepada masyarakat terhadap etika dan tanggungjawab dalam berinteraksi di dunia cyber melalui peningkatan kesadaran literasi masyarakat mengenai keamanan cyber. Selain itu, bagi kepolisian perlu kiranya menjalin berbagai macam bentuk kemitraan yang berkelanjutan dalam mendukung kualitas SDM dibidang IT, selain mendapatkan SDM terdidik dan terlatih yang dapat mendukung penyelidikan cyber crime.
Kata kunci: *Yurisdiksi Kriminal, Siber, Kepolisian Daerah Bali*

Pendahuluan

Salah satu fenomena revolusi industri 4.0 yang memperlihatkan pengaruh cukup siginifikan saat ini adalah internet. Setidaknya, perjalanan ruang dan waktu melalui internet telah memaksa ilmu pengetahuan dan teknologi untuk bergerak cepat tak terbendung. Namun demikian, perkembangan internet yang begitu pesat sebagai media informasia ada kalanya dapat menjadi pedang bermata dua, yaitu selain memberikan kontribusi bagi kesejahteraan, kemajuan serta peradaban manusia,

sekaligus juga menjadi sarana efektif dalam melakukan perbuatan melawan hukum.

Cyber crime sendiri dapat dikatakan sebagai bentuk kejahatan baru, karena kejahatan siber memiliki karakteristik yang sangat khusus, apabila dibandingkan dengan kejahatan-kejahatan konvensional lainnya. Bahkan kejahatan siber ini juga dikategorikan sebagai kejahatan yang bersifat transnasional, oleh karena kejahatan ini tidak mengenal adanya batas wilayah (borderless) serta waktu kejadian karena korban dan pelaku sering berada di negara yang berbeda (Petrus Reinhard Golose, 2006) . Sehingga kejahatan ini menjadi salah satu kejahatan yang cukup sulit untuk diselesaikan di negara mana pun seperti Indonesia.

Convention on Cybercrime tahun 2001 dapat saja menjadi alternatif kebijakan kriminalisasi di internet, namun dalam perkembangannya terdapat beberapa masalah mengenai pelaksanaan konvensi ini di komunitas internasional, dengan alasan konvensi ini lahir dalam tataran regional. Artinya banyak negara yang akan cenderung melakukan resistensi atau penolakan terhadap norma-norma, pengaturan, infrastuktur hukum, serta produk hukum yang lahir dalam lingkup regional dimana Negara tersebut bukan merupakan anggota.

Sebagai contoh, pada tanggal 22 Juni 2001, the European Committee on Crime Problems memutuskan membentuk suatu protokol tambahan (additional protocol) yang mengkriminalisasikan kejahatan terhadap penyebaran propaganda yang bersifat rasis dan xenophobic melalui jaringan komputer sebagai pelengkap dari Convention on Cybercrime tahun 2001. Terkait dengan hal tersebut, Amerika Serikat (AS) sebagai salah satu Negara yang meratifikasi konvensi, menolak tegas adanya protokol tambahan tersebut dengan alasan bahwa hal tersebut bertentangan dengan Amandemen pertama Konstitusi AS yang mengatur tentang kebebasan berekspresi (A. Cery Kurnia).

Berkaitan dengan kasus cyber crime, dalam pembahasan ini peneliti akan berfokus mengkaji permasalahan ini dengan melakukan penelitian di Polda Bali. Sebagai salah satu destinasi wisata nasional maupun internasional, Provinsi Bali yang menjadi bagian dari wilayah hukum Polda Bali, sesungguhnya menjadi salah satu daerah sasaran strategis bagi para pelaku cyber crime. Para pelaku kejahatan ini tidak hanya dilakukan oleh warga negara Indonesia saja, namun juga acap kali melibatkan warga negara asing yang berafiliasi dengan pelaku yang berada di luar negara Indonesia. Terhitung dari tahun 2020 sampai tahun 2022 kasus kejahatan cyber crime ini mengalami angka peningkatan yang cukup

signifikan, setidaknya sepanjang tahun 2020 terdapat 822 kasus dengan rincian 27 Laporan Polisi serta 795 Pengaduan Masyarakat, di tahun 2021 terdapat 617 kasus dengan rincian 48 Laporan Polisi serta 569 Pengaduan Masyarakat dan terakhir tahun 2022 terdapat 965 kasus dengan rincian 20 Laporan Polisi serta 945 Pengaduan Masyarakat.

Berbagai kasus cyber crime telah ditangani oleh Polda Bali dalam rangka menekan angka kejahatan di Indonesia, hanya saja jika ditelaah kembali terhadap praktiknya, sebagai kasus yang bersifat transnasional, tentu cukup menjadi sebuah hambatan personel kepolisian untuk segera mengungkap dan menangkap pelaku, yang disebabkan para pelaku yang melakukan kejahatan cyber di Indonesia cukup banyak yang terafiliasi dengan pelaku yang berada di negara lain, hal tersebut bisa di lihat dengan salah satu kasus cyber yang beberapa waktu lalu di tangani Polda Bali yaitu penangkapan para pelaku penyedia layanan judi online yang jaringan Kamboja, kendatipun dilakukan penangkapan terhadap sebagian pelaku tersebut, namun belum cukup untuk menekan kejahatan cyber tersebut, oleh karena server dari judi online tersebut berada di negara lain.

Berorientasi dari uraian di atas, maka pada kesempatan ini peneliti merasa tertarik melakukan suatu penelitian hukum dengan mengkaji sekaligus membahas mengenai konsep dan pengaturan yurisdiksi kriminal negara terhadap penanggulangan tindak pidana siber serta apakah konsep terhadap penanggulangan tindak pidana siber oleh kepolisian di Polda Bali telah ideal.

Method

Penelitian ini menggunakan jenis penelitian hukum empiris. Penelitian hukum empiris dalam bahasa Inggris, disebut empirical legal research. Menurut Abdulkadir Muhammad sebagaimana yang dikutip Muhaimin dalam bukunya (Muhaimin, 2020) menjelaskan "penelitian hukum empiris tidak bertolak dari hukum positif tertulis (peraturan perundang-undangan) sebagai data sekunder, akan tetapi dari prilaku nyata sebagai data primer yang diperoleh dari lokasi penelitian lapangan (field research). Prilaku nyata itu, hidup dan berkembang bebas seirama dengan kebutuhan masyarakat, ada yang dalam bentuk putusan pengadilan atau yang dalam bentuk adat istiadat kebiasaan". Kemudian akan digunakan beberapa jenis pendekatan meliputi pendekatan perundang-undangan, pendekatan konseptual serta pendekatan psikologi hukum. Sumber data yang digunakan dalam penelitian ini adalah sumber

data primer dan data sekunder sebagai data yang umumnya digunakan di dalam jenis penelitian hukum empiris. Dari sumber data tersebut kemudian akan dianalisis melalui analisis kualitatif.

Diskusi dan Hasil

Istilah tindak pidana berasal dari istilah yang dikenal hukum pidana (WVs) Belanda dan WvS Hindia Belanda (KUHP) yaitu *strafbaarfeit*. Kendati pun tidak ada penjelasan resmi mengenai *strafbaarfeit* itu, termasuk pula keseragaman oleh para ahli hukum dalam memberikan arti dan isi dari istilah itu, namun mengenai istilah tindak pidana ini tidak jarang pula acap kali dikatakan dalam bentuk istilah yang resmi dalam perundang-undangan pidana Indonesia.

Membahas mengenai tindak pidana sebagai fenomena sosial atas perilaku menyimpang yang selalu melekat dan tidak akan pernah berakhir sejalan dengan perkembangan dan dinamika sosial yang terjadi di masyarakat, dalam aspek kajian ini tindak pidana dimaksud adalah tindak pidana dunia maya atau tindak pidana siber (*cyber crime*) yang dalam aktifitas setiap pelakunya lebih menitikberatkan pemanfaatan sebuah teknologi informasi tanpa batas sebagai sarana utamanya.

Perlu kita ketahu bahwa pelaku *cyber crime* adalah mereka yang memiliki keahlian tinggi dalam ilmu computer, pelaku *cyber crime* umumnya menguasai algoritma dan ilmu pemrograman computer untuk membuat *script*/kode *malware*, mereka dapat menganalisis cara kerja sistem computer dan jaringan, dan mampu menemukan celah pasa sistem yang kemudian akan menggunakan sisi kelemahan tersebut untuk dapat masuk, sehingga tindakan kejahatan seperti pencurian data dapat berhasil dilakukan. Menurut Didik M. Arief Mansur dan Elisatris Gultom, bahwa *cyber crime* lahir disebabkan karena faktor kurangnya kemampuan atau pengetahuan dari aparat penegak hukum dalam menangani kasus siber (Sutarman, 2007).

Beberapa pendapat mengindentikkan tindak pidana siber dengan computer crime. The U.S. Department of Justice memberikan pengertien *computer crime* sebagai "*…any illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution*". Pengertian tersebut identik dengan yang diberikan oleh Organization of European Community Development, yang mendefinisikan *computer crime* sebagai: "*any illegal, unehtical or unauthorized behavior relating to the automatic processing and/or the transmission of data*" (Eliasta Ketaren, 2016).

Istilah mengenai *cyber crime* dalam *background paper* untuk lokakarya Kongres PBB X/2000 di Wina, Austria, sebagaimana yang dikutip Barda Nawawi Arief, di bagi ke dalam 2 (dua) kategori. Pertama, *cyber crime* dalam arti sempit (*in a narrow sense*) disebut *computer crime,* dan Kedua *cyber crime* dalam arti luas (*in a broader sense*) disebut *computer related crime* (Sahat Maruli T Situmeang, 2020). Sedangkan pengertian *cyber crime* secara umum adalah suatu perbuatan tanpa ijin dan melawan hukum dengan cara menggunakan komputer sebagai fasilitas utamanya atau target untuk melakukan kejahatan, dengan atau tanpa merubah atau merusak sistem komputer yang digunakan.

Kendatipun demikian terdapat juga ahli hukum lainnya yang memberikan pengertian mengenai *cyber crime* ini dengan makna lainnya, sebagaimana Widodo yang memberi penjelasan pengertian *cyber crime* dengan 2 (dua) kategori yakni dalam arti sempit dan arti luas. *Cyber crime* dalam arti sempit adalah kejahatan terhadap sistem komputer, sedangkan dalam arti yang luas mencakup kejahatan terhadap sistem atau jaringan komputer dan kejahatan menggunakan computer (Widodo, 2009). Sedangkan Judhariksawan dalam bukunya pengantar hukum telekomunikasi *cyber crime* ialah kegiatan yang memanfaatkan komputer sebagai media yang didukung oleh sistem telekomunikasi baik itu *dial up system*, menggunakan jalur telepon, atau *wireless system* yang menggunakan antena khusus yang nirkabel (Judhariksawan,2005).

Dengan demikian, *cyber crime* dapat dimaknai sebagai keseluruhan bentuk kejahatan yang ditujukan terhadap sistem komputer, jaringan komputer, dan para penggunan lainnya serta bentuk-bentuk kejahatan tradisional berupa tindak pidana dengan bantuan komputer.

Yurisdiksi merupakan salah satu masalah serius yang dihadapi penegak hukum jika berhadapan dengan kasus *cybercrime* yang melibatkan warga negara asing, oleh karena banyaknya kepentingan, tidak hanya kepentingan dari negara sendiri, namun juga kepentingan negara lain terhadap warga negaranya sendiri. Permasalahan mengenai yurisdiksi dalam *Convention on Cybercrime* yang dibuat oleh Dewan Eropa, secara khusus ditempatkan pada pasal tersendiri yakni pada pasal 22 yang terdiri dari 5 (lima) ayat, antara lain berbunyi sebagai berikut:

1. *Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles through 11 of this Convention, when the offence is committed:*
    a. *in its territory; or*

   b. *on board a ship flying the flag of that Party; or*
   c. *on board an aircraft registered under the laws of that Party; or*
   d. *by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.*
2. *Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.*
3. *Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.*
4. *This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.*
5. *When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution* (M.R, Afitrahim, 2012)

Instrument hukum memberikan landasan atau pedoman bagi penegak hukum yang diterapkan terhadap para pelaku *cyber crime*. Sebagai hukum positif, pembuatannya melalui mekanisme pembuatan Perundang-undangan, dan sekaligus melekat sifat *ius consitutum*, yakni menjadi hukum positif yang dapat memberikan sanksi bagi peristiwa ataupun perbuatan kriminal yang menggunakan komputer

Sebelum berlakunya Undang-undang Republik Indonesia Nomor 9 Tahun 2016 perubahan atas Undang-undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (disingkat UU ITE) yang mengatur kasus *cyber crime*. Penegak hukum menggunakan ketentuan KUHP dan ketentuan dalam beberapa undang-undang lain yang memiliki relevansi terhadap pengaturan tindak pidana *cyber crime* seperti Undang-undang Nomor 36 Tahun 1999 tentang telekomunikasi yang merupakan undang-undang selain KUHP yang memasukkan *cyber crime* sebagai salah satu pelanggaran dalam bidang telekomunikasi. Adapun pengaturan mengenai *cyber crime* di dalam undang-undang ini di atur dalam Pasal 38 dan Pasal 40 yang apabila di simpulkan, salah satu perbuatan yang termasuk dalam kategori *cyber crime* dalam pasal ini yaitu *illegal interception*.

Selain pengaturan tentang perbuatan yang termasuk dalam kategori *cyber crime*, berkenaan dengan yurisdiksi tindak pidana siber dalam pengaturan hukum nasional Indonesia, pengaturan yurisdiksi kriminal di dalam KUHP di atur Buku I pada Pasal 4 sampai dengan Pasal 9. Pengaturan yurisdiksi dalam rumusan KUHP ini menganut beberapa macam prinsip yurisdiksi, meliputi teritorial, perlindungan, nasional aktif, nasional pasif dan universal. Namun, khusus tentang tindak pidana siber sendiri, hemat penulis KUHP tidak mensyaratkan prinsip *dual criminality* yang bersifat terbatas untuk tindak pidana siber yang dilakukan di wilayah negara lain di luar Indonesia yang dalam konteks ini apabila berorientasi pada isi pasal 9 KUHP terdapat pengecualian dengan batasan yang di atur dalam substansi hukum internasional, sehingga apabila berorientasi pada Pasal 22 ayat (4) *Convention on Cybercrime* disebutkan negara peserta konvensi diperkenankan mempergunakan jenis-jenis yurisdiksi lainnya yang didasarkan hukum nasionalnya masing-masing. Artinya terdapat sebuah batasan untuk menjerat pelaku tindak pidana siber dengan sarana hukum pidana, sehingga tentu dapat menjadi celah untuk modus operandi tindak pidana siber atau tidak terjangkaunya perkembangan tindak pidana siber tertentu yaitu dengan memanfaatkan belum adanya harmonisasi atau pengaturan tindak pidana siber di suatu negara. Sedangkan dalam Undang-undang Nomor 36 Tahun 1999 tentang telekomunikasi tidak disebutkan secara gamblang dalam pasal tertentu, namun dari pengaturan Pasal 44 dapat disimpulkan apabila terjadi suatu pelanggaran terhadap gangguan telekomunikasi maka yang diterapkan ialah hukum Indonesia. Dan jika dicermati lebih jauh, prinsip yurisdiksi undang-undang ini cenderung menganut prinsip *objective territoriality* (teritorial objektif).

Hadirnya kebijakan Undang-undang Republik Indonesia Nomor 9 Tahun 2016 perubahan atas Undang-undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (disingkat UU ITE) tidak terlepas dari perkembangnya penggunaan teknologi. Kejahatan siber yang berkembang saat ini, merupakan dampak digitalisasi dan membatasi perbuatan-perbuatan yang dilarang menurut hukum. UU ITE sejatinya menjadi regulator berkenaan dengan transaksi elektronik dan kejahatan-kejahatan yang merupakan perluasan dari kejahatan yang tercantum dalam KUHP.

Beberapa muatan yang diatur dalam UU ITE meliputi transaksi elektronik, tindak pidana siber serta yurisdiksi tindak pidana siber. Khusus mengenai tindak pidana siber sebagai perbuatan yang dilarang di atur dalam pasal 27 sampai pasal 37. Konstruksi pasal-pasal tersebut mengatur

lebih detail tentang pengembangan modus-modus kejahatan tradisional sebagaimana tercantum dalam Kitab Undang-Undang Hukum Pidana (KUHP) (Yurizal, 2018). Sedangkan mengenai yurisdiksi tindak pidana siber sendiri di atur dalam pasal 2 dan 37 UU ITE. Ketentuan Pasal 2 UU ITE yang pada dasarnya menyatakan bahwa UU ITE berlaku terhadap setiap orang yang melakukan tindak pidana yang berada di dalam wilayah hukum Indonesia atau berada di luar wilayah hukum Indonesia dan mempunyai akibat hukum di wilayah hukum Indonesia atau di luar wilayah hukum Indonesia dan merugikan kepentingan hukum Indonesia. Ketentuan Pasal 2 UU ITE ini merupakan aturan yurisdiksi yang bersifat khusus atau *lex specialis* dari aturan yurisdiksi yang di atur dalam Buku I KUHP. Sehingga yurisdiksi kriminal dalam UU ITE hanya berlaku terhadap tindak pidana dalam UU ITE.

Pengaturan yurisdiksi kriminal dalam Pasal 2 UU ITE relative singkat dan padat sehingga dalam implementasinya diperlukan penafsiran dan pengempangan terhadap prinsip-prinsip yurisdiksi di dalam hukum internasional publik dan teori *locus delicti* dalam hukum pidana. Berdasarkan ketentuan Pasal 2 UU ITE prinsip yurisdiksi yang menjadi dasar berlakunya hukum pidana terhadap tindak pidana siber adalah:

1. Prinsip teritorial di dalam Pasal 2 UU ITE terkandung dalam rumusan yang berada di wilayah hukum Indonesia. Dalam rumusan selanjutnya ditegaskan juga prinsip teritorial objektif, yaitu dalam rumusan di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia. Di lain pihak dalam ketentuan ini tidak ada penegasan berlakunya prinsip teritorial subjektif, yang sangat penting dalam pemberantasan tindak pidana siber yang seringkali perbuatannya dimulai di suatu wilayah negara dan penyelesaiannya atau efeknya berada di wilayah negara lain. Namun demikian prinsip teritorial subjektif dapat digunakan dengan melakukan penafsiran.
2. Prinsip perlindungan dalam Pasal 2 UU ITE terkandung dalam rumusan di luar wilayah Indonesia dan merugikan kepentingan Indonesia. Prinsip perlindungan dalam ketentuan ini lebih luas dari yurisdiksi perlindungan yang ada dalam KUHP dan prinsip perlindungan umumnya yaitu untuk melindungi kepentingan vital suatu negara.

Permasalahan terkait yurisdiksi merupakan masalah vital yang didapatkan dalam penegakan terkait dengan tindak pidana siber, dikarenakan lokasi geografis, skala perbuatan, dan unsur lain yang menjadikan tindak pidana siber berbeda dari pidana konvensional lainnya,

membuat implementasi prinsip-prinsip yurisdiksi sulit untuk diterapkan. Hal ini tentu dapat di lihat dari berbagai hambatan aparat penegak hukum khususnya Kepolisian Daerah Bali yang masih memiliki beberapa hambatan yang salah satunya hambatan dalam aspek susbtantif hukum berkenaan dengan yurisdiksi sebagaimana yang di atur dalam rumusan pasal 2 Undang-undang Republik Indonesia Nomor 9 Tahun 2016 perubahan atas Undang-undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.Dalam rumusan pasal 2 tersebut menganut prinsip teritorial dan prinsip perlindungan yang dalam konteks ini prinsip teritorial hanya berorientasi kepada para pelaku yang melakukan tindak pidana diwilayah Indonesia saja, namun bagi warga negara asing, tidak semua negara yang memperbolehkan warga negaranya untuk di adili di Indonesia apabila melakukan kejahatan di luar wilayah negara Indonesia, sehingga pemberlakuan yurisdiksi teritorial ini sulit menjerat pelaku khususnya warga negara asing yang melakukan suatu kejahatan di luar wilayah yurisdiksi Indonesia. Sedangkan prinsip perlindungan yang berada di Pasal 2 UU ITE terkandung dalam rumusan di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia. Artinya prinsip perlindungan dalam ketentuan ini lebih cenderung diterapkan terhadap kejahatan-kejahatan yang merugikan kepentingan vital negara Indonesia.

Sedangkan bertalian dengan jenis tindak pidana siber lainnya rumusan dari pasal 2 UU ITE ini tentunya menjadi salah satu hambatan tersendiri dalam upaya penanggulangan tindak pidana siber di Indonesia oleh para aparat penegak hukum khususnya yang dilakukan para pelaku yang berada di luar wilayah Indonesia seperti penipuan dan pencurian data. Atau dengan kata lain jika negara Indonesia tidak memiliki perjanjian ekstradisi dengan negara lain yang memiliki kedaulatan atau yurisdiksinya sendiri, tentu akan berimplikasi dengan tidak adanya kepastian hukum bagi para warga negara Indonesia yang menjadi korban atas tindak pidana siber jenis lainnya yang tidak menyangkut kepentingan vital negara. Dalam hal ini mengenai hambatan Kepolisian Daerah Bali dalam penanggulangan tindak pidana siber berdasarkan aspek susbtansi hukum adalah mengenai yurisdiksi negara lain di mana para pelaku banyak yang melakukan tindak pidana siber dari luar negara Indonesia, sehingga untuk menjerat para pelaku membutuhkan waktu yang cukup lama dan kurang efektif.

Berorientasi dari masalah tersebut di atas, tentu kesulitan dari penegakan hukum terhadap kejahatan lintas negara ini dapat diklasifikasikan menjadi 3 (tiga) faktor yakni kesulitan penggunaan barang

bukti, kesulitan dalam investigasi, serta kesulitan melakukan pengadilan terhadap pelaku lintas negara (Ermanto Fahamsyah, Vicko Taniady, Kania Venisa Rachim, Novi Wahyu Riwayanti, 2022,) Serupa dengan pandangan yang dikemukakan Barbara Etter yang menjelaskan terkait kesulitan dalam timbulnya masalah yurisdiksi dalam kejahatan siber transnasional yakni:

1. Ketiadaan atas konsensus global mengenai jenis-jenis kejahatan komputer. Klasifikasi dari hukum domestik negara menyangkut permasalahan komputer cukup berbeda, seperti yang dibahas dalam landasan teori mengenai *cyber crime*. Artinya, sebuah instrumen hukum yang dapat menyatukan perbedaan tersebut harus hadir dalam upaya penyelenggaraan penegakan terhadap tindak pidana siber.
2. Kurangnya kualitas para penegak hukum terhadap penanganan tindak pidana siber.
3. Sifat transnasional yang dimiliki
4. Ketidakharmonisan hukum acara domestik negara terkait tindak pidana siber
5. Ketiadaan upaya sinkronisasi penegakan dan penanganan tindak pidana siber (dalam hal ekstradisi, investigasi, dan upaya bantuan lainnya) (Barda N. Arief, 2006).

Atas dasar tersebut tentu ruang siber harus diberlakukan dengan suatu parameter untuk pengelolaan/pemerintahan global melalui pengaturan bersama yang didasari beberapa parameter meliputi:

1. Pengalokasian pengaturan terkait yurisdiksi untuk negara-negara;
2. Harmonisasi regulasi terkait penegakan tindak pidana siber;
3. Sentralisasi organisasi yang berperan dalam pembuatan kebijakan dan kegiatan penegakan hukum terkait tindak pidana siber .

Berorientasi pada beberapa parameter di atas, tentu parameter-parameter tersebut dapat menjadi solusi dalam rangka mengatasi sulitnya penegakan hukum terhadap tindakan pada ruang siber. Pada poin ke 1 dan 2 dapat kita laksanakan dengan meratifikasi sebuah instrumen hukum internasional yang memiliki volume massa yang cukup memadai sekaligus terbuka secara universal, yakni dengan cara meratifikasi konvensi Budapest atau *Convention on Cybercrime* yang dibuat oleh Dewan Eropa atau setidak-tidaknya, menginisiasi model perjanjian multinasional dengan kerangka hukum Konvensi Budapest. Didalam konvensi tersebut terdapat beberapa pengaturan terkait yurisdiksi yang tentu dapat

dijadikan sebuah patokan dalam menyelesaikan konflik penentuan yurisdiksi suatu negara yang menjadi tempat di mana pelaku tindak pidana siber melakukan kejahatan.

Selanjutnya pada poin 3 dari parameter di atas yaitu keberadaan sebuah organ sentral dalam masalah penanganan tindak pidana siber dapat kita artikan dalam kancah domestik maupun internasional. Dalam ranah domestik, organ ini akan menjadi pengawas dan pengendali dalam sektor penegakan hukum di ruang siber. Sedangkan dalam konteks internasional, organ ini menjadi pusat penegakan hukum atas tindak pidana siber dalam konteks global, serta mengkonsolidasikan standar operasi atau pembuatan kebijakan yang bersifat preventatif dan responsive terhadap perkembangan penegakan tindak pidana siber. Pendapat penulis, satu-satunya organ internasional yang dapat memiliki kekuatan tersebut adalah Perserikatan Bangsa-Bangsa, namun sampai saat ini masih belum ada instrumen yang mengikat dari PBB terkait upaya penanggulangan tindak pidana siber.

Dengan demikian, secara umum hambatan penanggulangan tindak pidana siber oleh Kepolisian Daerah Bali apabila di analisa, selain adanya faktor struktur hukum yang menjadi aktor pelaksana peraturan perundang-undangan dan budaya hukum, hal yang paling krusial dalam menanggulangi tindak pidana siber tersebut cenderung terletak pada subtansi hukum khususnya terkait dengan permasalahan yurisdiksi. Dalam konteks ini, masalah hambatan dari aspek yurisdiksi ini terletak pada perbuatan para pelaku tindak pidana siber yang acap kali dilakukan di luar wilayah yurisdiksi Indonesia. Terlebih lagi apabila negara Indonesia sendiri tidak memiliki perjanjian ekstradisi dengan negara lain yang memiliki kedaulatan atau yurisdiksinya sendiri, tentunya kondisi ini akan berimplikasi dengan tidak adanya kepastian hukum bagi para warga negara Indonesia khususnya yang menjadi korban atas tindak pidana siber jenis lainnya yang tidak menyangkut kepentingan vital dari negara. Sehingga untuk menjerat para pelaku membutuhkan waktu yang cukup lama dan kurang efektif.

KESIMPULAN

Ketentuan Pasal 2 Undang-undang Republik Indonesia Nomor 9 Tahun 2016 perubahan atas Undang-undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, prinsip

yurisdiksi yang menjadi dasar berlakunya hukum pidana terhadap tindak pidana siber meliputi, prinsip teritorial dan prinsip perlindungan. Prinsip teritorial hanya berorientasi kepada para pelaku yang melakukan tindak pidana diwilayah Indonesia saja, namun bagi warga negara asing, tidak semua negara yang memperbolehkan warga negaranya di adili di Indonesia apabila melakukan kejahatan di luar wilayah negara Indonesia, sehingga pemberlakuan yurisdiksi teritorial ini cukup sulit menjerat pelaku khususnya warga negara asing yang melakukan suatu kejahatan di luar wilayah yurisdiksi Indonesia. Sedangkan prinsip perlindungan yang berada di Pasal 2 UU ITE terkandung dalam rumusan di luar wilayah hukum Indonesia serta merugikan kepentingan yang dimiliki Indonesia. Artinya prinsip perlindungan dalam ketentuan ini lebih cenderung diterapkan terhadap kejahatan yang dianggap dapat merugikan kepentingan keamanan negara Indonesia. Konsep penanggulangan tindak pidana siber saat ini di lihat dari aspek yurisdiksinya tentu untuk menjerat para pelaku membutuhkan waktu yang cukup lama dan dianggap belum ideal.

Sebagai masukan kiranya agar pemerintah meratifikasi Konvensi Budapest tentang *Cybercrime*. Sehingga kedepannya hasil ratifikasi tersebut dapat menjadi instrument bagi Indonesia menjalin kerja sama dengan negara peserta lain dalam mengaplikasikan yurisdiksi ekstrateritorial terutama apabila terjadi tindak pidana siber yang dilakukan pelaku dari luar wilayah Indonesia yang merugikan warga negara Indonesia serta diharapkan bagi Pemerintah harus memberi pemahaman kepada masyarakat terhadap etika dan tanggungjawab dalam berinteraksi di dunia cyber melalui peningkatan kesadaran literasi masyarakat mengenai keamanan cyber. Selain itu, bagi kepolisian perlu kiranya menjalin berbagai macam bentuk kemitraan yang berkelanjutan dalam mendukung kualitas SDM dibidang IT, disamping mendapatkan SDM terdidik dan terlatih yang dapat mendukung penyelidikan *cyber crim*e.

Bibliography

Arief, Barda N. 2006. *Tindak Pidana Mayantara Perkembangan Cybercrime di Indonesia*. Jakarta : PT. Raja Grafindo Persana

Fahamsyah, Ermanto, Taniady, Vicko, Rachim, Kania Venisa, Riwayanti, Novi Wahyu. 2022. *Penerapan Prinsip Aut Dedere Aut Judicare Terhadap Pelaku Cybercrime Lintas Negara Melalui Ratifikasi*

Budapest Convention. Jurnal Hukum dan Syariah De Jure, Vol. 14 No. 1. https://ejournal.uin-malang.ac.id

Golose,Petrus Reinhard. 2006. *Perkembangan Cyber Crime dan Upaya Penangananya oleh POLRI*, Buletin Hukum Perbankan dan Kebanksentralan. Vol. 4 No. 2

Judhariksawan,2005, *Pengantar Hukum Telekomunikasi*, Jakarta, PT Raja Grafindo Persada

Ketaren, Eliasta. 2016. *Cybercrime, Cyber Space, Dan Cyber Law*. Jurnal TIMES, Vol. V No 2 : 35-42.https://ejournal.stmik-time.ac.id

M.R, Afitrahim. 2012. *Yurisdiksi Dan Transfer Of Proceeding Dalam Kasus Cybercrime*. Tesis. Jakarta. Fakultas Hukum Universitas Indonesia

Mansur, Didik M. Arief dan Gultom, Elisatris. 2009. *Cyber Law : Aspek Hukum Teknologi Informasi*. Bandung : PT Refika Aditama

Widodo. 2009. *Sistem Pemidanaan Dalam Cyber Crime*. Yogyakarta : Laksbang Meditama

Muhaimin. 2020. *Metode Penelitian Hukum*. Cetakan Pertama. Mataram : Mataram University Press.

Yurizal. 2018. *Penegakan Hukum Tindak Pidana Cyber Crime di Indonesia*. Malang : Media Nusa Creative