PENEGAKAN HUKUM OLEH APARAT PENYIDIK *CYBER CRIME* DALAM KEJAHATAN DUNIA MAYA (*CYBER CRIME*) DI WILAYAH HUKUM POLDA DIY

Prasetiyo dan Mukhtar Zuhdy

Program Studi Ilmu Hukum Fakultas Hukum

Universitas Muhammadiyah Yogyakarta

Jalan Brawijaya, Tamantirto, Kasihan, Bantul, Yogyakarta

55183

prasetiyo.2015@law.umy.ac.id; mukhtarzuhdy@umy.ac.id

Abstrak

Kejahatan *cyber crime* saat ini sering terjadi dan korbannya tidak hanya orang, tetapi lembaga/instansi, bahkan Negara, hal ini dikarenakan perkembangan teknologi informasi dan internet yang cepat dan keterikatan manusia akan teknologi informasi, dari hal tersebut menimbulkan kejahatan teknologi dengan berbagai kepentingan. Pada tindak pidana *cyber crime* khususnya dalam penegakan hukumnya masih terdapat kendala-kendala yang mana dari faktor internal dan faktor eksternal penyidik *cyber crime*. Penulis melakukan penelitian hukum normatif dan penelitian dengan metode pengumpulan data study pustaka dan wawancara dengan Penyidik *cyber crime*. Hasil dari penelitian ini, yaitu dalam hal kendala penyelidikan dan penyidikan tindak pidana *cyber crime* yaitu ada beberapa aspek yakni aspek penyidik, alat bukti, fasilitas pendukung dan yurisdiksi, dalam hal proses penyelidikan dan penyidikan yaitu dalam hal hukum materil pada tindak pidana *cyber crime* diatur secara khusus yakni undang-undang Nomor 19 tahun 2016 tentang perubahan atas undang- undang Nomor 11 tahun 2008 tentang ITE, kesimpulan dalam hal kendala dalam penegakan hukum tindak pidana *cyber crime* yaitu dapat dibagi menjadi dua faktor yakni faktor internal dan eksternal penyidik *cyber crime*.

Kata Kunci : *cyber crime*, kendala penyidikan, penegakan hukum.

I. PENDAHULUAN

Perkembangan teknologi yang sangat cepat dan kebutuhan setiap orang yang semakin terbuka terhadap teknologi dari waktu ke waktu, dan dari hal tersebut banyak pihak-pihak yang berniat jahat untuk menyalahgunakan teknologi informasi dengan berbagai alasan dan tujuan tertentu.[1] Penggunaan internet yang canggih dan cepat tersebut memunculkan pula kejahatan yang sangat canggih dan sulit untuk diketahui pelakunya, hal ini disebabkan karena internet merupakan suatu media komunikasi yang tidak terlihat (maya), sehingga pelaku kejahatan dapat dengan mudah menghilangkan jejak tanpa dapat diketahui dengan jelas tujuan dan motif dari kejahatan yang dilakukan.

Tindak pidana *cyber crime* ini tidak sesederhana seperti yang kita ketahui khususnya dalam proses penegakan hukumnya, mulai dari undang-undang yang mengatur mengenai kejahatan *cyber crime,* hingga Pengadilan Negeri mana yang berwenang untuk mengadili perkara tersebut dan Badan Pengadilan yang mana yang berwenang mengadili perkara tersebut, dan tidak hanya itu saja tindak pidana *cyber crime,* sering kali kita menganggap bahwa hal tersebut kejahatan diruang lingkup pidana tetapi dalam kenyataanya tidak demikian, karena tindak pidana *cyber crime* ini selain diatur dalam KUHP, dan undang- undang nomor 19 tahun 2016 tentang perubahan undang-undang nomor 11 tahun 2008 Tentang Informasi Dan Transasksi Elektronik, ternyata beberapa pasal di KUH. Perdata juga mengatur khususnya mengenai perbuatan melawan hukum seperti “penghinaan”/pencemaran nama baik, walaupun dalam hal ini

[1] Maksun. 2013. *Kejahatan Siber Cyber Crime Suatu Pengantar*. Jakarta: Kencana, Hal. 2.

penulis tidak akan membahas proses hukum secara perdata namun penulis hanya ingin menjelaskan mengenai seberapa luas ruang lingkup tindak pidana *cyber crime* ini dan bagaimana mekanisme yang dilakukan oleh penegak hukum (Penyidik) dalam penanganan kejahatan *cyber crime* tersebut dan apa saja kendala yang dihadapi oleh Penyidik dalam penanggulangan kejahatan *cyber crime*. Maka dari itu penulis berharap setelah mengkaji dan melakukan penelitian terkait penentuan tempat dan waktu kejadian oleh penyidik dalam kejahatan dunia maya (*cyber crime*) yang akan melakukan penelitian di POLDA DIY akan mempermudah dan membantu serta memberikan sumbangsih bagi pengembangan ilmu hukum di bidang pidana khususnya mengenai *cyber crime,* dan juga memberi pengetahuan dalam hal mekanisme penentuan tempat dan waktu kejadian oleh penyidik dalam kejahatan *cyber crime* dan juga mengenai kendala yang dihadapi oleh penyidik dalam upaya penanggulangan kejahatan *cyber crime.*

Penanggulangan tindak pidana *cyber crime* sampai saat ini masih terdapat kendala-kendala yang dihadapi oleh kepolisian dalam menjalankan tugasnya, khususnya terhadap pelaksanaan peran laboratorium forensik POLRI sebagai pendukung penyidik secara ilmiah dalam sistem pradilan pidana di Indonesia.[2] Kendala-kendala yang dihadapi yaitu mengenai keterbatasan personil, keterbatasan penyidik dalam hal teknologi informasi, fasilitas yang belum memadai dan tidak *upto date* yang mana juga mempengaruhi hasil kerja dan pemeriksaan seperti laboratorium digital forensik masih sangat terbatas

[2] Sandi Oktaplandi, 2017, "Kendala Kepolisian Dalam Upaya Penanggulangan Tindak Pidana Cyber Crime di Indonesia", *E-Jurnal Gloria Yuris fakultas hukum UNTAN*, Vol. 5, Nomor 4, Februari 2017. Hal. 8- 10.

yang dimiliki oleh POLDA-POLDA di Indonesia , anggaran yang terbatas dan lain sebagainya yang mana hal ini perlu diperhatikan oleh Pemerintah demi kemajuan kinerja kepolisian Republik Indonesia, maka dari itu penulis sangat tertarik untuk melakukan penelitian bagaimana kenyataan dilapangan yang dihadapi kepolisian secara nyata dalam penanggulangan tindak pidana *cyber crime* .[3]

Perbuatan melawan hukum di dunia maya merupakan fenomena yang sangat mengkhawatirkan, mengingat tindakan *carding*, *hacking*, penipuan, terorisme dan penyebaran informasi destruktif telah menjadi bagian dari aktivitas kejahatan di dunia maya. Kenyataannya demikian sangat kontras dengan ketiadaan regulasi yang mengatur pemanfaatan teknologi informasi dan komunikasi di berbagai sektor, oleh karena itu untuk menjamin kepastian hukum, pemerintah berkewajiban melakukan regulasi terhadap berbagai aktivitas terkait dengan pemanfaatan teknologi informasi dan komunikasi tersebut.[4]

Ditinjau dari perspektif hukum pidana, upaya penanggulangan *cyber crime* dapat dilihat dari berbagai aspek, yaitu antara lain dari aspek kebijakan kriminalisasi (formulasi tindak pidana), aspek pertanggungjawaban pidana atau pemidanaan (termasuk aspek alat bukti/pembuktian), dan aspek jurisdiksi yang mana hal tersebut dapat membantu dalam hal penanggulangan *cyber crime*. Kegiatan siber tidak lagi sederhana, karena kegiatannya ini tidak lagi dibatasi

[3] Teguh Pihmono, 2018, " Peran Laboratorium Forensik POLRI Sebagai Pendukung Penyidik Secara Ilmiah Dalam Sistem Pradilan di Indonesia", *Juranal hukum khaira ummah*, Vol. 13, Nomor 1, Maret 2018, Hal. 10-11.
[4] Sunarso, Siswanto, 2009, *Hukum Informasi dan Transaksi Elektronik: Studi Kasus Prita Mulya Sari*, Jakarta: Rineka Cipta. Hal 40.

oleh teritorial suatu negara, yang mudah diakses kapanpun, dan dimanapun. Kerugian dapat terjadi, baik pada pelaku transaksi, maupun pada orang lain yang tidak melakukan transaksi di internet. Pembuktian merupakan hal yang sangat penting, mengingat informasi elektronik belum terakomodasi dalam sistem hukum acara di Indonesia secara komprehensif, dan ternyata juga sangat rentan untuk diubah, disadap, dipalsukan, dan dikirim ke berbagai penjuru dunia dalam waktu yang sangat singkat, dengan demikian dampak yang diakibatkannya bisa sangat kompleks dan rumit.

II. RUMUSAN MASALAH

1. Apa kendala yang dihadapi oleh aparat penyidik *cyber crime* dalam upaya penanggulangan kejahatan dunia maya *(cyber crime)* ?

III. METODE PENELITIAN

Metode yang digunakan adalah metode penelitian normatif yang merupakan prosedur penelitian ilmiah untuk menemukan kebenaran berdasarkan logika keilmuan hukum dari sisi normatifnya. Penelitian ini menitikberatkan pemakaian bahan pustaka dan data sekunder. Data sekunder tersebut terdiri atas bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier.[5] Bahan hukum primer diperoleh melalui Kitab Undang-undang Hukum Pidana, Kitab Undang-Undang Hukum Acara Pidana, Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi

[5] Mukti Fajar, 2010, *Dualisme Penelitian Hukum Normatif & Empiris*, Yogyakarta: Pustaka Pelajar.

Elektronik, dan peraturan lain yang terkait. Bahan hukum sekunder adalah semua dokumen yang merupakan informasi, atau kajian yang berkaitan dengan penelitian ini, yaitu seminar-seminar, jurnal-jurnal hukum, majalah-majalah, artikel-artikel, karya tulis ilmiah, dan beberapa sumber dari internet dan bahan hukum tersier adalah bahan hukum yang memberikan petunjuk atau penjelasan bermakna terhadap bahan hukum primer dan sekunder seperti kamus dan ensiklopedia yang relevan.

IV. HASIL PENELITIAN

A. 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

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

diperhatikan karena sangat berpengaruh untuk mengungkap kasus-kasus *cyber crime* yang dilaporkan oleh masyarakat, adanya unit *cyber crime* di lingkungan kepolisian membuktikan bahwa dibutuhkannya penyidik khusus yang memiliki kemampuan di bidang informasi dan transaksi 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 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 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, kemampuan bahasa inggris, kemampuan komputer forensik, kemampuan *mobile* forensik, kemampuan analisis jaringan transaksi keuangan dan komunikasi, dan kemampuan *cyber law*.

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

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.

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*.

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.

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 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] Melalui internet forensik, penyidik dapat mengetahui siapa saja orang yang mengirim *email*, kapan dan dimana keberadaan alamat 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]

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, 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:

[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

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

Tabel 1

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.

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].

Berdasarkan aspek yurisdiksi sesuai dengan hasil wawancara kepada penyidik *cyber crime* POLDA DIY yaitu AKP. Safpe Tambatua Sinaga 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

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

[9] Barda Nawawi Arief.2008.*Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime di Indonesia*. Jakarta: Raja Grifindo Persada. Hal. 107

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

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. 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.

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.

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

Pada kendala aspek yurisdiksi khususnya dalam hal ini untuk melakukan penanggulangan kejahatan *cyber crime* yang transnasional akan mengalami kesulitan, terutama pada kasus *hacking* yang mana pada tindak pidana tersebut sepakat semua negara didunia melarang dan masing-masing di negaranya membuat hukum untuk mengatur dan melindungi warga negaranya dan negaranya masing-masing, 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, Israel, Makau, Korea Utara, Georgia, dan lainnya.

Pada kendala ini tentu pemerintah Indonesia perlu mempertimbangkan hal-hal yang membuat penyidik *cyber crime* di 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.

V. SIMPULAN dan SARAN

A. Kesimpulan

Berdasarkan hasil penelitian dan pembahasan yang telah diuraikan, maka dapat dikemukakan beberapa kesimpulan yaitu:

1.Kendala-kendala yang dihadapi oleh kepolisian/penyidik dalam penegakan hukum tindak pidana *cyber crime* ini ada beberapa aspek yaitu :

a. Aspek Penyidik (Sumber Daya Manusia)

Pada kendala aspek penyidik ini yakni mengenai kemampuan penyidik/ skill penyidik dan juga dalam hal kemampuan personil penyidik secara jumlah pada ruang lingkup tindak pidana *cyber crime*, yang mana dalam hal kendala aspek penyidik ini dibagi menjadi dua kendala yaitu:

1). Kendala Kualitas Penyidik, dan

2). Kendala Kuantitas/Jumlah Personil Penyidik

b. Aspek Alat Bukti

Pada kendala aspek alat bukti ini yakni mengenai masalah yang dihadapi oleh penydik *cyber crime* dalam hal alat bukti yang pada

tindak pidana *cyber crime* yang mana alat bukti pada tindak pidana *cyber crime,* yang mana dalam hal barang bukti yang berbentuk digital, pelaku melakukan kejahatan dengan menggunkan peralatan/fasilitas umum, dan juga dalam hal keberadaan para saksi yang sering tidak pada tempat yang sama dengan korban dan atau pelaku, maka dalam hal kendala aspek alat bukti ini dibagi menjadi tiga yaitu:

1) Barang Bukti Digital Dihilangkan Jika Tidak Ditangani Dengan Tepat Waktu
2) Pelaku Menggunakan Fasilitas Umum Dalam Melakukan Tindak Pidana *Cyber Crime*
3) Keberadaan Para Saksi Tidak di Tempat yang Sama dengan Korban dan Pelaku

c. Aspek Fasilitas

Pada kendala aspek fasilitas ini yakni mengenai keterbatasan fasilitas pendukung penyidik *cyber crime* dalam melakukan penanggulangan tindak pidana *cyber crime* terutama dalam hal fasilitas laboratorium digital forensik, yang mana mayoritas POLDA-POLDA di seluruh Indonesia belum memiliki fasilitas ini, yakni yang POLDA-POLDA sudah memiliki laboratorium digial forensik di Indonesia hanya lima POLDA yaitu, POLDA METROJAYA, POLDA SUMUT, POLDA JATNG, POLDA JATIM, dan POLDA BALI.

d. Aspek yurisdiksi

Pada kendala aspek yurisdiksi ini yakni mengenai masalah penyidik *cyber crime* dalam melakukan penyelidikan dan penyidikan yang mana khusunya pada tindak pidana *cyber crime* yang transnasional, dalam kendala aspek yurisdiksi ini dapat dibagi menjadi dua kendala yaitu:

1) Pelaku Tindak Pidana *Cyber Crime* Berkewarganegaraan Yang Tidak Menganut dan Menerapkan Hukum Yang Sama Dengan Indonesia
2) Pelaku Tindak Pidana *Cyber Crime* Berkewarganegaraan Yang Tidak Ada hubungan Diplomatik Dengan Indonesia

B. Saran

1. POLRI diharapkan memperhatikan setiap Polda-Polda yang ada di semua provinsi seluruh Indonesia dalam hal sumber daya manusia dan fasilitas kerja, dikarenakan dalam tindak pidana *cyber crime* ini yang dihadapi adalah sebagian besar adalah pelaku-pelaku yang handal dalam teknologi informasi dan menggunakan peralatan dan sistem yang canggih pula.
2. POLRI diharapkan mengatur, membatasi dan mengawasi setiap warung internet, karena dari warung internet yang bebas dan tanpa ada standar tertentu, misalnya minimal harus memiliki kamera/CCTV aktif 24 jam, membatasi dalam akses internet pada situs- situs tertentu yang berbahaya dan lain sebagainya, hal tersebut agar setiap warung internet tidak menjadi sarang/tempat pelaku-pelaku tindak pidana *cyber crime.*

DAFTAR PUSTAKA

Buku :

Barda Nawawi Arief, 2008, *Tindak Pidana Mayantara*: *Perkembangan Kajian Cyber Crime di Indonesia*, Jakarta: Raja Grfindo Persada.

Maksun, 2013, *Kejahatan Siber Cyber Crime Suatu Pengantar*, Jakarta: Kencana.

Mukti Fajar, 2010, *Dualisme Penelitian Hukum Normatif & Empiris*, Yogyakarta: Pustaka Pelajar.

Sunarso, Siswanto, 2009, *Hukum Informasi dan Transaksi Elektronik: Studi Kasus Prita Mulya Sari*, Jakarta: Rineka Cipta.

Jurnal :

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

Sandi Oktaplandi, 2017, "Kendala Kepolisian Dalam Upaya Penanggulangan Tindak Pidana *Cyber Crime* di Indonesia*", E-Jurnal Gloria Yuris fakultas Hukum UNTAN*, Vol. 5, Nomor 4, Februari 2017.

Teguh Pihmono, 2018, "Peran Laboratorium Forensik POLRI Sebagai Pendukung Penyidik Secara Ilmiah Dalam Sistem Pradilan di Indonesia*", Jurnal Hukum Khaira Ummah*, Vol. 13, Nomor 1, Maret 2018.

Peraturan Perundang-Undangan:

Kitab Undang-Undang Hukum Pidana (KUHP).

Undang-Undang Nomor 8 Tahun 1981 Tentang Hukum Acara Pidana (KUHAP).

Undang-Undang RI Nomor 19 Tahun 2016 perubahan atas Undang- undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik**.**

Undang-Undang RI Nomor 2 Tahun 2002 Tentang Kepolisian Negara Republik Indonesia.

Peraturan Pemerintah RI Nomor 23 Tahun 2007 tentang Daerah Hukum Kepolisian Negara Republik Indonesia.

Peraturan Kepala Kepolisian Negara RI Nomor 14 Tahun 2012 Tentang Manajemen Penyidikan Tindak Pidana.

Peraturan Menteri KOMINFO Nomor 7 Tahun 2016 Tentan Administrasi Penyidikan Dan Penindakan Tindak Pidana Teknologi Informasi Dan Transaksi Elektronik.

Internet:

Sucipto, *komputer forensik*. http://www.seputarpengetahuan.com/2014/11/komputer-forensik-pengertian-dan-tujuan. Diakses pada tanggal 25 Oktober 2018, Pukul 22:57 Wib.

Wawancara:

Sinaga, Safpe Tambatua, 2019, *"Penyelidikan, Penyidikan Tindak Pidana Cyber Crime"*, Hasil Wawancara Pribadi: 27 Juni 2019, Unit *Cyber Crime* DITRESKRIMSUS POLDA DIY.