

FAKTOR PENYEBAB TERJADINYA KEJAHATAN *CYBER CRIME* YANG DILAKUKAN OLEH ORANG ASING DI BALI DITINJAU DARI PERSPEKTIF KRIMINOLOGI

Made Wisnu Adi Saputra¹, I Wayan Gde Wiryawan ², Kt. Sukawati Lanang
P.Perbawa ³

¹BIN Daerah Bali, E-mail: wisnuadspr@gmail.com

Info Artikel	Abstract
<p><i>Factors Causing the Occurrence of Cyber Crimes Perpetrated by Foreigners in Bali from a Criminological Perspective</i></p> <p>Keywords :</p>	<p><i>One of the negative impacts of the development of tourism in Bali triggers the development of criminal acts committed by foreigners. The purpose of this study is to find out (1) the factors causing the occurrence of cyber crimes committed by foreigners in Bali; and (2) efforts to overcome cyber crimes committed by foreigners in Bali. The research method used is a type of normative legal research. The results of the research show (1) The factors causing the occurrence of cyber crimes committed by foreigners in Bali have three elements: an act that is against the law; carried out by the foreigner and carried out for personal and/or group gain while on the other hand harming the other party either directly or indirectly. Pressure is generally caused by individual behavior that causes them to commit crimes. Another cause of crime is the opportunity (opportunity). The opportunity is wide open for foreigners in Bali to commit crimes including cyber crime; (2) Efforts to overcome cyber crimes committed by foreigners in Bali can be carried out by implementing cyber law or legal policies in the cyber field. However, the legal system in Indonesia has not specifically regulated cybercrime.</i></p> <p><i>Crime, Cyber, Person, Foreign, Bali</i></p>
<p>Faktor Penyebab Terjadinya Kejahatan <i>Cyber Crime</i> yang Dilakukan oleh Orang Asing di Bali Ditinjau dari Perspektif Kriminologi</p>	<p>Abstrak</p> <p>Salah satu dampak negatif dari perkembangan pariwisata di Bali memicu berkembangnya tindakan kriminal yang dilakukan oleh orang asing. Tujuan penelitian ini untuk mengetahui (1) faktor penyebab terjadinya kejahatan <i>cyber crime</i> yang dilakukan oleh orang asing di Bali; dan (2) upaya penanggulangan kejahatan <i>cyber crime</i> yang dilakukan oleh orang asing di Bali. Metode penelitian yang digunakan adalah jenis penelitian hukum normatif. Hasil penelitian menunjukkan (1) Faktor penyebab terjadinya kejahatan <i>cyber crime</i> yang dilakukan oleh orang asing di Bali memiliki tiga unsur: adanya perbuatan yang melawan hukum; dilakukan oleh orang asing tersebut dan dilakukan untuk mendapatkan keuntungan pribadi dan/atau kelompok sementara di lain pihak merugikan pihak lain baik langsung maupun tidak langsung. Tekanan (<i>pressure</i>) umumnya disebabkan karena perilaku individual yang menyebabkannya melakukan kejahatan. Penyebab kejahatan lainnya adanya kesempatan (<i>opportunity</i>). Kesempatan itu terbuka lebar bagi orang asing di Bali untuk melakukan kejahatan termasuk kejahatan <i>cyber crime</i>; (2)</p>

Kata kunci:	Upaya penanggulangan kejahatan <i>cyber crime</i> yang dilakukan oleh orang asing di Bali dapat dilakukan dengan penerapan <i>cyber law</i> atau kebijakan hukum di bidang <i>cyber</i> . Namun demikian, sistem perundang-undangan di Indonesia belum mengatur secara khusus mengenai <i>cybercrime</i> . Kejahatan, Cyber, Orang, Asing, Bali
--------------------	---

I. PENDAHULUAN

I.1 Latar Belakang Permasalahan

Sektor pariwisata merupakan salah satu sektor terbesar dan terkuat dalam perekonomian dunia. Sektor pariwisata menjadi salah satu pendorong utama perekonomian dunia karena terdapat beberapa keuntungan yang mampu memberikan devisa cukup besar bagi negara, memperluas lapangan pekerjaan dan memperkenalkan budaya negara. Pariwisata sekarang telah menjadi salah satu sektor ekonomi terbesar dan mempunyai tingkat pertumbuhan paling pesat dan menjadi salah satu sumber utama pendapatan bagi banyak negara di dunia. Melalui penerimaan devisa, penciptaan lapangan pekerjaan dan kesempatan berusaha, serta pembangunan infrastruktur menjadikan pariwisata sebagai salah satu penggerak utama (*key driver*) kemajuan sosio-ekonomi suatu negara.

Organisasi Pariwisata Dunia (*World Tourism Organization, UNWTO*) memperkirakan jumlah kunjungan wisatawan internasional akan mencapai 1,8 miliar pada tahun 2030 dengan tingkat pertumbuhan kunjungan per tahun sebesar 3,3 persen. Perkiraan UNWTO tersebut sudah tentu menggiurkan pelaku usaha pariwisata di berbagai negara. Sekarang muncul banyak daerah tujuan wisata baru di dunia di luar negara tujuan wisata yang secara tradisional menjadi tujuan favorit seperti Eropa dan Amerika Utara. Wilayah Asia dan Pasifik diperkirakan mempunyai pertumbuhan yang lebih tinggi dibanding kawasan lain, bahkan di negara tertentu pertumbuhannya jauh lebih tinggi. Bagi Indonesia, ini merupakan peluang sekaligus tantangan dalam pengembangan kepariwisataan nasional.¹

Provinsi Bali merupakan salah satu provinsi di Indonesia yang membangun pariwisatanya melalui pariwisata budaya. Pariwisata budaya merupakan pariwisata yang menggunakan potensi kebudayaan yang dimiliki oleh suatu daerah untuk dijadikan objek pariwisatanya. Di setiap kabupaten/kota di Provinsi Bali memiliki keunikan budaya dan tradisi dengan ciri khas masing-masing daerah yang menarik wisatawan untuk berlibur di Pulau Bali. Selain itu Pulau Bali memiliki unsure panorama alam yang lengkap untuk dijadikan objek pariwisata seperti adanya danau, sungai, gunung, pantai, dan hutan yang memanjang dari pesisir barat hingga timur Pulau Bali.

Sudah diakui dunia bahwa Bali merupakan salah satu daerah tujuan wisata utama di Indonesia. Jumlah wisatawan baik wisatawan asing maupun wisatawan domestik yang berkunjung ke Bali selalu meningkat dari tahun ke tahunnya. Peningkatan kunjungan wisatawan ke Bali terjadi karena daya tarik alam dan budaya Bali bagi wisatawan. Selain itu, peningkatan juga terjadi karena infrastruktur dan fasilitas lainnya yang terus berkembang. Bandara Ngurah Rai Bali sejak tahun 3013 telah memperluas dan meningkatkan fasilitasnya dengan dana Rp 2,8 trilyun yang meliputi perluasan terminal keberangkatan dan kedatangan domestik dan internasional. Dengan

¹ United Nations and World Tourism Organization (UNWTO), *Tourism Highlights 2017 Edition* (New York: Madrid, 2017).

rampungnya renovasi Bandara Ngurah Rai tahun 2013, kapasitasnya meningkat dari 14 juta penumpang menjadi 25 juta penumpang atau mengalami peningkatan sebesar 78,57 %. Angka ini merupakan kapasitas bandara terbesar di Indonesia saat ini (Kantor Imigrasi Kelas I Khusus Ngurah Rai Bali, 2013).

Data dari Dinas Pariwisata Provinsi Bali Tahun 2018 menunjukkan bahwa kunjungan wisatawan asing dalam 10 tahun terakhir meningkat yaitu dari 1.664.854 orang pada tahun 2007 menjadi 6.598.903 orang pada tahun 2017 yang berarti meningkat 4.934.049 orang atau meningkat 296,37%. Hal ini menunjukkan bahwa sektor pariwisata di Provinsi Bali memperlihatkan perkembangan yang baik dilihat dari dampak ekonomi yang disumbangkan pada Pendapatan Asli Daerah (PAD) Provinsi Bali. Peningkatan kunjungan wisatawan ke Indonesia juga membuat sektor pariwisata Bali mampu berperan sebagai sumber penerimaan negara yang diperoleh dari konsumsi wisatawan selama melakukan kunjungan ke daerah tujuan wisata di Provinsi Bali.²

Meskipun peningkatan jumlah wisman di Bali memberi dampak positif bagi PAD Provinsi Bali, namun tak dapat dipungkiri bahwa peningkatan kunjungan wisman tersebut juga membawa dampak negatif, salah-satunya meningkatnya kejahatan atau tindakan kriminal yang dilakukan oleh orang asing yang datang ke Bali tersebut.

Data statistik dari Kantor Imigrasi Klas I Khusus Ngurah Rai Bali menunjukkan jumlah orang asing yang terlibat kejahatan atau tindak kriminal umum dan khusus di Bali cukup banyak, mulai dari kasus paling ringan, seperti penyalahgunaan izin tinggal, penyebab kecelakaan lalu lintas, pembunuhan, narkoba, pedofilia hingga yang terakhir kejahatan *cyber crime* semakin meningkat. Selanjutnya data statistik kriminologi yang ada di Polda Bali menunjukkan pada pertengahan tahun 2018 ratusan warga negara China ditangkap Polda Bali di dua wilayah di tiga lokasi. Para pelaku ditangkap terkait kasus *cyber fraud* atau tindak pidana kejahatan internet. Dari tiga lokasi itu Polda Bali mengamankan 103 warga China.

Kedua lokasi tersebut ada di Denpasar dan satu lokasi ada di Badung. Tiga lokasi ditangkapnya ratusan warga China itu di antaranya di Jalan Perumahan Mutiara Abianbase No 1, Mengwi, Badung pihaknya mengamankan 49 orang. Dengan barang bukti ada 51 telepon, 1 laptop, 43 paspor, 5 handphone, 2 router, 2 printer, Hub 26 unit. Lokasi kedua adalah Jalan Bedahulu XI Nomor 39 Denpasar. Di lokasi itu, polisi mengamankan 32 orang dengan barang bukti 20 handphone, 13 router, 2 laptop, dan 1 paspor. Sedangkan TKP ketiga berada di Jalan Gatsu I Nomor 9 Denpasar. Polda Bali mengamankan 33 orang dengan barang bukti 3 router, 2 laptop, 38 paspor, dan 1 Hub.

Para pelaku telah melakukan penipuan. Korbannya adalah warga negara China lainnya. Mereka telah menipu warga China sendiri. Dengan cara ditelepon dari sini dan mereka membujuk korban sehingga para korban ini mentransfer uang kepada para pelaku. Dalam menjalankan aksinya melakukan penipuan, pelaku memiliki modus mengaku sebagai keluarga korban. Selain itu, pelaku juga mengaku sebagai aparat hukum dari China, sehingga para korban ini merasa terancam. Tidak hanya itu, mereka juga mengaku dari rumah sakit dan mengatakan keluarga korban mengalami kecelakaan.

I.2 Tujuan Penelitian

² Singagerda, 'Faktor-Faktor Penentu Aliran Investasi, Dan Perdagangan Pariwisata Serta Dampaknya Terhadap Permintaan Dan Penawaran Pariwisata Indonesia' (Institusi Pertanian Bogor, 2014).

Berdasarkan latar belakang yang telah dikemukakan di atas, maka tujuan penelitian ini adalah untuk mengetahui (1) faktor penyebab terjadinya kejahatan *cyber crime* yang dilakukan oleh orang asing di Bali; dan (2) upaya penanggulangan kejahatan *cyber crime* yang dilakukan oleh orang asing di Bali.

I.3 Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah jenis penelitian hukum normatif. Penelitian hukum normatif (*normative legal research*) merupakan penelitian yang dilakukan dengan cara mengkaji peraturan perundang-undangan yang berlaku atau diterapkan terhadap suatu permasalahan hukum tertentu. Penelitian hukum normatif meneliti hukum dari perspektif internal dengan objek penelitiannya adalah norma hukum.³ Penelitian normatif seringkali disebut dengan penelitian doktrinal, yaitu penelitian yang objek kajiannya adalah dokumen peraturan perundang-undangan dan bahan pustaka.⁴ Penelitian hukum normatif juga disebut penelitian yang difokuskan untuk mengkaji penerapan kaidah-kaidah atau norma dalam hukum positif.⁵ Menurut I Made Pasek Diantha penelitian hukum normatif berfungsi untuk memberi argumentasi yuridis ketika terjadi kekosongan, kekaburan dan konflik norma. Lebih jauh ini berarti penelitian hukum normatif berperan untuk mempertahankan aspek kritis dari keilmuan hukumnya sebagai ilmu normatif.⁶

II. PEMBAHASAN

II.1 Faktor Penyebab Terjadinya Kejahatan *Cyber Crime* yang Dilakukan oleh Orang Asing di Bali

Kehidupan manusia modern saat ini tidak dapat dilepaskan dari bahkan terkadang sangat bergantung pada kemajuan teknologi canggih/ maju (*high tech* atau *advanced technology*) di bidang informasi dan elektronik melalui jaringan internasional (internet). Keberadaan internet ini dimanfaatkan oleh masyarakat dunia dari berbagai kalangan untuk berbagai kegiatan, seperti mencari informasi, mengirim informasi dan melakukan kegiatan bisnis atau non bisnis. Kegiatan ini dikenal sebagai kegiatan telematika (*cyber activities*). Di dalam *cyber activities* peran teknologi sangat besar, karena semakin tinggi teknologi yang dimiliki maka semakin besar pula peluang masyarakat untuk menggunakan internet dalam kehidupan sehari-hari. Pengguna internet ini terbagi menjadi pengguna pasif dan aktif. Pengguna pasif adalah para pengguna yang hanya membuka *web pages* di internet (*browsing*) atau membaca informasi tanpa melakukan interaksi baik dengan *vendor/administrator* atau pengguna internet lainnya. Pengguna internet aktif adalah para pengguna yang melakukan interaksi dengan *vendor* atau dengan pengguna internet lainnya, contohnya, berbelanja secara *online*, mengirim surat elektronik (e-mail) dan lain sebagainya. Pengguna aktif ini juga dapat menggunakan media internet untuk melakukan tindakan yang dikategorikan sebagai kejahatan telematika (*cyber crime*). *Cyber crime* atau kejahatan telematika adalah tindakan kejahatan yang dilakukan dengan menggunakan media internet. Contohnya, tindakan yang disebut *carding*, adalah *cyber crime* dengan cara mencuri data kartu kredit dari

³ I Made Pasek Diantha, *Metodologi Penelitian Hukum Normatif Dalam Justifikasi Teori Hukum* (Jakarta: Prenada Media Group, 2017).

⁴ Peter Mahmud Marzuki, *Penelitian Hukum* (Jakarta: Kencana Prenada Media, 2011).

⁵ Johny Ibrahim, *Teori Dan Metodologi Penelitian Hukum Normatif* (Malang: Banyumedia, 2012).

⁶ I Made Pasek Diantha, *op.cit.* h.12.

nasabah suatu bank, sehingga si pelaku *carding* (*carder*) dapat menggunakan data tersebut untuk keuntungan pribadi.⁷

Kejahatan lain adalah pencurian kartu kredit, hacking beberapa situs, menyadap transmisi data orang lain, misalnya email, dan memanipulasi data dengan cara menyiapkan perintah yang tidak dikehendaki ke dalam programer komputer. Sehingga dalam kejahatan komputer dimungkinkan adanya delik formil dan delik materil. Delik formil adalah perbuatan seseorang yang memasuki komputer orang lain tanpa ijin, sedangkan delik materil adalah perbuatan yang menimbulkan akibat kerugian bagi orang lain. Adanya *cyber crime* telah menjadi ancaman stabilitas, sehingga pemerintah sulit mengimbangi teknik kejahatan yang dilakukan dengan teknologi komputer, khususnya jaringan internet dan intranet.⁸

Cybercrime atau kejahatan telematika sangat menggunakan komputer baik sebagai alat untuk mencapai tujuan dari kejahatan tersebut (*computer as a tool*) mau pun komputer sebagai target kejahatan (*computer as a target*). Pada dasarnya originalitas *cyber crime* adalah kejahatan dimana komputer sebagai target. Contohnya penyebaran virus atau *malicious ware*, sementara kejahatan dimana komputer sebagai alat adalah kejahatan tradisional yang menggunakan komputer sebagai sarana (contohnya *fraud* atau penipuan yang menggunakan *electronic mail* sebagai alat penyebaran informasi bagi si penipu). Kerugian yang timbul akibat adanya *cyber crime* ini dari tahun ke tahun semakin meningkat. Kerugian atas kejahatan ini akan terus meningkat dua kali lipat setiap tahunnya, apabila tidak segera diantisipasi.

Berkaitan dengan sifat, hakikat, dan luas lingkup *cyber crime* sebagian pakar berpendapat bahwa tindak pidana siber bukanlah kejahatan baru, tetapi kejahatan tradisional yang dilakukan di *cyber space* dan hanya merupakan kejahatan dengan menggunakan alat-alat baru yang membantu pelaku dalam melakukan kejahatannya. *Cyber crime* hampir sama dengan 'old fashioned' non-virtual crime. Peter Grabosky menyebutnya sebagai 'old wine in new bottles'. Sebagian pakar lainnya berpendapat bahwa *cyber crime* merupakan bentuk kejahatan baru yang berbeda dengan kejahatan-kejahatan di dunia nyata. Fokus kebaruan dari tindak pidana siber terletak pada ciri-ciri sosio-struktural lingkungan (*cyberspace*) tempat kejahatan terjadi.⁹ Menurut Susan W. Brenner ada jenis-jenis *cybercrime* yang memang merupakan kejahatan baru dan ada juga jenis-jenis kejahatan tradisional yang menggunakan komputer sebagai alat untuk melakukan kejahatan. Jenis-jenis *cyber crime* yang dapat dikatakan sebagai 'new crimes', misalnya, *hacking*, *cracking*, *Ddos attack*, dan *viruses* yang termasuk kategori 'crimes in which the computer is the target of the criminal activity'. Jenis-jenis *cyber crime* yang termasuk 'not new crime', misalnya, penipuan secara *online*, pencurian sejumlah dana atau informasi, penggelapan, pemalsuan, *stalking*, membuat dan atau menyebarkan pornografi anak, yang termasuk kategori "crimes in which the computer is a tool used to commit a crime; serta jenis *cyber crime* yang termasuk kategori *crimes in which the use of the computer is an incidental aspect of the commission of the crime*", seperti seseorang menggunakan komputer untuk menulis surat yang berisi ancaman. Komputer dalam hal ini hanya sebagai alat bukti.¹⁰ Pandangan yang hampir sama

⁷ Alcianno G. Gani, 'Cybercrime (Kejahatan Berbasis Komputer)', *Jurnal Dinamika*, 5.1 (2018) <<https://journal.universitassuryadarma.ac.id/index.php/jsi/article/view/18>>.

⁸ Muhammad E. Fuady, 'Cybercrime: Fenomena Kejahatan Melalui Internet Di Indonesia', *Jurnal Mediator*, 6.2 (2015), 255 <<https://ejournal.unisba.ac.id/index.php/mediator/article/view/1194>>.

⁹ Majid Yar, *Cybercrime and Society* (London: Sage Publication, 2006).

¹⁰ Ralph D. Clifford, *Cybercrime: The Investigation, Prosecution and Defense of Computer-Related Crime* (North Carolina: Carolina Academic Press, 2006).

dengan Susan Brenner dikemukakan oleh Yvonne Jewkes yang berpandangan bahwa tindak pidana siber dapat diklasifikasikan dalam dua kategori berikut:

a. *New crimes using new tools*

Kejahatan yang tidak dapat dilakukan dengan cara lain atau terhadap tipe korban lain, seperti *hacking* dan *viruses*.

b. *Old crimes using new tools*

Kejahatan konvensional yang dilakukan dengan menggunakan teknologi komputer dan teknologi informasi baru, seperti penipuan, pencurian identitas, dan *stalking*.¹¹

Menurut David Wall internet khususnya *cyber space* telah menciptakan tidak hanya kasus '*old wine in new bottles*' atau '*new wine in new bottles*' tetapi juga kasus yang termasuk '*new wine in no bottles*'.¹² Dalam pengertian yang terakhir, *cyber crime* tidak hanya sekedar kejahatan dilakukan dengan menggunakan atau melalui teknologi informasi dan komunikasi, tetapi terdapat kejahatan baru yang terjadi tanpa ruang fisik dan juga waktu. Hanya perbuatan dan akibat yang terjadi yang dapat diidentifikasi ruang fisik dan waktunya.¹³

Berdasarkan uraian di atas pengamatan terhadap berbagai bentuk/jenis *cyber crime* yang terjadi dapat disimpulkan bahwa *cyber crime* mencakup tindak pidana tradisional yang menggunakan teknologi informasi dan komunikasi sebagai alat atau media dan tindak pidana baru (*new crime*) yang hanya dapat terjadi di *cyber space* atau internet.

Ditinjau dari teori kriminologi khususnya teori-teori mikro (*microtheories*) seorang/kelompok orang dalam masyarakat melakukan kejahatan atau menjadi kriminal (*etiology criminal*). Konkritnya, teori-teori ini lebih bertendensi pada pendekatan psikologis atau biologis. Termasuk dalam teori-teori ini adalah *Social Control Theory* dan *Social Learning theory*. Ketiga, *Beidging Theories* yang tidak termasuk ke dalam kategori teori makro/mikro dan mendeskripsikan tentang struktur sosial dan bagaimana seseorang menjadi jahat. Namun kenyataannya, klasifikasi teori-teori ini kerap membahas epidemiologi yang menjelaskan rates of crime dan etiologi pelaku kejahatan. Termasuk kelompok ini adalah *Subculture Theory* dan *Differential Opportunity Theory*.¹⁴

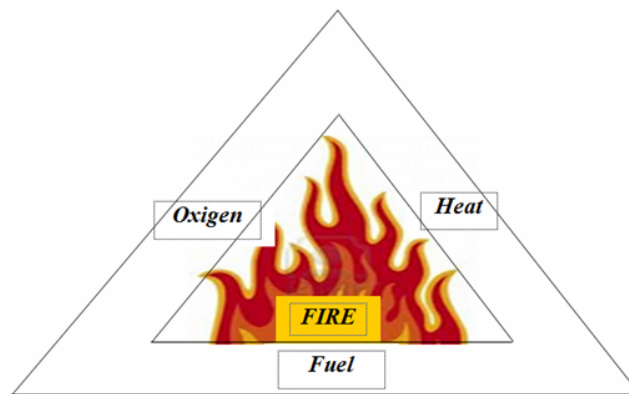
Muhammad Mustofa menjelaskan lebih lanjut penyebab terjadinya kejahatan termasuk *cyber crime* dengan Teori *Fire Triangle* sebagaimana digambarkan sebagai berikut:

¹¹ Galuh Kartiko, 'Pengaturan Terhadap Yurisdiksi Cyber Crime Ditinjau Dari Hukum Internasional', *Jurnal Arena Hukum*, 3.2 (2017) <<https://journal.trunojoyo.ac.id/rechtidee/article/view/695/616>>.

¹² David S. Wall, *Cybercrime* (UK: Polity Press, 2007).

¹³ Tessa Rantung, John Reimon Batmetan, Ahnes Montoh, I Gusti Ayu Mirahyanti, 'Analisa Penyebab Terjadinya Cybercrime', *Jurnal Keamanan Komputer*, 2.2 (2018) <<https://www.researchgate.net/publication/326138055>>.

¹⁴ I Ketut Rai Setiabudhi, Gde Made Swardhana, 'Kriminologi Dan Viktimologi' (Program Studi Magister Ilmu Hukum, Program Pasca Sarjana, Universitas Udayana, Denpasar, 2018).



Gambar 1. Teori Fire Triangle¹⁵

Dalam Teori *Fire Triangle* kejahatan diibaratkan dengan kebakaran yang terjadi bila ketiga unsur kebakaran yaitu *oxigen* (oksigen), *heat* (panas) dan *fuel* (bahan bakar) tersebut bertemu, maka kebakaran akan terjadi. Penyebab kebakaran tersebut bila ditarik dalam penyebab kejahatan, kejahatan bisa terjadi karena adanya *pressure*. *Pressure* bisa terjadi dari kondisi keuangan pelaku (*financial pressure*). Jika *pressure* ini bertemu dengan kesempatan (*opportunity*) dan adanya pembenaran dari pelaku (*razionalization*) maka terjadilah kejahatan yang bisa dilakukan oleh siapa saja¹⁶ termasuk orang asing di Bali.

Kejahatan umumnya terjadi karena tiga hal utama, yaitu: adanya tekanan untuk melakukan kejahatan, adanya kesempatan yang bisa dimanfaatkan serta adanya pembenaran terhadap tindakan tersebut. Pada prinsipnya penyebab kejahatan *cyber crime* yang dilakukan oleh orang asing di Bali memiliki tiga unsur, yaitu: adanya perbuatan yang melawan hukum (*illegal acts*); dilakukan oleh orang asing tersebut dan dilakukan untuk mendapatkan keuntungan pribadi dan/atau kelompok sementara di lain pihak merugikan pihak lain baik langsung maupun tidak langsung.

Tekanan atau *pressure* umumnya disebabkan karena perilaku individual yang menyebabkannya melakukan kejahatan. Bisa jadi tekanan itu disebabkan masalah keuangan (*financial pressure*) yang dipicu karena gaya hidup yang berlebihan, sikap tamak dan serakah, banyak hutang atau tanggungan dan sebagainya, yang menyebabkan seseorang “terpaksa” melakukan kejahatan. Kebiasaan buruk yang sudah mendarah daging dan tak bisa dihilangkan begitu saja, juga membuat seseorang bisa terdorong melakukan tindakan kejahatan, terlebih bila kebiasaan-kebiasaan tersebut memerlukan dana yang cukup banyak, seperti: berjudi, minuman keras, dan prostitusi. Semua kebiasaan tersebut memerlukan dana yang cukup besar untuk memenuhinya. Itu sebabnya, mengapa seseorang yang sudah kecanduan dengan kebiasaan buruk tersebut bisa melakukan kejahatan.

Penyebab kejahatan lainnya adalah adanya kesempatan atau *oppurtunity*. Kesempatan itu terbuka lebar bagi orang asing di Bali untuk melakukan kejahatan termasuk kejahatan *cyber crime*. Kejahatan bebas visa kunjungan dan lemahnya pengawasan bagi orang asing di Bali telah membuka kesempatan bagi orang-orang asing yang berkunjung ke Bali untuk melakukan kejahatan tersebut.

¹⁵ Muhammad Mustofa, *Metodologi Penelitian Krimonologi* (Jakarta: PT. Fajar Interpratama Mandiri, 2013).

¹⁶ *Ibid.*

II.2 Upaya Penanggulangan Kejahatan *Cyber Crime* yang Dilakukan oleh Orang Asing di Bali

Kebijakan penanggulangan *cybercrime* dengan hukum pidana termasuk bidang *penal policy* yang merupakan bagian dari *criminal policy* (kebijakan penanggulangan kejahatan). Dilihat dari sudut *criminal policy*, upaya penanggulangan kejahatan (termasuk penanggulangan *cybercrime*) tidak dapat dilakukan semata-mata secara parsial dengan hukum pidana (sarana penal), tetapi harus pula ditempuh dengan pendekatan integral/ sistemik.¹⁷ Sebagai salah satu bentuk *high tech crime* yang dapat melampaui batas-batas negara (bersifat *transnational/transborder*), merupakan hal yang wajar jika upaya penanggulangan *cybercrime* juga harus ditempuh dengan pendekatan teknologi (*techno prevention*). Di samping itu, diperlukan pula pendekatan budaya/kultural, pendekatan moral/edukatif, dan bahkan pendekatan global melalui kerjasama internasional.¹⁸

Operasionalisasi kebijakan penal meliputi kriminalisasi, dekriminalisasi, penalisasi dan depenalisasi. Penegakan hukum pidana tersebut sangat tergantung pada perkembangan politik hukum, politik kriminal, dan politik sosial. Oleh karena itu, penegakan hukum tidak hanya memperhatikan hukum yang otonom, melainkan memperhatikan juga masalah kemasyarakatan dan ilmu perilaku sosial.¹⁹

Berkenaan dengan kebijakan kriminalisasi perbuatan dalam dunia *cyber* (maya), dalam lokakarya/*workshop* mengenai *computer related crime* yang diselenggarakan dalam kongres PBB X pada bulan April 2000, dinyatakan bahwa negara-negara anggota harus berusaha melakukan harmonisasi ketentuan-ketentuan yang berhubungan dengan kriminalisasi, pembuktian, dan prosedur (*states should seek harmonization of the relevant provisions on criminalization evidence and procedure*). Jadi masalahnya bukan sekedar bagaimana membuat kebijakan hukum pidana (kebijakan kriminalisasi/formulasi/legislasi) di bidang penanggulangan *cybercrime* tetapi bagaimana ada harmonisasi kebijakan penal di berbagai negara. Ini berarti bahwa kebijakan kriminalisasi tentang masalah *cybercrime* bukan semata-mata masalah kebijakan nasional Indonesia, tetapi juga terkait dengan kebijakan regional dan internasional.

Melakukan kriminalisasi *cybercrime* ada lima hal yang perlu diperhatikan oleh pembentuk undang-undang (legislator), yaitu:

- a. Kriminalisasi harus merupakan upaya yang mendukung tujuan akhir kebijakan kriminal, yaitu melindungi dan mensejahterakan masyarakat.
- b. Perbuatan yang akan dikriminalisasi tersebut benar-benar dicela oleh masyarakat.
- c. Perlu diperhitungkan tentang keuntungan dan kerugian kriminalisasi.
- d. Perlu diupayakan agar tidak terjadi over-kriminalisasi yang dapat berpengaruh secara sekunder terhadap kepentingan masyarakat.
- e. Perlu disesuaikan antara kemampuan penegak hukum dengan penegakan hukum.²⁰

Kebijakan kriminalisasi atau formulasi hukum pidana di Indonesia yang berkaitan dengan masalah *cyber crime*, selama ini dapat diidentifikasi sebagai berikut:²¹

- a. Dalam Kitab Undang-Undang Hukum Pidana (KUHP)

¹⁷ Barda Nawawi Arief, *Pembaharuan Hukum Pidana Dalam Perspektif Kajian Perbandingan* (Bandung: Citra Aditya Bakti, 2015).

¹⁸ Marwin, 'Penanggulangan Cyber Crime Melalui Penal Policy', *Fiat Justitia Journal*, 7.2 (2018) <<http://ejournal.radenintan.ac.id/index.php/asas/article/view/1693>>.

¹⁹ Bambang Poernomo, *Kapita Selekta Hukum Pidana* (Yogyakarta: Liberty, 2008).

²⁰ H. Obsatar Sinaga, 'Penanggulangan Kejahatan International Cyber Crime Di Indonesia', *Padjadjaran Journal of Law*, 3.2 (2015) <<https://pustaka.unpad.ac.id/wp-content/uploads/2012/02/10>>.

²¹ Barda Nawawi Arief, *op.cit*, h. 127-128.

Perumusan tindak pidana di dalam KUHP kebanyakan masih bersifat konvensional dan belum secara langsung dikaitkan dengan perkembangan *cyber crime*, selain itu juga terdapat berbagai kelemahan dan keterbatasan dalam menghadapi perkembangan teknologi dan *high tech crime* yang sangat bervariasi. Contoh dalam hal menghadapi masalah pemalsuan kartu kredit dan transfer dana elektronik saja, KUHP mengalami kesulitan karena tidak adanya aturan khusus mengenai hal tersebut. Ketentuan yang ada hanya mengenai: (a) sumpah/keterangan palsu (Pasal 242); (b) pemaluan mata uang dan uang kertas (Pasal 244-252); (c) pemalsuan materai dan merk (Pasal 253-262); dan (d) pemalsuan surat (Pasal 263-276).

b. Undang-Undang di luar KUHP

- 1) Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi, mengancam pidana terhadap perbuatan: (1) memanipulasi akses ke jaringan telekomunikasi (Pasal 50 *jo* 22); (2) menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi (Pasal 55 *jo* 38); (3) menyadap informasi melalui jaringan telekomunikasi (Pasal 56 *jo* 40).
- 2) Pasal 26A Undang-Undang Nomor 20 Tahun 2001 tentang Perubahan Atas Undang-Undang Nomor 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi; Pasal 38 Undang-Undang Nomor 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang; dan Pasal 44 ayat (2) Undang-Undang Nomor 30 Tahun 2002 tentang Komisi Pemberantasan Tindak Pidana Korupsi; mengakui *electronic record* sebagai alat bukti yang sah.
- 3) Undang-Undang Nomor 32 Tahun 2002 tentang Penyiaran, antara lain mengatur tindak pidana:
 - a) Pasal 57 *jo* 36 ayat (5) mengancam pidana terhadap siaran yang: (1) bersifat fitnah, menghasut, menyesatkan/atau bohong; (2) menonjolkan unsur kekerasan, cabul, perjudian, penyalahgunaan narkotika dan obat terlarang; atau (3) mempertentangkan suku, agama, ras, dan antar golongan.
 - b) Pasal 57 *jo* 36 ayat (6) mengancam pidana terhadap siaran yang memperolokkan, merendahkan, melecehkan, dan/atau mengabaikan nilai-nilai agama, martabat manusia Indonesia, atau merusak hubungan internasional.
 - c) Pasal 58 *jo* 46 ayat (3) mengancam pidana terhadap siaran iklan niaga yang didalamnya memuat: a) promosi yang dihubungkan dengan ajaran suatu agama; ideologi, pribadi dan/atau kelompok, yang menyinggung perasaan dan/atau merendahkan martabat orang lain, ideologi lain, pribadi lain, atau kelompok lain; b) promosi minuman keras atau sejenisnya dan bahan atau zat adiktif; c) promosi rokok yang memperagakan wujud rokok; d) hal-hal yang bertentangan dengan kesusilaan masyarakat dan nilai-nilai agama; dan/atau e) eksploitasi anak di bawah umur 18 tahun.
- 4) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Undang-Undang ITE), Bab VII Perbuatan yang dilarang, memuat ketentuan pidana bagi setiap orang yang dengan sengaja dan tanpa hak atau melawan hukum mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik. Kriminalisasi *cyber crime* khususnya dalam Undang-Undang ITE dapat dibagi dalam dua kategori, yaitu perbuatan yang menggunakan komputer sebagai sarana kejahatan, dan perbuatan-perbuatan yang menjadikan komputer sebagai sasaran kejahatan. Kejahatan yang menggunakan komputer sebagai sarana adalah setiap tindakan yang mendayagunakan data komputer, sistem komputer, dan jaringan komputer sebagai alat untuk melakukan kejahatan di

ruang maya bukan ruang nyata. Kejahatan yang menjadikan komputer sebagai sasaran adalah setiap perbuatan dengan menggunakan komputer yang diarahkan pada data komputer, sistem komputer, atau jaringan komputer, atau ketiganya secara bersama-sama. Perbuatan tersebut dilakukan di ruang maya bukan ruang nyata, sehingga seluruh aktivitas yang dilarang oleh peraturan perundang-undangan terjadi di ruang maya.

Banyak terjadi tindak kejahatan Internet seperti *cyber crime* yang dilakukan oleh orang asing di Bali, tetapi yang secara nyata hanya beberapa kasus saja yang sampai ke tingkat pengadilan. Hal ini dikarenakan hakim sendiri belum menerima bukti-bukti elektronik sebagai barang bukti yang sah, seperti digital signature. Dengan demikian *cyber law* bukan saja keharusan melainkan sudah merupakan kebutuhan, baik untuk menghadapi kenyataan yang ada sekarang ini, dengan semakin banyak terjadinya kegiatan *cyber crime* maupun tuntutan komunikasi perdagangan mancanegara (*cross border transaction*) ke depan.²²

Karenanya, Indonesia sebagai negara yang juga terkait dengan perkembangan dan perubahan itu, memang dituntut untuk merumuskan perangkat hukum yang mampu mendukung kegiatan bisnis secara lebih luas, termasuk yang dilakukan dalam dunia virtual, dengan tanpa mengabaikan yang selama ini sudah berjalan. Karena, perangkat hukum yang ada saat ini ditambah *cyber law*, akan semakin melengkapi perangkat hukum yang dimiliki. Inisiatif ini sangat perlu dan mendesak dilakukan, seiring dengan semakin berkembangnya pola-pola bisnis baru tersebut. *cyber law* tersebut diperlukan untuk mengatur kejahatan-kejahatan baru yang bisa dikategorikan sebagai *cyber crime*.

III. PENUTUP

III.1 Simpulan

Berdasarkan hasil pembahasan yang telah diuraikan di atas, maka dapat disimpulkan hal-hal sebagai berikut:

1. Faktor penyebab terjadinya kejahatan *cyber crime* yang dilakukan oleh orang asing di Bali memiliki tiga unsur, yaitu: adanya perbuatan yang melawan hukum (*illegal acts*); dilakukan oleh orang asing tersebut dan dilakukan untuk mendapatkan keuntungan pribadi dan/atau kelompok sementara di lain pihak merugikan pihak lain baik langsung maupun tidak langsung. Tekanan atau *pressure* umumnya disebabkan karena perilaku individual yang menyebabkannya melakukan kejahatan. Bisa jadi tekanan itu disebabkan masalah keuangan (*financial pressure*) yang dipicu karena gaya hidup yang berlebihan, sikap tamak dan serakah, banyak hutang atau tanggungan dan sebagainya, yang menyebabkan seseorang “terpaksa” melakukan kejahatan. Kebiasaan buruk yang sudah mendarah daging dan tak bisa dihilangkan begitu saja, juga membuat seseorang bisa terdorong melakukan tindakan kejahatan, terlebih bila kebiasaan-kebiasaan tersebut memerlukan dana yang cukup banyak, seperti: berjudi, minuman keras, dan prostitusi. Semua kebiasaan tersebut memerlukan dana yang cukup besar untuk memenuhinya. Itu sebabnya, mengapa seseorang yang sudah kecanduan dengan kebiasaan buruk tersebut bisa melakukan kejahatan. Penyebab kejahatan lainnya adalah adanya kesempatan atau *opportunitiy*. Kesempatan itu terbuka lebar bagi orang asing di Bali untuk melakukan kejahatan termasuk kejahatan *cyber*

²² Heri Tahir, Riskawati, ‘Penanganan Kasus Cyber Crime Di Kota Makassar (Studi Pada Kantor Kepolisian Resort Kota Makassar)’, *Jurnal Tomalebbi*, 3.2 (2016) <<https://www.semanticscholar.org/paper/PENANGANAN-KASUS-CYBER-CRIME-DI-KOTA-MAKASSAR-PADA-Riskawati-Tahir/>>.

crime. Kejahatan bebas visa kunjungan dan lemahnya pengawasan bagi orang asing di Bali telah membuka kesempatan bagi orang-orang asing yang berkunjung ke Bali untuk melakukan kejahatan tersebut.

2. Upaya penanggulangan kejahatan *cyber crime* yang dilakukan oleh orang asing di Bali dapat dilakukan dengan penerapan *cyber law* atau kebijakan hukum di bidang *cyber*. Sistem perundang-undangan di Indonesia belum mengatur secara khusus mengenai *cyber crime*. Beberapa peraturan yang ada baik yang terdapat di dalam KUHP maupun di luar KUHP untuk sementara dapat diterapkan terhadap beberapa kejahatan, tetapi ada juga kejahatan yang tidak dapat diantisipasi oleh Undang-Undang ITE yang saat ini berlaku. Untuk memerangi *cybercrime* yang tingkat kriminalitasnya semakin tinggi di Indonesia, maka pemerintah perlu merevisi Undang-Undang ITE yang telah dirancang tersebut. Pemerintah sebaiknya mengoreksi kembali setiap hal yang tercantum dalam Undang-Undang ITE, kemungkinan ada poin-poin yang perlu direvisi sehingga *cyber law* di Indonesia dapat diterapkan dengan baik. Dengan demikian *cyber law* bukan saja keharusan melainkan sudah merupakan kebutuhan, baik untuk menghadapi kenyataan yang ada sekarang ini, dengan semakin banyak terjadinya kegiatan *cyber crime* maupun tuntutan komunikasi perdagangan mancanegara (*cross border transaction*) ke depan. Oleh karena itu, urgensi Indonesia sebagai negara yang juga terkait dengan perkembangan dan perubahan itu, memang dituntut untuk merumuskan perangkat hukum yang mampu mendukung kegiatan bisnis secara lebih luas, termasuk yang dilakukan dalam dunia virtual, dengan tanpa mengabaikan yang selama ini sudah berjalan. Karena, perangkat hukum yang ada saat ini ditambah *cyber law*, akan semakin melengkapi perangkat hukum yang dimiliki. Inisiatif ini sangat perlu dan mendesak dilakukan, seiring dengan semakin berkembangnya pola-pola bisnis baru tersebut.

III.2 Saran

Adapun saran-saran yang dapat diuraikan adalah:

1. *Cyber Law* perlu dibuat secara khusus sebagai *lexspecialis* untuk memudahkan penegakan hukum terhadap kejahatan tersebut.
2. Perlu hukum acara khusus yang dapat mengatur seperti misalnya berkaitan dengan jenis-jenis alat bukti yang sah dalam kasus *cyber crime*, pemberian wewenang khusus kepada penyidik dalam melakukan beberapa tindakan yang diperlukan dalam rangka penyidikan kasus *cyber crime*, dan lain-lain.
3. Spesialisasi terhadap aparat penyidik maupun penuntut umum dapat dipertimbangkan sebagai salah satu cara untuk melaksanakan penegakan hukum *Cyber Law*.
4. Disarankan untuk dibentuk *cyber police* di Indonesia. *Cyber police* dapat dibentuk dari gabungan antara kesatuan Polri dan berbagai kalangan yang kompeten di bidang IT dan dunia *cyber*. Pembentukan *cyber police* ini dapat dikatakan mirip dengan pembentukan KPK di Indonesia. Perbedaannya, KPK bertugas menanggulangi korupsi, sedangkan *cyber police* bertugas menanggulangi *cyber crime*. Pembentukan *cyber police* ini diharapkan akan mampu mengurangi tingkat kriminalitas *cyber crime* di Indonesia.

DAFTAR PUSTAKA

- Arief, Barda Nawawi, *Pembaharuan Hukum Pidana Dalam Perspektif Kajian Perbandingan* (Bandung: Citra Aditya Bakti, 2015)
- Clifford, Ralph D., *Cybercrime: The Investigation, Prosecution and Defense of Computer-Related Crime* (North Carolina: Carolina Academic Press, 2006)
- Diantha, I Made Pasek, *Metodologi Penelitian Hukum Normatif Dalam Justifikasi Teori Hukum* (Jakarta: Prenada Media Group, 2017)
- Fuady, Muhammad E., 'Cybercrime: Fenomena Kejahatan Melalui Internet Di Indonesia', *Jurnal Mediator*, 6.2 (2015), 255
<<https://ejournal.unisba.ac.id/index.php/mediator/article/view/1194>>
- Gani, Alcianno G., 'Cybercrime (Kejahatan Berbasis Komputer)', *Jurnal Dinamika*, 5.1 (2018) <<https://journal.universitassuryadarma.ac.id/index.php/jsi/article/view/18>>
- Gde Made Swardhana, I Ketut Rai Setiabudhi, 'Kriminologi Dan Viktimologi' (Program Studi Magister Ilmu Hukum, Program Pasca Sarjana, Universitas Udayana, Denpasar, 2018)
- Ibrahim, Johny, *Teori Dan Metodologi Penelitian Hukum Normatif* (Malang: Banyumedia, 2012)
- John Reimon Batmetan, Ahnes Montoh, I Gusti Ayu Mirahyanti, Tessa Rantung, 'Analisa Penyebab Terjadinya Cybercrime', *Jurnal Keamanan Komputer*, 2.2 (2018), 81–86 <<https://www.researchgate.net/publication/326138055>>
- Kartiko, Galuh, 'Pengaturan Terhadap Turisdiksi Cyber Crime Ditinjau Dari Hukum Internasional', *Jurnal Arena Hukum*, 3.2 (2017)
<<https://journal.trunojoyo.ac.id/rechtidee/article/view/695/616>>
- Marwin, 'Penanggulangan Cyber Crime Melalui Penal Policy', *Fiat Justitia Journal*, 7.2 (2018) <<http://ejournal.radenintan.ac.id/index.php/asas/article/view/1693>>
- Marzuki, Peter Mahmud, *Penelitian Hukum* (Jakarta: Kencana Prenida Media, 2011)
- Mustofa, Muhammad, *Metodologi Penelitian Krimonologi* (Jakarta: PT. Fajar Interpratama Mandiri, 2013)
- Organization, United Nations and World Tourism, *Tourism Highlights 2017 Edition* (New York: Madrid, 2017)
- Poernomo, Bambang, *Kapita Selekta Hukum Pidana* (Yogyakarta: Liberty, 2008)
- Riskawati, Heri Tahir, 'Penanganan Kasus Cyber Crime Di Kota Makassar (Studi Pada Kantor Kepolisian Resort Kota Makassar)', *Jurnal Tomalebbi*, 3.2 (2016)
<<https://www.semanticscholar.org/paper/PENANGANAN-KASUS-CYBER-CRIME-DI-KOTA-MAKASSAR-PADA-Riskawati-Tahir/>>
- Sinaga, H. Obsatar, 'Penanggulangan Kejahatan International Cyber Crime Di Indonesia', *Padjadjaran Journal of Law*, 3.2 (2015)
<<https://pustaka.unpad.ac.id/wp-content/uploads/2012/02/10>>

Singagerda, 'Faktor-Faktor Penentu Aliran Investasi, Dan Perdagangan Pariwisata Serta Dampaknya Terhadap Permintaan Dan Penawaran Pariwisata Indonesia' (Institusi Pertanian Bogor, 2014)

United Nations and World Tourism Organization (UNWTO), *Tourism Highlights 2017 Edition* (New York: Madrid, 2017).

Wall, David S., *Cybercrime* (UK: Polity Press, 2007)

Yar, Majid, *Cybercrime and Society* (London: Sage Publication, 2006)