BAB IV

HASIL PENELITIAN dan PEMBAHASAN

A. Mekanisme Penentuan Tempat dan Waktu Kejadian Oleh Penyidik Dalam Kejahatan Dunia Maya (*Cyber Crime)*

1. Mekanisme Penentuan Tempat Kejadian Perkara (*Locus Delicti*) Dalam Kejahatan Dunia Maya (*Cyber Crime)*

Penentuan tempat kejadian perkara (*locus delicti*) dalam tindak pidana *cyber crime* sangat sulit dengan banyak faktor yang mepengaruhi mulai dari faktor internal hingga faktor eksternal dan jelas ini adalah menjadi hambatan oleh para penyidik tindak pidana *cyber crime* khususnya, yaitu dikarenakan aspek global yang menimbulkan kondisi seolah-olah dunia tidak ada batasnya (*borderless*) yang mana semua orang dapat melakukan intraksi dan transaksi tanpa batas waku dan tempat melalui internet, keadaan ini dapat mengakibatkan pelaku, korban serta tempat dilakukannya tindak pidana (*locus delicti*) terjadi di wilayah yang berbeda-beda.

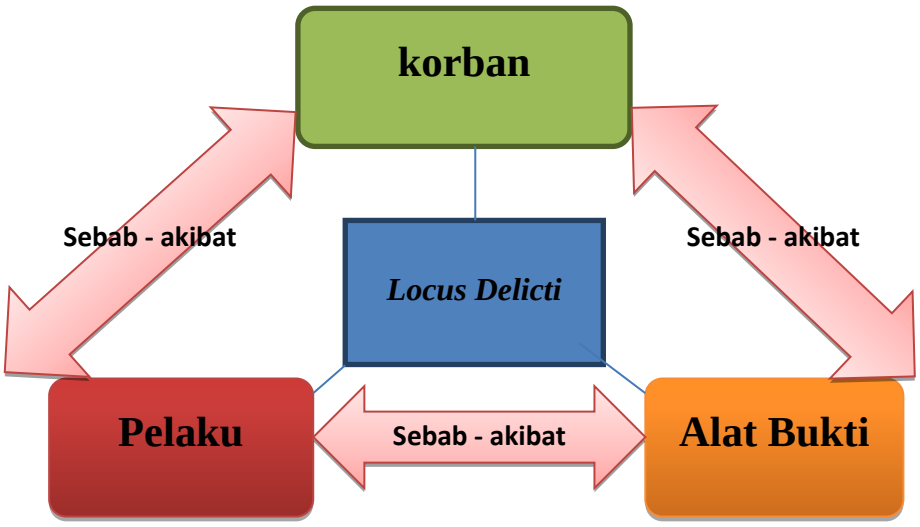
Penentuan *locus delicti* secara umum yang digunakan oleh ilmu hukum pidana saat ini apakah masih relevan bila diterapkan dalam penentuan *locus delicti cyber crime* mengingat sifat *cyber crime* yang lintas batas wilayah dan negara. Adanya instrument hukum untuk memberantas *cyber crime* ini dilakukan sebagai salah satu usaha dalam pembaharuan hukum pidana nasional, dimana sesuai dengan teori sosiologi hukum, bahwa perubahan

sosial mengakibatkan perubahan hukum, karena hukum selalu tertinggal dari perkembangan teknologi sehingga dengan adanya pembaharuan hukum pidana nasional diharapkan hukum dapat mengakomodasi perkembangan teknologi informasi atau setidaknya menjamin adanya kepastian hukum dalam pemanfaatan teknologi informasi, khususnya internet. Penentuan *locus delicti cyber crime* pada dasarnya tetap memakai teori-teori pidana yang telah ada yaitu sebagai berikut teori perbuatan materil, yaitu tempat tindak pidana ditantukan oleh pembuat jasmaniah yang dilakukan oleh si pembuat dalam mewujudkan tindak pidana, teori instrument (alat), yaitu dalam teori ini tempat terjadinya delik ialah tempat bekerjanya alat yang dipakai si pembuat, dan teori akibat, yaitu teori ini ukurannya adalah menikuti pada tempat terjadinya akibat tersebut terjadi.[1]

Berikut gambar alur penentuan tempat kejadian perkara :

Gambar 4.1

Alur Penentuan Tempat kejadian perkara



[1] Wawancara dengan AKP. Safpe Tambatua Sinaga (Penyidik) Unit *Cyber Crime* POLDA DIY, pada tanggal , 27 juni 2019 pukul 08.29 Wib.

(*sumber: Unit Cyber Crime DITRESKRIMSUS POLDA DIY*)

Berdasarkan gambar tersebut diatas mengenai dalam alur penentuan tempat kejadian perkara dalam tindak pidana *cyber crime* yang mana antara pelaku, korban, dan alat bukti saling kesinambungan dalam penentuan tempat kejadian perkara dalam suatu tindak pidana *cyber crime*, dalam hal ini sebenarnya sama saja dengan tindak pidana pada umumnya hanya saja yang membedakan yaitu alat yang digunakan atau instrument dalam tindak pidana *cyber crime* yakni serba teknologi informasi yang digunakan dalam melakukan kejahatan oleh pelaku tindak pidana *cyber crime*.

Mekanisme dalam penentuan tempat kejadian perkara (*locus delicti)* dalam tindak pidana *cyber crime* kepolisian RI khususnya di Unit *Cyber Crime* DITRESKRIMSUS POLDA DIY, yang mana sebagai tempat penulis melakukan penelitian, sesusai wawancara yang penulis telah lakukan dengan penyidik *cyber crime* yaitu bapak AKP. Safpe Tambatua Sinaga, S.kom, yang mana pada prakteknya dalam menentukan tempat kejadian perkara tindak pidana *cyber crime* yaitu dengan beberapa teori-teori yang relevan dengan tindak pidana pada umumnya yakni menggunakan teori perbuatan,bekerjanya alat dan akibat, hanya saja disesuaikan dengan prakteknya pada raung lingkup *cyber crime* yakni sebagai berikut:

a. Tempat Terjadinya Perbuatan Tersebut Dilakukan (*Theory of The Uploader*)

Pada teori ini penyidik dapat menentukan tempat kejadian perkara (*locus delicti*) dengan berdasarkan tempat dimana terjadinya atau dilakukannya pengiriman (di-*upload)* melalui media elekronik yang mana dalam bentuk suatu konten atau perbuatan yang mengakibatkan kerugian pada pihak-pihak tertentu sehingga menjadi tindak pidana *cyber crime* atas tindakan pelaku tersebut. Pada prakteknya teori ini cukup sering digunakan oleh para penyidik *cyber crime* yang tentunya berdasarkan kebutuhan dan untuk mempermudah proses penegakan hukum, misalnya berkaitan dalam hal alat bukti dan saksi-saksi yang berada pada suatu tempat/wilayah hukum yang sama dengan pelaku tindak pidana *cyber crime* tersebut, maka pada prakteknya jika menggunakan teori ini yang menangani kasus mulai dari penyelidikan, penyidikan, penuntutan, hingga proses persidangan dilakukan oleh lembaga kepolisian, kejaksaan dan lembaga peradilan yang bertanggung jawab atas wilayah hukum tersebut yang mana sesuai dengan tempat pelaku melakukan aksi nya dalam melakukan tindak pidana *cyber crime.*

b. Tempat Dimana Dampak Kejahatan Tersebut Terjadi (*Theory of The Downloader*)

Pada teori ini penyidik dapat menentukan tempat kejadian perkara (*locus delicti*) dengan berdasarkan tempat dimana dampak kejahatan tersebut terjadi atau tempat dimana korban melakukan *downloading* (mengunggah) atau melihat postingan/ konten yang merugikan korban atas tindak pidana *cyber crime* tersebut. Pada

prakteknya teori ini sangat sering digunakan oleh para penyidik *cyber crime* dalam menentukan *locus delicti* yang tentunya berdasarkan kebutuhan dan untuk mempermudah proses penegakan hukum, dalam teori ini biasanya berawal dari korban yang melaporkan kepada kepolisian dengan bukti-bukti elektronik (digital) atau juga sudah berbentuk *hard file* dan kepolisian melakukan penyelidikan dan menentukan tempat kejadian perkaranya sesuai dengan tempat korban/ pelapor yang merasa dirugikan, maka pada prakteknya jika menggunakan teori ini yang menangani kasus mulai dari penyelidikan, penyidikan, penuntutan, hingga proses persidangan dilakukan oleh lembaga kepolisian, kejaksaan dan lembaga peradilan yang bertanggung jawab atas wilayah hukum tersebut yang mana sesuai dengan tempat korban/ pelapor yang merasa dirugikan terhadap konten atau perbuatan yang dilakukan oleh pelaku melalui media elektronik yang mana hal tersebut merupakan tindak pidana *cyber crime*.

c. Alat Yang Dipergunakan dan Alamat *Server* Dalam Melakukan Kejahatan

Pada teori ini penyidik dapat menentukan tempat kejadian perkara (*locus delicti*) dengan berdasarkan dimana alat yang dipergunakan atau dioprasikan oleh pelaku dan atau penyidik melakukan pelacakan berdasarakan *IP address* atau di mana alamat *server* secara fisik berlokasi tempat mereka dicatat atau disimpan sebagai data elektronik dalam melakukan tindak pidana *cyber crime* tersebut tentunya

dengan menggunakan peralatan-peralatan khusus yang dimiliki oleh kepolisian. Pada prakteknya teori ini cukup sering juga digunakan oleh para penyidik *cyber crime* yang tentunya berdasarkan kebutuhan dan untuk mempermudah proses penegakan hukum, jadi jika penyidik menggunakan teori ini yang menangani kasus mulai dari penyelidikan, penyidikan, penuntutan, hingga proses persidangan dilakukan oleh lembaga kepolisian, kejaksaan dan lembaga peradilan yang bertanggung jawab atas wilayah hukum tersebut yang mana sesuai dengan tempat pelaku melakukan aksi nya dalam melakukan tindak pidana *cyber crime* tersebut karena penyidik menentukan tempat kejadian berasarkan diamana alat yang dipergunakan untuk melakukan aksinya dan juga berdasarkan alamat *server* atau alamat *internet protocol* yang digunakan oleh pelaku tindak pidana *cyber crime* tersebut yang mengakibatkan kerugian kepada pihak lain.

Berdasarkan beberapa teori diatas yang digunakan dalam menentukan tempat kejadian perkara (*locus delicti*) yang paling sering digunakan oleh para penyidik yaitu teori tempat dimana dampak kejahatan tersebut terjadi (*theory of the downloader*) yang mana sesuai dengan tempat korban/pelapor hal ini dikarenakan dapat dikatakan sebagian besar jenis-jenis tindak pinda *cyber crime* ini adalah delik aduan, yang mana korban yang merasa dirugikan membuat laporan ke kepolisian di daerah terdekat dengan alamat korban, maka lembaga kepolisian melakukan koordinasi dengan pihak kepolisian yang

berwilayah hukum sama dengan terduga pelaku, dan dilanjutkan proses hukum mulai dari penyelidikan hingga proses persidangan oleh lembaga kepolisian, kejaksaan, hingga peradilan di tempat atau wilayah hukum yang sama dengan korban/pelapor.

Persoalan tentang tempat terjadinya tindak pidana (*locus delicti*) tidak hanya penting dalam perspektif hukum pidana formil, akan tetapi juga dalam perspektif hukum pidana pada umumnya. Secara umum kepastian mengenai tempat terjadinya tindak pidana (*locus delicti*) penting pula terhadap beberapa hal berikut ini:

1) Berkaitan dengan kompetensi relatif dari pengadilan, yaitu menentukan pengadilan negara mana yang berwenang mengadili tindak pidana yang terjadi di suatu tempat tertentu. Kepastian tempat tindak pidana (*locus delicti*) penting dan perlu diperhitungkan berhubung setiap pengadilan memiliki wilayah yuridiksi yang berbeda satu dengan yang lainnya. Pengadilan hanya dapat menangani atau mengadili kasus yang hanya berada dalam jangkauan wilayah administratif kabupaten / kotamadya, pengadilan dapat menangani perkara-perkara yang diajukan. Dengan demikian, dengan diketahuinya tempat terjadinya tindak pidana (*locus delicti*) maka, diketahui pula pengadilan mana yang berwenang mengadili terhadap tindak pidana yang terjadi yang berada di wilayah administratifnya (kewenangan relatif).

2) Berkaitan dengan ruang lingkup berlakunya aturan pidana Indonesia sebagaimana yang telah diatur dalam Pasal 2 sampai dengan Pasal 9 KUHP. Dalam ketentuan Pasal 2 KUHP menyatakan, “Bahwa aturan pidana Indonesia berlaku bagi setiap orang (warga Negara Indonesia ataupun WNA) yang melakukan perbuatan pidana di Indonesia”. Sehingga dengan diketahuinya tempat terjadi tindakan pidana (*locus delicti*) misalkan terjadi diluar negeri maka aturan pidana tidak berlaku bagi setiap orang kecuali yang diatur dalam Undang – Undang. Misalnya hanya berlaku bagi warga Negara Indonesia yang melakukan tindakan tertentu saja, sebagaimana yang telah diatur dalam Pasal 5 ayat (1) ke -2 KUHP yang menyatakan: Aturan pidana dalam perundang- undangan Indonesia berlaku bagi warga negara Indonesia yang diluar indonesia melakukan : Ke -2 salah satu perbuatan yang oleh suatu aturan pidana dalam perundang–undangan Indonesia dipandang sebagai kejahatan sedangkan menurut undang-undang negara negara dimana perbuatan dilakukan, diancam pidana.
3) Berkaitan dengan pengecualian seperti yang dimaksudkan dalam Pasal 9 KUHP. Berdasarkan ketentuan Pasal 9 KUHP telah ditentukan bahwasanya ketentuan Pasal 2-5, 7 dan 8 berlakunya dibatasi oleh pengecualian yang telah diakui dalam hukum international. Dengan adanya pembatasan ketentuan Pasal 9

KUHP tersebut dapat diartikan apabila dalam wilayah teritorial terjadi tindak pidana internasional, maka asas territorial sebagaimana yang ditentukan dalam Pasal 2 KUHP tidak berlaku mutlak. Sebab meskipun tindak pidana yang terjadi berada di wilayah territorial Indonesia tidak diadili berdasarkan peraturan pidana Indonesia melainkan peraturan negara lain, hal ini disebabkan karena menurut peraturan pidana internasional setiap negara memiliki kewenangan yang sama terhadap tindak pidana international yang terjadi dimanapun *locus delicti* dari kejahatan internasional tersebut.

4) Berkaitan dengan adanya syarat, bahwa sebuah tindakan dapat dikatakan perbuatan pidana apabila dilakukan ditempat umum, misalnya suatu tindakan pidana yang menodai nilai - nilai kesusilaan di tempat umum seperti yang telah diatur dalam Pasal 281 KUHP, hal yang berkaitan dengan syarat ini dikatakan suatu perbuatan tindak pidana apabila tidak sesuai tempatnya pelaksanaannya, seperti yang dicontohkan diatas apabila dilakukan dalam tempat tertutup hal itu bukan merupakan tindak pidana namun jika dilakukan ditempat umum meskipun dilakukan oleh pasangan resmi secara hukum, tetap perbuatan tersebut dianggap perbuatan tindak pidana karena dianggap menciderai nilai kesusilaan.
5) Salah satu syarat mutlak sahnya surat dakwaan.

Menentukan *locus delicti* atau tempat kejadian perkara suatu tindakan *cyber crime,* sesuai wawancara penulis dengan penyidik di DITRESKRIMSUS *Cyber Crime* POLDA DIY metode yang diterapkan oleh penyidik khususnya di wilayah hukum POLDA DIY dan Indonesia adalah seperti yang sudah penulis paparkan, namun sebagai perbandingan dengan negara lain dalam hal ini penulis memilih untuk membandingkan dengan negara Amerika Serikat dalam hal penentuan tempat kejadian perkara khususnya pada tindak pidana *cyber crime,* yaitu Amerika Serikat mempunyai teori tersendiri dalam penentuan *locus delicti* dalam perkara *cyber crime* yang diungkapkan oleh AKP.Safpe Tambatua Sinaga, yaitu sebagai berikut:[2]

1) *Theory of The Uploader and The Downloader*, teori ini menekankan bahwa dalam dunia *cyber* terdapat 2 (dua) hal utama yaitu *uploader* (pihak yang memberikan informasi ke dalam *cyber space*) dan *downloader* (pihak yang mengakses informasi), dan pada teori ini relevan dengan teori perbuatan dan teori akibat yang mana juga digunakan untuk menentukan tempat kejadian pada tindak pidana konvensional.
2) *Theory of Law of The Server*, dalam pendekatan ini, penyidik memperlakukan *server* di mana halaman web secara fisik berlokasi tempat mereka dicatat atau disimpan sebagai data elektronik, dan pada teori ini relevan dengan teori perbuatan dan

[2] Wawancara dengan AKP. Safpe Tambatua Sinaga (Penyidik) Unit *cyber crime* POLDA DIY, pada tanggal , 27 juni 2019 pukul 08.29 Wib

teori bekerjanya alat yang mana juga digunakan untuk menentukan tempat kejadian pada tindak pidana konvensional.

3) *Theory of International Space*, menurut teori ini, *cyber space* dianggap sebagai suatu lingkungan hukum yang terpisah dengan hukum konvensional dimana setiap negara memiliki kedaulatan yang sama, yang mana pada teori ini berkaitan dengan asas teritorial, nasionalitas aktif dan pasif yang mana berdasarkan pasal 2-8 KUHP, yang mana untuk menentukan tempat kejadian melihat dari asas-asas tersebut yang mana pada teori ini digunakan untuk tindak pidana *cyber crime* transnasional.

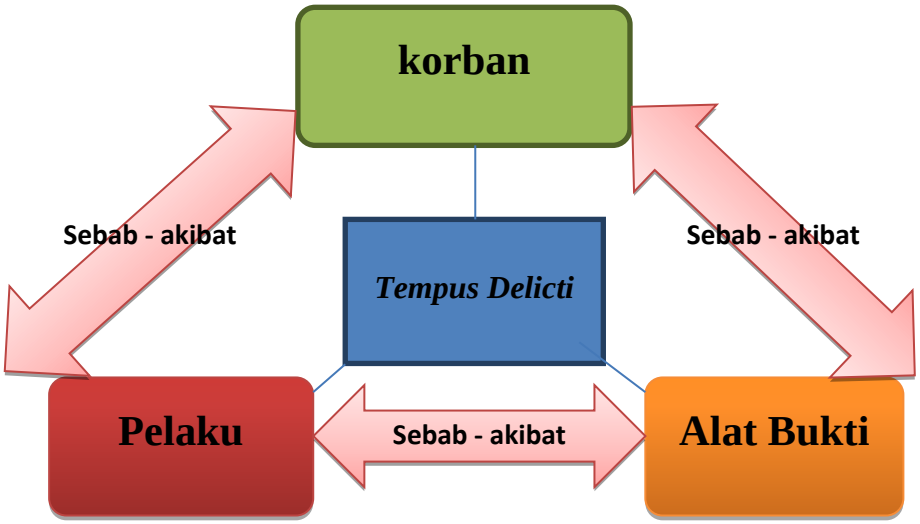
2. Mekanisme Penentuan Waktu Kejadian Perkara (*Tempus Delicti*) Dalam Kejahatan Dunia Maya (*Cyber Crime)*

Penentuan waktu kejadian perkara (*tempus delicti*) dalam tindak pidana *cyber crime* sebenarnya sama seperti penentuan *locus delicti* yang sudah penulis paparkan dan jika dibandingkan dengan kejahatan biasa pada umumnya tidak jauh berbeda yang mana hal yang membedakan dalam kejahatan *cyber crime* adalah media yang digunakan, media yang digunakan dalam melakukan kejahatan tersebut adalah media elektronik seperti laptop, komputer, ponsel *android*, dan lain sebagainya yang mana masih banyak lagi media elektronik yang canggih pada saat ini, maka dari itu *cyber crime* digolongkan menjadi kejahatan khusus.

Berikut gambar alur penentuan tempat dan waktu kejadian perkara:

Gambar 4.2

Alur Penentuan Waktu kejadian perkara



(*sumber: Unit Cyber Crime DITRESKRIMSUS POLDA DIY*)

Berdasarkan gambar tersebut diatas mengenai dalam alur penentuan waktu kejadian perkara dalam tindak pidana *cyber crime* yang mana antara pelaku, korban, dan alat bukti saling kesinambungan dalam penentuan waktu kejadian perkara dalam suatu tindak pidana *cyber crime*, dalam hal ini sebenarnya sama saja dengan tindak pidana pada umumnya hanya saja yang membedakan yaitu alat yang digunakan atau instrument dalam tindak pidana *cyber crime* yakni serba teknologi informasi yang digunakan dalam melakukan kejahatan oleh pelaku tindak pidana *cyber crime*.

Mekanisme dalam penentuan waktu kejadian perkara ini juga menggunakan beberpa teori atau metode yang digunkan oleh penyidik *cyber crime* di DITRESKRIMSUS POLDA DIY, yang mana penyidik dalam hal ini berpatokan pada pasal 8 dalam Undang-Undang ITE yang

secara garis besar berisikan penjelasan mengenai waktu pengiriman dan waku penerimaan pada praktek yang dilakukan dalam ruang lingkup teknologi informasi yang mana dalam menentukan waktu kejadian pada tindak pidana *cyber crime* dapat merujuk pada Pasal 8 ayat (4) huruf a dan b dan, dalam hal ini juga relevan dengan teori pada tindak pidana konvensional yakni teori perbuatan dan teori akibat dan pada ruang ringkup *cyber crime* menjadi teori pengiriman dan penerimaan yang mana sesuai dengan Pasal 8 ayat (4) huruf a dan b Undang- Undang ITE yaitu:[3]

a. **Waktu Pengiriman (Waktu Mengakses/Mengunggah Sebuah Konten ke Media Elektronik)**

   Pada metode/teori ini penyidik dapat menentukan waktu kejadian perkara (t*empus delicti*) ketika Informasi Elektronik dan/atau dokumen elektronik memasuki sistem informasi pertama yang berada di luar kendali Pengirim (pelaku), jadi dalam teori ini yang pertama kali diselidiki oleh penyidik yaitu mengenai waktu pengiriman (*uploading*) dari pelaku tindak pidana *cyber crime* tersebut, tentunya dalam hal ini kepolisian/penyidik bekerja dengan alat pendukung yang mereka miliki sesuai standar oprasional prosedur (SOP) yang telah ditentukan dan berdasarkan aturan dan undang-undang yang berlaku.

b. **Waktu Korban Menerima Perlakuan Yang Merugikan Melalui Media Elektronik (Waktu Penerimaan).**

[3] Wawancara dengan AKP. Safpe Tambatua Sinaga (Penyidik) Unit *cyber crime* POLDA DIY, pada tanggal , 27 juni 2019 pukul 08.29 Wib

Pada metode/teori ini juga tidak jauh berbeda dengan teori pertama dalam penentuan waktu kejadian perkara (*tempus delicti*) hanya saja dengan metodi perbandingan terbalik yang mana pada metode pertama yang menjadi penentu adalah waktu dari pengiriman (*uploading*) sedangkan pada meode ini adalah yang menjadi penentu waktu kejadian perkara (*tempus delicti*) adalah waktu penerimaan (*downloading*) yang mana ketika Informasi Elektronik dan/atau dokumen elektronik memasuki sistem informasi terakhir yang berada di bawah kendali penerima (korban/ yang dirugikan), jadi dalam teori ini yang pertama kali diselidiki oleh penyidik yaitu mengenai waktu penerimaan (*downloading*) dari korban tindak pidana *cyber crime* tersebut, tentunya dalam hal ini kepolisian/penyidik bekerja dengan alal pendukung yang mereka miliki sesuai standar oprasional prosedur (SOP) yang telah ditentukan dan berdasarkan aturan dan undang-undang yang berlaku.

Berdasarkan dua teori tersebut diatas dalam menentukan waktu kejadian perkara (*tempus delicti*) penyidik lebih sering menggunakan teori waktu korban menerima perlakuan yang merugikan melalui media elektronik atau waktu melakukan *downloading* terhadap konten yang merugikan korban, dan sebenarnya dalam penentuan waktu kejadian perkara ini mengikuti atau saling bersinabungan dengan tempat terjadinya perkara yang mana pada waktu yang sama penyelidik telah menentukan tempat

kejadian perkara maka setelah itu langsung menyelidiki mengenai kapan tindak pidana itu diterima oleh korban atau dilakukan oleh pelaku, maka secara otomatis ketika tempat kejadian perkara sudah ditemukan atau ditentukan maka mengenai waktu kejadian perkara secara otomatis akan mengikuti dan ditemukan atau dapat ditentukan oleh penyidik.

3. Contoh Kasus dan Analisis Kasus Dalam Penentuan Tempat dan Waktu Kejadian (*Locus dan Tempus Delicti*) Berdasarkan Teori-Teori Yang Digunakan Oleh Penyidik.

a. Kasus Posisi

Tindak pidana *cyber crime* yang pernah terjadi dan di tangani oleh penyidik Unit *cyber crime* DITRESKRIMSUS POLDA DIY, dan telah melakukan proses persidangan di Pengadilan Negeri Yogyakarta yang mana telah diputus serta memiliki kekuatan hukum tetap (*inkracht*) dengan Putusan Nomor 311/Pid.Sus/2017/PN Yyk dalam perkara terdakwa:[4]

Nama : Kiki Emilia Handayani

Tempat Lahir : Mataram

Umur/ Tanggal lahir : 32 Tahun/ 29 Juni 1985

Jenis Kelamin : Perempuan

Kebangsaan : Indonesia

[4]Putusan Pengadilan Negeri Yogyakarta. https://putusan.mahkamahagung.go.id/putusan/904b295bc3c10d6f891735602399f2b8, Diakses pada tanggal 28 Juni 2019 pukul 18.20 Wib.

Tempat Tinggal : Jl. Lestari Penan RT:01/RW:040 Penjarakan Krya, Ampenan, Lombok, NTB atau Jl. Ade Irma Suryani Gang Panda 4 No. 43 Monjok, Kelurahan Salaparan Kota Mataram, NTB

Agama : Islam

Pekerjaan : PNS di PEMPROV Nusa Tenggara Barat

b. Kronologi Kasus

KEH yang bertempat tinggal di jalan Lestari Penan RT 01/RW 040, Penjarakan Karya, Ampenan, Lombok, NTB atau jalan Ade Irma Suryani Gang Panda 4 No. 43 Monjok Kelurahan Selaparan Kota Mataram NTB atas perbuatannya telah merugikan beberapa orang yang salah satunya adalah pelapor sekaligus korban yaitu MQ yang bertempat tinggal di jalan Celeban UH 3/543 RT 25 RW 6 Kelurahan Tahunan Kecamatan Umbulharjo Kota Yogyakarta. Berawal pada bulan Desember 2016, korban MQ berencana untuk berlibur ke Lombok dengan sarana pesawat terbang dari Yogyakarta bersama teman-temannya yaitu saksi RA dan saksi YT. Pada saat itu korban MQ mendapatkan informasi dari saksi RA bahwa tersangka KEH menjual tiket pesawat dengan harga murah karena sedang promo. Adanya informasi mengenai tiket promo yang harganya pasti jauh lebih murah daripada membeli tiket langsung di bandara membuat korban MQ tertarik dan menghubungi tersangka KEH melalui nomor whatsapp yang didapatkan dari saksi RA. Setelah korban MQ

berkomunikasi dengan tersangka KEH untuk mengetahui lebih lanjut tentang harga promo tiket pesawat yang ditawarkan ternyata harga yang ditawarkan memang jauh lebih murah dari harga normal yaitu tiket pesawat Jogja-Lombok sebesar Rp 500.000,00 sekali jalan padahal harga normalnya adalah Rp 1.000.000,00 s/d Rp 1.400.000,00. Melalui *whatsapp* korban MQ juga menanyakan tentang pekerjaan tersangka KEH dan bagaimana tersangka KEH dapat menjual tiket pesawat dengan murah, saat itu tersangka menyatakan dirinya bekerja sebagai PNS di Dinas Perhubungan Provinsi NTB dan tersangka KEH dapat menjual tiket murah karena ada paket promo khusus tahun 2017. Saat korban MQ telah melakukan transaksi pembayaran tiket melalui transaksi-elektronik yaitu dengan transfer ke rekening tersangka KEH, kemudian tersangka KEH mengirimkan tiket dalam bentuk *PDF* (*portable document format*) melalui *whatsapp*. Harga tiket yang tercantum dalam bentuk *PDF* tersebut harganya lebih mahal dari pada harga/nilai yang dibayarkan saksi kepada tersangka KEH yang menurut tersangka KEH harga promo. Atas kejadian tersebut korban MQ sempat curiga dan bertanya kepada tersangka, namun saat itu tersangka KEH menyatakan harga yang tercantum dalam tiket tersebut bukan harga promo sedangkan harga yang dibayarkan korban MQ adalah harga promo dari agen sehingga harganya lebih rendah dari harga yang tercantum dalam tiket. Penjelasan tersangka KEH tersebut membuat korban MQ percaya akan adanya harga tiket promo tersebut.

Menjelang keberangkatan korban MQ dan teman-temannya ke lombok, tersangka KEH mengirimkan tiket dalam bentuk kode *booking*. Selanjutnya untuk memastikan keaslian kode booking tersebut, korban MQ mendatangi kantor *LION AIR* di Bandara Adisutjipto, dan ternyata kode *booking* tersebut benar-benar asli. Maka korban MQ dan teman-temannya benar-benar berangkat dari Yogyakarta ke Lombok dengan tiket promo yang dibeli dari tersangka KEH tersebut sehingga korban MQ percaya kepada tersangka KEH bahwa tersangka KEH menjual tiket pesawat promo sehingga harganya murah. Saat korban MQ kembali dari Lombok, tersangka KEH melalui *whatsapp* menawarkan tiket pesawat dengan harga murah kembali kepada korban MQ dengan alasan yang sama yaitu sedang promo. Tersangka KEH juga menawarkan kepada korban MQ untuk menjual kembali tiket promo tersebut. Jika korban MQ menjual kembali tiket promo tersebut maka korban MQ dapat mengambil sejumlah keuntungan dan akan diberikan potongan harga untuk *reseller*. Atas tawaran dari tersangka KEH tersebut, korban MQ tertarik untuk membeli tiket promo kepada tersangka untuk dijual kembali dengan mengambil sejumlah keuntungan.

Pada kenyataannya tersangka KEH telah membohongi dan menyesatkan korban MQ karena pada waktu itu sebenarnya tidak ada tiket pesawat yang keuntungan dari penjualan barangnya tersebut, dijual dengan harga promo. Sebelum diketahuinya mengenai informasi

palsu mengenai harga tiket pesawat tersebut, pelayanan atas penawaran tiket promo dari tersangka KEH semula berjalan dengan baik dan lancar. Semua berhasil diberangkatkan sehingga untuk selanjutnya tiap kali tersangka KEH menawarkan tiket pesawat promo dengan harga murah melalui *whatsapp* tersangka KEH kepada korban MQ dan pada intinya tersangka KEH melalui *chat whatsapp* menawarkan ada tiket promo lagi. Adapun persyaratan yang diberikan oleh tersangka KEH apabila korban MQ berminat untuk menjadi *reseller* yaitu dalam pemesanan tiket promo tersebut tidak boleh terlalu dekat dengan hari keberangkatan. Korban MQ yang telah percaya dengan kata-kata tersangka dalam *chat whatsapp* tersebut, kemudian menyampaikan kepada teman-temannya/ *agen* korban MQ mengenai adanya promo tiket pesawat tersebut.

Penawaran menarik yang ditawarkan oleh tersangka KEH membuat korban MQ membeli tiket kepada tersangka KEH dan menjual tiket itu kembali kepada saksi AG, saksi PHS dan saksi EO. Selain dijual kepada para saksi, korban MQ juga menjual ke konsumen lainnya dan ada yang digunakan sendiri. Para saksi setelah memesan tiket kepada korban MQ dan kemudian menyerahkan uang pembayaran tiket pesawat tersebut. Selanjutnya korban MQ mentransfer uang tersebut melalui rekening korban MQ yaitu di Bank BNI Syariah dengan nomor rekening 0449843860, yang ditujukan ke rekening tersangka di Bank BNI dengan nomor rekening 0497466688

hingga seluruhnya berjumlah sekitar Rp 502.299.000,00 (lima ratus dua juta dua ratus sembilan puluh sembilan ribu rupiah). Atas tiket pesanan atau yang dibeli oleh konsumen melalui korban MQ kepada tersangka KEH, korban memperoleh keuntungan sekitar Rp 100.000,- s/d Rp 200.000,- per tiket dan korban MQ memberikan uang kepada saksi AG, saksi PHS dan saksi EO kadang-kadang Rp Rp 50.000,- atau Rp 100.000,-. Awalnya proses pemesanan tiket berjalan lancar dan tidak ada kendala bahwa tiket tersebut palsu atau tidak dapat diberangkatkan. Namun sekitar tanggal 15 bulan Juli tahun 2017 tersangka KEH menelepon kepada saksi RA dan menyatakan bahwa pemesanan tiket pesawat mulai tanggal 17 dan seterusnya bulan Juli tahun 2017 tidak dapat dicetak dan uang pemesanan yang telah dikirim telah digunakan tersangka KEH untuk kepentingan lain. Fakta selanjutnya yang terungkap yaitu tersangka KEH selama ini membeli tiket pesawat melalui agen tiket yang bernama " JATA TOUR " yang beralamat di jalan Panca Usaha Blok A 12 Mataram NTB dengan harga normal bukan harga promo, jadi uang yang korban MQ kirim hanya diputarkan tersangka dan yang paling akhir tidak dapat tiket pesawat. Sebagai contoh sejumlah Rp 1.000.000,00 namun dijual kepada korban MQ atau korban lainya sejumlah Rp. 500.000,00 atau Rp 700.000,00. Jadi saat pembelian tiket ke Jata Tour tersangka KEH tombok (terpaksa menambah uang) atau menambahi duluan, namun dalam tomboknya atau menambahnya tetap pakai uang saksi atau

korbannya lainya dengan cara, semisal pemesanan pada bulan Januari dan pemberangkatan pada bulan Januari juga dia menambahi terlebih dahulu dengan menggunakan uang pada pemesanan bulan Januari namun pemberangkatan bulan Agustus, dikarenakan oleh terdakwa untuk bulan Agustus belum dibelikan. Dengan adanya pengakuan tersangka KEH mengenai aksi penipuan yang dilakukannya, korban MQ kemudian mendatangi kontor agen travel JATA TOUR dan bertemu dengan saksi LL salah satu karyawan agen JATA TOUR yang selama ini melayani tersangka KEH. Saat itu saksi LL menyampaikan bahwa bahwa selama ini tersangka KEH dalam melakukan pembelian tiket pesawat tetap dengan harga normal, dan tidak ada harga promo dari *agen* JATA TOUR selama ini. Atas kejadian tersebut korban MQ mengalami kerugian sejumlah Rp 397.530.000,00 (tiga ratus sembilan puluh tujuh juta lima ratus tiga puluh ribu rupiah), kerugian tersebut dihitung dari jumlah penumpang yang mendapatkan tiket sedangkan uang atas pemesanan tiket pesawat tersebut telah korban kirim melalui transfer kepada tersangka. Jumlah konsumen yang uang pembelian tiketnya telah korban transfer kepada tersangka namun tidak jadi diberangkatkan adalah sekitar 300 tiket sebagaimana keterangan saksi yang saksi sampaikan dalam Berita Acara Saksi dalam berkas perkara. Fakta selanjutnya yang terungkap yaitu tersangka KEH selain menawarkan tiket pesawat dengan harga promo juga sering

menawarkan tiket dengan harga lelang yaitu harganya lebih rendah dari pada harga promo.

Akibat dari para pembeli tiket yang melalui korban MQ banyak yang tidak dapat diberangkatkan, mereka marah-marah kepada korban MQ dan korban juga harus mengembalikan uang yang telah diserahkan para pembeli kepada korban MQ. Dalam hal ini korban MQ juga telah berusaha untuk mengembalikan sebagian uang tiket para pembeli yang melalui korban dan akan diganti semuanya. Atas perbuatan tersangka KEH, korban MQ tidak jadi memperoleh keuntungan atas pembelian tiket karena atas keuntungan yang korban peroleh dari penjualan tiket kepada konsumen telah digunakan korban untuk memesan tiket yang ditawarkan oleh tersangka namun belum ada pembelinya. Korban MQ mengalami kerugian sekitar Rp. 397.530.000,00 (tiga ratus sembilan puluh tujuh juta lima ratus tiga puluh ribu rupiah) dan atas kerugian yang korban alami tersebut tersangka KEH baru mengembalikan sekitar Rp 27.200.000,00 dalam bentuk sepeda motor tersangka yang diserahkan tersangka kepada korban MQ yang korban hargai Rp 15.000.000,00 dan sisanya ditransfer tersangka kepada korban.

Motif pelaku/tersangka KEH melakukan perbuatan yang melanggar hukum dengan menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam kasus ini yaitu MQ melalui transaksi elektronik karena uang tersebut akan

digunakan pelaku untuk membayar hutang-hutangnya. Perbuatan pelaku ini tidak hanya terjadi sekali waktu tetapi jauh sebelum pelaku KEH dilaporkan atas kasus ini, pelaku juga pernah melakukan hal yang sama sebelumnya dengan alasan/motif yang sama, namun permasalahan sebelumnya dapat diselesaikan dengan adanya penggantian kerugian dengan menjual harta benda pelaku KEH. Pihak keluarga KEH juga membenarkan atas perbuatan pelaku yang tidak hanya sekali dua kali melakukan tindak pidana menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen.

c. Pasal Yang Dilanggar Oleh Terdakwa Berdasarkan Tuntutan Pidana Yang Diajukan Oleh Jaksa Penuntut Umum dan Putusan Pengadilan Negeri Yogyakarta

Pada kasus ini setelah mendengar keterangan Saksi-saksi dan Terdakwa serta memperhatikan barang bukti yang diajukan di persidangan dan mendengar pembacaan tuntutan pidana yang diajukan oleh Penuntut Umum, maka pasal yang dilanggar oleh Terdakwa dan sanksi yang diberikan atas perbuatannya berdasarkan Putusan Nomor 311/Pid.Sus/2017/PN Yyk adalah sebagai berikut:[5]

1) Menyatakan Terdakwa Kiki Emilia Handayani terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik

[5] Ibid

sebagaimana dimaksud dalam Pasal 28 ayat (1) sebagaimana dalam Dakwaan Kesatu melanggar pasal 45 A ayat (1) UU RI No. 19 Tahun 2016 tentang Perubahan UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

2) Menjatuhkan pidana terhadap Terdakwa Kiki Emilia Handayani dengan pidana penjara selama 2 (dua) tahun dikurangi selama terdakwa berada dalam tahanan dan terdakwa membayar denda sebesar Rp.10.000.000,- (sepuluh juta rupiah) subsidair menjalani hukuman selama 2 (dua) bulan kurungan.

d. Analisis Kasus Dalam Penentuan Tempat dan Waktu Kejadian (*Locus dan Tempus Delicti*) Berdasarkan Teori-Teori Yang Digunakan Oleh Penyidik

Pada kasus tindak pidana *cyber crime* yakni penyebaran berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik tersebut diatas, yang mana sebagai pelaku tindak pidana (Terdakwa) adalah KEH dan yang dirugikan atas tindak pidana tersebut (Pelapor) adalah MQ. Pada kasus ini dalam hal penentuan tempat dan waktu kejadian perkara (*locus dan tempus delicti*) berdasarkan teori- teori yang digunakan oleh penyidik yaitu sebagai berikut:

1) Penentuan Tempat Kejadian (*Locus Delicti*)

Pada kasus ini dalam hal penentuan tempat kejadian perkara (*locus delicti*) berdasarkan beberapa teori yang ada maka

penyidik di Unit *Cyber Crime* DITRESKRIMSUS POLDA DIY dalam kasus penyebaran berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik ini menggunakan teori "tempat dimana dampak kejahatan tersebut terjadi (*theory of the downloader*)" yang mana pada teori ini penyidik menentukan tempat kejadian perkara (*locus delicti*) dengan berdasarkan tempat dimana dampak kejahatan tersebut terjadi atau tempat dimana korban melakukan *downloading* (mengunggah) atau melihat postingan/konten yang merugikan korban atas tindak pidana *cyber crime* tersebut.

Pada prakteknya teori ini memang sangat sering digunakan oleh para penyidik *cyber crime* dalam menentukan *locus delicti* yang tentunya berdasarkan kebutuhan dan untuk mempermudah proses penegakan hukum, dalam teori ini biasanya berawal dari korban yang melaporkan kepada kepolisian dengan bukti-bukti elektronik (digital) atau juga sudah berbentuk *hard file* dan kepolisian melakukan penyelidikan dan menentukan tempat kejadian perkaranya sesuai dengan tempat korban/ pelapor yang merasa dirugikan, maka pada prakteknya jika menggunakan teori ini yang menangani kasus mulai dari penyelidikan, penyidikan, penuntutan, hingga proses persidangan dilakukan oleh lembaga kepolisian, kejaksaan dan lembaga peradilan yang bertanggung jawab atas wilayah hukum tersebut yang mana sesuai dengan

tempat korban/ pelapor yang merasa dirugikan terhadap konten atau perbuatan yang dilakukan oleh pelaku melalui media elektronik yang mana hal tersebut merupakan tindak pidana *cyber crime*. Pada kasus ini kita juga bisa melihat dalam hal alamat pelaku dan korban yakni tidak ditempat atau wilayah hukum yang sama yang mana pelaku bertempat tinggal di Mataram, NTB dan melakukan tindak pidananya juga disana sedangkan korban bertempat tinggal di Yogyakarta, tetapi dalam proses hukum dilakukan di Yogyakarta karena dalam menentukan tempat kejadian perkara (*locus delicti*) yaitu berdasarkan teori "tempat dimana dampak kejahatan tersebut terjadi (*theory of the downloader*)".

2) Penentuan Waktu Kejadian (*Tempus Delicti*)

Pada kasus ini dalam hal penentuan waktu kejadian perkara (*tempus delicti*) berdasarkan beberapa teori yang ada maka penyidik di Unit *Cyber Crime* DITRESKRIMSUS POLDA DIY yaitu dalam kasus penyebaran berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik ini menggunakan teori "waktu korban menerima perlakuan yang merugikan melalui media elektronik", pada metode/ teori ini dalam menentuankan waktu kejadian perkara (*tempus delicti*) yang menjadi penentu waktu kejadian perkara (*tempus delicti*) adalah waktu penerimaan (*downloading*) yang

mana ketika Informasi Elektronik dan/atau dokumen elektronik memasuki sistem informasi terakhir yang berada di bawah kendali penerima (korban/yang dirugikan), jadi dalam teori ini yang pertama kali diselidiki oleh penyidik yaitu mengenai waktu penerimaan (*downloading*) dari korban tindak pidana *cyber crime* tersebut, jadi jika kita lihat pada kasus yang terjadi maka menenukan waktu kejadian perkara (*tempus delicti*) berdasarkan teori "waktu korban menerima perlakuan yang merugikan melalui media elektronik" yakni ketika MQ menerima dan melihat postingan penyebaran berita bohong tersebut yang menjadi penentu dalam menentukan waktu kejadian perkara (*tempus delicti*).

4. Rekapitulasi Laporan/Pengaduan di Unit *Cyber Crime* DITRESKRIMSUS POLDA DIY Pada Tindak Pidana *Cyber Crime* Dari Tahun 2015 Hingga Tahun 2018

Penulis telah melakukan penelitian kepada penyidik *cyber crime* yang menangani kasus- kasus *cyber crime* yang dilaporkan di Unit *Cyber Crime* DITRESKRIMSUS POLDA DIY, dan penulis mendapatkan data rekapitulasi laporan/pengaduan pada tindak pidana *cyber crime* dari tahun 2015 hingga tahun 2018, agar pembaca dapat melihat jenis, jumlah, kenaikan dan penurunan kasus *cyber crime* yang dilaporkan di Unit *Cyber Crime* DITRESKRIMSUS POLDA DIY, maka penulis membuat hasil data rekapitulasi tersebut dalam bentuk tabel yakni sebagai berikut:

Tabel 4.1

Data Laporan/ Pengaduan Terkait Tindak Pidana *Cyber Crime* Dari Tahun 2015 Hingga Tahun 2018 di Unit *Cyber Crime* DITRESKRIMSUS POLDA DIY

NO	JENIS KASUS *Cyber Crime*	KETENTUAN PIDANA	TAHUN				JUMLAH	KET.
			2015	2016	2017	2018		
1	Pembobolan Keamanan Akun/*Hacking*	Pasal 30 UU. ITE	22	4	37	27	90	5 selesai
2	Penipuan Online	Pasal 28 ayat (1) UU. ITE	204	202	446	296	1.418	26 selesai
3	Pencemaran Nama Bik	Pasal 27 ayat (3) UU. ITE	35	47	70	53	205	38 selesai
4	Pornografi Online	Pasal 27 ayat (1) UU. ITE	2	9	16	2	29	9 selesai
5	Pencurian	Pasal 30 Jo. Pasal 46 dan 48. UU. ITE	3	4	12	19	38	4 selesai
6	Pemerasan / pengancaman	Pasal 27 ayat (4) dan Pasal 29. UU. ITE	5	1	13	11	30	3 selesai
7	Penistaan Agama	Pasal 28 ayat (2). UU. ITE	1	2	3	3	9	-

(*sumber: Unit Cyber Crime DITRESKRIMSUS POLDA DIY*)

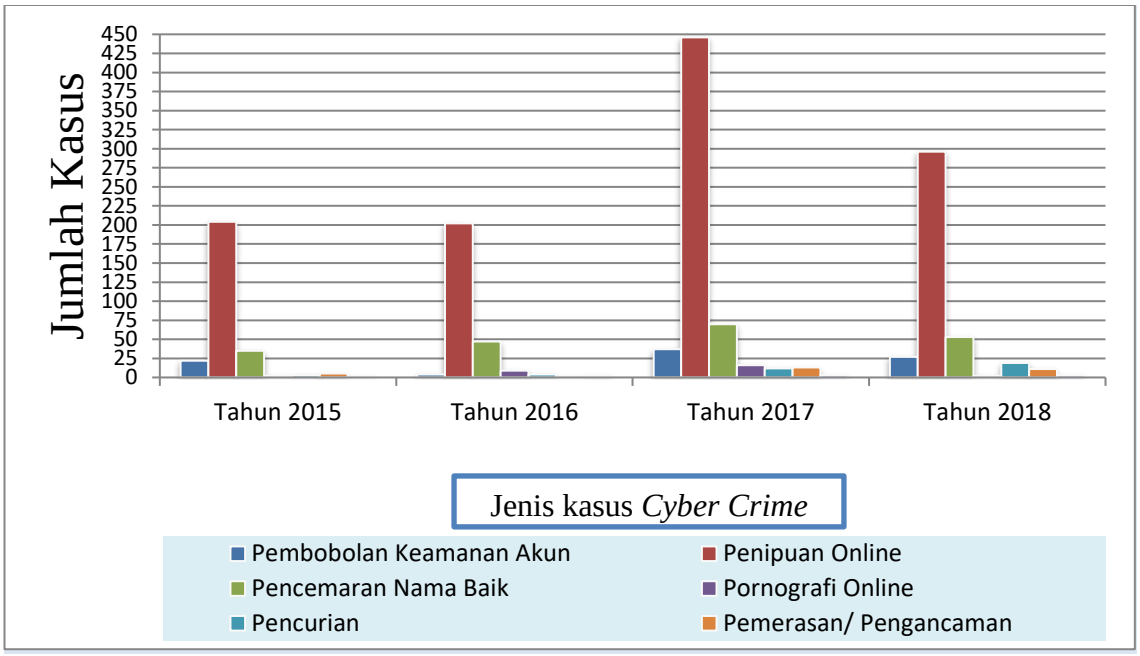
Pada data laporan/ pengaduan masyarakat kepada pihak kepolisian/ penyidik di DITRESKRIMSUS Unit *cyber crime* POLDA DIY selama 4 (empat) tahun yaitu tahun 2015 hingga tahun 2018 yang mana kita dapat melihat dari 7 (tujuh) jenis kasus *cyber crime* yang dilaporkan oleh masyarakat yang mana tindak pidana *cyber crime* penipuan online sebagai kasus terbanyak yang dilaporkan yakni setiap tahunnya sebanyak lebih dari dua ratus kasus dan ditahun 2017 mecapai hingga lebih dari empat ratus kasus, dan selanjutnya meyusul pada kasus pencemaran nama baik menjadi kasus yang cukup banyak dilaporkan yang mana sebagian besar delik yang diadukan berasal dari media sosial, bila kita melihat dari kasus- kasus yang lainya seperti *hacking/*pembobolan akun dari 4 (empat) tahun tersebut hanya paling banyak yaitu puluhan kasus tidak mencapai hingga ratusan kasus, penistaan agama adalah kasus yang paling sedikit dilaporkan yang mana jika kita lihat dari tahun ke tahun dari kurun waktu 4 (empat) tahun tersebut kasus yang dilaporkan maksimal hanya 3 (tiga) kasus, dan pada kasus pemerasan juga tidak terlalu banyak tiap tahunnya hanya belasan kasus yang dilaporkan, selanjutnya pada kasus pencurian dengan menggunakan eknologi informasi juga tidak terlalu banyak kasus yang dilaporkan yakni maksimal hanya mencapai belasan kasus dari tahun ke tahun, maka kita dapat mengambil kesimpulan bahwa banyaknya kasus yang dilaporkan berdasarkan banyaknya aktifitas orang- orang pada media tersebut misalnya pada media sosial mulai dari berjualan secara online hingga hanya sekedar hiburan hampir semua orang mempunyai akun- akun media sosial dan mengoprasikannya dari kebiasaan

tersebut maka pihak- pihak tertentu banyak yang memanfaatkannya dan melakukan kejahatan yang disebut kejahatan *cyber crime.*

Melihat dari laporan/ pengaduan masyarakat kepada pihak kepolisian/ penyidik di DITRESKRIMSUS Unit *cyber crime* POLDA DIY terkait tindak pidana *cyber crime* berdasarkan tabel diatas maka jika kita lihat dalam bentuk persentase dalam bentuk diagram maka kita dapat melihat lebih jelas kasus mana yang paling banyak dan paling sedikit dilaporkan kepada pihak kepolisian/ penyidik Unit *cyber crime* POLDA DIY, berikut persentase dalam bentuk diagram laporan/ aduan masyarakat kepada penyidik *cyber crime* POLDA DIY :

Gambar 4.3

Grafis Laporan Tindak pidana *Cyber Crime* Dari Tahun 2015 Hingga Tahun 2018 di Unit *Cyber Crime* DITRESKRIMSUS POLDA DIY



(*sumber: Unit Cyber Crime DITRESKRIMSUS POLDA DIY*)

Pada gambar/grafis diatas mengenai persentase laporan tindak pidana *cyber crime* berdasarkan laporan masyarakat kepada penyidik *cyber crime* di Unit *Cyber Crime* DITRESKRIMSUS POLDA DIY mulai tahun 2015 hingga tahun 2018 yang mana kenaikan dan penurunan jumlah laporan dari tindak pidana *cyber crime* khususnya pada 7 (tujuh) kasus yang pernah dilaporkan yaitu kasus pembobolan keamanan akun/ *hacking*, pencemaran nama baik, pencurian, penistaan agama, penipuan online, pornografi online, dan juga pemerasan/ pengancaman.

Pada gambar diagram persentase laporan kita bisa melihat bahwa dari tahun ke tahun kejahatan yang paling banyak terjadi yaitu pada kasus penipuan online yang maksimalnya mencapai 446 kasus pada tahun 2017 dan minimalnya mencapai 202 kasus yaitu pada tahun 2016, hal ini merupakan angka yang sangat tinggi dan berdasarkan hasil penelitian penulis total kasus penipuan online ini mulai dari tahun 2015 hingga tahun 2018 jumlah kasus yang dilaporkan sebanyak 1.418 kasus yang mana yang terselesaikan hanya 26 kasus, dan pada kasus-kasus yang lain tidak terlalu banyak laporan yang diterima oleh penyidik *cyber crime* POLDA DIY, tetapi tetap saja kasus yang terselesaikan massih jauh dari jumlah angka yang telah dilaporkan, dalam hal tentu saja kita bisa ambil kesimpulan bahwa masih banyak kendala- kendala yang menjadikan proses penegakan hukum khususnya pada tindak pidana *cyber crime* ini sangat lambat dan apa yang menjadi penyebab penipuan *online* ini menjadi kasus yang paling banyak terjadi, dalam hal hambatan/kendala penulis akan membahas pada pembahasan berikutnya.

Pada mekanisme penentuan tempat dan waktu kejadian oleh penyidik dalam kejahatan dunia maya (*cyber crime*), yang mana penyidik dalam hal ini mengalami kesulitan yang lebih jika dibandingkan dengan penentuan tempat dan waktu kejadian perkara dalam tindak umum. Pada tindak pidana *cyber crime* kita ketahui bahwa tempat kejadian perkara (*locus delicti*) tidak hanya berdasarkan teritorial dan atau tidak ada batasan tempat pelaku melakukan tindak pidana *cyber crime* dan korban juga belum tentu ditempat yang sama dengan pelaku, selain itu dalam tindak pidana *cyber crime* ini alat/instrument yang dilakukan dalam melakukan tindak pidana serba elektronik dan canggih, maka dalam hal ini penyidik dalam melakukan penyelidikan dan penyidikan khususnya dalam hal penentuan tempat dan waktu kejadian menggunakan teori-teori khusus yang sesuai dengan tindak pidana *cyber crime* ini.

Penentuan tempat kejadian perkara (*locus deliti*) dalam tindak pidana *cyber crime* menggunakan beberapa teori- teori yakni, dengan menggunakan teori tempat terjadinya perbuatan tersebut dilakukan/ tempat pelaku mengirimkan konten terkait korban (*theory of the uploader*) yang mana pada teori ini dalam menentukan tempat kejadian dilihat berdasarkan tempat dimana pelaku melakukan aksinya dalam kejahatan *cyber crime* yang menimbulkan korban, dan selanjutnya teori yang digunakan adalah teori tempat dimana dampak kejahatan *cyber crime* tersebut terjadi/ tempat korban mengunggah konten yang merugikan dirinya (*theory of the downloader*) yang mana dalam teori ini penyidik dalam menentukan tempat kejadian melihat berdasarkan tempat dimana korban mengunggah suatu konten yang merugikan dirinya, dan teori berikutnya adalah

teori alat yang digunakan dan alamat *server* dalam melakukan kejahatan dalam hal ini penyidik dalam menentukan tempat kejadian perkara melihat berdasarkan dimana alat/instrument berada yang dipergunakan untuk melakukan tindak pidana *cyber crime* dan juga melihat berdasarkan alamat server yang di gunakan oleh pelaku tindak pidana *cyber crime* tersebut. Pada teori-teori tersebut yakni berdasarkan yurisprudensi dan atau putusan- putusan hakim terdahulu dalam ha kasus yang sama, karena mengenai *locus delicti* pada tindak pidana *cyber crime* belum diatur dan disebutkan dalam undang-undang secara jelas.

Penentuan waktu kejadian perkara (*locus deliti*) dalam tindak pidana *cyber crime* menggunakan beberapa teori-teori yakni, teori waktu dalam melakukan tindak pidana (waktu mengakses/mengunggah sebuah konten ke media elektronik) yang mana berdasarkan teori ini penyidik dalam menentukan waktu kejadian perkara melihat berdasarkan waktu pengiriman yang dilakukan oleh pelaku tindak pidana *cyber crime*, selanjutnya menggunakan teori waktu korban menerima atau mengunggah konten yang merugikan melalui media eelektronik yang mana dalam teori ini penyidik menentukan waktu kejadian perkara berdasarkan waktu korban menerima konten yang merugikan dirinya. Pada teori-teori dalam menentukan waktu kejadian perkara ini berdasarkan pasal 8 ayat (4) huruf a dan b UU ITE.

Pada penanganan kasus *cyber crime* khususnya dalam hal penentuan tempat dan waktu kejadian sebenarnya tidak jauh berbeda dengan tindak pidana umum, hanya saja terlihat lebih khusus dan sedikit berbeda dikarenakan perbedaan menggenai modus- modus pelaku, tempat pelaku dan korban dan alat

atau instrument yang digunakan oleh pelaku serba elektronik, maka dari itu metode yang digunakan dalam penentuan tempat dan waktu kejadian dalam tindak pidana *cyber crime* ini juga sesuai kebutuhan.

B. Kendala yang Dihadapi Oleh Aparat Penegak Hukum Dalam Upaya Penanggulangan Kejahatan Dunia Maya *(Cyber Crime)*

Kendala dalam upaya penanggulangan *cyber crime* oleh aparat kepolisian khususnya di Unit *Cyber Crime* DITRESKRIMSUS POLDA DIY yang mana sebagai objek penelitian penulis dalam melakukan penelitian, menurut hasil penelitian yang telah dilakukan penulis terdapat beberapa kendala yang menghambat upaya penanggulangan *cyber crime*, penulis kemudian membaginya ke dalam 4 (empat) aspek berdasarkan hasil wawancara dengan AKP.Safpe Tamabatua Sinaga dan penelusuran referensi lainya, yaitu:[6]

1. Aspek Penyidik (Sumber Daya Manusia)

Penyidik kepolisian memiliki peran penting dalam upaya penanggulangan *cyber crime*, dimana kemampuan/ kualitas penyidik dan jumlah personil penyidik di setiap unit *cyber crime* harus memadai dan diperhatikan karena sangat berpengaruh untuk mengungkap kasus-kasus *cyber crime* yang dilaporkan oleh masyarakat, adanya unit *cyber crime* dilingkungan kepolisian membuktikan bahwa dibutuhkannya penyidik khusus yang memiliki kemampuan di bidang informasi dan transaksi

[6] Wawancara dengan AKP. Safpe Tambatua Sinaga (Penyidik) Unit *Cyber Crime* POLDA DIY, pada tanggal , 27 juni 2019 pukul 08.29 Wib

elektronik guna menangani kejahatan-kejahatan di dunia maya secara maksimal, dalam hal ini penulis akan menjelaskan mengenai kendala aspek penyidik sesuai dengan data dan hasil wawancara penulis dengan penyidik di Unit *Cyber Crime* DITRESKRIMSUS POLDA DIY, yang mana mengenai aspek penyidik dalam penanggulangan kejahatan *cyber crime* penyidik sendiri memiliki kendala yang mana mulai dari kualitas penyidik dan kuantitas penyidik/ jumlah personil penyidik yakni sebagai berikut:

a. Kualitas Penyidik

Pada instansi kepolisisan khususnya di Unit-Unit *Cyber Crime* di setiap POLDA di Indonesia khususnya di POLDA DIY dalam hal kualitas penyidik masih banyak masalah, hai ini dikarenakan belum adanya pendidikan khusus untuk para calon-calon penyidik *cyber crime* yang memberikan pengetahuan terkait *cyber* kepada para calon- calon penyidik *cyber crime* yang khususnya menangani masalah dan cara kerja yang profesional dalam melakukan penanggulangan terhadap tindak pidana *cyber crime,* maka dari itu dalam prakteknya di setiap POLDA termasuk di Unit *Cyber Crime* DITRESKRIMSUS POLDA DIY sendiri semua penyidik *cyber crime* adalah penyidik pegawai negeri sipil (PPNS) yang mana bukan dari akademi kepolisian atau berdsarkan pendidikan khusus penyidik- penyidik tindak pidana *cyber crime* dari POLRI tetapi diambil dari sipil atau Kementerian KOMINFO yang berdasarkan rekrutmen dan aturan yang ada,

mempunyai keahlian terkait teknologi informasi dan transaksi elektronik yang mana penyidiknya disebut PPNS (penyidik pegawai negeri sipil) tetapi status PPNS tersebut juga termasuk dalam anggota kepolisian jika dinyatakan lulus dalam seleksi sebagai penyidik *cyber crime* POLRI.

Kendala dalam hal kualitas penyidik sendiri dapat dilihat dari aspek kekuatan dan kemampuan satuan Unit *Cyber Crime* di suatu POLDA yang mana dalam hal ini di Unit *Cyber Crime* DITRESKRIMSUS POLDA DIY memiliki sebanyak 15 personil yang bertugas di unit *cyber crime*, dari 15 orang tersebut belum ada yang memiliki sertifikasi program *Certified Ethical Hacker* (*CEH*) dan sertifikasi program *Computer Hacking Forensic Investigator Certification* (*CHFI*) untuk melakukan pemeriksaan barang bukti digital di laboratorium digital forensik, selain itu kemampuan penyidik dalam menangani kasus-kasus *cyber crime* belum cukup memadai karena masih terkendala dalam hal- hal, seperti :

1) Kemampuan bahasa inggris
2) Kemampuan komputer forensik
3) Kemampuan *mobile* forensik
4) Kemampuan analisis jaringan transaksi keuangan dan komunikasi
5) Kemampuan *cyber law*

Berdasarkan penjelasan mengenai kendala/ masalah dalam penanggulangan tindak pidana *cyber crime* dari aspek kualitas

penyidik tersebut diatas kita dapat melihat dan menilai khususnya untuk kualitas penyidik-penyidik Unit *Cyber Crime* DITRESKRIMSUS POLDA DIY masih memiliki banyak yang perlu dikembangkan dalam hal kualitas sumber daya manusianya agar dapat melakukan penanggulangan tindak pidana *cyber crime* secara baik dan profesional.

b. Jumlah Personil Penyidik

Pada instansi kepolisisan khususnya di Unit- unit *Cyber Crime* di setiap POLDA di Indonesia khususnya di Unit *Cyber Crime* DITRESKRIMSUS POLDA DIY dalam hal kuantitas/ jumlah penyidik masih mengalami kekurangan pada setiap unit *cyber crime*, dengan sangat terbatasnya jumlah personil penyidik menimbulkan masalah dimana tidak sebanding dengan banyaknya laporan atau aduan yang masuk dari masyarakat, tentu dalam hal ini berimbas pada lambatnya ditangani laporan tindak pidana *cyber crime* oleh pihak kepolisian/penyidik. Pada prakteknya di Unit *Cyber Crime* DITRESKRIMSUS POLDA DIY sendiri dari segi jumlah penyidik tindak pidana *cyber crime* hanya 15 penyidik saja padahal laporan yang masuk sangat banyak tentu ini mengakibatkan lambatnya penanganan kasus yang dilaporkan, maka dalam prakteknya sesuai wawanacara penulis dengan penyidik di Unit *Cyber Crime* DITRESKRIMSUS POLDA DIY dalam penanganan kasus tindak pidana *cyber crime* bukan berdasarkan laporan yang lebih cepat

dilaporkan yang ditangani terlebih dahulu tetapi berdasarkan jumlah kerugian yang lebih diprioritaskan, maka dalam hal ini tentu tidak adil secara penegakan hukum, tetapi inilah yang terjadi dilapangan karena keterbatasan jumlah penyidik.

Kendala dalam hal kuantitas/ jumlah penyidik sendiri dapat dilihat dari aspek kekuatan dan kemampuan satuan Unit *Cyber Crime* DITRESKRIMSUS POLDA DIY hanya memiliki sebanyak 10 personil yang bertugas di unit *Cyber Crime*, dari kelima belas tersebut menduduki tugas masing-masing yaitu :

1) KANIT/ Kepala Unit *Cyber* 1 personil
2) Tim Analis 2 personil
3) Tim Pengawas 2 personil
4) Unit Lidik Sidik 10 personil

Berdasarkan penjelasan mengenai kendala/ masalah dalam penanggulangan tindak pidana *cyber crime* dari aspek kuantitas/jumlah penyidik tersebut diatas kita dapat melihat dan menilai/mengukur kemampuan satuan kerja khususnya di Unit *Cyber Crime* DITRESKRIMSUS POLDA DIY, tentunya masih membutuhkan tambahan jumlah personil penyidik agar dapat melakukan penanggulangan tindak pidana *cyber crime* secara tepat waktu dan professional, mengingat saat ini semangkin maraknya tindak pidana *cyber crime* yang mengikuti perkembangan teknologi informasi.

2. Aspek Alat Bukti

Pada tindak pidana *cyber crime* dalam hal alat bukti berbeda dengan alat bukti pada tindak pidana umum dimana sasaran atau media *cyber crime* merupakan data-data atau sistem elektronik dengan dihubungkan ke internet, dan selain itu masih banyak dan bebasnya warung internet (warnet) dan fasilitas umum lainnya yang mana ini menjadi masalah/ kendala terhadap penyidik *cyber crime*, dalam hal ini penulis akan menjelaskan secara rinci mengenai kendala aspek alat bukti sesuai dengan data dan hasil wawancara penulis dengan penyidik di Unit *Cyber Crime* DITRESKRIMSUS POLDA DIY, yang mana mengenai aspek alat bukti dalam penanggulangan kejahatan *cyber crime* sendiri memiliki kendala yang mana mulai dari alat bukti digital mudah dihilangkan dan atau dihapus jika tidak ditangani dengan cepat dan tepat dalam suatu tindak pidana *cyber crime*, dan pelaku menggunakan fasilitas umum dalam melakukan tindak pidana *cyber crime*, yakni penjelasannya sebagai berikut:

a. Barang Bukti Digital Mudah Dihilangkan Jika Tidak Ditangani Dengan Tepat Waktu

Barang bukti dalam tindak pidana *cyber crime* sesuai prakteknya merupakan dalam bentuk digital dikarenakan yang dijadikan sasaran dalam tindak pidana *cyber crime* merupakan data-data atau sistem elektronik yang mana misalnya dalam kasus *hacking* dan lain sebagainya dan atau melakukan pencemaran nama baik atau

penipuan secara *online* yang mana semua instrument yang digunakan ialah serba elektronik dengan dihubungkan ke internet yang sifatnya mudah diubah, dihapus, atau disembunyikan oleh pelaku kejahatan *cyber crime*, maka dari itu pada prakteknya dalam hal alat bukti dalam tindak pidana *cyber crime* lebih sulit jika dibandingkan dengan alat bukti pada tindak pidana umum yang mana pada tindak pidana umum alat buktinya dalam bentuk fisik dan tidak mudah untuk dihilangkan jejaknya yang mana hal ini sangat bertolak belakang dengan tindak pidana *cyber crime* dalam hal alat bukti khususnya.

Berdasarkan penjelasan mengenai kendala/masalah dalam penanggulangan tindak pidana *cyber crime* dari aspek alat bukti tersebut diatas kita dapat mengetahui bagaimana kendala yang dihadapi penyidik- penyidik di setiap Unit *Cyber Crime*, tentunya dalam hal ini agar setiap penyidik dapat melakukan penanggulangan tindak pidana *cyber crime* secara tepat waktu dan professional, melihat dari masalah dalam hal alat bukti maka perlu didukung dengan banyaknya sosialisasi dengan masyarakat agar dapat melaporkan secara cepat jika menjadi korban tindak pidana *cyber crime* dan juga perlu dukungan dalam hal peralatan agar dapat melacak dan melakukan proses-proses penyelidikan dan penyidikan secara cepat dan tepat.

b. Pelaku Menggunakan Fasilitas Umum Dalam Melakukan Tindak Pidana *Cyber Crime*

Pada kasus- kasus tindak pidana *cyber crime* tidak sedikit pelaku tindak pidana *cyber crime* dalam melakukan aksinya menggunakan fasilitas umum dalam mengakses dan berbuat sesuatu dengan media elektronik dengan sambungan internet menggunakan fasilitas warung internet (warnet) dan atau fasilitas umum lainya, dan kita ketahui warung internet (warnet) di Indonesia masih dengan bebasnya beroprasi tanpa ada regulasi dan pengawasan dari pemerintah ataupun penegak hukum yang ada sedangkan penyidik dalam melakukan penyelidikan dalam tindak pidana *cyber crime* untuk melakukan pelacakan pelaku berdasarkan alamat *server* atau informasi *IP Address* dari alat elektronik pelaku maka dalam hal ini tentu menjadi kendala dalam menangkap pelaku dan mengenai alat bukti akan semangkin rumit. Pelaku-pelaku tindak pidana *cyber crime* juga memanfaatkan hal tersebut agar jejak digitalnya tidak dapat dijadikan alat bukti atau sulit mengenai pembuktian dalam kejahatan *cyber crime.*

Berdasarkan penjelasan dalam hal kendala dalam penanggulangan tindak pidana *cyber crime* dari aspek alat bukti tersebut diatas kita dapat mengetahui bagaimana kendala yang dihadapi penyidik- penyidik di setiap Unit *Cyber Crime*, tentunya dalam hal pelaku menggunakan fasilitas umum dalam melakukan tindak pidana *cyber crime*, yang mana ini merupakan masalah yang sangat serius dan sampai saat ini belum ada tindakan dari pemerintah

dan penegak hukum dalam hal regulasi dan pengawasan terhadap penyedia fasilitas elektronik umum (warnet) yang mana hal tersebut dapat membuka peluang pelaku tindak pidana *cyber crime* semangkin banyak melakukan aksi- aksinya dengan cara tersebut dan tentunya penyidik dalam melakukan penylidikan akan semangkin sulit dan membuat penanganan tidak selesai tepat waktu atau bahkan pelaku dapat meloloskan diri dari jeratan hukum, tentu dari masalah ini perlu perhatian secara khusus agar penyidik-penyidik *cyber crime* dapat melacak dan melakukan proses penyelidikan dan penyidikan secara cepat dan tepat.

c. Keberadaan Para Saksi Tidak di Tempat Yang Sama Dengan Korban dan Pelaku

Pada tindak pidana *cyber crime* sangat berbeda dengan tindak pidana umum, khususnya dalam hal alat bukti yang berkaitan dengan saksi-saksi,yang mana pada tindak pidana *cyber crime* saksi- saksi belum tentu keberadaannya di lokasi/ tempat yang sama dengan korban dan atau pelaku, padahal keterangan saksi merupakan hal yang penting dalam proses penegakan hukum khususnya dalam kasus tindak pidana *cyber crime* dan termasuk alat bukti sesuai pasal 184 ayat (1) huruf a KUHAP yang mana keterangan saksi merupakan termasuk dari alat bukti yang sah. Saksi korban dalam kasus *cyber crime* berperan sangat penting dan tapi pada prakteknya jarang sekali terdapat saksi dalam kasus *cyber crime* dikarenakan saksi korban yang berada di luar daerah

atau bahkan berada di luar negeri, hal tersebut tentu mengakibatkan penyidik sulit untuk melakukan pemeriksaan saksi dan pemberkasan hasil penyelidikan. Penuntut umum juga tidak mau menerima berkas perkara yang tidak dilengkapi dengan berita acara pemeriksaan saksi khususnya saksi korban dan harus dilengkapi dengan berita acara penyumpahan saksi karena kemungkinan besar saksi tidak dapat hadir di persidangan dikarenakan jarak kediaman saksi yang cukup jauh, hal tersebut mengakibatkan kurangnya alat bukti yang sah jika berkas perkara tersebut dilimpahkan ke pengadilan untuk disidangkan sehingga terdakwa beresiko akan dinyatakan bebas, dan hal serupa dialami oleh penyidik Unit *Cyber Crime* DITRESKRIMSUS POLDA DIY dimana sangat kesulitan menangani kasus *cyber crime* terkait aspek alat bukti yang berkaitan dengan saksi-saksi, namun beda halnya ketika pelaku *cyber crime* tertangkap tangan dalam melakukan aksi kejahatannya dimana alat bukti dapat langsung diamankan oleh petugas kepolisian yang tentunya tidak terlalu membutuhkan saksi-saksi dalam hal tersebut.

Berdasarkan penjelasan diatas mengenai kendala dalam penanggulangan tindak pidana *cyber crime* dari aspek alat bukti tersebut diatas kita dapat mengetahui bagaimana dan apa- apa saja kendala yang dihadapi penyidik- penyidik di setiap Unit *Cyber Crime*, khususnya dalam hal alat bukti yang berkiatan dengan saksi- saksi yang keberadaannya tidak sama dengan korban dan atau pelaku yang

mana dari hal tersebut menjadi kendala dan membutuhkan anggaran dan cara kerja yang lebih jika dibandingkan dengan penanganan pada kasus- kasus pidana umum, tentu dalam hal ini perlu diperhatikan oleh POLRI agar kinerja penyidik-penyidik *cyber crime* dapat melakukan penaggulangan hukum dalam tindak pidana *cyber crime* secara maksimal.

3. Aspek Fasilitas

Pada tindak pidana *cyber crime* dalam mengungkap kasus-kasus *cyber crime* dibutuhkan fasilitas yang mampu menunjang kinerja aparat kepolisian/penyidik, fasilitas tersebut berupa laboratorium forensik komputer yang digunakan untuk mengungkap data-data yang bersifat digital serta merekam dan menyimpan bukti-bukti yang berupa *soft copy* (gambar, program, *html*, suara, dan lain sebagainya). Komputer forensik merupakan salah satu cabang ilmu forensik yang berhubungan dengan bukti hukum yang ditemukan dalam komputer maupun media penyimpanan secara digital. Komputer forensik dikenal sebagai digital forensik, adapun tujuannya ialah untuk mengamankan dan menganalisis bukti digital, serta memperoleh berbagai fakta yang objektif dari sebuah kejadian atau pelanggaran keamanan dari sistem informasi, berbagai fakta tersebut akan menjadi bukti yang akan digunakan dalam proses hukum.[7] Contohnya, melalui internet forensik, penyidik dapat mengetahui siapa saja orang yang mengirim *email*, kapan dan dimana keberadaan alamat

[7] Hendy Sumadi.2015. "Kendala Dalam Menanggulangi Tindak Pidana Penipuan Transaksi Elektronik Di Indonesia". *Jurnal Wawasan Hukum,* Vol. 33, Nomor 2, September 2015. Hal. 52

pengirim berdasarkan *server* pengirim, dan dalam contoh lain kita bisa melihat siapa pengunjung *website* secara lengkap dengan *informasi IP Address*, alat elektronik yang dipakainya dan keberadaannya serta kegiatan apa yang dilakukan pada *website* tersebut.[8]

Pada kenyataannya dalam hal fasilitas masih banyak mengalami masalah yang mana fasilitas yang tidak memadai sedangkan laporan dsan tindak pidana *cyber crime* terus meningkat, berdasarkan hasil wawancara dan penelitian penulis dengan salah satu penyidik di Unit *Cyber Crime* DITRESKRIMSUS POLDA DIY, yaitu dengan bapak AKP. Safpe Tambatua Sinaga, S.kom, yang mana beliau menjelaskan dalam hal keadaan fasilitas yang digunakan dalam penanganan kasus *cyber crime* dan dari puluhan POLDA dari setiap provinsi di Indonesia hanya beberapa POLDA yang sudah memiliki laboratorium digital forensik, termasuk POLDA DIY sendiri juga belum mempunyai laboratorium digital forensik, dan pada masalah ini pada prakeknya bagi POLDA- POLDA yang belum memiliki laboratorium digital forensik maka dibantu oleh POLDA-POLDA yang sudah memiliki laboratorium digital forensik, dalam hal ini agar lebih jelas penulis akan membuat daftar dalam bentuk tabel POLDA mana saja yang sudah memiliki laboratorium digital forensik yakni sebagai berikut:

[8] http://www.seputarpengetahuan.com/2014/11/komputer-forensik-pengertian-dan-tujuan diakses pada tanggal 25 Oktober 2018 Pukul 22:57 Wib

Tabel 4.2

Daftar POLDA Yang Sudah Memiliki Laboratorium Digital Forensik di Indonesia

No	Nama POLDA	TIPE/ Klasifikasi Polda	POLDA-POLDA yang Dibantu Dalam Kasus-Kasus *Cyber Crime*
1	POLDA METRO JAYA	A+ (A khusus)	Berkoordinasi dengan BARESKRIM POLRI membantu semua POLDA diseluruh wilayah hukum Indonesia yang membutuhkan bantuan terutama untuk POLDA- POLDA di Indonesia bagian timur yang belum memiliki laboratorium digital forensik.
2	POLDA SUMUT	B	Membantu semua POLDA di wilayah hukum pulau Sumatera, yaitu POLDA Aceh, Sumatera Barat, Riau, Kepri, Jambi, Bengkulu, Sumatera Selatan, Babel, dan POLDA Lampung.
3	POLDA JATENG	A	Membantu POLDA di wilayah hukum pulau Jawa bagian tengah yaitu termasuk POLDA DIY.
4	POLDA JATIM	A	Membantu semua POLRES dan POLSEK yakni instansi kepolisian bawah POLDA JATIM dan di wilayah hukum JATIM
5	POLDA BALI	A	Membantu semua POLDA di wilayah hukum Indonesia bagian tengah, yakni POLDA-POLDA yang ada di Sulawesi, Nusa Tenggara, dan Kalimantan.

(*sumber: Diolah Secara Pribadi Dari Hasil Wawancara Dengan Penyidik di Unit Cyber Crime DITRESKRIMSUS POLDA DIY*)

Berdasarkan penjelasan dari tabel tersebut kita dapat mengukur kemampuan setiap POLDA di Indonesia dalam menangani kasus- kasus tindak pidana terkhusus bagi kasus- kasus yang harus menggunakan laboratorium digital forensik dalam proses penyidikan tindak pidana *cyber crime*, yang mana pada kenyataanya dari puluhan POLDA yang ada Indonesia hanya lima POLDA yang sudah memiliki laboratorium digital forensik tentu hal ini menjadi masalah utama dalam penanggulangan tindak pidana *cyber crime.*

Fasilitas laboratorium digital forensik yang digunakan penyidik yaitu *Cyber Crime Investigation Satelit Office* (CCISO) dan *Strategic Informasi and Tactical Operation Centre (SITOC)* yang meliputi sebagai berikut:

a. Laboratorium *Cyber Crime Investigation Satelit Office (CCISO)* yang terdiri :

1) Laboratorium Komputer Forensik
2) Laboratorium *Mobile Phone* Forensik
3) Laboratorium *Audio Video* Forensik

b. Laboratorium *Strategic Informasi and Tactical Operation Centre (SITOC)* yang terdiri :

1) Laboratorium Analisis Komunikasi
2) Laboratorium Analisis Keuangan
3) Laboratorium *Command Center*

Adapun peralatan lain yang dibutuhkan oleh setiap penyidik *cyber crime*, yaitu *mobile direction finder*, *Cellebrite*, *check post*, *CDR*, *monitoring center/ monitoring social media* dan lain-lain. Semua peralatan dan laboratorium dan semua sarana prasarana juga membutuhkan akreditasi yang digunakan untuk pemeriksaan barang bukti digital.

Unit *Cyber Crime* DITRESKRIMSUS POLDA DIY, yang mana sebagai tempat penelitian penulis belum memiliki fasilitas berupa laboratorium digital forensik, yang mengakibatkan terkendalanya upaya penanggulangan *cyber crime* diwilayah hukum POLDA DIY, dalam hal ini POLDA DIY bekerja sama dengan POLDA Jawa Tengah dalam proses penyelidikan dan penyidikan yang kasus *cyber crime* tersebut memerlukan laboratorium forensik, sehingga dalam hal ini pada fakta praktek dan dilapangan masih banyak yang perlu ditingkatkan lagi dalam hal fasilitas di POLDA DIY. AKP Safpe Tambatua Sinaga, S.kom mengungkapkan bahwa fasilitas yang digunakan unit *cyber crime* POLDA DIY bukan hanya kurang memadai tetapi memang sangat tidak memadai untuk mendukung proses penanganan kasus *cyber crime* sehingga masih menjadi kendala dalam kinerja petugas kepolisian.

Berdasarkan penjelasan diatas mengenai kendala dalam penanggulangan tindak pidana *cyber crime* dari aspek fasilitas tersebut kita dapat mengetahui bagaimana dan apa-apa saja masalah yang berkaitan dengan fasilitas serta POLDA-POLDA mana saja yang sudah dan belum memiliki fasilitas lengkap khususnya fasilitas yang digunakan untuk

menangani tindak pidana *cyber crime*, yang mana dari keterbatasan fasilitas di mayoritas POLDA akan menjadi kendala dan membuat penanganan menjadi lambat dan tidak maksimal, tentu dalam hal ini perlu diperhatikan oleh pemerintah dan POLRI agar kinerja penyidik-penyidik *cyber crime* dalam tindak pidana *cyber crime* secara maksimal.

4. Aspek yurisdiksi

Pada penanggulangan tindak pidana *cyber crime* memiliki kendala dalam aspek yurisdiksi, yang mana tindak pidana *cyber crime* ini merupakan tindak pidana yang pelaku dan korban tidak hanya di negara yang sama dan juga tidak selalu berkewarganegaraan yang sama yakni tindak pidana *cyber crime* ini juga merupakan tindak pidana transnasional, pada sistem hukum pidana yang berlaku saat ini, hukum pidana pada umumnya hanya berlaku di wilayah negaranya sendiri (asas teritorial) dan untuk warga negaranya sendiri (asas personal/nasional aktif), hanya delik-delik tertentu yang dapat digunakan asas nasional pasif dan asas universal yang mana delik-delik tersebut termasuk kerjahatan *cyber crime*[9], dalam aspek yurisdiksi maka ada beberapa masalah dalam penanggulangan kejahatan *cyber crime* yakni sebagai berikut[10]:

a. Pelaku Tindak Pidana *Cyber Crime* Berkewarganegaraan Yang Tidak Menganut dan Menerapkan Hukum Yang Sama Dengan Indonesia

[9] Barda Nawawi Arief, Op. cit. Hal. 107

[10] Wawancara dengan AKP. Safpe Tambatua Sinaga (Penyidik) Unit *cyber crime* POLDA DIY, pada tanggal , 27 juni 2019 pukul 08.29 Wib

Pada kendala aspek yurisdiksi khususnya dalam hal pelaku tindak pidana *cyber crime* berkewarganegaraan yang tidak menganut dan menerapkan hukum yang sama dengan Indonesia, hal ini dalam melakukan penanggulangan kejahatan *cyber crime* yang transnasional atau lintas negara akan mengalami kesulitan, sedangkan dalam hal yurisdiksi telah diatur dalam Pasal 2 Undang-undang Nomor 19 tahun 2016 perubahan atas Undang-undang Nomor 11 tahun 2008 tentang informasi dan transaksi elektronik, yaitu: "Undang-undang ini berlaku untuk setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam undang-undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau diluar wilayah hukum indonesia dan merugikan kepentingan Indonesia".

Undang-undang ITE memiliki jangkauan yurisdiksi tidak semata-mata untuk perbuatan hukum yang berlaku di Indonesia dan atau dilakukan oleh warga negara Indonesia, tetapi juga berlaku untuk perbuatan hukum yang dilakukan di luar wilayah hukum (yurisdiksi) Indonesia baik oleh warga negara Indonesia (WNI) maupun warga negara asing (WNA) atau badan hukum Indonesia maupun badan hukum asing yang memiliki akibat hukum di Indonesia, mengingat pemanfaatan teknologi informasi untuk informasi dan transaksi elektronik dapat bersifat lintas teritorial atau universal. Yang dimaksud dengan "meugikan kepentingan indonesia" adalah meliputi tetapi tidak

terbatas pada merugikan kepentingan ekonomi nasional, perlindungan data strategis, harkat dan martabat bangsa, pertahanan dan keamanan negara, kedaulatan negara, warga negara, serta badan hukum Indonesia. Adapun beberapa hal yang mana di Indonesia di larang di undang-undang ITE namun di beberapa negara-negara tidak melarangnya yakni sebagai berikut:

1) Pornografi *Online*

   Pada tindakan pornografi online di Indonesia dilarang pada undang- undang ITE tepatnya pada pasal 27 ayat (1) UU ITE, namun masih banyak negara- negara yang melegalkan pornografi yaitu, Amerika serikat, Belanda, Kolombia, Uruguay, Kanada, Spanyol, dan lainnya, maka dalam hal ini jika korban berkewarganegaraan WNI dan pelakunya berkewarganegaraan dari negara- negara tersebut dalam hal pornografi maka susah ditindak secara hukum.

2) Penistaan Agama

   Pada tindakan menistakan agama juga menjadi rumit yang mana di Indonesia dilarang pada undang- undang ITE tepatnya pada pasal 28 ayat (2) UU ITE, namun masih banyak negara- negara yang tidak melarang dalam hal penistaan agama yaitu, Amerika serikat, Korea Selatan,Vietnam, Kanada, dan lainnya, maka dalam hal ini jika korban atau yang merasa dirugikan berkewarganegaraan WNI

dan pelakunya berkewarganegaraan dari negara- negara tersebut dalam hal pornografi maka susah ditindak secara hukum.

Berdasarkan penjelasan tersebut diatas dapat diketahui mengenai kendala yang dihadapi oleh penyidik dalam aspek yurisdiksi khususnya mengenai pelaku tindak pidana *cyber crime* yang yang melakukan hal-hal yang di Indonesia dilarang namun dinegaranya tidak dilarang maka dalam penanganan kasus-kasus *cyber crime* yang berkaitan dengan hal tersebut susah untuk lakukan proses hukum.

b. Pelaku Tindak Pidana *Cyber Crime* Berkewarganegaraan Yang Tidak Ada Hubungan Diplomatik Dengan Indonesia

Pada kendala aspek yurisdiksi khususnya dalam hal pelaku tindak pidana *cyber crime* berkewarganegaraan yang tidak ada hubungan diplomatik dengan indonesia, hal ini dalam melakukan penanggulangan kejahatan *cyber crime* yang transnasional atau lintas negara akan mengalami kesulitan, terutama pada kasus *hacking* yang mana pada tindak pidana tersebut sepakat semua negara didunia melarang dan masing- masing dinegaranya membuat hukum untuk mengatur dan melindungi warga negaranya dan negaranya masing-masing tentunya, namun dalam hal ini penyidik akan mengalami kesulitan jika menangani kasus tindak pidana *hacking* yang mana korbannya adalah WNI atau badan hukum di negara Indonesia namun pelakunya berkewarganegaraan yang tidak ada hubungan diplomatik dengan Indonesia, maka dalam hal ini akan menjadi kendala penyidik

cyber crime dalam melakukan proses hukum, adapun beberapa negara yang tidak ada hubungan diplomatik dengan negara Indonesia adalah:

1) Israel
2) Makau
3) Korea Utara
4) Georgia

Pada kendala ini tentu pemerintah Indonesia perlu mempertimbangkan hal-hal yang membuat penyidik *cyber crime* Indonesia dapat melakukan tindakan dengan cepat mengingat dalam tindak pidana *cyber crime* alat bukti/ jejak digitalnya dapat dihilangkan secara singkat dan pelaku tindak pidana *cyber crime* tersebut dapat lepas begitu saja tanpa terjerat hukum, khususnya dalam masalah ini yaitu dalam kasus *hacking* yang mana dari tindakan peretasan dalam menimbulkan kerugian korban yang mana korban tidak hanya orang secara pribadi tapi negara.

Berdasarkan penjelasan-penjelasan mengenai berbagai kendala yang dihadapi oleh aparat penegak hukum atau penyidik dalam upaya penanggulangan kejahatan dunia maya *(cyber crime)*, dapat dibagi menjadi empat masalah/ kendala yang mana mulai dari kendala dalam aspek penyidik, aspek alat bukti, aspek fasilitas, dan aspek yurisdiksi, dari masalah-masalah tersebut tentunya mengakibatkan efek buruk pada proses penegakan hukum dalam tindak pidana *cyber crime* khususnya dalam tahapan penyelidikan dan

penyidikan, maka dari hal-hal tersebut POLRI dan pemerintah harus lebih memikirkan dan meminimalis masalah-masalah yang sudah ada agar para penyidik *cyber crime* dapat melakukan tugasnya dengan baik dan profesional.