Syntax Literate: Jurnal Ilmiah Indonesia p–ISSN: 2541-0849
e-ISSN: 2548-1398
Vol. 7, No. 3 Maret 2022

PENETAPAN TERSANGKA DALAM PENYIDIKAN TINDAK PIDANA TRANSNATIONAL CYBERCRIME MENURUT SISTEM HUKUM DI INDONESIA

Mustika Indah Jelita Sinaga
Universitas Kristen Indonesia, Indonesia
Email: tikasinaga@yahoo.com

Abstrak

Permasalahan dalam penelitian ini terbagi menjadi 2 (dua), yaitu (1) Bagaimana konstruksi yuridis penetapan tersangka dalam tindak pidana transnational cybercrime dalam hukum positif di Indonesia? (2) Bagaimana perbandingan penanganan tindak pidana *transnational cybercrime* di Indonesia dengan Amerika Serikat dan Inggris? Metode Penelitian: Metode penelitian ini adalah yuridis normatif. Pembahasan: Konstruksi yuridis penetapan tersangka dalam tindak pidana *transnational cybercrime* masih menggunakan KUHAP sebagai dasarnya dan didukung oleh Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik dan Peraturan Kepala Kepolisian Negara Republik Indonesia No. 14 Tahun 2012 Tentang Manajemen Penyidikan Tindak Pidana yang telah dirubah menjadi Peraturan Kepala Kepolisian Negara Republik Indonesia No 6 Tahun 2019. Hal tersebut menjadi kesulitan tersendiri oleh aparat penegak hukum, dikarenakan kasus-kasus *transnational cybercrime* selalu berhubungan dengan *Telecommunication Fraud*, sehingga ketika terjadi penangkapan, maka dilakukan prosedur lidik sesuai SOP dimana sering kali korbannya tidak berada di dalam negeri atau ada di dalam negeri tapi tidak kelihatan/tidak muncul/tidak melapor. Akibatnya sulit untuk pembuktiannya dan korbannya di luar negeri yang pada akhirnya kejahatan yang bisa ditemukan adalah pelanggaran imigrasi. Perbandingan konstruksi yuridis penetapan tersangka dalam tindak pidana transnational cybercrime di Indonesia dengan sistem hukum di negara-negara dengan teknologi informasi terdepan tidak ada yang berbeda, yaitu kepolisian dapat menetapkan tersangka apabila sudah memiliki 2 (dua) alat bukti permulaan. Namun demikian, untuk negara Amerika Serikat dan Inggris, telah memiliki pengaturan khusus terkait dengan kejahatan *cybercrime.* Hal tersebut berbeda dengan Indonesia yang masih menggunakan peraturan lama dalam menjerat pelaku tindak pidana transnasional *cybercrime.*

Kata Kunci: penetapan tersangka; pidana; *transnational cybercrime*

Abstract

The problem in this study is divided into 2 (two), namely (1) How is the juridical construction of the determination of suspects in cybercrime transnational crime in positive law in Indonesia? (2) How does the handling of transnational cybercrime in Indonesia compare with the United States and Great Britain? Research Methods: This research method is normative juridical. Discussion: Juridical

How to cite: Mustika Indah Jelita Sinaga (2022) Penetapan Tersangka dalam Penyidikan Tindak Pidana Transnational Cybercrime Menurut Sistem Hukum di Indonesia, *Syntax Literate: Jurnal Ilmiah Indonesia, 7*(3).
E-ISSN: 2548-1398
Published by: Ridwan Institute

construction of determining suspects in transnational cybercrime crimes still uses the Criminal Procedure Code as its basis and is supported by Law Number 19 of 2016 concerning Information and Electronic Transactions and Regulation of the Head of the Indonesian National Police No. 14 of 2012 concerning Management of Criminal Investigations which has been renewed with Regulation of the Head of the Indonesian National Police No. 6 of 2019 This is a particular difficulty for law enforcement officers, because transnational cybercrime cases are always related with Telecommunication Fraud, so that when an arrest is made, it is conducted a procedure according to the SOP. Often the victims are not domestic or domestic but are invisible / not appearing / not reporting. As a result, it is difficult to prove it and its victims abroad, in the end the crime that can be found is immigration violations. There is no big difference in the judicial construction of the determination of suspects in transnational cybercrime crimes in Indonesia with the legal system in countries with advanced information technology. However, for the United States and the United Kingdom, they already have special arrangements related to cybercrime crime. This is different from Indonesia, which still uses the old regulations in snaring transnational cybercrime perpetrators.

Keywords: *suspect; criminal; transnational cybercrime*

Pendahuluan

Perkembangan teknologi informasi (Information Technology) yang pesat ini telah mengubah cara hidup manusia. Manusia mempergunakan teknologi bukan hanya untuk membuat hidup mereka lebih nyaman, tetapi juga menggantungkan sebagian aktivitas hidup mereka pada teknologi. Di sisi lain, teknologi seolah berlomba dengan para pelaku kejahatan yang memanfaatkan kecanggihan teknologi itu sendiri untuk menciptakan berbagai macam tindak kejahatan.

Keadaan ini terjadi karena dalam perkembangannya teknologi informasi berhasil menghilangkan batas-batas wilayah negara dalam melakukan aktivitas perdagangan internasional. Hilangnya batas-batas wilayah negara itu berganti dengan keterhubungan antar jaringan yang satu dengan jaringan yang lain, yang mempermudah para pelaku kejahatan dalam memperluas jangkauan tindak kejahatan yang para pelaku kejahatan lakukan yang membuat para pelaku tindak pidana *cybercrime* terus semakin kreatif menciptakan modus-modus kejahatan baru.

Di sisi lain, cepatnya perkembangan teknologi di dunia juga membuat tidak meratanya standard teknologi di tiap negara, sehingga beberapa negara secara teknologi lebih kuat dari yang lain. Tentu saja ini juga menjadi *loophole/*kelemahan tersendiri dan kelemahan-kelemahan itu dimanfaatkan oleh para pelaku kejahatan baik dalam skala lokal maupun internasional. Kejahatan-kejahatan berbasis teknologi internet ini disebut *cybercrime.*

Definisi *cybercrime* secara umum dapat diartikan sebagai pelanggaran hukum yang memanfaatkan teknologi komputer berbasis penggunaan teknologi informasi. Sutarman mengatakan, *cybercrime* biasanya dilakukan oleh seseorang maupun sekelompok orang yang melakukan kejahatannya dengan menggunakan sarana komputer dan alat

komunikasi lainya, dengan cara memasuki sistem milik orang lain tanpa ijin secara illegal atau merusak data, mencuri data, dan menggunakannya juga secara ilegal (Sutarman, Widiana, & Amin, 2007).

Cybercrime disebut sebagai bentuk tindak pidana kejahatan kejahatan yang timbul karena pemanfaatan teknologi internet. Sebagai komparasi, Forester dan Morrison**,** pakar komputer asal Amerika Serikat menggambarkan bahwa kejahatan komputer merupakan suatu tindak kriminal di mana alat/senjata yang dipakai untuk melakukan tindak pidana kejahatan tersebut adalah komputer (Forester & Morrison, 1994). Sementara itu seorang pakar digital forensik lain, Eoghan Casey mengatakan bahwa *cybercrime* adalah suatu terminologi yang dipakai untuk mendeskripsikan aktivitas kejahatan yang mempergunakan komputer atau jaringan/jejaring komputer sebagai alat/senjata sasaran kejahatan tersebut atau sebagai tempat terjadinya kejahatan (Casey, 2011).

Secara umum, definisi *cybercrime* yang dapat diterima oleh hampir seluruh negara di dunia adalah *"*tindak pidana yang dilakukan dengan pemanfaatan teknologi komputer atau teknologi informasi*".* Itulah sebabnya kerap kali para ahli menyebut *cyber crime* sebagai *computer crime.* Alat dari tindak kejahatan atau media yang dipakai untuk melakukan kejahatan itu adalah komputer. Beberapa opini lain juga mengatkan bahwa *cybercrime* adalah identik dengan *computer crime.*

Cybercrime dapat juga didefinisikan sebagai:

> "*Offences that are committed against the individuals or the groups of people with criminal motives which intentionally harm the reputation of the target /the victim or cause physical or mental harm, or loss, to the target / the victim directly or indirectly, by using modern telecommunication networks such as internet networks including chatrooms, emails, notice boards and social media groups or mobile phones (Bluetooth/SMS/MMS)"* (Casey, 2011).

Terjemahan bebasnya adalah:

> "Setiap bentuk serangan atau tindakan yang ditujukan kepada perorangan atau kelompok dengan motif criminal/kejahatan yang dengan sengaja mengancam reputasi korban baik secara fisik maupun mental atau yang menyebabkan kerugian bagi korban langsung atau tidak langsung dan kejahatan itu dilakukan dengan menggunakan sistem jaringan telekomunikasi baik internet maupun *mobile telephone".*

Definisi itu kemudian diperluas oleh Departemen Kehakiman Amerika Serikat dengan mendefinisikan *computer crime* sebagai: "*Any illegal acts which is requiring knowledge of computer technology or informatioan technology/system for its perpetration, investigation, or prosecution".* Terjemahannya adalah: Setiap tindakan melawan hukum yang memerlukan pengetahuan teknologi komputer untuk melakukan kejahatannya dan memerlukan juga teknologi komputer untuk menyelidiki dan menggugatnya secara hukum.

Tindak pidana *Cybercrime* yang mempergunakan teknologi berbasis utama komputer dan jaringan telekomunikasi ini pada dasarnya berdasarkan jenis aktivitas

yang dilakukannya ini dapat digolongkan dalam beberapa macam seperti pada uraian berikut ini: (Besar, 2020)

1. *Unauthorized access* yakni; memasuki secara paksa atau menerobos kedalam suatu sistem jaringan computer diaggap melakukan kejatahatan kejahatan ini; misal *probing* dan *port;*
2. *Illegal content*; kejahatan yang dengan sengaja memasukkan informasi tentang suatu hal yang melanggar, yang tidak etis, melanggar kesusilaan atau yang buruk yang tidak benar seperti misalnya hoax atau konten pornografi yang dianggap mengganggu ketertiban umum. Contoh: Penyebaran virus secara sengaja; pada umumnya dilakukan dengan menggunakan email.
3. Data *forgery*; suatu tindak kejahatan yang dijalankan untuk memalsukan data pada dokumen-dokumen penting penting milik lembaga, institusi, perusahaan yang ada di internet. Biasanya yang penyimpanan datanya berbasis web.
4. *Cyber espionage, sabotage, and extortion*; Pelaku c*yber espionage* ini melakukan kegiatan mata-mata terhadap pihak lawan dengan cara memanfaatkan fungsi internet. Biasanya pelaku kejahatan jenis ini memasuki sistem komputer si target/korban dan menerobos tanpa ijin target/korban.
5. *Sabotage and extortion* adalah pengambilalihan atau penguasaan sebuah sistem yang dilakukan dengan sengaja dengan cara melakukan pengrusakan dan penghancuran terhadap data dan sistem, sehingga terjadi gangguan terhadap program komputer atau jaringan komputer yang terkoneksi dengan internet.
6. *Cyber stalking*; biasanya kejahatan ini dilakukan untuk megirimkan teror/*bully*/pelecehan/gangguan terhadap seseorang dengan pemanfaatan komputer; misalnya pengiriman e-mail yang dilakukan berulang-ulang. Hal itu bisa terjadi karena sangat mudah untuk membuat email tanpa harus memberikan identitas diri.
7. *Carding;* adalah jenis ejahatan yang biasanya dilakukan seseorang dengan mencuri nomor kartu kredit milik orang lain lalu dengan nomor curian itu si pelaku melakukan transaksi di internet.
8. *Hacking* dan c*racking*; adalah 2 tindak kejahatan yang berbeda. Pelakunya disebut *Hacker* dan *Cracker*; *Hacker* adalah seseorang yang memasuki sistem targetnya untuk membongkar dan mengetahui program yang dimasuki. Pelaku *Hacking* biasanya adalah seseorang yang memiliki skill baik di bidang Teknologi informasi, kadang bahkan ahli, dengan *skill* baik dan memiliki minat/hobby besar untuk mempelajari sistem komputer secara detail dalam hal meningkatkan kemampuannya.. Biasanya mereka adalah para *programmer.* Sedangkan *Cracking* dilakukan oleh seseorang yang sengaja melakukan aksi-aksi pengrusakan/penerobosan sistem secara ilegal di internet. *Cracking* dimulai dengan membajak akun seseorang, situs web, probing, atau menyebarkan virus, dengan tujuan melumpuhkan target sasaran. Tindakan yang bertujuan melumpuhkan target tersebut dikenal sebagai DoS (*Denial Of Service*). Yang disebut *Dos attack* adalah *cyber attack* atau serangan yang ditujukan pada suatu sistem computer untuk target dan membuat sistem tersebut

crashed atau *hanged* sehingga sistem menjadi lumpuh dan tidak dapat memberikan layanan.

9. *Cybersquatting and typosquatting*; biasanya kejahatan *cybersquatting* dilakukan dengan mendaftarkan nama domain perusahaan milik orang lain yang kemudian si pelaku kejahatan berusaha menjual kembali kepada perusahaan tersebut dengan harga yang lebih mahal. Sementara jenis kejahatan yang dilakukan dengan cara membuat domain yang mirip dengan nama domain milik orang lain disebut tuposquatting. *Biasanya domain tersebut merupakan nama domain saingan perusahaan.*
10. *Hijacking;* pada jenis kejahatan ini si pelaku kejahatan dengan sengaja membajak karya orang lain, biasanya disebut *software piracy* atau pembajakan terhadap perangkat lunak/software.
11. *Cyber terorism;* ini adalah jenis kejahatan yang ditujukan kepada pemerintah atau warganegara dengan cara melakukan *cracking* ke situs pemerintah atau militer untuk tujuan teror. Salah satu kasus *cyber terrorism* yang cukuo terkenal adalah kasus Ramzi Yousef yang dituduh sebagai dalang serangan ke gedung WTC. Ia ditangkap karena terbukti menyimpan detail teknis file serangan dalam bentuk enkripsi di laptopnya. Kasus terkenal lain adalah kasus Doktor Nuker yang selama kurang lebih lima tahun mengelola isi situs halaman web yang berisi propaganda-propaganda anti-Amerika, anti-Israel, dan pro-Bin Laden (*defacing*).

Kejahatan dunia maya berkembang lebih luas lagi melahirkan modus kejahatan *cybercrime* yang akhirnya bahkan jauh lebih luas dan melibatkan beberapa negara yang disebut *transnational cybercrime.*

Secara general kejahatan transnasional atau *transnational crime* adalah bentuk kejahatan yang dilakukan dengan melibatkan lebih dari satu negara. Artinya, tindak kejahatannya menyangkut warga negara dari dua atau lebih negara atau dilakukan di beberapa negara dan seringkali kejahatan ini mempergunakan prasarana dan sarana serta metoda-metoda yang melewati batas-batas teritorial suatu negara, melibatkan beberapa negara.

Berdasarkan hal tersebut, maka faktor utama yang menjadi identitas sebuah kejahatan transnasional adalah kejahatan-kejahatan tersebut sebenarnya terjadi di dalam satu batas wilayah negara tertentu, tetapi ada sebagian dari unsur kejahatan tersebut berkaitan dengan negara-negara lain, misalnya tempat kejadiannya di beberapa negara, atau warga negara si pelaku kejahatan yang berasal dari beberapa negara, sehingga muncul dua atau lebih negara yang berkepentingan /terlibat atau yang terkait dengan kejahatan itu.

Faktor "melibatkan negara lain" ini lah yang membedakan jenis tindak Pidana *transnational cybercrime* dengan kejahatan pada umumnya. Pada jenis kejahatan transnasional, sifat internasionalnya bisa meliputi aspek-aspek yang apa saja yang terkait baik pelaku individu, negara yang terlibat, benda-benda terkait, publik dan privat.

Transnational cybercrime sering diartikan sebagai kejahatan dunia maya yang melibatkan lebih dari satu negara, yang dilakukan secara terorganisir, artinya dengan persiapan, perencanaan, pengarahan atau pengendalian yang dilakukan di negara lain dan berakibat bagi pihak-pihak yang dirugikan oleh negara-negara yang terlibat dalam kejahatan itu. Karena melibatkan lebih dari satu negara maka upaya penanggulangan *cybercrime* ini sering kali dalam penanganannya menemukan masalah dalam perihal yurisdiksi.

Pangkal dari pengertian yurisdiksi adalah kompetensi hukum negara terhadap orang, benda atau peristiwa (hukum) atau kekuasaan negara. Yurisdiksi juga diartikan oleh banyak ahli sebagai suatu hak, hak atau kewenangan mutlak yang dimiliki oleh sebuah negara yang memungkinkan negara tersebut membuat peraturan-peraturan hukum, menjalankannya dan memaksakan pemberlakuannya dalam hubungannya dengan orang, benda, hal atau masalah yang berada dan atau terjadi di wilayah suatu negara. Yurisdiksi juga merupakan bentuk refleksi dari jati diri suatu negara, prinsip dasar kedaulatan negara, bentuk persamaan derajat dari bangsa suatu negara dan serta prinsip tidak campur tangan antar negara. Yurisdiksi juga merupakan bentuk kedaulatan yang sangat penting dan krusial yang dapat menciptakan, memulai atau mengubah, serta mengakhiri suatu relasi atau kewajiban hukum.

Yurisdiksi di *cyberspace* terutama pada kejahatan transnasional, berdasar dari hukum internasional. Atas dasar prinsip-prinsip yurisdiksi dalam hukum internasional lah negara-negara di seluruh dunia dianjurkan oleh badan-badan dunia untuk berpartisipasi mengambil angkah-langkah dan pandangan yang sama dalam menjawab pertanyaan mengenai yurisdiksi internet. Hal ini disebabkan karena karakter utama *cybercrime* yang bersifat *"borderless"* atau tidak mengenal batas-batas negara sehingga dalam upaya penanggulangannya tentu memerlukan bentuk-bentuk koordinasi dan kerjasama antar negara. Permasalahan *cybercrime* dan perkembangannya menunjukkan kondisi yang kompleks dan penting dan sudah sewajarnya negara-negara di dunia mengadakan kerjasama-kerjasama internasional.

Menurut perusahaan keamanan teknologi informasi internasional *Symantec*, dalam Laporan Tahunannya *Internet Security Threat Report* volume 17, pada tahun 2011, Indonesia termasuk negara yang menempati peringkat ke 10 dengan aktivitas kejahatan *cyber* tertinggi sepanjang tahun (Symantec, 2014). Ini baru penelitian tahun 2011; pada tahun ini saja angka ini menunjukkan bahwa Indonesia menyumbang 2,4% kejahatan *cyber* di dunia. Angka ini juga menggambarkan kenaikan 1,7% dibanding tahun 2010, ketika Indonesia masih menempati peringkat ke 28. Peningkatan yang sangat signifikan dan pesat ini tak lain disebabkan oleh terus meningkatnya jumlah pengguna internet di Indonesia. Pada tahun 2015, *Cybercrime* POLRI mencatat ada 800.000 akun penyebar Hoax dan 100.000 akun penyebar *"hate speech"* di Media Sosial (medsos). Riset yang dilakukan oleh jejaring sosial Facebook dan Twitter pada tahun 2016 menunjukkan bahwa Indonesia sudah masuk dalam 4 besar pengguna jejaring sosial terbanyak di dunia. Pada Tahun 2018, POLRI mengumumkan bahwa angka *cybercrime* di Indonesia adalah Nomor 2 tertinggi di Indonesia setelah Jepang. Angka kejahatan yang disebut

sebagai Nomor dua di dunia itu menyangkut lebih dari 90.000.000 kasus (Kominfo.go.id, 2018).

Kejahatan dunia maya atau *cybercrime* terus berkembang dengan cepat dan pesat sejalan dengan pesatnya perkembangan teknologi informasi itu sendiri. Kejahatan-kejahatan itu memiliki berbagai bentuk dari mulai yang paling sederhana seperti melakukan perusakan atas suatu *website* (*hacking dan cracking*), pencurian uang, *(carding*), pornografi, pemerasan, pelanggaran hak cipta, pencurian dan pembajakan data dan sebagainya. Setiap bentuk perkembangan kecanggihan teknologi informasi selalu diikuti dengan modus-modus kejahatan baru yang juga sama canggihnya.

Masalah cybercrime adalah masalah yang rumit dan tidak mudah untuk diselesaikan. Faktor utama kerumitannya adalah karena cybercrime merupakan suatu jenis kejahatan yang tidak mengenal batas wilayah hukum sehingga kejahatan tersebut dapat terjadi tanpa memerlukan interaksi langsung antara pelaku dengan korbannya. Tempat kejadian perkaranya tidak mudah untuk ditentukan. Tindakan melakukan kejahatannyapun dapat dilakukan dari belahan bumi manapun, dan korbannya juga dapat berada dimana saja.

Untuk mengantisipasi kejahatan-kejahatan *cyber*, negara-negara dengan teknologi terdepan seperti Amerika Serikat dan Inggris melakukan pengaturan yang ketat terhadap aktivitas di *cyberspace* terlebih ketika fakta-fakta di lapangan menunjukkan kegiatan *cybercrime* semakin hari semakin *sophisticated*. Upaya-upaya antisipasi ini kemudian melahirkan apa yang disebut sebagai *cyber law* atau undang undang yang mengatur segala aktivitas *cyber*.

Hukum Internasional adalah instrumen hukum yang menjadi acuan Permasalahan *cybercrime* yang saat ini banyak menjadi pemikiran dunia. Rujukan negara-negara di dunia dalam hal instrument hukum internasional itu adalah konvensi tentang kejahatan dunia *cyber* (yang disebut *Convention on Cyber Crime*) 2001. Konvensi ini digagas oleh negara-negara Europa Union/Uni Eropa, sebuah rganisasi regional eropa yang menjadi penggasnya. Dalam perkembangannya konvensi ini kemudian menjadi dasar dari pemikiran penanganan masalah *cybercrime* dan bahkan banyak negara yang memiliki komitmen dalam mencegah dan menanggulangi kejahatan *cyber*, meratifikasi dan mengaksesnya. Negara-negara yang tergabung dalam Uni Eropa (*Council of Europe*) ini, pada tanggal 23 November 2001 menyelenggarakan *Convention on Cybercrime* di kota Budhapest ini.

Antisipasi *Cyber crime* adalah *Cyber law*, yang pada dasarnya merupakan bentuk hukum yang ruang lingkupnya meliputi semua aspek yang berhubungan dengan subjek hukum yang memanfaatkan dunia cyber dalam melakukan kegiatan apa saja baik dalam hubungannya sebagai pribadi maupun tidak.

Pengaturan atas tindakan-tindakan yang berhubungan dengan aktivitas *cyber* itu dimulai setiap kali seseorang (atau subjek hukum) memasuki dunia *cyber* dan *"on line".* Dengan meningkatnya berbagai modus tindak pidana *cybercrime* kemudian lahirlah Undang-undang Informasi dan Tranksaksi Elektronik No. Tahun 2008 yang berisi 13 Bab dan 53 pasal yang disempurnakan dengan Undang-Undang Nomor 19 Tahun 2016

tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Masalah *transnational cybercrime* adalah masalah yang sudah yang menjadi perhatian serius bagi negeri ini, terlebih dengan masuknya Indonesia dalam perdagangan global yang artinya seluruh aspek kehidupan di Indonesia, baik itu sosial, bisnis, ekonomi akan mendapatkan dampak yang signifikan dari kegiatan di dunia *cyber* ini. Publik sudah mulai terbiasa mendengar adanya kasus-kasus kejahatan yang berhubungan dengan dunia *cyber* seperti pencurian uang *(carding*), pencurian akun jejaring sosial, penyerangan /penyebaran dengan ciptaan-ciptaan virus atau pembobolan dan perusakan *website (hacking & cracking)*, bahkan penyebaran ideologi-ideologi jahat yang merusak kerukunan masyarakat.

Pada masa-masa awal munculnya berbagai kasus yang berkaitan dengan *transnational cybercrime* di Indonesia, pihak aparat tentu saja mengalami kesulitan untuk melakukan penyelidikan dan penyidikan serta menjerat pelaku *cybercrime*. Sebagai negara yang baru saja memasuki dunia *cyber,* pengaturan yang jelas atas tindakan-tindakan yang berhubungan dengan kejahatan dunia maya tentu saja menjadi kendala yang serius, bukan saja karena kurangnya ahli-ahli komputer yang dapat membantu aparat dalam mengungkapkan sebuah kejahatan yang berbasis teknologi informasi, atau kurangnya aparat yang mememiliki pengetahuan teknologi yang mendalam, akan tetapi juga karena pada waktu itu belum ada peraturan khusus yang mengaturnya. Pada masa masa awal tersebut, tindakan-tindakan kejahatan di dunia *cyber* tidak dilihat sebagai kejahatan yang serius karena beberapa faktor yang dilihat oleh Penulis sebagai berikut:

1. Pada waktu itu (sebelum lahirnya Undang-undang ITE) sistem pembuktian di Indonesia hanya berpegang pada Pasal 184 Kitab Undang-undang Hukum Acara Pidana, yang belum mengenal istilah bukti elektronik (*digital evidence*) sebagai bukti yang sah berdasarkan undang-undang, sehingga kerap kali ketika sebuah kejahatan terjadi, namun tidak dapat diproses sampai ke meja hijau karena dianggap tidak cukup bukti, meskipun sebenarnya ada bukti elektronik.
2. Ketiadaan peraturan yang jelas yang mengatur dunia *cyber* di Indonesia, pada waktu itu, baik itu yang mengatur mengenai masalah kewajiban-kewajiban, jaminan keamanan, jaminan kerahasiaan maupun perlindungan hukum dalam melakukan transaksi perdagangan di dunia *cyber.*

   Sistem pembuktian hukum acara pidana di Indonesia yaitu *stelsel wettelijk* menekankan bahwa hanya alat-alat bukti yang sah menurut undang-undang yang dapat dipergunakan untuk memenuhi pembuktian. Pengertiannya adalah, selain dari ketentuan yang dimaksud tersebut, tidak bisa dipergunakan sebagai alat bukti yang sah.

   Lahirnya *Cyber Law* Indonesia lewat Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (untuk selanjutnya disebut Undang-Undang ITE) yang disahkan pada tanggal 21 April 2008 menjadi penerangan bagi permasalahan *cyber* di negeri ini. UU ITE memang tidak sempurna, tetapi sedikit

banyak menjawab tantangan kejahatan di dunia maya, akan tetapi bukan berarti masalah-masalah *cybercrime* di Indonesia sudah dapat diatasi dan ditangani dengan baik atau dengan *correct*. Undang-Undang ITE ini tentu sangat jauh dari kata sempurna. Masalah-masalah menjadi kendala dalam penyelesaian kasus-kasus-kasus *cybercrime* di Indonesia juga sama dihadapi banyak negara di seluruh dunia, yaitu pengaturan yang sama di semua negara mengenai masalah penentuan tempat kejadian perkara yaitu *Locus* dan *Tempus Delictie* dalam Penetapan Tersangka.

Undang-undang ITE telah mengakui alat bukti Digital atau bukti elektronik sebagai alat bukti yang sah di hadapan pengadilan dalam tatanan sistem hukum di Indonesia,. Kehadiran UU ITE ini pada dasarnya memperluas ketentuan Pasal 184 KUHAP mengenai alat-alat bukti yang sah dan diakui oleh Pengadilan. Untuk menentukan alat bukti yang sah dari suatu kejahatan dunia *cyber* diperlukan ahli *digital forensic* (Abdul Aziz, 2005) yang akan bekerja berdasarkan suatu *standard operating procedure* ((SOP), 2018) (SOP) tertentu.

Penentuan alat bukti yang sah dari suatu tindak pidana *cyber* ini akan berdampak pada penentuan mengenai tempat dan waktu kejadian perkara atau *locus delictie* dan *tempus delictie* yang penentuannya dalam banyak hal memiliki perbedaan antara *cybercrime* dengan kejahatan konvensional. Penentuan *locus & tempus delicti* tersebut dalam penetapan tersangka kasus-kasus *transnational cybercrime*, merupakan bagian dari konstruksi penetapan Tersangka dan penanganan kasus transnational cybercrime. Namun demikian, tidak adanya pengaturan khusus atau panduan dalam penindakan para tersangka kasus transnational cybercrime, membuat penanganan kasus-kasus Transnational Cybercrime sering kali tidak maksimal. Hal tersebut juga pernah terjadi pada beberapa kasus kejahatan penipuan dan pemerasan lintas negara yang dilakukan oleh segerombolan warga negara asing namun melaksanakan operasinya di Indonesia dan korbannya di Indonesia dan berbagai belahan bumi. Banyak dari kasus-kasus itu, maka terlihat bahwa penanganan terhadap para pelaku cybercrime transnasional hanya di proses secara administrasi keimigrasian, yaitu deportasi. Hal tersebut dikarenakan tidak adanya pengaturan yang jelas dalam penindakan tindak pidana transnational cybercrime di Indonesia. Polisi masih kesulitan menangani kasus-kasus tersebut dengan tuntas.

Atas dasar penjelasan di atas, maka Penulis akan mengkaji suatu penelitian yang berjudul Penetapan Tersangka Dalam Penyidikan Tindak Pidana *Transnational Cybercrime* Menurut Sistem Hukum Di Indonesia.

Metode Penelitian

1. Tipe Penelitian

Penelitian tesis ini bersifat yuridis normative. Penyusunan penelitian ini dibuat dengan memberikan pemahaman terhadap permasalahan dengan meneliti bahan sekunder atau bahan-bahan Pustaka. Penelitian ini juga memberikan analisis terhadap masalah norma yang dialami oleh hukum dogmatif dan kegiatan mendeskriptifkan norma hukum itu dirumuskan dengan norma hukum (membentuk peraturan

perundangan). Penelitian yuridis normatif ini juga dihubungkan dengan fakta-fakta yang secara nyata terjadi dalam pelaksanaan peraturan perundang-undangan serta asas-asas hukum dan teori-teori hukum dan praktek di dalam penetapan tersangka dalam tindak pidana *transnational cybercrime.*

2. Objek Penelitian

a) Pengaturan penetapan tersangka secara umum dalam hukum positif

b) Pengaturan penetapan tersangka *cybercrime* dan *transnational cybercrime*

3. Jenis Data

Jenis data yang akan Penulis gunakan dalam penelitian ini diperoleh dari Kitab Undang-undang Hukum Pidana (KUHP), Kitab Undang-undang Hukum Acara Pidana (KUHAP), Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE), juga Ketentuan *Convention On Cybercrime 2001* yang terkait dengan Hukum Positif Indonesia. Data-data sekunder yang menjadi bahan rujukan peulisan ini diperoleh Penulis dari bahan-bahan kepustakaan berupa dokumen-dokumen hukum, buku-buku, jurnal-jurnal, makalah, berita berita online dan lain-lain. Secara khusus Penulis melakukan wawancara dengan KANIT IV, Subdit III DittipidSiber, Bareskrim MABES POLRI untuk mengetahui langsung bagaimana penetapan Tersangka ini terjadi pada prakteknya di lapangan, dan kendala apa saja yang dihadapi. Demikian pula mengenai data Tertier akan penulis peroleh dari berbagai dictionary termasuk dictionary hukum juga kamus-kamus, ensiklopedia, dan berbagai data yang berfungsi sebagai pendukung data primer dan data sekunder.

4. Spesifikasi Penelitian

Penulis memilih penelitian deskriptif sebagai spesifikasi penelitian ini. Penelitian ini secara khusus menelaah inti dari permasalahan dalam penelitian ini dengan menggambarkan peraturan perundang-undangan yang berlaku dan dikaitkan dengan teori-teori hukum dalam praktek pelaksanaannya dan dengan demikian akan teruraikan/tergambarkan lah fakta-fakta yang secara nyata terjadi dalam penetapan tersangka *transnational cybercrime.*

5. Fokus Studi

Fokus studi dalam penelitian ini adalah terkait dengan hukum pidana, secara khusus membahas masalah Penetapan Tersangka pada kasus-kasus *transnational cybercrime* yang bertujuan agar kasus-kasus *transnational cybercrime* dapat ditangani dengan tuntas.

6. Metode Pendekatan

Penulis secara spesifik akan menggunakan metode analisis data kualitatif untuk menjawab dan memecahkan permasalahan yang ditelaah dalam penelitian ini,. Metode pendekatan yang digunakan Penulis dalam penelitian ini menggunakan pendekatan undang-undang (*statute approach*), yang artinya penulis akan meneliti dan menelaah semua undang-undang dan regulasi yang terkait dengan isi permasalahan hukum yang sedang ditangani sehingga dapat ditarik kesimpulan yang dapat dipertanggungjawabkan;

7. Teknik Pendekatan

Teknik pendekatan yang digunakan dalam penelitian ini adalah dengan statute approach atau biasa disebut sebagai pendekatan undang-undang. Pendekatannya menggunakan data sekunder. Pada data sekunder, yaitu data yang diperoleh langsung melalui penelusuran kepustakaan atau dari dokumen resmi termasuk juga wawancara dengan instansi yang sudah menangani penetapan tersangka yaitu Kanit IV, Subdit III Dittipidsiber Bareskrim MABES POLRI. Hal ini penting dilakukan, tujuannya agar Penulis memilah-milah data yang ada dan kemudian menganalisisnya berdasarkan pada peraturan/ketentuan perundang-undangan.

8. Metode Pengolahan

Sebagai upaya untuk dapat menjawab atau memecahkan masalah dalam penelitian ini, Penulis akan menggunakan metode analisis data kualitatif, karena data yang diperoleh bersifat kualitas bukan kuantitas. Setelah pengumpulan data maka selanjutnya akan dilakukan pengolahan data dan analisis secara kualitatif, sehingga dapat ditarik kesimpulan yang dapat dipertanggungjawabkan.

9. Teknik Penyajian Data

Data yang telah diuraikan tersebut kemudian akan disajikan secara deskriptif dengan metode deduktif sehingga dapat diperoleh kejelasan penyelesaian apatyang dari sana dapat ditarik kesimpulan atas hal-hal yang bersifat umum menuju ke hal yang lebih khusus.

Hasil dan Pembahasan

1. Tentang Perkembangan Regulasi *International Cybercrime*

Salah satu instrumen hukum internasional publik yang mengatur masalah *cybercrime* yang paling banyak mendapatkan perhatian negara-negara di dunia dan sampai sekarang menjadi referensi pembentukan hukum di banyak negara adalah konvensi tentang kejahatan *cyber* (*Convention on Cyber Crime*) 2001 yang digagas oleh Uni Eropa. Pada awalnya Konvensi ini dibuat oleh sebuah organisasi regional eropa, tetapi dalam perkembangannya akhirnya konvensi ini dapat diratifikasi dan diakses oleh berbagai negara di seluruh dunia yang memiliki komitmen dalam upaya mengatasi kejahatan *cyber* yang saat ini semakin berkembang dan menjadi kejahatan lintas Negara yang disebut *transnational cybercrime* . Negara-negara yang tergabung dalam Uni Eropa (*Council of Europe*) pada tanggal 23 November 2001 di kota Budapest, Hongaria adalah pihak penggagas yang bersepakat dalam *Convention on Cybercrime* ini dan kemudian melanjutkan konvensi ini dalam tahap lanjut dengan memasukkannya dalam *European Treaty Series* dengan Nomor 185. European Treaty adalah bentuk ikatan kesepakatan diantara negara-negara Uni Eropah. Konvensi ini akan berlaku secara efektif setelah diratifikasi oleh minimal 5 (lima) negara yang didalamnya termasuk ratifikasi yang dilakukan oleh 3 (tiga) negara anggota *Council of Europe*.

Oleh karena banyak Negara yang mengikuti dan meratifikasi konvensi tersebut, maka isi konvensi itu kemudian menjadi model bagi pengaturan hukum

cybercrime di berbagai Negara. Oleh karenanya menjadi penting bagi Negara kita untuk merujuk konvensi ini sebagai salah satu pembanding bagi pengaturan *cybercrime* di Indonesia.

Substansi konvensi mencakup area yang cukup luas dan melahirkan ketentuan-ketentuan dan kebijakan kebijakan yang berhubungan dengan *cybercrime* (*criminal policy*) yang bertujuan untuk melindungi masyarakat dari *cybercrime*, baik melalui Undang-Undang maupun kerjasama-kerjasama internasional. Hal ini dilakukan untuk mencapai keamanan bersama sehubungan dengan semakin meningkatnya intensitas digitalisasi, konvergensi, dan globalisasi yang berkelanjutan dari teknologi informasi yang juga memberikan dampak negatif yaitu meningkatnya tindak pidana *cybercrime* bahkan *transnational cybercrime.*

Sejauh ini ada 30 negara menandatangani konvensi yang menggalang hukum internasional untuk memerangi kejahatan di dunia maya, namun hanya delapan yang menerapkan peraturan tersebut dalam undang-undang nasionalnya. Menurut laporan Dewan Uni Eropa, pada saat konvensi itu dibicarakan, diperkirakan terdapat sekitar 600 juta pengguna internet pada tahun 2002, artinya dua kali lebih banyak dibanding tahun 1999. Sementara itu riset mencatat sebanyak 4,66 miliar orang di seluruh dunia telah menggunakan internet hingga Januari 2021. Angka ini naik 316 juta atau 7,3 persen sejak Januari 2020.

Kejahatan di internet diperkirakan mengakibatkan kerugian sekitar 150 miliar hingga 200 miliar Euro (180 miliar Dolar AS) pada tahun 2003. Riset terakhir menyebutkan, kerugian tahunan dari *cybercrime* secara global telah mencapai US$ 600 miliar atau setara Rp 8.160 triliun (asumsi US$1 = Rp 13.600) pada tahun 2017, yang didorong meningkatnya kecanggihan para *hacker* (peretas) dan bertambah banyaknya kejahatan di toko online dan mata uang digital *Cryptocurrency* (Crytocurrency, 2020).

Sebelum *Convention on Cybercrime* tahun 2001, untuk mengatasi bahaya hacking dan cracking yang merupakan kejahatan *cybercrime* ini, sebenarnya Kongres PBB juga sudah dua kali membahas masalah *cybercrime* ini yaitu pada Kongres VIII Tahun 1990 di Havana dan pada Kongres X Tahun 2000 di Wina.

Berbagai Forum Internasional dan masyarakat internasional membahas permasalahan *cybercrime* dan perkembangannya dari waktu ke waktu dan melahirkan sejumlah regulasi internasional untuk menjawab tantangan atas kejahatan *cybercrime yang* semakin meningkat. Regulasi Internasional dalam masalah *cybercrime* yang menjadi acuan banyak negara di dunia antara lain adalah:

1) United Nations (UN)

Perserikatan Bangsa-Bangsa (PBB) terus menerus melakukan pengawasan terhadap perkembangan computer related crime, yang dimulai pada tahun 1990 dengan *Eighth UN Congress on the Prevention of Crime and Treatment of Offender, Havana, Cuba 27 August – 7 September 1990* Dalam Resolusi Kongres PBB tersebut, negara-negara dihimbau untuk lebih giat

mengintensifkan usaha-usaha untuk memerangi *computer related crime* dengan melakukan tindakan-tindakan sebagai berikut: (Suseno, 2012)

a) Modernisasi hukum pidana materil dan hukum acara pidana nasional termasuk upaya-upaya untuk (1) menjamin adanya penerapan hukum dalam hal tindak pidana dan investigasi kewarganegaraan serta pembuktian yang fair dan memadai dalam proses peradilan, dan jika diperlukan segera melakukan perubahan yang diperlukan. (2) Apabila tidak/belum ada pengaturan, maka yang dapat dilakukan adalah membuat aturan tentang tindak pidana serta prosedur investigasi dan pembuktian, untuk mengatasi aktivitas kriminal yang baru dan canggih ini. (3) Memperhatikan/menetapkan kewenangan untuk menyita atau mengembalikan aset-aset hasil *computer related crime*.
b) Mengadopsi usaha-usaha penegakkan hukum agar masyarakat, aparat pengadilan dan penegak hukum alert terhadap masalah *computer-related crimes* dan pentingnya mencegah tindak pidana kejahatan tersebut.
c) Meningkatkan langkah-langkah upaya pengamanan komputer melalui upaya-upaya pencegahan/preventif, dengan memperhitungkan masalah-masalah terkait seperti perlindungan privasi, penghormatan terhadap hak asasi manusia dan kebebasan-kebebasan fundamental serta setiap mekanisme pengaturan penggunanan/pemanfaatan komputer.
d) Mengadopsi pelatihan-pelatihan yang memadai untuk Para Penegak Hukum pejabat dan aparat yang bertanggungjawab atas pencegahan, penyidikan, penuntutan dan pengadilan mengenai tindak pidana ekonomi dan *computer-related crimes* seperti Polisi, Jaksa dan Hakim.
e) Melakukan kolaborasi dengan organisasi-organisasi yang berhubungan (*rules of etics*) dalam penggunaan komputer dengan dunia pendidikan dan menjadikannya sebagai bagian dari kurikulum dan training informatika.
f) Menjalankan kebijakan-kebijakan untuk korban *computer-related crimes* yang sesuai dengan *United Nations Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power*, termasuk restitusi/pengembalian aset yang diperoleh dari kejahatan.

Pada tahun 2000 Persatuan Bangsa-bangsa menyelenggarakan *The Tenth UN Congress on The Prevention on Crime and the Treatment of Offender di Vienna* dengan tema khusus yaitu *Crime and Justice, meeting the challenges of the 21st century* (Nations, 2000) yang menghasilkan beberapa kesimpulan yaitu :

a) *Computer related crime should be criminalized* (Semua jenis kejahatan yang terkait dengan komputer harus dolriminalisasi/diproses secara pidana).
b) Adequate procedural laws were needed for the investigation and prosecution of cyber criminal (Hukum Acara Pidana yang cukup dan memadai diperlukan untuk melakukan penyidikan dan penuntutan terhadap para pelaku tindak pidana cybercrime).
c) *Goverment and industry should work together towards the common goal of preventing and combating computer crime so as to make the internet*

a secure place (Kerjasama antara pemerintah dan industri harus dilakukan demi mencapai tujuan bersama pencegahan dan pemberantasan kejahatan komputer agar internet menjadi tempat/domain yang aman.

d) *Improved international cooperation was needed in order to trace criminals on the internet* (perlu dilakukan peningkatan kerjasama erat international untuk tujuan melacak pelaku perbuatan *cybercrime*).

e) *The united Nations should take the further action with regard to the provision of technical cooperation and assistance concerning crime related to computer networks.* (PBB harus mengambil langkah-langkah ke depan yang berhubungan dengan bantuan kerjasama teknis mengenai penanggulangan hal-hal yang berhubungan dengan kejahatan computer).

PBB juga melakukan upaya untuk membuat Negar-ngara di dunia melakukan upaya pencegahan dan pemberantasan *transnational cybercrime* dengan menyelenggarakan *A United Nation Symposium on The Challenge of Berderless Cybercrime*, yang berkaitan dengan penandatanganan Palermo Convention Against Transnational Organized Crime, pada bulan Desember 2000 (UNCATOC) (Broadhurst & Grabosky, 2005). Palermo Convention 2000 dikenal sebagai Konvensi yang berisi ketentuan yang mengatur kerjasama Internasional, cukup luas yang mencakup banyak manifestasi dari *high-tech crime* yang paling umum.

Dalam dokumen *United Nations Convention Against Transnational Organized Crime* pasal 3 ayat 2, suatu kejahatan dapat dikategorikan sebagai kejahatan transnasional apabila :

a) *It is commited in more than one state*; (jika dilakukan di lebih dari satu negara)

b) *It is commited in one state but a substansial part of its preparation, planning, direction or control takes place in another state*; (Jika dilakukan di satu Negara akan tetapi persiapan, perencanaan, pengarahan atau pengendaliannya terjadi di Negara lain)

c) *It is commited in one state but involves an organized criminal group that engages in criminal activities in more than one state*; (jika dilakukan di satu Negara tetapi ada keterlibatan kelompok kriminal yang terorganisir yang terlibat dalam kegiatan kriminal di lebih dari satu Negara.

d) *It is commited in one state but has substansial effects in another state*; (jika dilakukan di satu Negara namun kerugiannya berdampak di negara lain).

2) The Group of Eight (G8)

Kelompok G8 yang terdiri dari negara-negara Indutri yitu Jerman, Kanada, Perancis, Italy, Jepang, Inggris, Rusia dan Amerika Serikat dalam Meeting of Justice and Interior Ministers of The Eight yang terselenggara pada tanggal 9-10 desember 1997 membahas dua hal penting yaitu meningkatkan kemampuan untuk melakukan penyidikan dan penuntutan tindak pidana teknologi tinggi (high tech crime) dan memperkuat regim hukum Internasional

untuk melakukan ekstradisi dan bantuan timbal balik dan menjamin bahwa tidak ada pelaku tindak pidana yang memperoleh tempat aman di dunia ini. Menurut G8 ada 2 bentuk ancaman terhadap keamanan umum yaitu (Www.justice.gov, 2020):

a) *Sophisticated criminals targeting computer and telecommunications system to obtain or alter valuable information without authority and may attempt to disrupt critical commercial and public systems*. (Para pelaku kejahatan tingkat tinggi yang menjadikan komputer dan sistem telekomunikasi sebagai target untuk membobol dan memperoleh informasi berharga tanpa izin otoritas dan mencoba untuk mengganggu sistem- sistem perdagangan penting dan sistem- sistem yang berhubungan dengan publik).
b) *Criminal, including members of organized crime groups and terorists, are using these new technologies to facilitate traditional offenses*. (Para pelaku kejahatan, kelompok penjahat terorganisir dan para teroris, menggunakan system teknologi baru untuk memfasilitasi para pelaku kejahatan tradisional).

3) Council of Europe (COE

Council of Europe adalah organisasi supranasional yang berada di Eropa yang dibentuk pada tahun 1985 oleh komite ahli Europe committee onc crime problems untuk mempertimbangkan berbagai masalah hukum yang ditimbulkan oleh kejahatan computer / computer related crime. Salah satu laporan yang dihasilkan pada September 1989 tersebut ialah bentuk bentuk kejahatan cybercrime yang harus diatur dalam hukum nasional tiap negara.

Pada April 1997 Komite ini menyusun instrumen Internasional yang komprehensif tentang tindak pidana *cybercrime* yaitu *Convention on Cybercrime* dan selesai pada tahun 2001. Komite inilah yang melaksanakan tugas tersebut selama 4 tahun dengan melalui 27 draft Konvensi sebelum sampai Final Draft *Convention on Cybercrime* sampai diterima oleh European Committee on Crime Problems dalam rapat pleno Juni 2001 dan lahirlah *Convention on Cybercrime* yang ditandatangani pada 23 November 2001 di Budapest, Hongaria.

2. Perbandingan Penegakkan Hukum dan Penanganan Tindak Pidana *Transnasional Cybercrime* di Indonesia Dengan Sistem Hukum di Amerika Serikat dan Inggris

Convension on *Cybercrim*e memberikan indikasi bahwa dunia harus memerangi kejahatan penyalahgunaan TI (Teknologi Informasi) atas maraknya kejahatan internasional yang sangat serius, gawat dan harus segera ditangani. Penyalahgunaan TI telah menjadi salah satu agenda dan kejahatan di tingkat global yang bersamaan dengan perkembangan globalisasi. Kejahatan di tingkat global ini menjadi ujian berat bagi setiap negara untuk memeranginya. Tentunya alat yang digunakan oleh negara untuk memerangi *cybercrime* ini adalah hukum yang difungsikan; salah satunya adalah untuk mencegah terjadinya dan menyebarnya *cybercrime*, serta

melakukan penindakan jika *cybercrime* terbukti telah menyerang atau merugikan masyarakat dan negara.

Faktanya, ketersediaan Teknologi Informasi tentu tidak dengan sendirinya muncul begitu saja ke permukaan, melainkan sudah barang tentu menyangkut banyak pihak yaitu pihak penyedia jasa internet yang disebut ISP (*Internet Service Provider*) termasuk di dalamnya penyedia jaringan akses (*connection provider*), penyedia *content* (*Information provider*) dan penyedia *search engine* yang lazim disebut portal serta pihak yang lain disebut sebagai pemilik informasi.

Dalam penetapan tersangka tindak pidana *transnational cybercrime* di Indonesia, aparat penegak hukum harus memiliki alat bukti permulaan yang cukup sebagaimana diatur dalam Pasal 17 KUHAP. Selain dari pada itu, Pasal 183 KUHAP menyatakan Hakim tidak boleh menjatuhkan pidana kepada seseorang kecuali apabila dengan sekurang-kurangnya dua alat bukti yang sah ia memperoleh keyakinan bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukannya.

Di samping itu dalam Pasal 6 ayat (2) UU No. 14 Tahun 1970 tentang Ketentuan-ketentuan Pokok Kekuasaan Kehakiman juga menyatakan senada bahwa tiada seorang jua pun dapat dijatuhi pidana, kecuali apabila pengadilan karena alat-alat bukti yang sah menurut undang-undang, mendapat keyakinan, bahwa seseorang yang dapat dianggap bertanggungjawab, telah bersalah atas perbuatan yang dituduhkan atas dirinya.

Berdasarkan ketentuan dalam pasal tersebut, pembuktian dalam perkara pidana ada dua syarat yang harus dipenuhi, yaitu adanya keyakinan hakim dan keyakinan tersebut harus didasarkan pada alat bukti yang telah ditentukan oleh undang-undang, dalam hal ini KUHP. Selanjutnya berkaitan dengan kejahatan *cybercrime* semuanya serba maya.

Dalam kejahatan ini biasanya pelaku melakukan aksinya seorang diri ataupun kelompok dalam ruangan pribadi yang bersifat *privacy*. *Privacy* bagi mereka merupakan hal yang tak dapat disangkal. Perbuatan tersebut membutuhkan ketenangan dan kreativitas yang tinggi dalam menggunakan komputer. Disamping itu juga semua piranti yang digunakan dalam kejahatan.

Amerika Serikat dan Inggris, punya undang-undang untuk memerangi kejahatan dunia maya dan memiliki strategi nasional dalam menangani kejahatan *cybercrime*. Amerika Serikat sudah lebih dulu mengakui dokumen elektronik yang dihasilkan dalam praktek bisnis. Sejak awal Januari 2001, divisi tindak pidana computer dan HAKI Departemen Kehakiman AS telah melahirkan kebijakan-kebijakan khusus yang berkaitan dengan pengakuan dokumen elektronik sebagai alat bukti yang sah di pengadilan.

Dalam *FBI's Cybercrime Report 2017,* Kepolisian Amerika Serikat menumumkan hasil riset mereka yang mengenai 20 negara tertinggi yang menjadi korban *cybercrime* selain Amerika Serikat. Negara Bagian di Amerika Serikat yang paling rentan dalam kejahatan di dunia maya ini adalah California, New York, dan

Florida; sementara Negara Kanada menduduki puncak tertinggi dalam daftar korban asing dari kejahatan *cybercrime*. Negara-negara India, Inggris, Australia, dan Prancis juga menduduki posisi 5 besar. 4 Kejahatan Internet yang paling banyak dilakukan memiliki kasus non-pembayaran / non-pengiriman di tempat pertama, dengan lebih dari 81.000 insiden yang dilaporkan terjadi dimana orang tidak dibayar untuk layanan mereka atau tidak menerima produk yang mereka pesan (Morgan, 2017).

Sementara Indonesia punya UU ITE, Amerika Serikat memiliki Peraturan tentang pelanggaran-pelanggaran *cybercrime* dalam berbagai undang-undang yaitu: *Acces Device Fruade Act of 1984, Computer Fraud and Abuse Act of 1986, Transportation of Obsence Matters for Sale or Distribution, National Infrastructure Protection Act of 1996, Communication Decency Act of 1996, the Cyberspace Electronic Security Act of 1999," dan the "Patriot Act of 2001.*

Ditinjau dari sisi praktikal penegakan hukum, investigasi-investigasi dilakukan oleh FBI dilakukan dengan bekerjasama dengan berbagai instansi di setiap negara bagian di Amerika Serikat seperti *Homeland Security*. FBI bekerjasama dengan *of the Internet Crime Complaint Center* (IC3). Dalam laman resmi FBI disebutkan :

> *"The mission of the Internet Crime Complaint Center (IC3) is to provide the public with a reliable and convenient reporting mechanism to submit information to the FBI concerning suspected Internet-facilitated fraud schemes and to develop effective alliances with law enforcement and industry partners. Information is analyzed and disseminated for investigative and intelligence purposes to law enforcement and for public awareness*."
>
> Terjemahan bebasnya adalah: "Misi dari *the Internet Crime Complaint Center* (IC3) adalah menyediakan mekanisme sistem pelaporan yang handal dan nyaman kepada publik untuk menyampaikan informasi kepada FBI mengenai dugaan skema penipuan yang difasilitasi Internet dan untuk mengembangkan aliansi yang efektif dengan para penegak hukum dan mitra industri. Informasi dianalisis dan disebarluaskan untuk tujuan investigasi dan intelijen untuk penegakan hukum dan untuk kesadaran masyarakat."

Amerika Serikat juga memiliki *Cyber Action Team*, suatu bentuk *Task Force* yang bertugas untuk untuk memberikan respon yang cepat terhadap gangguan komputer dan keadaan darurat di ruang virtual. Mereka adalah agen khusus atau ilmuwan komputer, dan semuanya memiliki pelatihan lanjutan dalam bahasa komputer, penyelidikan forensik, dan analisis perangkat lunak.

Tim lain yang juga disiapkan adalah *National Cyber Forensics and Training Alliance* organisasi ini dibentuk pada tahun 1997 dan berbasis di Pittsburgh. *National Cyber Forensics and Training Alliance* telah menjadi model internasional untuk menyatukan penegak hukum, industri swasta, dan akademisi untuk membangun dan berbagi sumber daya, informasi strategis, dan mengancam intelijen untuk mengidentifikasi dan menghentikan ancaman *cyber* yang muncul dan mengurangi ancaman yang ada.

Hal yang sama juga terdapat pada negara Inggris, dimana Parlemen Inggris telah mengeluarkan *Data Protection Act of 1984 and the Computer Misuse Act of 1990.* Dalam melakukan penanggulangan terhadap *cybercrime Secretary of State for the Home Department* telah mengeluarkan kebijakan berupa:

1) *Coordinate activity across Government to tackle crime and address security on the internet in line with the strategic objectives laid out in the UK Cyber Security Strategy*. (Koordinasi aktivitas lintas Pemerintah untuk menghadapi kejahatan dan keamanan internet dengan tujuan strategis mengamankan dunia cyber di seluruh Inggris Raya).
2) *Reduce the direct harms by making the internet a hostile environment for financial criminals and child sexual predators, and ensuring that they are unable to operate effectively through work to disrupt crime and prosecute offenders.* (Mengurangi/menghalangi bahaya serangan langsung terhadap system dengan cara membuat lingkungan yang tidak ramah/keras terhadap para pelaku kejahatan finansial dan para pelaku kejahatan sexual terhadap anak sehigga membuat mereka tidak dapat mengiperasikan kegiatan kejahatan mereka melalui system internet);
3) *Raise public confidence in the safety and security of the internet, not only through tackling crime and abuse, but through the provision of accurate and easy-to-understand information to the public on the threats.* (Meningkatkan kepercayaan publik dalam hal keamanan dan kenyamanan internet, tidak hanya dengan menghadang kejahatan internet tapi juga melalui edukasi-edukasi yang akurat dalam menyampaian informasi-informasi yang berhubungan dengan kejahatan *cyber*).
4) *Support industry leadership to tackle cyber crime, and work with industry to consider how products and online services can be made safer and security products easy to use.* (memberi dukungan penuh kepada pelaku industri yang berhubungan dengan jasa dan produk-produk online yang membangun untuk menjawab/menangani kejahatan *cyber*);
5) *Work with international partners to tackle the problem collectively***.** (Meningkatkan kerjasama-kerjasama internasional dengan lembaga-lembaga internasional dan negara-negara di dunia dalam hal penangkalan kejahatan *cyber*).

Kebijakan tersebut mengkoordinasikan kegiatan di seluruh Pemerintah untuk mengatasi kejahatan dan mengatasi keamanan di internet sesuai dengan tujuan strategis yang ditetapkan dalam *UK Cyber Security Strategy*. Mengurangi kerugian langsung dengan membuat internet menjadi lingkungan yang tidak bersahabat bagi penjahat keuangan dan predator seksual anak, dan memastikan bahwa mereka tidak dapat beroperasi secara efektif melalui pekerjaan untuk mengganggu kejahatan dan melakukan penuntutan terhadap pelaku. Meningkatkan kepercayaan publik akan keamanan dan keamanan internet, tidak hanya melalui penanganan kejahatan dan penyalahgunaan, namun melalui penyediaan informasi yang akurat dan mudah dipahami kepada publik mengenai ancaman tersebut. Mendukung kepemimpinan

industri untuk mengatasi kejahatan di dunia maya, dan bekerja sama dengan industri untuk mempertimbangkan bagaimana produk dan layanan online dapat dibuat lebih aman dan produk keamanan mudah digunakan dan bekerjalah dengan mitra internasional untuk mengatasi masalah secara kolektif.

Apakah undang-undang ITE memenuhi kebutuhan negeri ini dalam menyelesaikan masalah-masalah *cybercrime* khususnya *transnational cybercrime*? Di Amerika Serikat misalnya, selain undang-undang, setiap terjadi perkembangan kejahatan yang membahayakan keamanan negara, pemerintah federal atau setiap pemerintah negara bagian langsung mengeluarkan dokumen yang berlaku sebagai ketentuan setara dengan undang-undang, yang disebut *cyber security document* yang dibuat sebagai bentuk proteksi keamanan sistem informasi misalnya:

1. The National Strategy to secure Cyberspace, yang dikeluarkan pada bulan Febuari 2003.
2. *International Strategy for Cyberspace*, dikeluarkan pada bulan Mei 2011.
3. *Departement of Defense Strategy for Operating in Cyberspace*, dikeluarkan pada bulan Juli 2011

Berikut adalah beberapa perbandingan undang-undang yang ada di Indonesia dengan Amerika Serikat dan Inggris;

Tabel 1
Perbandingan Jumlah Peraturan Penunjang Pencegahan dan Penegakkan Hukum Kejahatan Transnational Cybercrime

Indonesia	Amerika Serikat	Inggris
KUHP	Cyberlaw: Electronic Transaction Act (UETA) (Undang-undang Transaksi Electronik	Data Protection Act of 1984 (Undang-undang Data Proteksi)
UU ITE	National Cyber Forensics and Training Alliance (Regulasi Nasional siber Forensik)	The Computer Misuse Act of 1990 (Undang-undang penyalahgunaan Komputer)
	Acces Device Fruade Act of 1984 (Undang-undang penyalahgunaan perangkat elektronik)	Theft Act, 1990 (Undang-undang Pencurian Elektronik)
	Computer Fraud and Abuse Act of 1986 (Undang-Undang Penipuan dan Penyalahgunaan Komputer tahun)	
	Transportation of Obsence Matters for Sale or Distribution (Regulasi Transportasi barang distribusi)	
	Communication Decency Act of 1996 (Undang-	

	undang Kepatutan Komunikasi)
	National Infrastructure Protection Act of 1996 (Undang-Undang Perlindungan Infrastruktur Nasional)
	the Cyberspace Electronic Security Act of 1999 Undang-undang Elektronik dunia maya)
	The "Patriot Act of 2001 (Undang-undang Patriot 2001)

Amerika Serikat juga memberikan prioritas tinggi dalam masalah keamanan dunia maya mereka dengan mengeluarkan dokumen *"International Strategy for Cyberspace"* pada tahun 2011, yang disebut juga sebagai bagian dari politik luar negeri Amerika Serikat. Strategi ini merupakan strategi pertama yang dikeluarkan AS yang menghubungkan dan mengikat AS dengan seluruh dunia dalam isu cyber yang sangat luas. Strategi ini juga merupakan panduan AS dalam menghadapi semua tantangan keamanan teknologi informasi dalam dunia cyber. Oleh karena itu pada April 2015, Departemen Pertahanan AS mengeluarkan "*The Departement Of Defense (DoD) Cyber Strategy"* untuk menjawab pada wilayah apa dan bagaimana Lembaga pertahanan AS tersebut harus meraih tujuan-tujuan serta prioritas yang tertuang dalam *International Strategy for Cyberspace* 2011.

Kesadaran untuk mengembangkan keamanan cyber dan mempersiapkan strategi dalam menghadapi ancaman dan tantangan dunia digital sudah sejak lama disadari oleh AS. Namun intensitas pengembangan cyberpower sangat terlihat dalam kebijakan-kebijakan pemerintah AS kurang lebih dalam 10 tahun terakhir. Berikut beberapa kebijakan keamanan cyber yang dirilis oleh pemerintah AS dalam 10 tahun terakhir.

Kebijakan-kebijakan Smerika Serikat yang memproritaskan masalah kemanan dunia maya (Cyber security) ini ditunjukkan dalam berbakai kebijakan khusu yang mengatur masalah keamanan cyber selama 7 tahun terakhir sebagaimana table berikut ini.

Tabel 2
Dokumen Kebijakan *Cyber Security* Amerika Serikat

Tahun	Nama Dokumen	Lembaga Penerbit
2003	The National Strategyto Secure Cyberspace	Gedung Putih
2009	Cyberspace policy Review	Gedung Putih
2011	International Strategy for Cyberspace	Gedung Putih
2011	Department of Defense Strategy for Operating Cyberspace	Departemen Pertahanan Amerika Serikat
2015	The Department of Defense Cyber Strategy	Departemen Pertahanan Amerika Serikat
2016	Department of State International Cyberspace Policy Strategy	Departemen Luar Negeri Amerika Serikat

Penulis berpendapat, apabila berpijak pada hasil wawancara Penulis dengan AKBP Endo Priambodo selaku Kanit IV Subdit III DitTipidsiber Bareskrim Polri, MABES POLRI, maka baik Amerika Serikat, Inggris dan Indonesia telah memiliki pengaturan hukum yang lebih dari cukup untuk penegakan hukum *cybercrime*, khususnya dalam bentuk formulasi undang-undang. Namun demikian, khusus untuk Negara Indonesia, oleh karena peraturan perundang-undangan yang digunakan adalah berupa KUHAP yang didukung oleh Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik dan Peraturan Kepala Kepolisian Negara Republik Indonesia No. 14 Tahun 2012 Tentang Manajemen Penyidikan Tindak Pidana, maka perlu dibentuk pengaturan khusus setingkat undang-undang terkait dengan *transnasional cybercrime* di Indonesia.

Hal tersebut sesuai dengan Resolusi Kongres PBB VIII/1990 mengenai "*computer-related crime*" mengajukan beberapa kebijakan antara lain sebagai berikut:

1. Dalam rangka upaya menanggulangi *cyber crime* itu, Resolusi Kongres PBB VIII/1990 mengenai *"Computer-related crimes"* mengajukan beberapa kebijakan antara lain sebagai berikut:
   a) Menghimbau negara anggota untuk mengintensifkan upaya-upaya penanggulangan penyalahgunaan komputer yang lebih efektif dengan mempertimbangkan langkah-langkah sebagai berikut:
   b) Melakukan modernisasi hukum pidana material dan hukum acara pidana.
   c) Mengembangkan tindakan-tindakan pencegahan dan pengamanan komputer.
   d) Melakukan langkah-langkah untuk memberikan rasa sensitif warga masyarakat, aparat pengadilan dan penegak hukum, terhadap pentingnya pencegahan kejahatan yang berhubungan dengan komputer (untuk selanjutnya dalam kutipan ini disingkat dengan inisial "*cyber crime*)

e) Melakukan secara intensif upaya-upaya pelatihan (*training*) bagi para hakim, pejabat dan aparat penegak hukum mengenai kejahatan ekonomi dan "*Cyber Crime.*
f) Memperluas "*rules of ethics*" dalam penggunaan komputer dan mengajarkannya melalui kurikulum informasi.
g) Mengambil langkah-langkah pengembangan kebijakan-kebijakan yang berhubungan dengan perlindungan saksi dan korban "*cyber crime* sesuai dengan deklarasi PBB mengenai korban dan mengambil langkah-langkah untuk mendorong melaporkan adanya "*cyber crime* ".

2. Menanjurkan negara-negara anggota untuk meningkatkan kegiatan-kegiatan nasional dalam rangka mencegah dan menanggulangi "*cyber crime* ".
3. Merekomendasikan kepada komite pengendalian dan pencegahan kejahatan (*Commitee on Crime Prevention and Control*) PBB untuk:
   a) Menyebarluaskan pedoman dan standar untuk membantu negara anggota menghadapi "*cyber crime*" di tingkat nasional, regional dan internasional.
   b) Mengembangkan penelitian dan analisis lebih lanjut guna menemukan cara-cara baru menghadapi permasalahan *Cyber crime* " di masa yang akan datang.
   c) Selalu melakukan pembahasan dengan semua pihak mengenai "*cybercrime*" Ketika meninjau mengimplementasikan perjanjian ekstradisi dan bantuan kerja sama di bidang pencegahan dan penanggulangan kejahatan (Barda Nawawi Arief, 2018).

Berdasarkan hal tersebut, maka menurut Penulis, diperlukan pembentukan peraturan perundang-undangan terkait dengan teknologi informasi, seperti mengatur delik melawan hukum menggunakan nama domain atau pengaturan masalah security mengingat kejahatan *cybercrime* merupakan *global crime*, maka perlu adanya suatu pengaturan dan asas-asas yang memungkinkan menarik pelaku yang berada di luar Indonesia yang merugikan Indonesia.

Kesimpulan

Berdasarkan pembahasan di atas, maka kesimpulan dalam penelitian ini adalah: 1) Penanganan penetapan tersangka dalam tindak pidana *transnational cybercrime* di Indonesia masih menggunakan Kitab Undang-undang Hukum Acara Pidana (KUHAP) sebagai dasar implementasi penanganan kasus-kasus *transnational cybercrime* dan didukung oleh Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik dan Peraturan Kepala Kepolisian Negara Republik Indonesia No. 14 Tahun 2012 Tentang Manajemen Penyidikan Tindak Pidana yang telah diperbaharui dengan Peraturan Kepala Kepolisian Negara Republik Indonesia No. 16 Tahun 2019. Hal tersebut menjadi kesulitan tersendiri bagi aparat penegak hukum dalam penanganan kasus-kasus *transnational cybercrime* dikarenakan kasus-kasus *transnational cybercrime* sebagian besar adalah *Telecommunication Fraud* yang melibatkan beberapa negara sehingga ketika terjadi penangkapan dilakukan prosedur lidik sesuai SOP, namun sering kali korbannya tidak berada di dalam negeri atau ada di dalam negeri tapi

tidak kelihatan / tidak muncul / tidak melapor. Akibatnya sulit dilakukan pembuktiannya atau pembuktian memerlukan waktu dan terkendala teknis, karena korbannya di luar negeri sehingga jejak kejahatan bukan saja lenyap tapi korban tidak dapat dihadirkan sehingga pada akhirnya kejahatan yang bisa ditemukan adalah pelanggaran imigrasi. 2) Sama seperti di Indonesia dalam penanganan tindak pidana *transnasional cybercrime* di negara-negara dengan teknologi terdepan seperti Amerika Serikat dan Inggris, kepolisian setiap negara bagian dapat melakukan penetapan tersangka apabila sudah memiliki 2 (dua) alat bukti permulaan. Perbedaannya adalah Amerika Serikat dan Inggris, telah memiliki berbagai peraturan-peraturan khusus dalam bentuk undang-undang maupun kebijakan-kebijakan yang spesifik yang misalnya berhubungan dengan *cybercrime security* saja, atau *network system* saja atau pengaturan IP dan domain saja dll. Amerika dan Inggris juga memiliki *Team Squad*, *Task Force* khusus serta SOP yang mendetail secara khusus, terkait dengan kejahatan *transnational cybercrime.* Hal tersebut berbeda dengan Indonesia yang masih menggunakan KUHAP konvensional dan UU ITE dalam menjerat pelaku tindak pidana *transnational cybercrime.*

BIBLIOGRAFI

(SOP), Standard Operational Procedure. (2018). adalah penetapan tertulis mengenai apa yang harus dilakukan, kapan, dimana, dan oleh siapa. SOP dibuat untuk menghindari terjadinya variasi dalam proses pelaksanaan kegiatan yang akan mengganggu kinerja organisasi secara keseluruhan. SOP merupakan mekanis. Retrieved from www.library.binus.ac.id. Google Scholar

Abdul Aziz, Faris. (2005). Digital Forensic. *Digital Forensic*. Google Scholar

Barda Nawawi Arief, S. H. (2018). *Masalah penegakan hukum dan kebijakan hukum pidana dalam penanggulangan kejahatan*. Prenada Media. Google Scholar

Besar. (2020). Kejahatan dengan menggunakan Sarana Teknologi Informasi. Retrieved from https://business-law.binus.ac.id/2016/07/31/kejahatan-dengan-menggunakan-sarana-teknologi-informasi. Google Scholar

Broadhurst, Rod, & Grabosky, Peter. (2005). *Cyber-crime: The challenge in Asia* (Vol. 1). Hong Kong University Press. Google Scholar

Casey, Eoghan. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet*. Academic press. Google Scholar

Crytocurrency. (2020). Crytocurrency adalah Mata uang digital bersifat virtual yang disimpan dalam bentuk data binary dan dijamin oleh Criptography. Retrieved from https://www.investopedia.com website: https://www.investopedia.com. Google Scholar

Forester, Tom, & Morrison, Perry. (1994). *Computer ethics: Cautionary tales and ethical dilemmas in computing*. Mit Press. Google Scholar

Kominfo.go.id. (2018). Polri: Indonesia Tertinggi Kedua Kejahatan Siber di Dunia. Google Scholar

Morgan, Steve. (2017). *Cybercrime report, 2017*. Google Scholar

Nations, United. (2000). Tenth United Nations Congress on The Prevention of Crime and the Treatment Offenders. Google Scholar

Suseno, Sigid. (2012). *Yurisdiksi Tindak Pidana Siber*. Refika Aditama. Google Scholar

Sutarman, H., Widiana, I. Gde, & Amin, Ihsan. (2007). *Cyber crime: modus operandi dan penanggulangannya*. LaksBang Pressindo. Google Scholar

Symantec. (2014). Internet Security Threat Report. Retrieved from symantec.com website: http://www.symantec.com/threatreport/ Google Scholar

Www.justice.gov. (2020). Bentuk Ancaman Terhadap Keamanan Umum yang Lebih Besar Dari yang Pernah ada. Retrieved from https://www.justice.gov/criminal/cybercrime/g82004/97Communique.pdf. Google Scholar