Indonesian Journal of Applied and Industrial Sciences (ESA)
Vol. 3, No. 3, 2024 : 319 - 328

Law Enforcement of State Jurisdiction in Hacking Crimes

Kharisma Ika Nurkhasanah, Zydane Maheswara Prasetyo
Program Studi Hukum, Universitas Tidar
Corresponding Author: Kharisma Ika Nurkhasanah
Kharismaika07@gmail.com

A R T I C L E I N F O

Keywords : Enforcement, Law, Jurisdiction, Cybercrime, Hacking

Received : 07 April
Revised : 26 April
Accepted: 30 May

A B S T R A C T

Along with the development of information and communication technology, apart from having a positive impact with ease of communication and transactions, there are also negative impacts such as the emergence of crimes in cyberspace or cybercrime. Law enforcement regarding various types of cyber crime turns out to be problematic in practice, especially regarding purchasing problems. This research aims to determine and analyze law enforcement and secret regulations for hacking crimes as well as legal policies regarding the implementation of cyber law in hacking crimes in Indonesia. The author employs a statutory approach and a conceptual approach as part of a normative juridical research methodology. This research results show that cyber crime fraud is regulated in Article 2 of the ITE Law which applies the principle of extra-territorial fraud. Indonesia can implement this through international cooperation which includes extradition, mutual legal assistance, and collaboration between law enforcers. Handling problems that occur internationally and nationally related to cross-border activities and extraterritorial consequences, is carried out with a global approach in a universal regulatory mechanism, there may be a single legal framework and depends on regional mechanisms and on national legal systems that provide effective handling of digital threats.

Penegakan Hukum Yuridiksi Negara dalam Tindak Pidana Peretasan

Kharisma Ika Nurkhasanah, Zydane Maheswara Prasetyo
Program Studi Hukum, Universitas Tidar
Corresponding Author: Kharisma Ika Nurkhasanah
Kharismaika07@gmail.com

A R T I C L E I N F O

Kata Kunci: Penegakan, Hukum, Yurisdiksi, Kejahatan Siber, Peretasan

Received : 07 April
Revised : 26 April
Accepted: 30 Mei

A B S T R A K

Seiring dengan berkembangnya teknologi informasi dan komunikasi, selain memperoleh dampak positif dengan kemudahan berkomunikasi dan bertransaksi, namun terdapat pula dampak negatif seperti halnya timbulnya kejahatan-kejahatan dalam dunia maya atau kejahatan siber. Penegakan hukum atas berbagai jenis kejahatan siber ternyata banyak terkendala dalam praktik, terutaman mengenai problematika yurisdiksi. Tujuan dari penelitian ini adalah untuk mengidentifikasi dan mengevaluasi kebijakan hukum terkait penerapan hukum siber terhadap kejahatan peretasan di Indonesia, serta penegakan hukum dan pengendalian yurisdiksi atas kejahatan peretasan. Penulis menggunakan pendekatan konseptual dan perundang-undangan dalam metodologi penelitian yuridis normatif. Temuan penelitian menunjukkan bahwa Pasal 2 UU ITE yang menggunakan konsep yurisdiksi ekstrateritorial mengatur yurisdiksi atas kejahatan dunia maya. Indonesia dapat mewujudkan hal ini dengan bekerja sama dengan negara lain untuk menegakkan hukum, ekstradisi, dan saling mendukung secara hukum. Penanganan permasalahan yurisdiksi internasional dan nasional terkait kegiatan lintas batas dan konsekuensi ekstrateritorial, dilaksanakan dengan pendekatan global dalam mekanisme peraturan universal, kemungkinan terdapat kerangka hukum tunggal dan bergantung pada mekanisme regional serta pada sistem hukum nasional yang memberikan keefektifan penanganan atas ancaman digital.

PENDAHULUAN

Perkembangan teknologi menciptakan banyak pilihan kriminal. Banyaknya kasus pidana digital yang telah sampai ke persidangan menunjukkan hal tersebut. Penyalahgunaan teknologi, termasuk pemalsuan, peretasan, hoax, dan internet, merupakan salah satu contoh yang ditangani. Meningkatnya kebutuhan akan teknologi jaringan komputer menjadi salah satu faktor penyebab terjadinya *Cybercrime* dunia maya. Jaringan komputer sangat penting untuk melaksanakan tugas-tugas penting masyarakat. *Cybercrime* dunia maya didefinisikan sebagai setiap perilaku kriminal yang dilakukan melalui jaringan elektronik global di dunia maya dengan menggunakan komputer atau perangkat elektronik lainnya, seperti telepon pintar atau telepon seluler.

Penyelesaian keterkaitan antara yurisdiksi internasional dan nasional, aktivitas lintas batas dan konsekuensi ekstrateritorial, yang membawa baik perorangan maupun badan hukum dalam tanggung jawab hukum menjadi persoalan. Informasi berupa data yang menjadi kunci segala aktivitas di era digital tidak hanya berjalan di ruang virtual, melainkan terhubung dengan penyimpanan fisik yang secara teritorial berada di wilayah hukum suatu negara. Namun, beberapa kendala dalam menentukan yurisdiksi yang tepat dan peraturan hukum yang efektif secara umum harus diingat bahwa informasi disalurkan melalui wilayah beberapa negara bagian. Selain itu, kemampuan teknis untuk mengatur aktivitas di dunia maya terbatas baik secara obyektif maupun subyektif.

Peretasan dalam perkembangannya mengarah pada kegiatan yang digunakan untuk keperluan bersifat merugikan, dimana penggunaanya menjadi disalahgunakan dengan kompetensi yang semakin luas. Peretas menggunakan cara dalam memahami sistem dan penggunaannya di suatu sasaran dengan melakukan penyusupan atau pengaksesan jaringan pada komputer yang menjadi incaran. Selanjutnya, hal ini dicapai dengan menargetkan kerentanan sistem komputer; dengan kata lain, peretas membobol situs web orang lain tanpa izin atau persetujuan. Peretas dapat masuk dan mengakses situs orang lain meskipun situs tersebut telah dilengkapi *cyber security*. Hal ini merupakan kejahatan siber karena telah menyalahgunakan situs pribadi milik orang lain.

Sub permasalahan akan digali sesuai dengan latar belakang informasi di atas untuk memudahkan pembahasan, yaitu sebagai berikut :

1. Bagaimana penegakan hukum dan pengaturan yurisdiksi kejahatan peretasan?
2. Bagaimana kebijakan hukum terhadap pelaksanaan cyberlaw kejahatan peretasan di Indonesia?

TINJAUAN PUSTAKA

Jonathan Rosenoer membagi ruang lingkup *Cyberlaw* menjadi : "hak cipta, hak merek, pencemaran nama baik, *hate speech* atau penistaan, penghinaan, fitnah, peretasan, *viruses, illegal access*, pengaturan sumber daya internet, keamanan pribadi, kehati-hatian, *criminal liability*, *procedural issues* seperti yurisdiksi, pembuktian, penyelidikan, transaksi elektronik, pornografi, pencurian melalui internet, perlindungan konsumen, *e-commerce, e-government*". Penegakan hukum atas berbagai jenis kejahatan siber umumnya yang banyak

terkendala dalam praktik ialah problematika yurisdiksi. Penentuan yurisdiksi yang tidak pasti dalam ruang siber sebagaimana yang dikemukakan Tien S. Saefullah bahwa: "Komunikasi dan informasi multimedia bersifat internasional, multiyurisdiksi, dan tanpa batas; oleh karena itu, belum jelas bagaimana yurisdiksi suatu negara dapat diterapkan dalam penggunaannya. Yurisdiksi suatu negara, sebagaimana diakui oleh hukum internasional dalam pengertian konvensional, didasarkan pada batas-batas geografis dan waktu. teknologi data".

METODOLOGI

Jenis penelitian ini ialah yuridis normatif yang melibatkan analisis norma dan mengidentifikasi prinsip-prinsip hukum untuk menangani penyelidikan hukum tertentu. Soerjono Sukanto mengemukakan bahwa penelitian hukum normatif bertumpu pada kajian literatur hukum yang ada untuk mengumpulkan informasi dan wawasan. Pendekatan yang digunakan oleh penulis, yaitu pendekatan perundang-undangan *(statute approach)* dan pendekatan konseptual *(conceptual approach)*. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) merupakan salah satu bahan hukum utama yang penulis gunakan dalam penelitian ini. Sedangkan bahan hukum sekunder berasal dari buku, jurnal, dan media online. Penulis mengumpulkan bahan-bahan hukum dengan menelaah berbagai literatur atau kepustakaan *(library research)* dan studi dokumen *(documentary research)* serta metode deduktif dalam menganalisis bahan hukum.

HASIL PENELITIAN DAN PEMBAHASAN

Penegakan Hukum dan Pengaturan Yurisdiksi Kejahatan Peretasan

Kejahatan peretasan diatur dalam Pasal 30 ayat (1), (2), dan (3) UU ITE, yang pada pokoknya menjelaskan bahwa "seseorang yang berupaya, dengan sengaja dan tanpa izin, memasuki atau mengakses sistem elektronik orang lain". Pasal 46 ayat (1), (2), dan (3) UU ITE yang mengatur terkait sanksi pidana atas pelanggaran yang tercantum dalam Pasal 30 tersebut. Kemudian diatur pula pemberatan penjatuhan pidana terhadap pelaku peretasan sesuai dengan subyek dan obyek kejahatan yakni Berdasarkan Pasal 52 Ayat (2) UU ITE, siapa pun yang melakukan kegiatan peretasan terhadap sistem elektronik yang digunakan untuk layanan publik atau milik pemerintah dapat dikenakan sanksi pidana. Jika peretas menyasar situs milik pemerintah yang terkait langsung dengan keselamatan atau stabilitas negara, maka akan dikenakan sanksi pidana sesuai Pasal 52 ayat (3) UU ITE. Penegakan hukum terhadap pelaku kejahatan peretasan sesuai dengan UU ITE dengan mengedepankan kolaborasi dari aparat penegak hukum meliputi pihak kepolisian, kejaksaan, dan pengadilan.

Terdapat tiga macam yurisdiksi meliputi: "kewenangan untuk menetapkan undang-undang yang berkaitan dengan hukum pidana, kewenangan untuk melaksanakan atau melaksanakan tindakan yang dipilih oleh badan legislatif, dan kewenangan untuk menegakkan tindakan hukum yang dilakukan oleh lembaga eksekutif atau ditentukan oleh pengadilan." Ada

beberapa pertimbangan yang banyak digunakan untuk menentukan undang-undang mana yang akan berlaku, antara lain :

a. Teritorialitas subyektif, atau penekanan pada penentuan keabsahan suatu undang-undang tergantung pada lokasi perbuatan dan penyelesaian kejahatan di negara yang berbeda, merupakan salah satu ciri utamanya.
b. Teritorialitas obyektif, yaitu undang-undang yang berlaku adalah undang-undang yang menimbulkan akibat utama perbuatan itu dan merugikan negara secara serius.
c. Asas kewarganegaraan, yang menyatakan bahwa negara mempunyai kewenangan untuk memastikan kewarganegaraan pelaku berdasarkan hukum.
d. Gagasan kewarganegaraan pasif, yang menekankan pada kewarganegaraan korban sebagai dasar yurisdiksi.
e. Jika yang menjadi korban adalah negara atau pemerintah, maka konsep perlindungan yang menyatakan bahwa hukum dapat dilaksanakan berdasarkan niat negara untuk membela kepentingan negara dari kejahatan yang dilakukan di luar wilayahnya sering digunakan.
f. Konsep universalitas pada akhirnya diperluas hingga mencakup kejahatan terhadap kemanusiaan, meskipun pada awalnya dinyatakan bahwa negara mana pun mempunyai wewenang untuk menahan dan menghukum pelaku bajak laut. Ide ini dapat digunakan untuk pembajakan online, menganggap virus, carding, cracking, dan pencurian komputer sebagai pelanggaran yang sangat berat.

Yurisdiksi universal mengizinkan negara untuk mengadili kejahatan-kejahatan tertentu meskipun tidak ada kaitannya untuk mencakup kejahatan siber. Dengan demikian, penerapannya dapat menyelesaikan masalah yurisdiksi yang terkait dengan dilakukannya kejahatan siber termasuk dimana kejahatan itu terjadi, siapa yang akan menyelidikinya, dan dimana kejahatan itu akan dituntut. Yurisdiksi universal juga disesuaikan dengan sifat transnasional dari kejahatan siber sebagai pelakunya yang menimbulkan kerugian pada korban di lebih dari satu negara. Akan tetapi, masih belum ada kejelasan sejauh mana dampak yurisdiksi universal harus diterapkan pada kejahatan siber.

Prinsip "*universal interest jurisdiction*" sebagai penentuan yurisdiksi kejahatan siber sejatinya bisa dikaji melalui asas-asas hukum internasional. Terdapat asas teritorial yang mengacu pada keberlakuan peraturan hukum pidana bagi seluruh kejahatan yang terjadi di dalam wilayah negara, baik dilakukan oleh warga negaranya sendiri atau warga asing. Selain itu, ada pula asas personal atau nasionalitas aktif yang berfokus pada keberlakuan hukum pidana bagi segala kejahatan yang dilakukan oleh warga negara, di tempat mana saja dan di luar wilayah negara.

Pasal 2 UU ITE menyatakan bahwa: "Undang-undang ini berlaku bagi setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam undang-undang ini, baik di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang mempunyai akibat hukum di wilayah hukumnya. Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan

kepentingan Indonesia." Bagian ini berisi peraturan yurisdiksi. Dengan demikian, dapat disimpulkan bahwa konsep yurisdiksi ekstrateritorial dianut oleh UU ITE. Mengingat pemanfaatan teknologi informasi untuk informasi dan transaksi elektronik dapat bersifat lintas teritorial atau universal, maka UU ITE mempunyai ruang lingkup yurisdiksi yang juga mencakup perbuatan hukum yang dilakukan oleh warga negara Indonesia atau warga negara asing yang mempunyai akibat hukum di Indonesia.

Dalam Pasal 22 *Convention on Cybercrime* 2001 mengatur ketentuan yurisdiksi bersifat teritorial yang menyatakan bahwa: "Perjanjian ini mencakup pesawat terbang yang terdaftar berdasarkan undang-undang negara tersebut, kapal yang mengibarkan benderanya, dan penduduknya yang berada di luar negeri namun tunduk pada hukum negara tersebut. Ini juga mencakup tanah negara-negara tersebut". Konsultasi harus dilakukan untuk memastikan yurisdiksi hukuman jika timbul perselisihan tentang yurisdiksi. Melalui struktur kolaborasi internasional yang andal, terdapat kepastian dalam proses penyidikan dan penuntutan baik di dalam negeri maupun internasional. Demikian pula, suatu negara dapat menerapkan yurisdiksi teritorialnya jika pelaku dan sistem komputer yang ditargetkan berada di wilayahnya, atau jika penyerang berada di wilayahnya namun korbannya tidak berada di wilayahnya.

Pelaku kejahatan siber seringkali berada di tempat secara fisik yang sama dengan korban, sehingga menjadikan tempat terjadinya kejahatan atau yurisdiksinya mudah ditentukan. Namun di ruang siber, pelaku tindak pidana tidak perlu berada di tempat terjadinya kejahatan yang senyatanya. Dalam hal ini, asas perlindungan mampu diterapkan pula dengan pertimbangan bahwa asas teritorial tidak menyiapkan basis yurisdiksi secara lengkap bahwa kejahatan dilakukan di luar wilayah teritorial negara pelaku. Asas perlindungan hanya diterapkan pada tipe kejahatan khusus dengan mengedepankan pada kegiatan pelaku yang berakibat ancaman serius atas kepentingan nasional.

Yurisdiksi pidana: Menggunakan yurisdiksi teritorial, yurisdiksi ekstrateritorial atas kejahatan dunia maya yang dilakukan di dalam batas negara lain, dan yurisdiksi ekstrateritorial atas kejahatan dunia maya yang dilakukan di luar batas negara mana pun adalah contoh yurisdiksi semu yang dapat diterapkan pada kejahatan dunia maya ketika menerapkan hukum pidana nasional. Solusi untuk hal ini adalah meratifikasi satu-satunya konvensi yang mengikat terkait kejahatan dunia maya, seperti Konvensi Dewan Eropa tentang Kejahatan Dunia Maya dengan protokol tambahan kedua terkait peningkatan kerjasama dan pengungkapan bukti elektronik. Konvensi Kejahatan Dunia Maya dan protokol tambahannya tersebut dapat menjadi alat yang memudahkan Indonesia dalam rangka menerapkan yurisdiksi ekstra teritorial untuk mengatasi dan menegakkan hukum terkait kejahatan siber seperti peretasan dalam konteks transnasional.

Kebijakan Hukum terhadap Pelaksanaan *Cyberlaw* Kejahatan Peretasan di Indonesia

Untuk memerangi kejahatan dunia maya, berbagai strategi diterapkan melalui kebijakan pidana. Hal tersebut antara lain menjadikan pelanggaran terhadap peraturan UU ITE sebagai tindakan ilegal, menyelaraskan ketentuan

hukum nasional dengan hukum internasional untuk memberantas kejahatan siber, dan menegakkan penegakan hukum dengan memberikan sanksi pidana kepada pelaku kejahatan siber. Selain itu, dapat diterapkan pula mengenai kebijakan non penal dalam hal penyusunan kebijakan-kebijakan di luar hukum pidana sebagai strategi preventif kejahatan siber, mengedepankan sosialisasi terkait potensi terjadinya *cybercrime,* hingga meningkatkan kolaborasi antar penegak hukum maupun dengan sektor swasta dalam rangka membangun *security system* di dunia siber atau dengan jalan membentuk kerjasama kelembagaan dalam tingkat nasional hingga internasional.

Ide-ide baru dapat memperjelas kemungkinan solusi dan rekomendasi yang dapat diterapkan untuk memperkuat penegakan hukum siber di Indonesia. Hal ini dapat mencakup pengembangan kebijakan baru yang lebih responsif terhadap perubahan teknologi oleh pemerinta, serta upaya untuk meningkatkan kesadaran masyarakat tentang ancaman kejahatan siber. Kejahatan peretasan juga melibatkan aspek lintas batas yang semakin marak terjadi. Peretas seringkali beroperasi di luar negeri, sehingga penegakan hukum siber di Indonesia juga memerlukan kerja sama internasional yang erat. Kerja sama ini mencakup pertukaran informasi, ekstradisi, dan penanganan kasus peretasan lintas batas yang efektif. Dalam menghadapi tantangan perubahan dan perkembangan hukum siber di Indonesia, penting untuk memiliki pendekatan yang holistik dan berkelanjutan. Hal ini melibatkan perbaikan berkelanjutan dalam kerangka hukum, peningkatan kapasitas aparat penegak hukum dan kesadaran masyarakat terhadap keamanan siber serta kerja sama yang kuat dengan lembaga internasional. Adanya pendekatan komprehensif tersebut, Indonesia menjadi lebih efektif mengatasi ancaman peretasan dan menjaga keamanan siber negara di tengah perubahan dunia digital yang terjadi.

Sehubungan dengan hal tersebut, Indonesia dapat menggunakan Undang-Undang Nomor 1 Tahun 2006 tentang Gotong Royong dalam Situasi Pidana sebagai landasan hukum dan pedoman dalam melakukan kerja sama dengan negara lain dalam gotong royong dalam situasi pidana. Perlunya penanganan kejahatan siber dengan tanggung jawab untuk melaksanakan kolaborasi dengan negara-negara yang berpotensi menjadi lokasi persembunyian atau melakukan kejahatan siber itu sendiri bermula dari pertumbuhannya yang semakin rumit. Dengan demikian, mampu menjadi salah satu strategi preventif kejahatan siber lintas yurisdiksi dengan penerapan Sistem Bantuan Timbal Balik dalam Masalah Pidana (*Mutual Legal Assistance*).

KESIMPULAN DAN REKOMENDASI

Pasal 2 UU ITE mengatur yurisdiksi kejahatan siber, khususnya kejahatan hacking. Perjanjian ini menerapkan prinsip yurisdiksi ekstrateritorial, yang memungkinkan penerapannya melalui kerja sama internasional seperti bantuan hukum timbal balik, ekstradisi, dan kerja sama yang konsisten antara lembaga penegak hukum di sektor publik dan swasta. mudah beradaptasi. Penanganan permasalahan yurisdiksi internasional dan nasional terkait kegiatan lintas batas dan konsekuensi ekstrateritorial, dilaksanakan dengan pendekatan global yang mengedepankan pada gagasan kemungkinan kerangka hukum tunggal di

seluruh dunia dan mekanisme peraturan universal, kemungkinan terdapat kerangka hukum tunggal dan bergantung pada mekanisme regional serta berfokus pada sistem hukum nasional yang memberikan keefektifan penanganan atas ancaman digital.

Kesadaran hukum dan sosialisasi terhadap masyarakat adalah strategi preventif dalam kejahatan siber dengan upaya perlindungan terhadap hak serta kebebasan berekspresi. Reformulasi regulasi menjadi hal yang pokok mengingat ancaman kejahatan siber yang terus berkembang. Indonesia juga harusnya dapat meratifikasi *Convention on Cybercrime* untuk dapat meningkatkan kolaborasi dengan negara-negara peserta jika terjadi kejahatan siber yang mengancam Indonesia, terutama jika pelakunya beroperasi di luar wilayah Indonesia.

PENELITIAN LANJUTAN

Dalam penulisan artikel ini peneliti menyadari masih banyak kekurangan baik dari segi bahasa, penulisan, dan bentuk penyajian mengingat keterbatasan pengetahuan dan kemampuan dari peneliti sendiri. Oleh karena itu, untuk kesempurnaan artikel, peneliti mengharapkan kritik dan saran yang membangun dari berbagai pihak.

DAFTAR PUSTAKA

Adolf, Huala. *Aspek-Aspek Hukum Pidana Internasional*. Jakarta: Raja Grafindo Persada, 1996.

Ba'abud, Mohammad Fadel Roihan, and Dodik Setiawan Nur Heriyanto. *Application of The Principles of Extraterritorial Jurisdiction Towards Personal Data Breach Committed Cross-Country Borders*. *Uti Possidetis: Journal of International Law*. Vol. 5, 2024. https://doi.org/10.22437/up.v5i1.28300.

Budhijanto, Danrivanto. *Hukum Telekomunikasi, Penyiaran, & Teknologi Informasi*. Bandung: Refika Aditama, 2010.

Hamzah, Andi. *Aspek-Aspek Pidana Di Bidang Komputer*. Jakarta: Sinar Grafika, 1992.

Hariyono, Akbar Galih, and Frans Simangunsong. "Perlindungan Hukum Korban Pencurian Data Pribadi (Phishing Cybercrime) Dalam Perspektif Kriminologi." *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance* 3, no. 1 (2023): 428–39. https://doi.org/10.53363/bureau.v3i1.191.

Hartono, Bambang, and Recca Ayu Hapsari. "Mutual Legal Assistance Pada Pemberantasan Cyber Crime Lintas Yurisdiksi Di Indonesia." *Jurnal S* 25, no. 1 (2019).

Irpan. "Law Enforcement Jurisdiction In Cybercrime." *The 1th Proceeding International Conference And Call Paper Sultan Agung Islamic University* 1, no. 1 (2020): 307–17.

Muhaimin. *Metode Penelitian Hukum*. Mataram: Mataram University Press, 2020.

Nugraha, Riko. "Perspektif Hukum Indonesia (Cyberlaw) Penanganan Kasus Cyber Di Indonesia." *Jurnal Ilmiah Hukum Dirgantara* 11, no. 2 (2021): 44–56.

Putra, Akbar Kurnia. "Analisis Hukum Yurisdiksi Tindak Kejahatan Siber (Cybercrime) Berdasarkan Convention on Cybercrime." *Jurnal Ilmu Hukum* 7, no. 1 (2016): 22–54.

Putra, Jay Sadikin Abdul Azis Mandala. "Hacking As A Challenge For Change And The Development Of Cyber Law In Indonesia." *Jurnal Ilmu Hukum Tambun Bungai* 8, no. 2 (2023): 162–91.

Rosenoer, Jonathan. *Cyberlaw: The Law of Internet*. New York: Springger, 1997.

Saragih, Masdin, Henry Aspan, and Andysah Putera Utama Siahaan. "Violations of Cybercrime and the Strength of Jurisdiction in Indonesia." *The International Journal Of Humanities & Social Studies* 5, no. 12 (2017): 210–29.

Singgi, I Gusti Ayu Suanti Karnadi, I Gusti Bagus Suryawan, and I Nyoman Gede Sugiartha. "Penegakan Hukum Terhadap Tindak Pidana Peretasan Sebagai Bentuk Kejahatan Mayantara (Cyber Crime)." *Jurnal Konstruksi Hukum* 1, no. 2 (2020): 334–39. https://doi.org/10.22225/jkh.2.1.2553.334-339.