ANALISIS YURIDIKSI UNIVERSAL TERHADAP KEJAHATAN SIBER YANG DILAKUKAN WARGA NEGARA TIONGKOK DI BALIKPAPAN

Zaqia Bachraq[1]

Abstract: *The Universal State Jurisdiction Law has not been fully implemented in the case of cyber crimes in Balikpapan, Indonesia. This cyber crimes commited by 42 Chinese Nationalty in Balikpapan, the cyber crimes committed by them are illegal access and online fraud. This case is handled by The Universal State Jurisdiction Law who has a legal instrument of law number 11 of 2008 concerning information and electronic transactions which also discucced cyber crimes in it. However, in its implementation it turns out that only laws related to immigration violations are applied. The Universal State Jurisdiction Law is not applied due to several reasons. The reasons is Indonesia has not ratified the Budapest Convention and Indonesia does not have an extradition treaty with China. So there is no binding basis for China to return the citizens to be prosecuted in Indonesia.*
Keywords: *Cyber Crimes, Juridiction, China.*

Pendahuluan

Kemajuan teknologi, informasi dan komunikasi dewasa ini memberikan banyak kemudahan bagi masyarakat terlebih lagi perkembangan internet yang membuat berbagai transaksi menjadi mudah tanpa harus melakukan pertemuan secara langsung. Namun kemajuan ini juga memunculkan berbagai resiko seperti kejahatan siber yang dilakukan oleh pihak-pihak yang tidak bertanggung jawab.

Kejahatan siber merupakan tindakan kriminal non tradiosional yang berbasis teknologi komputer dan internet (Wahid & Labib, 2005). Dalam arti luas, tindakan ilegal yang dilakukan dengan menggunakan teknologi komunikasi dan informasi serta jaringan internet disebut sebagai kejahatan siber yang meliputi kegiatan penyerangan terhadap sistem keamanan komputer dan data yang diproses oleh sistem komputer demi mencapai keuntungan pribadi dan merugikan orang lain (Syafnidawaty, 2020).

Kejahatan siber yang memiliki sifat *transbiundaries* atau tidak terbatas teritorial mengakibatkan terjadi tindakan kejahatan di ruang siber atau internet yang juga dikenal dunia maya, maka hal ini tentu akan menjadi urusan banyak pihak termasuk negara. Sehingga dalam dunia internasional terdapat pengelompokan jenis kejahatan siber yaitu, *offence against Confidentiality, integrity and availability of computer systems data, content related offences, copyright and trademark related offences, Computer related offences, combination offences, cyberterrorism, cyberwarfare,* dan *cyber laundering* (Prawiro, 2018).

Indonesia merupakan salah satu negara yang sering mengalami kejahatan siber, seperti *phising, carding, ransomware attack, online fraud, SIM swap, deface website and email skimming, OTP fraud, data forgery, illegal content, cyber terrorism, syber espionage* dan penjiplakan situs orang lain. Hal ini membuat pemerintah Indonesia membuat undang-undang yang mengatur mengenai informasi dan transaksi elektronik untuk menangani masalah-masalah tersebut.

Kejahatan siber di Indonesia menurut direktorat tindak pidana siber menyatakan bahwa penanganan kasus kejahatan siber masih dibawah 50%, dengan jumlah kasus kejahatan siber yang mencapai lebih dari 3 ribu kasus. Hal ini membuat banyak pihak-

[1] Mahasiswa Program S1 Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Mulawarman. E-mail :

pihak yang tidak bertanggung jawab mudah melakukan kejahatan mereka. Seperti kasus *illegal access* yang dilakukan 42 warga negara asing (WNA) dari Tiongkok di Balikpapan, Kalimantan Timur. Pada April 2016 pihak imigrasi bandara Sultan Aji Muhammad Sulaiman dan Polres Balikpapan melakukan penangkapan warga negara asing yang akan melakukan penerbangan ke kota Medan, namun WNA tersebut tidak membawa passport sehingga ditahan karena pelanggaran imigrasi (PRO Balikpapan, 2016).

Setelah dilakukannya pemeriksaan terhadap 42 WNA, ternyata terindikasi melakukan tindak kejahatan siber yang kemudian dilakukan penangkapan terhadap WNA tersebut. Pada tanggal 27 April 2016 sebanyak 8 anggota Interpol Republik Rakyat Tiongkok yang didampingin oleh Kabaq Kejahatan Internasional divisi Hubungan Internasional Mabes Polri mendatangi lokasi dimana pelaku melakukan kegiatan *illegal access* di Jalan Jendral Sudirman Balikpapan dan melakukan pemeriksaan tindakan kejahatan siber yang dilakukan oleh WNA (PRO Balikpapan, 2016).

Kejahatan siber yang dilakukan oleh WNA tersebut termasuk dalam UU Informasi dan Transaksi Elektronik nomor 8 tahun 2011 yang telah diubah menjadi UU nomor 19 tahun 2016 pasal 27-30 tentang perbuatan yang dilarang. Dalam hal ini pelaku dapat dikenakan pidana pada pasal 2 KUHP yang berlaku di Indonesia bagi setiap orang yang melakukan tindakan pidana di wilayah kedalutan Indonesia (Direktorat Jendaral Peraturan Perundang-undangan, 2016).

Kasus kejahatan ini menjadi dilematis karena terjadi antara dua negara yaitu Indonesia dan Republik Rakyat Tiongkok yang menyebabkan pelaksanaan hukumnya menyangkut yuridiksi kedua negara. Terlebih lagi kejahatan yang dilakukan merupakan kejahatan siber yang merupakan kejahatan tanpa batas wilayah, dan dalam prinsip yuridiksi pada hukum internasional memiliki dasar yang sama yaitu wilayah yang jelas dimana kejahatan terjadi (Arianti, 2014).

Sebenarnya prinsip yuridiksi pada hukum internasional tersebut dapat menjadi landasan bagi pemerintah Indonesia dalam melakukan tindak pidana, namun setelah melakukan berbagai macam pemeriksaan, para pelaku hanya dijatuhi sanksi pasal 71 hurud d UU nomor 06 tahun 2011 tentang keimigrasian, yaitu deportasi. Terkait kelanjutan pemeriksaan atas kasus yang dilakukan para WNA, pihak kepolisian Tiongkok meminta untuk dilakukan di negara mereka (Hazliansyah, 2016).

Padahal instrumen hukum internasional yang mengatur masalah kejahatan siber telah ada dalam *Convention of Cybercrime* pada tahun 2001 yang dilakukan oleh Uni Eropa. Dalam konvensi tersbebut telah mengatur jenis kejahatan siber apa saja yang dapat dipidanakan, serta juga mengatur pemberlakukan yuridiksi. Subtansi dalam konvensi tersebut mencakup area yang luas, bahkan terdapat kebijakan yang bertujuan untuk melindungi masyarakat dari kejahatan siber (Putra, 2014).

Kerangka Teori dan Konsep

Yurisdiksi

Yurisdiksi berarti bentuk kedaulatan dan berkaitan dengan kepemilikan hukum. Kedaulatan disini berarti negara yang merdeka. Kedaulatan menjadi instrument penting bag Negara untuk data menentukan ketetapan hukum nasionalnya (Halim & Azhar, 2020). Yurisdiki secara etimologis berasal dari kata *yuris* yang berarti kepunyaan menurut hukum dan dictio yang berarti sabda, ucapan dan perkataan. Menurut James

George Dalam arti luas yurisdiksi berarti kekuasaan Negara untuk menetapkan hukumuntuk menerapkan hukum dan untuk menuntut atau mengadili (Suseno, 2012:53).

Secara umum Negara-negara didunia memiliki karakteristik yang berbeda-bedadalam melaksanakan yurisdiksi secara historis dan geografis. Seiring dengan berkembangnya teknologi transportasi dan komunikasi, aktivitas manusia relatif tidak lagi dipengaruhi dengan faktor geografis (Suyudi, 2017). Penerapan yurisdiksi dilaksanakan dengan beberapa prinsip secara umum (Juwana,2006), yaitu:

a. Prinsip teritorial yang merupakan implementasi dari konsep kedaulatan teritorial yang dimiliki negara yang berdaulat. Berdasarkan prinsip teritorial, suatu Negaramemiliki yurisdiksi terhadap setiap tindak pidana dan pelakunya yang dilakukan diwilayahnya. Prinsip ini merupakan prinsip yurisdiksi yang utama di gunakan dalam melaksanakan yurisdiksi Negara. Prinsip ini dibagi menjadi 2 yaitu: (Adolf, 2002)
    i. Prinsip teritorial subjektif yang berarti suatu Negara dapat menerapkan yurisdiksi teritorialnya terhadap tindak pidana yang dilakukan di wilayahnya, namun penyelesaiannya dilakukan atau terjadi di wilayah Negara lain.
    ii. Prinsip teritorial objektif yang berarti suatu Negara dapat menerapkan yurisdiksi teritorialnya terhadap tindak pidana yang dilakukan di Negara lain namun penyelesaiannya dilakukan atau terjadi diwilayah negaranya dan mengganggu ketertiban sosial dan ekonomi di negaranya.

    Ketentuan prinsip ini terdapat pada pasa 2 KUHP, yang dimaksudkan kepada setiap warga Negara Indonesia maupun warga Negara asing serta mencakup tanah daratan, laut dan udara. Dalam hal ini Indonesia memiliki kedaulatan untuk menciptakan hak untuk menuntut, mengadili, dan menghukum setiap orang yang melakukan tindak pidana di wilayah Indonesia.
b. Prinsip nasional aktif, prinsip ini digunakan dalam pelaksanaan yurisdiksi Negara berdasarkan pada nasionalitas atau kewarganegaraan. Yang berarti berdasarkan prinsip ini Negara mempunyai yurisdiksi terhadap warga negaranya yang melakukan tindak pidana didalam yurisdiksi Negara lain. Adanya ikatan nasionalitas atau warga Negara dengan negaranya ditunjukkan dalam prinsip ini (Adolf , 2002). Prinsip nasional aktif terdapat dalam Pasal 5 KUHP yang berbunyi, sebagai berikut :

    "(1) Ketentuan pidana dalam perundang-undangan Indonesia berlaku bagi warganegara yang di luar Indonesia melakukan : Ke-1. Salah satu kejahatan tersebut dalam Bab I dan II Buku kedua dan Pasal-Pasal 160, 161, 240, 279, 450, dan

    451. Ke-2. Salah satu perbuatan yang oleh suatu ketentuan pidana dalam perundang-undangan Indonesia dipandang sebagai kejahatan, sedangkan menurut perundangundangan negara di mana perbuatan dilakukan diancam dengan pidana. (2) Penuntutan perkara sebagaimana dimaksud dalam butir 2 (dua) dapat dilakukan juga jika terdakwa menjadi warga negara sesudah melakukan perbuatan."
c. Prinsip Nasional Pasif, prinsip ini didasarkan pada nasionalitas atau

kewarganegaraan, dalam hal ini kewarganegaraan korban. Berdasarkan prinsip ini suatu Negara memiliki yurisdiksi untuk mengadili pelaku tindak pidana di luar neegaranya yang menimbulkan kerugian kepada warga negaranya, dasarnya adalah bahwa setiap Negara berhak untuk melindungi warga negaranya di luar negeri apabila Negara teritorial tempat tindak pidana dilakukan tidak mengadili pelaku.

d. Prinsip Perlindungan, prinsip ini digunakan untuk menerapkan yurisdiksi suatu Negara berdasarkan perlindungan kepentingan Negara yang bersifat vital, contohnya seperti keamanan dan intergritas atau kepentingan ekonomi Negara. Atas prinsip ini Negara memiliki yurisdiksi terhadap WNA yang melakukan tindak pidana di luar wilayah Negara tersebut dan mengancam keamanan dan keutuhan Negaranya.
e. Prinsip Universal, prinsip universal digunakan dalam melaksanakan yurisdiksi Negara berdasar pada tindak pidana yang membahayakan kepentingan masyarakat internasional secara keseluruhan. Berbeda dengan prinsip-prinsip yang lain, prinsip ini dilaksanakan tidak berdasarkan hubungan antara Negara dengan tindak pidana tersebut. Berdasarkan the Princeton principle on universal jurisdiction, yurisdiksi universal adalah yurisdiksi yang diberlakukan terhadap terhadap sifat kejahatan yang tanpa melihat tempat kejahatan dilakukan, kebangsaan dari pelaku kejahatan, kebangsaan korban kejahatan dan keterkaitan lain dengan Negara yang melaksanakan yurisdiksi. Terdapat beberapa jenis kejahatan yang termasuk dalam yurisdiksi universal yaitu pembajakan, perbudakan, kejahatan perang, kejahatan terhadap perdamaian, kejahatanterhadap kemanusiaan, genosida dan penyiksaan, yang antara lain kejahatan tersebut termasuk dalam kejahatan berat dalam hukum internasional.

Dalam penegakan hukum tindak pidana siber, ketidakmampuan suatu Negara untuk mengungkap kejahatan transnasional yang ruang lingkupnya luas dan tersebar akan menimbulkan masalah berkaitan dengan prinsip yurisdiksi. Hal tersebut mempengaruhi penegakan hukum dalam penanganan kasus kejahatan siber baik Negara-negara maju yang memiliki kemampuan relatif tinggi sekalipun. (Suseno, 2009:41-42)

***Convention on Cybercrime* (Konvensi Budapest)**

Convention on Cybercrime atau konvensi Budapest merupakan konvensi pertama yang membahas regulasi seputar kejahatan di dunia maya atau *cybercrime*. Pada tahun 2001 bulan November konvensi Budapest pertama kali digelar di kota Budapes, Hongaria. Konvensi Budapest dikenal juga sebagai *Convension of cybercrime* yang telah dimasukkan kedalam *European Treaty Serie* dengan Nomor 185, karena memang yang mengusungkan konvensi ini adalah Dewan Eropa di Strashburg, Perancis dengan para dewan dari Negara-Negara pengamat di Eropa antara lain, Tiongkok, Kanada, Jepang, dan Filipina. Pada awal pertemuannya konvensi Budapest membahas seputar substansi kejahatan siber yang mencakup area yang cukup luas, serta kebijakan kriminalisasi pelaku kejahatan siber dengan tujuan melindungi masyarakat dari kejahatan siber melalui undang-undang maupun kerjasama Internasional.

Menurut para ahli terdapat tujuan dan pertimbangan terkait dengan

diselenggarakannya konvensi Budapest. Amrulloh dkk pada tahun 2009 menyebutkan tujuan dan pertimbangan diselenggarakannya konvensi ini antara lain:
"1. Harmonisasi unsur-unsur hukum domestic pidana substantive pelanggaran dibidang kejahatan cybercrime, yang merujuk dan sesuai dengan undang-undang yang berlaku dan mendorong kerjasama internasional."
"2. Menyediakan untuk pidana kekuatan domestik prosedural hukum yang diperlukan untuk investigasi dan penuntutan tindak pidana tersebut serta pelanggaran lainnya yang dilakukan dengan menggunakan sistem komputer atau bukti dalam kaitannya dengan yang dibentuk elektronik."
"3. Mempersiapkan sebuah cara yang efektif untuk melakukan kerjasama internasional antar negara."

Sama seperti halnya hukum nasional yang ada di Indonesia Konvensi Budapest juga turut mengatur dan menetapkan bentuk-bentuk kejahatan siber apa saja yang dapat di kriminalisasi melalui konvensi ini, antara lain: (Geneva Convention Dan Budapest Convention, 2001)

1. *Illegal Content* (Konten Illegal), merupakan kegiatan melenggar hukum dengan cara memasukkan data dan informasi yang tidak baik ke dalam internet yang dapat diakses oleh orang lain.
2. *Illegal access* (akses illegal), merupakan kegiatan mengakses sistem komputer atau data dari internet dengan tanpa izin dari pemiliknya, data tesebut yang mencakup pelanggaran dasar dari ancaman-ancaman yang berbahaya dari segi serangan keamanan data dan sistem komputer.
3. *Illegal interception* (penyadapan illegal), merupakan kegiatan mendengan pengiriman dan pemancaran suara dengan tanpa izin.
4. *Data Interferece* (gangguan data), merupakan kegiatan pengrusakan data dalam sistem komputer dengan tanpa izin. Contohnya seperti memasukkan kode-kode jahat (*malicious codes*) , virus dan Trojan Jours ke suatu sistem komputer yang merupakan pelanggaran menurut ketentuan pasal ini.
5. *System Interference* (Gangguan Sistem), merupakan kegiatan memasukkan, menyebarkab, merusak, menghapus atau menyembunyikan data komputer sehingga mengganggu sistem internet sebuah perangkat.
6. *Misuse of Device* (Penyalahgunaan Perangkat) adalah penyalahgunaan perangkat atau *Misuse of Device* merupakan kegiatan memodifikasi hardware maupun software untuk mendapatkan akses dari sebuah komputer ataupun jaringan
7. *Computer-related Forgery* (Pemalsuan yang erhubungan dengan komputer), merupakan kegiatan pemalsuan yang berkaitan dengan teknologi informasi atau komputer.
8. *Computer-related Fraud* (penipuan yang berhubungan dengan komputer), merupakan kegiatan penipuan dan pemalsuan yang berhubungan dengan jaringan komputer
9. *Content Related Offences; Child Pornography*, merupakan kegiatan penyebaran konten pornografi anak.
10. *Offence related of infringements of copyright and related rights*, merupakankegiatan yang berhubungan dengan pelanggaran hak cipta atau hak yang terkait. Point-point hasil kovensi Budapest pada saat itu diterbitkan kedalam *European*

Treaty Series (Surat Perjanjian Eropa) yang diratifikasi oleh banyak negara kemudian

di terapkan dalam hukum nasionalnya. Konvensi Budapest juga telah mengatur hukum pidana yang subtantif terhadap pelaku-pelaku kejahatan siber.

Metode

Metode penelitian yang digunakan adalah deskriptif dengan menggunakan data sekunder dan data primer yang dikumpulkan dengan teknik studi literatul. Data-data tersebut berasal dari buku, jurnal, dan juga internet yang berhubungan dengan kejahatan siber yang dilakukan warga negara tiongkok di balikpapan dan kenapa hukum yuridiksi universal tidak dapat dilakukan dalam kejahatan siber yang dilakukan.

Pembahasan

Pelanggaran Siber yang dilakukan WN Tiongkok di Balikpapan dan PenangananHukumnya

Pada tahun 2016 kepolisian daerah Balikpapan Kalimantan timur mendeteksi adanya kejahatan siber atau cybercrime yang terjadi di kota Balikpapan. Sebanyak 42 WNA Tiongkok diamankan karna terindikasi melakukan penipuan online yang merupakan salah satu jenis kejahatan siber atau cybercrime yaitu computer related offences.

Kegiatan yang dilakukan oleh 42 pelaku adalah dengan melakukan pemerasan terhadap beberapa pejabat negara yang butuh bantuan hukum, dengan berpura-pura menjadi pihak yang dapat menolong para pejabat dalam kasus-kasus hukum yang dihadapi korban. Pelaku melakukan pemerasan terhadap para korbannya yang merupakan WN Tiongkok dan Taiwan.

Dalam kasus 42 WN Tiongkok yang ditangkap di Balikpapan diketahui bahwa para pelaku masuk ke Indonesia menggunakan visa kunjungan wisata yang kemudian dimanfaatkan untuk melakukan tindak pidana siber yaitu penipuan yang berbasis dengan komputer dan jaringan internet.

Penipuan online termasuk dalam kejahatan siber yang biasanya dilakukan tidak menggunakan profil atau data diri yang sebenarnya seperti fenomena kejahatan yang dilakukan 42 WNA Tiongkok ini mereka melakukan penipuan dengan menggunakan alamat IP Indonesia dan memalsukan data dan menggunakan Jaringan internet untuk menipu para korbannya guna menghasilkan keuntungan pribadi.

Tindakan tersebut dilakukan di pemukiman mewah di Balikpapan dengan menggunakan perangkat lengkap komputer yang ditemukan oleh Kapolres Balikpapan AKBP Jefri Dian Juniarta dan didampingi oleh Kepala Satuan Resersi Kriminal (Kasatreskrim) polres Balikpapan AKP Kalfaris Triwijaya Lalo.

Kejahatan siber yang diindikasikan terhadap pelaku berdasarkan hasil pemeriksaan adalah penipuan online dengan memalsukan data diri mereka dan berpura- pura menjadi pejabat atau aparat kepolisian guna memeras korbannya yang kebanyakan adalah warga negara asing yang ada di Indonesia serta Tiongkok.

Korbannya adalah merupakan pejabat tinggi yang terjerat kasus hukum seperti korupsi dll. Sehingga para pelaku memanfaatkan keadaan tersebut dengan mengaku sebagai pihak yang dapat memudahkan para pejabat tersebut dalam kasus hukumnya, namun dengan membayar sejumlah uang yang bernilai cukup besar kepada para pelaku. Dari hasil penipuan tersebut para pelaku digaji oleh pimpinan mereka sebesar 12- 15juta/bulan dan atasannya mendapat penghasilan sekitar 30-50jt/bulannya.

Pemeriksaan terhadap 42 pelaku ini tidak hanya dilakukan oleh kepolisian

yang ada Balikpapan namun 8 orang anggota Interpol datang ke Indonesia untuk melakukan pemeriksaan pada tanggal 27 April 2016, didampingi oleh Kabag Kejahatan internasional Divisi Hubungan Internasional Mabes Polri. Dalam hasil pemeriksaan ditemukan beberapa alat bukti berupa sebuah perangkat komputer dan alat pendukung lainnya.

Setelah ditetapkan menjadi tersangka, kepolisian daerah Balikpapan tidak menetapkan hukuman terkait dengan tindak pidana siber yang dilakukan oleh tersangka. Para pelaku dijerat hanya dengan pasal 71 huruf D UU Nomor 6 tahun 2011 tentang pelanggaran keimigrasian yang dilakukan pelaku yaitu deportasi. Hal itu juga merupakan permintaan dari Interpol Tiongkok karena banyaknya korban yang melapor dari negaranya (PRO Balikpapan, 2016).

Pengambilan keputusan hukuman terkait dengan kejahatan siber tentu saja menjadi tidak mudah mengingat dalam penanganannya kejahatan siber atau cybercrime yang termasuk dalam kejahatan transnasional berkaitan dengan prinsip double criminality karena biasanya tidak hanya melibatkan satu negara, yang artinya penanganan hukum kejahatan siber atau cybercrime tidak akan terlepas dengan yurisdiksi. Kemampuan suatu negara untuk melacak dan mengungkap kejahatan siber pada akhirnya akan mempengaruhi penegakan hukum di negara lain (Suseno, 2009:41- 42).

Dalam regulasi yang ada di Indonesia kasus penipuan online yang dilakukan oleh 42 WN Tiongkok ini diatur dalam UU ITE yang termasuk dalam kejahatan computer related offences atau kejahatan yang menggunakan komputer dalam pelaksanaannya yaitu pada pasal 27 ayat 4 yang berbunyi:

a. Setiap orang dengan sengaja tanpa hal mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diakssnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan
b. Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi dan Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian.Setiap orang dengan sengaja, dan tanoa gak mendistribusikan danatau menstransmisikan dan/atau membuat dapat diaksesnya informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.
c. Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau menstransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.

Sanksinya terdapat dalam pasal 45 UU ITE yang berbunyi:

a. Setiap orang yang dengan sengaja dan tanpa hak mendistrbusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan sebagaimana dimaksud dalam pasal 27 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp.1.000.000.000,00 (satu miliar rupiah)
b. Setiap orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian sebagaimana

dimaksud dlam pasal 27 ayat (2) dipidana dengan penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp.1.000.000.000,00 (satu miliar rupiah).

c. Setiap orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik sebagaimana dimaksud dalam pasal 27 ayat (3) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp.750.000.000,00 (tujuh ratus lima puluh juta rupiah).
d. Setiap orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau pengancaman sebagaimana dimaksud dalam pasal 27 ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp.1.000.000.000,00 (satu miliar rupiah).
e. Ketentuan sebagaimana dimaksud pada ayat (3) merupakan delik aduan.

Namun pada penerapannya terdapat banyak kritik terhadap aturan kejahatan siber di Indonesia terkait jenis-jenis kejahatan siber yang diatur oleh UU ITE. Karena seperti perkembangan kejahatan siber dari tahun 1970an yang awalnya hanya seputar peretasan, pengurasakan, virus komputer, intrupsi komputer dan penipuan indentitas dan berkembang di era 2000an dengan berbagai macam jenis pengelompokan kejahatan siber yang ada. Maka, kejahatan siber yang diklasifikasikan saat ini bersifat kontemporer yang sewaktu-waktu bisa saja berubah dan berkembang (Pradipta, 2009).

Kejahatan siber juga telah diatur dalam hukum positif Indonesia, yaitu dalam UU No. 19 Tahun 2016 tentang Perubahan Atas UU NO.11 tahun 2008 tentang Informasi dan Transaksi Elektronik atau UU ITE. UU ITE awalnya adalah dipergunakan untuk kebutuhan perlindungan kepada para konsumen atau para pelaku usaha yang melakukan kegiatan usahanya secara daring (UU ITE, 2008).

UU ITE juga memiliki yurisdiksi yang berlaku sebagaimana telah diatur bahwa setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang- Undang ini, dimana setiap orang yang melakukan perbuatan hukum baik yang berada di wilayah Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di Indonesia atau di luar wilayah hukum Indonesia merugikan kepentingan Indonesia.

Melalui poin-poin dalam UU ITE, tampak bahwa kejahatan siber dapat dikriminalisasi dalam upaya pencegahan dan pemberantasannya oleh aparat penegak hukum dengan ketentuan yang memadai. Namun, kembali lagi sebenarnya di Indonesia selain UU ITE masih belum signifikan terkait dengan UU ITE karena pendefinisian jenis jenis kejahatan sibernya tidak spesifik sehingga masih diperlukan regulasi lain, yang biasanya dari kerjasama bilateral maupun multilateral yang dapat lebih mengikat karena pada dasarnya sifat dari kejahatan siber merupakan *transboundaries crime*.

Karena pada kasus 42 WN Tiongkok ini menyangkut dengan 2 negara maka perlu sebuah acuan dalam hukum internasional dalam penanganannya. Dalam dunia internasional terdapat sebuah aturan yang telah mengatur penyalahgunaan dunia maya. Pada tahun 2001 telah diadakan pertemuan antar negara-negara Uni Eropa membahas terkait produk hukum yang kemudian mengatur penyalahgunaan yang ada didunia maya. Pertemuan tersebut menghasilkan sebuah aturan yang pertemuan tersebut kemudian disebut convention on cybercrime atau dikenal juga dengan

Konvensi Budapest.

Penanganan Kejahatan siber dalam Konvensi Budapest dan Yurisdiksi Universal

Convetion on cybercrime merupakan hasil dari *Council of Europe* yang di bentuk pada tahun 2001 di kota Budapest, Hungaria. Konvensi ini dibentuk karena adanya kebutuhan yerkait regulasi khusus dalam menangani kejahatan siber di dunia. Meskipun lahir dari tataran regional Eropa, namun pada perkembangannya negara manapun di dunia yang memiliki komitmen dalam upaya mengatasi kejahatan siber, diperbolehkan untuk meratifikasi dan mengaksesnya.

Tujuan diadakannya konvensi ini adalah sebuah upaya dari mengatasi kejahatan-kejahatan yang berkaitan dengan teknologi informasi dan komunikasi atau berkaitan dengan komputer dan internet, dengan cara menyelaraskan hukum nasional, meningkatkan proses investigasi serta meningkatkan proses investigasi serta kerjasama antar negara dalam penanganan kejahatan siber.

Konvensi Budapest ini dapat menjadi alternatif penyelesaian dilema seperti dalam kasus penipuan online yang dilakukan oleh 42 WNA Tiongkok. Namun pada perkembangannya terdapat beberapa masalah dalam hal penerimaan terhadap segala keputusan yang dihasilkan konvensi ini. Hal ini dikarenakan bahwa konvensi ini merupakan bentukan dari suatu regional, artinya akan banyak negara yang akan cenderung melakukan resistensi atau penolakan terhadap norma-norma, pengaturan, infrastruktur hukum, produk hukum yang lahir dalam lingkup regional oleh negara yangbukan berasal dari regional eropa.

Seperti yang terjadi pada tanggal 22 Juni 2001, *the committee on crime problems* memutuskan untuk membentuk suatu protokol tambahan (*additional protocol*) yang mengkriminalisasikan kejahatan tehadap penyebaran propaganda yang bersifat rasis dan *xenophobic* melalui jaringan komputer sebagai pelengkap dari Convention on *Cybercrime* tahun 2001. Terkait dengan hal ini, Amerika Serikat (AS) sebagai salah satu negara yang meratifikasi konvensi, menolak secara tegas adanya protokol tambahan tersebut dengan alasan bahwa hal tersebut bertentangan dengan Amandemen pertama dari Konstitusi AS yang mengatur tentang kebebasan berekspresi (Cedric,2001).

Dalam *convention on cybercrime*, kasus penipuan online yang di lakukan oleh 42 orang warga negara Tiongkok ini termasuk dalam pasal 8 yang mengatur tentang *Computer Related Fraud* atau penipuan yang menggunakan teknologi komputer dan internet dalam pelaksanaannya.

Terdapat beberapa point subtantif yang berisikan jenis kejahatan siber yang diatur dalam konvensi ini yaitu article 2 sampai 13. Sementara yang terkait dengan aturan hukumnya atau procedural law terdapat dalam article 14 sampai 21, serta article 2 mengatur yurisdiksi. Para negara yang meratifikasi kovensi ini wajib menerapkan pasal-pasal tersebut dalam hukum nasionalnya (Council of Europe, 2001).

Pada penanganannya apabila terdapat kejahatan siber lintas negara antara negara penandatangan *convention on cybercrime* ini, akan diadili negara wajib untuk memidanakan pelaku tindak pidana berdasarkan dengan *convention on cybercrime* dengan prosedur dalam negri mereka untuk mendeteksi, menginvestigasi dan menuntut kejahatan yang dilakukan pelaku serta mengumpulkan bukti tindak pidana elektronik apapun.

Apabila Konvensi Budapest diterapkan terhadap tindak pidana yang dilakukan

oleh 42 warga negara Tiongkok di Balikpapan ini maka Indonesia akan sedikit mendapat kemudahan dalam penerapan yurisdiksi universal terhadap para pelaku. Terdapat beberapa kewajiban yang ditetapkan terhadap pelaku tindak pidana siber, yaitu:

a. Menetapkan pelanggaran dan sanksi pidana berdasarkan undang-undang domestik mereka untuk 4 kejahatan yang berkaitan dengan komputer seperti penipuan/pemalsuan, pornografi anak, pelanggaran hak cipta, dan pelanggaran keamanan seperti hacking, intersepsi illegal data, erta gangguan item yang mengkromi interitas dan ketersediaan jaringan. Penanda tangan juga harus membuat undang-undang menetapkan yurisdiksi atas tindak pidana tersebut dilakukan di atas wilayah mereka.
b. Menetapkan prosedur domestik untuk mendeteksi, investigasi dan menuntut kejahatan komputer serta mengumpulkan bukti tindak pidana elektronik apapun. Prosedur tersebut termasuk menjaga kelancaran data yang disimpan dalam komputer dan komunikasi elektronik, sistem pencarian dan penyitaan, intersepsi real-time dari data. Pihak konvensi harus menjamin kondisi dan pengamanan diperlukan untuk melindungi hak asasi manusia dan prinsip proporsionalitas.
c. Membangun sistem yang cepat dan efektif untuk kerjasama internasional. konvensi ini menganggap pelanggaran siber dapat diekstradisikan dan mengizinkan pihak penegak hukum di suatu negara untuk mengumpulkan bukti yang berbasis komputer. Konvensi ini juga menyerukan untuk membangun jaringan 24 jam dan 7 hari dalam seminggu untuk memberikan bantuan langsung dengan penyelidikan lintas-perbatasan.
d. Jenis pidana yang diancamkan terhadap pelaku kejahatan siber berdasarkan
convention on cybercrime.

Selain itu, berdasarkan ketentuan konvensi Budapest penegakan hukum tindak pidana siber tidak terlepas dengan yurisdiksi, terutama mengenai ruang berlakunya hukum pidana menurut tempat, luas dan tersebarnya potensi locus delicti dalam tindak pidana siber, hal ini akan menimbulkan masalah berkaitan dengan prinsip yurisdiksi atau terjadi konflik yurisdiksi. Pemberlakuan yurisdiksi universal, membutuhkan kerjasama dari negara-negara yang diawali dari adanya ratifikasi terhadap tindak pidana siber, dengan adanya kesamaan penegakan hukum, maka meminimalisir terjadinya pemanfaatan celah hukum dikarenakan yurisdiksi negara.

Penanganan bersama yang diperlukan dalam kasus seperti yang terjadi di Balikpapan ini berbenturan dengan kedaulatan suatu negara. Atas dasar tersebut yurisdiksi menjadi suatu aturan yang diperlukan untuk mengatasinya. Masyarakat internasional dalam hal ini harus memiliki keinginan bersama untuk menanggulangi tindak pidana yang berdampak pada suatu negara.

Terdapat beberapa prinsip dalam yurisdiksi antara lain teritorial, universal nasional aktif, nasional pasif dan prinsip perlindungan. Prinsip-prinsip tersebut sebagian besar berpatokan terhadap locue delicti dalam pelaksanaannya atau memperhatikan dengan penuh tempat terjadinya peristiwa dalam pengambilan keputusannya.

Yurisdiksi universal menjadi satu satunya asas yurisdiksi yang mengizinkan negara atau organisasi internasional untuk mengklaim yurisdiksi tanpa perlu mempersoalkan locus delicti dan kewarganegaraan pelaku. Asas ini mengedepankan

kewenangan untuk menangani kejahatan lebih kepada perlindungan terhadap kepentingan-kepentingan tertentu dari negara-negara yang ada di dunia.

Penerapan yurisdiksi universal pada dasarnya merupakan sebuah upaya mencegah terjadinya impunity (pembebasan hukuman atau denda) yang biasanya dilakukan oleh negara asalnya melalui mekanisme hukum nasionalnya. Sehingga pada akhirnya yurisdiksi universal sangat terkait erat dengan persoalan politik.

Yurisdiksi universal lebih pada kewenangan (*authorizes*) dibandingkan dengan kewajiban (*obliges*) negara untuk menuntut dan menghukum pelaku. Dalam melaksanakan yurisdiksi terdapat beberapa etika yang dibutuhkan dalam hukum internasional, dibutuhkan permohonan ekstradisi dari Requesting state kepada Requested State. Dengan demikian, keterbatasan atau permasalahan teritorial bisa dijembatani melalui kerjasama dengan negara-negara lainnya untuk proses penegakan hukum. Sehingga, tidak akan terjadi penegakan hukum tersebut apabila tidak ada perjanjian bilateral maupun multilateral dalam penyerahan pelaku tindak pidana atau dalam kerja sama penyidikan, penuntutan, dan peradilan. Namun, perjanjian tersebut juga tidak bersifat mutual karna pada umumnya penegakan hukum dapat dilaksanakan dengan berlandaskan asas resiprositas atau timbal balik (Cedric, 2001).

Sesuai dengan ketentuannya Indonesia memiliki hak untuk mengajukan ekstradisi atau yurisdiksi universal terhadap Tiongkok untuk mengadili 42 warga negaranya karena penipuan online yang dilakukan di wilayah kedaulatan Indonesia sertatelah diatur didalam hukum nasional Indonesia di dalam UU ITE pasal 27 ayat 4.

Permasalahan yurisdiksi di Indonesia juga tercantum pada pasal 37 UU ITE yang berbunyi "Setiap Orang dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada di wilayah yurisdiksi Indonesia.". Pasal ini menjelaskan salah satu makna 'memiliki akibat hukum di wilayah indonesia' yang dimaksud dalam pasal 2 UU ITE bahwa sepanjang objek atau target-yaitu sistem elektronik dari perbuatan yang dilarang berada di Indonesia maka ketentuan dalam UU ITE berlaku bagi pelaku.

Dalam pemberlakuannya, asas yurisdiksi universal tidak mensyaratkan adanya nexus dengan Negara maupun locus delicti berbeda dengan asas yurisdiksi yang lainnya yang dimana negara akan mudah menentukan apakah negara tersebut mempunyai yurisdiksi atas suatu kejahatan atau tidak dengan melihat kepada hubungan yang muncul dari suatu peristiwa dengan negara tersebut.

Dengan kata lain meskipun terdapat sebuah hubungan atau perjanjian internasional bilateral dalam hal ini antara Indonesia dan Tiongkok. Yurisdiksi universal tetap bisa diajukan oleh Indonesia yang menjadi tempat terjadinya tindak pidana siber yang dilakukan oleh ke 42 WNA Tiongkok ini namun dengan tidak mengesampingkan perjanjian internasional atau kesepakatan terkait ekstradisi (penyerahan tersangka kasus kriminal) diantara kedua nya.

Sementara pada tahun 2016, pelanggaran tindak pidana siber yang dilakukan WN Tiongkok terjadi. Indonesia tidak memiliki perjanjian dengan Tiongkok tentang kejahatan siber maupun ekstradisi sehingga apabila melihat dari sisi hubungan atau kerjasama antar 2 negara ini Indonesia tidak berkewajiban atau tidak ada sebuah keharusan untuk memulangkan ke 42 pelaku ini ke negara asalnya.

Analisis penerapan Yurisdiksi Universal Terhadap Pelanggaran Siber yang dilakukan WN Tiongkok di Balikpapan serta hambatannya

Kejahatan yang dilakukan oleh 42 WNA tiongkok termasuk dalam kejahatan siber yaitu dengan melakukan penipuan online terhadap para korbannya, di Indonesia penanganan hukum pada kasus seperti ini diatur dalam UU ITE pada pasal 27 ayat 4 yang mengatur tentang setiap orang yang melakukan penipuan/pemerasan melalui jaringan komputer dan internet dengan hukuman dipenjara selama paling lama 6 tahun atau denda paling banyak Rp.1000.000.000,00 (satu milyar rupiah) (UU ITE, 2016).

Namun, karena para pelaku merupakan warga negara asing dalam hal ini adalah Tiongkok maka, hukum nasional Indonesia tidak dapat berjalan dengan mudah begitu saja mengingat harus memperhatikan banyak hal seperti hubungan bilateral kedua negara, yurisdiksi, maupun perjanjian internasional yang ada agar tidak terjadi perdebatan tentang negara mana yang akan menerapkan hukumannya.

Terdapat beberapa acuan dan standar apabila Indonesia ingin menerapkan hukumanya atau membuat para pelaku dihukum di Indonesia dimana tempat kejahatan dilakukan dengan menggunakan undang-undang yang telah diatur oleh Indonesia. Seperti, melaksanakan yurisdiksi universal, mengajukan permintaan ekstradisi, ataukerjasama internasional dalam penegakan hukum terkait dengan tindak pidana siber.

Indonesia memiliki dasar hukum dalam pelaksanaan pemidaan yang melibatkan negara lain yaitu, Undang-Undang Nomor 1 Tahun 1979 Tentang Ekstradisi dan penyitaan asset, dan Undang-Undang Nomor 1 Tahun 2006 Tentang Bantuan Timbal Balik dalam Masalah Pidana (*mutual assistance in criminal matters*). Permintaan ekstradisi tidak serta merta merupakan pengembalian asset hasil tindak pidana yang dibawa pelaku kejahatan. Kedua bentuk perjanjian eksradisi dan mutual assistance in criminal matters ini harus saling melengkapi dan bukan dilihat secara terpisah. Hal ini berarti permintaan ekstradisi harus dilengkapi dengan permintaan bantuan timbal balik dalam masalah pidana terutama pegusutan dan pengembalian asset tindak pidana dari pelaku kejahatan (Undang-Undang Nomor l5, 2008).

Dengan berlandaskan prinsip diplomasi, Ekstradisi membutuhkan kerjasama terlebih dahulu antar negara. Meskipun terdapat undang-undang terkait ekstradisi tetap butuh kerjasama yang lebih spesifik membahas mengenai kerjasama Indonesia dengan negara yang bersangkutan, seperti contohnya, Indonesia memiliki perjanjian ekstradisi dengan Republik Sosialis Viet Nam (*Ekstradition Treaty Between The Republic Of Indonesia And The Socialist Republic Of Vietnam*).

Penerapan yurisdiksi universal merupakan hubungan baik yang berkesinambungan, dengan kata lain bertimbal balik. Dalam hal ini Tiongkok dan Indonesia tidak memiliki perjanjian yang mengikat terkait dengan ekstradisi. Sehingga dalam kasus kejahatan siber yang terjadi di Balikpapan tersebut yang dilakukan Indonesia hanya pendeportasian, pemerintah Indonesia tidak dapat berbuat banyak.

Dalam menanggulangi tindak pidana siber yang sifatnya melintasi batas negara seperti yang dilakukan WN Tiongkok ini belum maksimal. Mengingat dari sisi aturan pun Indonesia belum mengesahkan Rancangan Undang-undang Pengesahan *European Union Convention On Cybercrime*, 2001 (Konvensi Dewan Eropa Tentang Tindak Pidana Siber 2001). Jika disahkan tidak menutup kemungkinan ekstradisi atau penindakan hukum kepada 42 pelaku yang merupakan WN Tiongkok ini menjadi hak

dari Indonesia, kerena undang-undang tersebut menjelaskan dalam isi pokok Konvensi tentang kerjasama Internasional dimuat mengenai prinsip-prinsip umum, yaitu:

a. Prinsip-prinsip umum berkaitan dengan kerjasama internasional
b. Prinsip-prinsip yang berkaitan dengan ekstradisi
c. Prinsip-prinsip umum berkaitan dengan bantuan timbal balik dan informasi spontan
d. Prosedur-prosedur tentang permintaan bantuan timbal balik dengan tidak adanya perjanjian-perjanjian internasional yang berlaku; dan kerahasiaan dan pembatasan penggunaan.

Sehingga apabila Indonesia meratifikasi perjanjian tersebut, meskipun tidak ada perjanjian timbal balik ataupun ekstradisi, Indonesia memiliki komitmen kuat untuk menanggulangi tindak pidana siber. Hal ini membuat Indonesia bisa meminimalisir tindak pidana siber karena pelaku tidak dapat mengelak suatu tuntutan pidana, karena adanya unsur locus de licti, kewarganegaraan pelaku, kewarganegaraan korban dan lokasi korban.

Selain itu, pelaksanaan yurisdiksi atas tindak pidana siber tersebut ditempuh melalui kerjasama internasional agar hukum dan keadilan tetap ditegakkan tanpa melanggar kedaulatan negara lain. Kerjasama internasional yang dapat dilakukan antara lain, ekstradisi, bantuan hukum timbal balik, kerjasama antar penegak hukum seperti kepolisian dengan kepolisian dan lain-lain.

Dalam kerjasama membutuhkan kelengkapan perangkat teknologi informasi dan komunikasi yang sejajar dengan yang dimiliki negara lain atau menyesuaikan kebutuhan antar negara yang melakukan kerjasama. Oleh karena itu kerjasama internasional akan ditindaklanjuti dengan bantuan untuk meningkatkan sarana prasarana dan kemampuan aparat penegak hukum di bidang teknologi informasi dan komunikasi. Namun, dalam hal ini Indonesia dan Tiongkok tidak memiliki perjanjian khusus mengenai ekstradisi dan keamanan sibernya.

Seperti pada kasus Nikolov Indonesia dan Bulgaria memiliki perjanjian bilateral terkait dengan ekstradisi, sehingga Indonesia berhak mengklaim Nikolov untuk dilakukan tindakan hukum di Indonesia dengan menggunakan aturan yang berlaku atas dasar kerugian yang berdampak terhadap Indonesia sebagai lokasi tempat kejahatan berlangsung.

Sedangkan pada kasus antara Indonesia dan Tiongkok tidak memiliki perjanjian ekstradisi serta tidak meratifikasi Konvensi Budapest sebagai dasar penerapan yurisdiksi internasional. Sehingga pendeportasian menjadi yang paling mungkin dilakukan.

Menurut kepolisian Tiongkok apabila Indonesia meratifikasi menjadikan kejahatan siber dapat ditanggulangi dengan maksimal karena jika tidak memberlakukan yurisdiksi universal, tidak menutup kemungkinan pelaku dihukum di negara yang menjadi tempat terjadinya pelanggaran dan oleh negara yang menjadi korban kejahatannya. Sehingga para pelaku dihukum dengan tepat sesuai dengan aturan internasional yang ada dan apabila terjadi hukuman oleh ke dua negara pun ini tidak menjadi adil bagi pelaku. Karena hukuman yang diterima kedua kali untuk kasus sama merupakan hal yang tidak tepat dan bersinggungan dengan prinsip keadilan.

Namun dalam hal ini tindakan kepolisian Tiongkok yang menarik pulang warga negara nya untuk diadili di Tiongkok juga bukan merupakan tindakan yang

menghinakan hukum di Indonesia, mengingat 42 tersangka ini belum sampai pada tahap pengadilan atas kejahatan siber yang dilakukan. Selain itu korban dan pelaku secara keseluruhan juga merupaka warga negara Tiongkok.

Meskipun apabila mengacu pada prinsip Yurisdiksi Universal dalam hal ini Indonesia tetap memiliki hak dalam memberlakukan hukum nya terhadap para pelaku karena berpengaruh terhadap nama baik Indonesia atau sekedar hanya untuk memberi efek jera terhadap pelaku atau jaringannya yang terdapat dikota-kota lain di Indonesia. Namun berdasarkan prinsip nasionalitas maka hal yang dilakukan oleh kepolisian Tiongkok merupakan sebuah tindakan perlindungan terhadap warga negaranya dalam hal ini yang menjadi korban maupun pelaku kejahatan.

Kesimpulan

Dalam penerapan Yuridiksi Universal bagi kejahatan siber yang dilakukan oleh 42 WNA Tiongkok di Balikpapan ini tidak sepenuhnya dilakukan. padahal Indonesia sudah memiliki instrument atau dasar hukum penanganan tindak pidana kejahatan siber yang terdapat pada UU nomor 11 tahun 2008 tentang informasi dan transaksi elektronik. Namun dalam UU tersebut hanya sebatas pada yuridiksi ekstrateritorial bukan universal, selain itu Indonesia juga tidak melakukan ratifikasi dalam konvensi budapest yang dalam konvensi tersebut telah mengatur mengenai kejahatan siber.

Daftar Pustaka

Adolf, Huala. 2002. Aspek-Aspek Negara Dalam Hukum Internasional. Jakarta:PT.Raja Grafindo Persada.

Cedric J. Magnin, The 2001 Council of Europe on Cyber-Crime: A Efficient Tool toFight Crime in Cyber-Space, LLM Dissertation on Santa Clara University.

Direktorat Tindak Pidana Siber (Dittipidsiber). 2021. “Laporan kejahatan siber 2014-2017, https//patrolisiber.id/statistic, diakses pada tanggal 12 November 2021

Halim, Abdul & Azhar. 2020. Hukum Internasional (sebuah pengenalan).Palembang: Unsri Press.

Hazliansyah. 2016. “42 warga Negara Cina dan Taiwan diciduk, diduga pelaku kejahatan siber”, https://www.republika.co.id/berita/o56pzl280/42-warga-cina-dan- taiwan-diciduk-diduga-pelaku-kejahatan-siber, diakses pada tanggal 12 Juni 2021

Juwana, Hikmanto. 2006. Yurisdiksi Negara;Hukum Internasional. Jakarta. UI Press.

Pradipta, Ryobi. 2019. “Yurisdiksi Negara pada Cybercrime”. Universitas Muhammadiyah Magelang

Prawiro, M. 2018. “cyber crime : Pengertian, Jenis, dan Metode Kejahatan Cybercrime”, https://www.maxmanroe.com/vid/teknologi/pengertian-cyber- crime.html, diakses pada tanggal 10 November 2021

Suseno, Sigid. 2012. Yurisdiksi tindak pidana siber. Bandung:PT.Refika Aditama

Wahid, Abdul & Mohammad Labib. 2005. Kejahatan Mayantara. Bandung:PT.Refika Aditama