YURISDIKSI TERHADAP CYBERCRIME

Wardana, Hendra Kusuma

KKB KK-2 TH 29/10 War y

Pembimbing : Minarno, Nur Basuki

COMPUTER CRIMES

2010

A B S T R A K S I

Penentuan *locus delictie* dalam perkara *cybercrime* berkaitan dengan penentuan yurisdiksi (*cyberjurisdiction*) untuk menerapkan hukum pidana suatu negara serta berkaitan kompetensi pengadilan untuk memeriksa dan mengadili perkara (*Jus Puniendi*), jika dalam tindak pidana tersebut terdapat satu atau lebih unsur asing, maka kekuasaan pidana suatu negara tidak dapat secara sepihak diterapkan begitu saja ketentuan hukum pidana nasionalnya tanpa mempertimbangkan kemungkinan penerapan hukum pidana negara lain. Disamping itu, penentuan *locus delictie* dalam perkara *cybercrime* sangat sulit untuk ditentukan, sehingga untuk menentukan locus delictie guna menentukan yurisdiksi digunakan pendekatan-pendekatan beberapa faktor pendukung berdasarkan teori-teori yurisdiksi mengingat tindak pidana tersebut dilakukan di dalam *cyberspace* yang sifatnya tidak mengenal batas wilayah serta dapat dilakukan lintas negara, karena orang dapat melakukan tindak pidana *cybercrime* dimana saja dan akibat yang ditimbulkan bisa saja terjadi ditempat atau wilayah lain yang berbeda dengan tempat atau wilayah tindak pidana *cybercrime* dilakukan. Menjadi permasalahan adalah tidak jelasnya faktor konstitutif untuk menentukan yurisdiksi *cybercrime*, apakah berdasarkan tempat kejadian perkara? apakah berdasarkan negara tempat pelaku berada? apakah berdasarkan tempat dimana akibat konstitutif berada atau apakah berdasarkan negara tempat pemilik komputer yang diserang ? atau keseluruhan faktor tersebut menjadi satu ?. Dalam penanganan *cybercrime* banyak negara menggunakan pendekatan berbeda dalam menerapkan yurisdiksinya, sehingga terkadang menimbulkan konflik yurisdiksi diantara negara-negara tersebut.

Disamping itu, alat bukti sebagaimana di atur dalam Pasal 184 ayat (1) KUHAP dalam praktik kurang dapat mengakomodir sebagai landasan yuridis manakala alat-alat bukti yang dipergunakan untuk melakukan pembuktian delik *cybercrime* dengan menggunakan media alat bukti digital (*digital evidence*), baik berupa informasi elektronik maupun dokumen elektronik. Namun, dengan disahkannya Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (Selanjutnya disebut UU ITE), terdapat kepastian hukum terhadap alat bukti elektronik sebagaimana diatur dalam Pasal 5 UU ITE sehingga upaya menjerat pelaku *cybercrime* dapat dilakukan.

Hanya saja, tidak semua informasi maupun dokumen elektronik memiliki integritas dan validitas sehingga mempunyai kekuatan pembuktian di persidangan.

Tesis ini merupakan *legal research* dengan menggunakan metode pendekatan *statute approach*, *conceptual approach* dan *comparative approach* dalam tesis ini akan dibahas lebih jauh mengenai penerapan asas yurisdiksi *cybercrime* dalam hukum pidana internasional, serta wewenang yurisdiksi yang dimiliki Indonesia berdasarkan Pasal 2 KUHP serta Pasal 2 UU No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Penerapan asas yurisdiksi tersebut didasarkan pada pendekatan asas *locus delictie* yang diatur dalam Pasal 84 ayat 1 KUHAP dengan pendekatan teori-teori dalam yurisprudensi terkait penerapan *locus delictie* tersebut. Disamping itu, mengingat tidak semua informasi maupun dokumen elektronik memiliki integritas dan validitas sehingga mempunyai kekuatan pembuktian di persidangan, maka dalam tesis ini akan dibahas mengenai standard yang digunakan dalam menilai validitas dan intergritas suatu bukti elektronik sebagai alat bukti yang sah di persidangan berdasarkan ketentuan dalam UU ITE serta prosedur yang telah diterapakan secara internaswional, sehingga penggunaan bukti elektronik dapat secara konsisten dilakukan. Akhir kata, semoga tesis ini dapat menjadi bacaan yang bermanfaat dan menambah wawasan bagi pembacanya.

Keywords: Cyber Jurisdiction, Locus Delictie,Digital Evidence, Court Examination

A B S T R A C T

Determining the location of the act (locus delictie) in the case of cybercrime is related to a decides of jurisdiction (Cyber Jurisdiction) in order to implement the subtantive criminal law of a country. A country would not be able to decline jurisdiction merely because of foreign elements involved. Determining of *locus delictie* is also to decides which court has power to issues a decree or to decides a case (*Jus Puniendi*). Courts will have power to decide when they consider that cybercrime are usually occurred in the territory over where the jurisdiction exist, and with the lack of guidance by the statutes on this point, they will likely to use various of approaches in determining the location of the act. Jurisdiction in cybercrimes is a tricky issue because internet based activities which are inherently decentralised and ubiquitous. Above all, it is unclear just what constitutes jurisdiction: is it the place of the act, the country of residence of the perpetrator, the location of the effect, or the nationality of the owner of the computer that is under attacked? Or all of these at once?. these at once? It appears that countries think differently on this issue. Particularly with cybercrimes that are connected with many countries, the various jurisdiction clauses described in numerous countries show varying and diverging jurisdiction clauses will be clashed resulting in jurisdiction conflicts.

Beside, the use of Electronic Information and Electronic Document as a means of digital evidence in cybercrime cannot be applied directly in criminal verification because in Art 184 Section (1) KUHAP has been arranged by limited kinds of evidences. However, After Information and Electronic Transaction Act No.11 of 2008 (UU ITE) validated, there are legal certainty of electronic evidences that has been arranged in the

Art 5 of ITE. The acceptance of electronic evidence in Indonesia courts posed a considerable challenge to the prosecutor on presentment of such digital evidence for evidentiary purposes. But, in fact there are not all of electronic information and electronic document had both integrity and validity as evidentiary value in court examination. So that, this thesis focus on analyzing several constituting factor to the use of digital evidence at the Indonesian court.

This thesis is legal research and it used statute approach method, conceptual approach and comparative approach. This thesis will explain further about the implementation of the cybercrime jurisdiction principles under international substantive criminal law by analyzing the cybercrime statutes of numerous countries apply to their cybercrime laws, and analysing the implementation of Art 2 KUHP and Art 2 Information and Electronic Transaction Act that provides the jurisdiction authority of Indonesia based on territoriality and effect principles approached and also the other principles that constituting factor of locus delictie for determine jurisdiction. Besides, this thesis also analyzing further about the overall purpose of a standard in order to provides principles to develop policy, procedures, practices and documentation required for establishing the integrity and authenticity of the digital evidence as to the evidentiary requirements in a legal proceeding.

Keywords: Cyber Jurisdiction, Locus Delictie, Digital Evidence, Court Examination