

KEBIJAKAN KRIMINAL PENANGANAN KEJAHATAN MAYANTARA PADA SATUAN RESERSE KRIMINAL ACEH TENGGARA

Rivandioza

Pascasarjana UMSU/Unit I Tindak Pidana Umum Polres Aceh Tenggara

Email: rivandioza@gmail.com

Abstrak

Kejahatan mayantara merupakan kejahatan jenis baru yang melibatkan perangkat komputer dan fasilitas internet. Kejahatan jenis baru tentu saja membutuhkan regulasi baru agar kejahatan mayantara tersebut dapat tertangani dengan baik dan bijaksana. Terbentuknya regulasi baru tersebut, memberikan sebuah kebijakan kriminal untuk memberikan rasa aman dan nyaman bagi pemakai fasilitas internet. Beberapa kasus di Aceh Tenggara terkait dengan kejahatan mayantara telah tertangani dengan baik. Kasus kejahatan mayantara yang terjadi di Aceh Tenggara itu, merupakan cerminan, bahwa sebagian masyarakat masih belum mampu memanfaatkan fasilitas internet untuk sesuatu yang sifatnya positif. Perlu adanya edukasi yang lebih masif, agar masyarakat bijak memanfaatkan internet itu. Meskipun terdapat beberapa hambatan dan kendala dalam menyelesaikan kasus pidana mayantara tersebut, namun reserse kriminal Aceh Tenggara dapat menyelesaikan kasus tersebut dengan baik.

Kata kunci: kebijakan, kriminal, kejahatan, mayantara

1. PENDAHULUAN

Teknologi informasi dan media elektronika telah mengubah perilaku masyarakat dan peradaban manusia secara global. Perpaduan antara media elektronika dan teknologi informasi telah memacu percepatan globalisasi yang mana dunia menjadi tanpa batas (*borderless*) dan menyebabkan perubahan sosial yang secara signifikan berlangsung dengan cepat.

Teknologi informasi saat ini menjadi pedang bermata dua, karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan peradaban dunia, sekaligus menjadi sarana efektif perbuatan melawan hukum. (Ramli, 2004: 1). Teknologi informasi dan media elektronika menjadi simbol pelopor yang akan mengintegrasikan seluruh sistem dunia, baik dalam aspek sosial, budaya, ekonomi dan keuangan. Dari sistem-sistem kecil lokal dan nasional, proses globalisasi dalam tahun tahun terakhir bergerak cepat, bahkan terlalu cepat menuju suatu sistem global. Dunia akan menjadi (*global village*) yang menyatu, saling mengetahui dan terbuka, serta sangat bergantung satu sama lain.

Internet membawa manusia kepada ruang atau dunia baru yang tercipta yang dinamakan *Cyberspace*. *Cyberspace* adalah sebuah dunia komunikasi berbasis komputer (*Computer Mediated Communication*) yang menawarkan realitas virtual (*virtual reality*).

Cyberspace yang memberi harapan akan kemudahan bertransisi di dunia tanpa batas itu ternyata tidak selamanya demikian karena dalam *cyberspace* juga terdapat sisi gelap yang perlu diperhatikan yang dikarenakan oleh rasa keingintahuan pengguna internet menimbulkan

kecemasan atas terjadinya penyimpangan atau penyalahgunaan jaringan internet tersebut yang dikenal dengan istilah *cybercrime* atau kejahatan mayantara yang telah menjadi perhatian dunia.

Penanganan dengan hukum pidana merupakan salah satu cara yang dapat dipergunakan untuk mengatasi jenis kejahatan baru ini terutama dengan kebijakan kriminalisasi yang tepat dengan memperhatikan segala aspek mulai dari pertanggung-jawaban pidana, aspek yurisdiksi, pemidanaan sampai dengan perbaikan terhadap ketentuan perundang-undangan yang sudah ada, dan penyusunan undang-undang khusus mengenai tindak pidana (*cyber crime*).

2. METODE PENELITIAN

Cyber Crime dalam Perspektif Aturan Perundang-undangan di Indonesia

Cyber crime atau kejahatan mayantara adalah penggunaan jaringan komputer dengan segala macam cara atau metode yang bertujuan kriminal dan/atau kriminal yang menggunakan teknologi tinggi dengan menyalahgunakan teknologi digital. (Wahid & Labib, 2005: 103).

Kejahatan mayantara adalah suatu kejahatan yang dilakukan baik oleh seseorang, sekelompok orang dan korporasi (badan hukum) dengan cara menggunakan atau dengan sarana komputer atau sistem komputer atau jaringan komputer. Kejahatan mayantara sesuai dengan namanya terjadi di dunia maya (virtual) sehingga memiliki karakteristik yang berbeda dengan kejahatan yang sifatnya tradisional. (Ali, 2012: 4).

Kejahatan komputer atau kejahatan mayantara adalah upaya untuk memasuki dan

atau menggunakan komputer atau fasilitas jaringan komputer tanpa izin dan dengan melanggar hukum dengan atau tanpa menyebabkan perubahan dan atau kerusakan pada fasilitas komputer yang dimasukkan atau digunakan. Kejahatan mayantara mencakup potensi kegiatan ilegal, yang pada umumnya kejahatan ini dibagi menjadi dua kategori, yaitu (1) kejahatan yang menjadi jaringan komputer dan divais secara langsung menjadi target; (2) kejahatan yang berhubungan dengan jaringan komputer atau divais, dengan target utamanya adalah jaringan komputer independen atau *device*. (Sumarwani, 2014: 288)

Pada dasarnya, kejahatan dunia maya atau apa yang sering disebut sebagai kejahatan dunia maya adalah kejahatan pada umumnya, tetapi perbedaannya adalah bahwa kejahatan tersebut dilakukan di media teknologi canggih saat ini. Ada hal yang membedakannya adalah *tempus* dan *locus delicti* dari kejahatan ini. Munculnya fenomena baru ini bagi sebagian orang telah mengubah perilaku mereka dalam berinteraksi dengan manusia lain, yang terus menyebar ke bagian lain kehidupan manusia, sehingga menciptakan norma-norma baru, nilai-nilai baru dan sebagainya.

Kejahatan mayantara tidak akan terlepas dari apa yang disebut dengan internet. Agus Raharjo mengatakan bahwa internet sebagai suatu jaringan komputer antarnegara atau antarbenua yang berbasis *Protocol Transmission Control/Internet protocol (TCP/IP)*. (2002: 59).

Sampai saat ini istilah “*cyber crime*” belum ada kesatuan pendapat bahkan tidak ada pengakuan internasional mengenai istilah baku, tetapi ada yang menyamakan istilah *cyber crime* dengan *computer crime*”. Demikian juga sampai saat ini belum ada istilah baku atau definisi secara yuridis untuk menunjuk jenis kejahatan ini, dan lebih dikenal sebagai *cyber crime*.

Berdasarkan modus operandinya, *cyber crime* terdiri dari dua jenis kejahatan, yaitu:

1. Kejahatan yang sasaran/targetnya adalah fasilitas serta sistem teknologi komunikasi informasi. Para pelaku menggunakan sarana ini untuk menyerang atau merusak sarana teknologi informasi lainnya yang menjadi target. Pada posisi ini komputer/internet adalah alat sekaligus korban kejahatan. Kejahatan ini lebih dikenal *hacking/cracking* yang menyerang program-program operasi jaringan komputer. Ini mempunyai sifat sebagai kejahatan baru (*new category of crime*).
2. Kejahatan umum/biasa yang difasilitasi oleh teknologi komunikasi informasi. Jenis kejahatan ini telah ada sebelum

teknologi informasi bergerak menuju kearah penyalahgunaannya, contohnya penipuan kartu kredit, pencemaran nama baik, terorisme, pornografi dan sebagainya. Ini merupakan kejahatan yang bersifat biasa (*Ordinary crime*) yang pengaturannya telah terdapat dalam KU *crime* lainnya yakni, *cybercrime* dirumuskan sebagai perbuatan melawan hukum yang dilakukan dengan memakai jaringan komputer sebagai sarana/ alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. (Wahid, 2005: 50)

Walaupun kejahatan dunia maya atau *cyber crime* umumnya mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer sebagai unsur utamanya, istilah ini juga digunakan untuk kegiatan kejahatan tradisional dimana komputer atau jaringan komputer digunakan untuk mempermudah atau memungkinkan kejahatan itu terjadi. Selain pendapat kedua pakar tersebut, masih banyak pakar yang memberikan pengertian mengenai kejahatan *siber*. Namun sebagian besar belum menetapkan batas-batas yang jelas antara kejahatan *siber* dan kejahatan komputer.

Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis utama komputer dan jaringan telekomunikasi ini, banyak klasifikasi pengelompokan mengenai kejahatan *cyber crime*, dalam beberapa literatur dan praktiknya dikelompokkan dalam beberapa bentuk yang di jelaskan oleh Nawawi Arief, (2006: 13-14) antara lain:

1. *Unauthorized access to computer system and service*
Kejahatan yang dilakukan dengan memasuki/menyusup kedalam suatu sistem jaringan secara tidak sah tanpa ijin atau tanpa sepengetahuan dari pemilik sistem komputer yang dimasuki.
2. *Illegal Contents*
Merupakan kejahatan dengan memasukan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum.
3. *Dataforgery*
Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai scriptless document melalui internet.
4. *Cyber Expionage*
Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan

mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (computer network sistem).

5. *Cyber Sabotage and Extortion*

Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.

Berdasarkan beberapa literatur yang di jelaskan dalam bukunya Abdul Wahid (2005:76), bahwa Ari Juliano Gema berpendapat dalam prakteknya, *cyber crime* memiliki karakter yang khas dibandingkan kejahatan konvensional, antara lain:

1. Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis tersebut terjadi di ruang/wilayah maya (*cyberspace*), sehingga tidak dapat dipastikan yurisdiksi hukum negara mana yang berlaku terhadapnya;
2. Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang bisa terhubung dengan internet;
3. Perbuatan tersebut mengakibatkan kerugian materil maupun immateril (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan kejahatan konvensional;
4. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya;
5. Perbuatan tersebut seringkali dilakukan secara transnasional/melintasi batas negara.

Cyber crime memiliki ciri-ciri khusus yaitu :

1. *Non-violence* (tanpa kekerasan);
2. Sedikit melibatkan kontak fisik;
3. Menggunakan peralatan (*equipment*) dan teknologi;
4. Memanfaatkan jaringan telematika (telekomunikasi, media dan informatika) global. (Nitibaskara, 2001: 45)

Apabila mengikuti kasus-kasus *cyber crime* yang terjadi dan jika hal tersebut dikaji dengan menggunakan kriteria hukum pidana konvensional, maka hukum *cyber crime* bukanlah kejahatan yang sederhana. Untuk menjerat pelaku kejahatan melalui internet, Tim penyusun RUU KUHP juga telah berusaha memasukkan pasal-pasal baru untuk menghadapi masalah *cyber crime* yaitu Pasal 188 untuk data komputer, Pasal 189 untuk terminal komputer, Pasal 190 untuk akses ke sistem komputer dan Pasal 191 tentang jaringan telepon yang termasuk jaringan komputer.

Barda Nawawi Arief (2003: 224) telah menyarikan delik-delik menjadi:

1. Delik terhadap kerahasiaan, integritas, dan ketersediaan data dan sistem computer termasuk disini:
 - a. mengakses sistem komputer tanpa hak (*illegal access*);
 - b. tanpa hak menangkap/mendengar pengiriman dan pemancaran (*illegal interception*)
 - c. tanpa hak merusak data (*data interference*);
 - d. tanpa hak mengganggu sistem (*system interference*);
 - e. menyalahgunakan perlengkapan (*misuse related of devices*)
2. Delik-delik yang berhubungan dengan komputer (pemalsuan dan penipuan dengan komputer; *computer related offences; forgery and fraud*).
3. Delik-delik yang bermuatan pornografi anak (*conten related offences*).
4. Delik-delik yang berhubungan dengan hak cipta.

Jika dilihat dalam peraturan perundang-undangan yang konvensional, maka perbuatan pidana yang dapat digunakan dibidang *cyber crime* adalah; penipuan, kecurangan, pencurian dan perusakan, yang dilakukan secara langsung (dengan menggunakan bagian tubuh secara fisik dan pikiran) oleh si pelaku. Sementara itu jika hal tersebut dilakukan dengan memanfaatkan sarana komputer, maka *cyber crime* dapat berbentuk sebagai berikut (Arief, 2005: 8):

1. Penipuan komputer (*computer fraud*) yang mencakup:
 - a. Bentuk dan jenis penipuan adalah berupa pencurian uang atau harta benda dengan menggunakan komputer/siber dengan melawan hukum, ialah dalam bentuk penipuan data dan penipuan program, yang terinci adalah:
 - 1) Memasukkan intruksi yang tidak sah, ialah dilakukan oleh seorang yang berwenang atau tidak, yang dapat mengakses suatu sistem dan memasukkan instruksi untuk keuntungan sendiri dengan melawan hukum (transfer).
 - 2) Mengubah data input, yang dilakukan seseorang dengan cara memasukkan data untuk menguntungkan diri sendiri atau orang lain dengan cara melawan hokum (memasukkan daftar gaji pegawai melebihi yang seharusnya).
 - 3) Merusak data, dilakukan seseorang untuk merusak *print-out* atau

- output* dengan maksud untuk mangaburkan, menyembunyikan data atau informasi dengan itikad tidak baik.
- 4) Penggunaan komputer untuk sarana melakukan perbuatan pidana, ialah dalam pemecahan informasi melalui komputer yang hasilnya digunakan untuk melakukan kejahatan, atau mengubah program.
 - b. Perbuatan pidana penipuan, yang sesungguhnya dapat termasuk unsur perbuatan lain, yang pada pokoknya dimaksudkan menghindarkan diri dari kewajiban (pajak) atau untuk memperoleh sesuatu yang bukan hak/milikinya melalui sarana komputer.
 - c. Perbuatan curang untuk memperoleh secara tidak sah harta benda milik orang lain, misalnya seseorang yang dapat mengakses komputer mentransfer rekening orang ke rekeningnya sendiri, sehingga merugikan orang lain.
 - d. Konspirasi penipuan, ialah perbuatan pidana yang dilakukan beberapa orang bersama-sama untuk melakukan penipuan dengan sarana komputer.
 - e. Pencurian ialah dengan sengaja mengambil dengan melawan hukum hak atau milik orang lain dengan maksud untuk dimilikinya sendiri.
2. Perbuatan pidana penggelapan, pemalsuan pemberian informasi melalui komputer yang merugikan pihak lain dan menguntungkan diri sendiri.
 3. *Hacking*, ialah melakukan akses terhadap sistem komputer tanpa seizin atau dengan melawan hukum sehingga dapat menembus sistem, pengamanan komputer yang dapat mengancam berbagai kepentingan.
 4. Perbuatan pidana komunikasi, ialah *hacking* yang dapat membobolkan sisten *on-line* komputer yang menggunakan sistem komunikasi.
 5. Perbuatan pidana perusakan sistem komputer, baik merusak data atau menghapus kode-kode yang menimbulkan kerusakan dan kerugian. Termasuk dalam golongan perbuatan ini adalah berupa penambahan atau perubahan program, informasi, media, sehingga merusak sistem, demikian pula sengaja menyebarkan virus yang dapat merusak program dan sistem komputer, atau pemerasan dengan

menggunakan sarana komputer/telekomunikasi.

6. Perbuatan pidana yang berkaitan dengan hak milik intelektual, hak cipta, dan hak paten, ialah berupa pembajakan dengan memproduksi barangbarang tiruan untuk mendapatkan keuntungan melalui perdagangan. Jenis perbuatan pidana tersebut di atas dapat berlaku jika komputer dihubungkan dengan teknologi telekomunikasi dan informasi, sehingga menjadi *cyber crime*, terutama dengan perkembangan teknologi internet.

3. HASIL PENELITIAN dan PEMBAHASAN

Kasus Kejahatan Dunia Maya Yang Di Tangani Oleh Polres Aceh Tenggara

1. Ujaran kebencian

Kasus ujaran kebencian yang dilakukan Melinda Br Hasibuan seorang Pegawai Negeri Sipil asal Aceh Tenggara. Gara-gara tulisannya di akun *Facebook* dan *Twitter* miliknya yang mencaci maki salah seorang masyarakat. Awal permasalahannya sangatlah sepele hal itu terjadi pada hari rabu tanggal 27 Agustus 2018 sekitar pukul 14.00 WIB di Pom Bensin Lawe Desky, Kutacane Aceh Tenggara. Pada saat Melinda Br Hasibuan sedang mengantri untuk membeli pertamax 95 dijalur mobil, setelah Melinda Br Hasibuan mengantri dan mendapat bagian paling depan oleh petugas Stasiun Pengisian Bahan Bakar Umum SPBU tidak dilayani karena menggunakan sepeda motor, dan oleh petugas SPBU disuruh untuk mengantri dijalur motor yang antriannya cukup panjang. Kesal karena tidak dilayani Melinda Br Hasibuan pulang ke tempat kos-kosannya yang beralamat di Desa Lawe Perbunga Kec. Lawe Desky Kab. Aceh Tenggara.

Sekitar pukul 15.00 WIB Melinda Br Hasibuan sempat membaca berita di media elektronik tentang antriannya yang diliput oleh wartawan yang sedang meliput kejadian di SPBU, Melinda Br Hasibuan merasa kesal dan emosi kemudian menulis status di media sosial Facebook miliknya. Dengan menggunakan telepon genggam jenis I-Phone 7 miliknya Ia menulis kata-kata “Warga yang Miskin, Tolol dan Tak Berbudaya, Teman-teman Aceh Tenggara jangan isi bensin di Pom Bensin Lawe Desky”. Dan satu lagi ia menulis “Masyarakat bangsat. Kakak mau beli pertamak 95 mentang-mentang pake motor harus antri dijalur mobil trus gak dilayani. Malah disuruh antri dijalur motor yang stuck panjangnya gak ketulungan. Diskriminasi. Emangnya aku gak bisa bayar apa”.

Tulisan Melinda Br Hasibuan tersebut banyak menuai emosi masyarakat Aceh Tenggara yang tidak terima dengan apa yang ditulis oleh Melinda Br Hasibuan. Melinda Br Hasibuan dilaporkan oleh masyarakat Aceh Tenggara ke Kepolisian Resor Aceh Tenggara. Oleh Kepolisian Resor Aceh Tenggara Melinda Br Hasibuan ditetapkan sebagai tersangka.

Bahwa status yang ditulis oleh Melinda Br Hasibuan pada media sosial *Facebook* miliknya dapat dilihat atau dibaca secara *default* (standar) oleh pengguna media sosial *Facebook* lainnya yang berstatus sebagai teman Akun *Facebook* Melinda Br Hasibuan. Status tersebut dapat disebar atau di repaht oleh pengguna media sosial *Facebook* teman MELINDA BR HASIBUAN, serta dapat di *Screen Capture* (tangkapan layar yang diabadikan) oleh pengguna media sosial *Facebook* yang berstatus teman dengan MELINDA BR HASIBUAN sehingga status tersebut dapat disebar pada media sosial lain dan bisa dibaca oleh pengguna media sosial lain yang bukan teman pada Akun *Facebook* MELINDA BR HASIBUAN.

Bahwa status atau tulisan Melinda Br Hasibuan yang menyebut kata “Warga yang Miskin, Tolol dan Tak Berbudaya, Teman-teman Aceh Tenggara jangan isi bensin di Pom Bensin Lawe Desky” jelas ditunjukkan kepada masyarakat yang tinggal dalam wilayah Aceh Tenggara yang identik dengan suku Alas. Hal tersebut telah menimbulkan reaksi keras dari masyarakat Aceh Tenggara ataupun orang Aceh Tenggara merasa dihina dan dicemarkan nama baiknya, baik secara pribadi maupun secara reputasi nama Aceh Tenggara pada umumnya.

Oleh karena perbuatannya tersebut Melinda Br Hasibuan oleh Penyidik Kepolisian Aceh Tenggara dikenakan pasal 27 ayat (3) dan pasal 28 ayat (2) junto Pasal 45 ayat (1 dan 2) Undang-Undang Nomor 19 Tahun 2016 Perubahan Atas Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Melinda Br Hasibuan sempat ditahan oleh Penyidik Kepolisian Aceh Tenggara di Rumah Tahanan (Rutan) Polres Aceh Tenggara pada tanggal 30 Agustus 2018 dengan nomor surat penahanan: No.SP.Han/52/VIII/2018/Reskrim, sejak tanggal 30 Agustus 2018 sampai dengan tanggal 01 September 2018. Akan tetapi pada tanggal 1 September 2018 permintaan penangguhan penahanan oleh keluarga Melinda Br Hasibuan dikabulkan, dengan nomor surat penangguhan penahanan: SPP.Han./17/IX/2018/Reskrim. Melinda Br Hasibuan hanya ditahan

dua hari saja. Oleh Jaksa Penuntut Umum Melinda Br Hasibuan tidak ditahan.

2. Kasus Judi Online

Lima pemuda asal desa Lawe terlibat kasus dugaan judi *online*. Mereka semua sudah ditetapkan sebagai Tersangka. Para Tersangka ini digerebek polisi saat berada di sebuah rumah warga di desa Lawe. Berdasarkan hasil pemeriksaan kelima pemuda tersebut ditetapkan sebagai Tersangka. Kasat Reskrim Polres Aceh Tenggara AKP Ari Kabri akan mengembangkan perkara tersebut dan sudah mengantongi nama sang bandar asal Medan tersebut. Pola perekrutan penjudi yang dilakukan Bandar hanya dengan mendaftarkan rekening milik penjudi ke si Bandar. Hasil dari perjudian itu bagi hasil dengan Bandar.

Pengungkapan jaringan praktik judi online di Aceh Tenggara itu bermula saat petugas Sat Narkoba Polres Aceh Tenggara melakukan razia minuman keras (miras) dan narkoba. Ketika menggerebek salah satu rumah warga yang di duga tempat nongkrong anak-anak muda, personel Sat narkoba Aceh Tenggara mendapati sejumlah orang bermain judi online.

Untuk menentukan telah terjadinya tindak pidana, Aparat Penegak Hukum harus membuktikan bahwa tersangka terdakwa telah memenuhi unsur-unsur pidana yang disangkakan atau didakwakan. Pembuktian bahwa unsur-unsur pidana telah terpenuhi juga harus berdasarkan alat-alat bukti yang telah diatur dalam undang-undang serta keyakinan hakim.

Pengaturan perjudian dalam ruang siber diatur dalam **Pasal 27 ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik** sebagaimana yang telah diubah oleh **Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik** yang berbunyi:

“Setiap Orang dengan sengaja dan tanpa hak mendistribusikan, mentransmisikan, dan/atau membuat dapat diaksesnya Informasi atau Dokumen Elektronik yang memiliki muatan perjudian”.

Ancaman terhadap pelanggaran ini diatur dalam **Pasal 45 ayat (2) Undang-Undang Nomor 19 Tahun 2016**, yakni:

“Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian sebagaimana dimaksud dalam Pasal 27 ayat (2) dipidana dengan pidana penjara

paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 1 miliar”.

3. Kasus Prostitusi Online

Polres Aceh Tenggara telah menangkap pelaku prostitusi online, pelaku ini merupakan DPO (Daftar Pencarian Orang) Daerah Kepolisian Polda Metro Jaya yang melarikan diri ke Kutacane Aceh Tenggara melalui jalur darat. Pelaku merupakan seorang mucikari yang menawarkan pekerja sek komersil di daerah Jakarta. Namun di antara para pekerja seks komersil yang di tawarkan kepada laki-laki hidung belang diantaranya ada beberapa anak dibawah umur. Pelaku menggunakan modus dengan memasang foto-foto para pekerja sek komersil di suatu situs dengan harapan mendapatkan pelanggan. Ketika ada yang memboking salah satu pekerja sek komersil pelaku menghubungi wanita yang pelaku pasang foto disitus, dan menentukan dimana mereka kencana dan berapa fee yang akan didapatkan oleh pelaku.

Dua pekerja seks komersil yang masih dibawah umur dan sekaligus korban, oleh pelaku di tawarkan kepada laki-laki hidung belang bisa kencana dengan dua wanita tersebut sekaligus. Setelah chek in di kamar hotel dan memasukan korban ke kamar, pelaku mendapatkan uang dari pelanggannya. Akibat perbuatannya pelaku di jerat Pasal 76 I jo Pasal 88 Undang-Undang nomor 35 Tahun 20014 tentang perlindungan anak, atas perubahan Undang-Undang Nomor 23 Tahun 2002 atau Pasal 45 Ayat (1) sub Pasal 27 Ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Kendala Polisi dalam Melakukan Penyidikan Terhadap Kasus Cyber Crime

Kesulitan bagi Penyidik Kepolisian dalam melakukan Penyidikan terhadap kasus kejahatan dunia maya atau *cyber crime* adalah dalam mengusut pelaku mengenai identitas pelaku yang kerap menggunakan nama samaran bukan nama yang sebenarnya. Sulitnya menemukan *locus* atau tempat kejadian tindak pidana cyber crime sering terjadi, karena pelaku bisa saja berpindah-pindah tempat ketika melakukan kejahatan *cyber crime*. Dalam kasus ujaran kebencian di media sosial Penyidik harus terlebih dahulu memanggil ahli bahasa untuk membuat terang suatu kalimat atau ucapan yang tertulis dimedia sosial tersebut apakah terpenuhi unsure ujaran kebenciannya, dan penyidik pun terkadang harus memanggil ahli hukum pidana untuk membuat terang perkara bahwa ucapan

atau kalimat ujaran kebencian tersebut merupakan suatu tindak pidana.

Kesulitan lainnya adalah dalam memperoleh alat bukti elektronik, para pelaku terkadang sudah menghilangkan data-data bukti kejahatannya baik itu di computer atau di smartphone, sehingga Penyidik harus mendapatkan bukti fisik dari computer atau smartpjhone yang dipergunakan untuk melakukan kejahatan dunia maya atau *Cyber crime* untuk di periksa secara digital forensic untuk mendapatkan bukti yang akurat.

1. Kendala Teknis Internal

a. Pengelolaan Sumber Daya Manusia

Ketika perekrutan anggota Polri baru tidak boleh ada nepotisme dalam proses perekrutan anggota, apa pun jabatan orang tua calon anggota yang akan mendaftar Polri, tidak ada pula uang suap untuk bisa lolos seleksi, apalagi naik jabatan. Siapa pun yang ingin menjadi anggota Polri atau memangku jabatan tinggi, harus mampu bersaing secara cerdas dan sehat. Rekrutmen adalah proses seleksi calon-calon anggota baru yang berasal dari masyarakat. Tentunya untuk bisa memperoleh anggota polisi yang profesional, dia harus dipilih dari calon-calon yang berkualitas, memenuhi standar-standar yang sudah ditentukan kepolisian. Di sini berarti proses selesksinya harus sesuai prinsip yang sudah diterapkan, bersih, transparan, *akuntable*, dan humanis, juga berkualitas. Harus benar-benar dilakukan pemilihan terhadap calon-calon itu kualitas-kualitas yang dibutuhkan baik fisiknya kemudian kesehatannya, intelektualnya, kesehatan jiwanya, psikologisnya, ini harus memenuhi standar sehingga nantinya menjadi anggota Polri yang berkualitas, tanggap, tanggon, tenggrinas.

Bahwa kemudian calon-calon anggota Polri yang ketika mendaftar hanya lulusan Sekolah Menengah Umum/Kejuruan atau sederajat lainnya menjadi kedala kurangnya pengetahuan hukum bagi anggota-anggota Polri yang baru. Untuk meningkatkan ke profesionalan kinerja anggota Polri, Kepolisian bekerja sama dengan Universitas-Universitas di beberapa kota-kota besar seperti di Jakarta, Medan, Surabaya, Bandung, Semarang, Makasar, dan kota-kota besar lainnya untuk membuka kelas-kelas hukum yang di buka di Kantor Kepolisian dan anggota-anggota Kepolisian yang belum bersarjana hukum diwajibkan untuk mengikuti kuliah dan lulus menjadi sarjana hukum. Terlebih lagi syarat

untuk menjadi Penyidik minimal harus Sarjana Hukum.

Lebih khusus lagi, syarat menjadi penyidik itu sendiri diatur lagi dalam Peraturan Pemerintah Nomor 27 Tahun 1983 tentang Pelaksanaan Kitab Undang-Undang Hukum Acara Pidana sebagaimana yang telah diubah oleh Peraturan Pemerintah Nomor 58 Tahun 2010 Perubahan Atas Peraturan Pemerintah Nomor 27 Tahun 1983 tentang Pelaksanaan Kitab Undang-Undang Hukum Acara Pidana ("PP 58/2010").

Penyidik adalah [Pasal 2 PP 58/2010]:

- a. pejabat Kepolisian Negara Republik Indonesia; dan
- b. pejabat pegawai negeri sipil.

Lalu apa syarat-syarat untuk menjadi penyidik itu? Apakah harus sarjana hukum? Untuk menjawabnya, kami mengacu pada Pasal 2A ayat (1) PP 58/2010:

(1) Untuk dapat diangkat sebagai pejabat penyidik Kepolisian Negara Republik Indonesia sebagaimana dimaksud dalam Pasal 2 huruf a, calon harus memenuhi persyaratan:

- a. *berpangkat paling rendah Inspektur Dua Polisi dan berpendidikan paling rendah sarjana strata satu atau yang setara;*
- b. *bertugas di bidang fungsi penyidikan paling singkat 2 (dua) tahun;*
- c. *mengikuti dan lulus pendidikan pengembangan spesialisasi fungsi reserse kriminal;*
- d. *sehat jasmani dan rohani yang dibuktikan dengan surat keterangan dokter; dan*
- e. *memiliki kemampuan dan integritas moral yang tinggi*

Namun, dalam hal pada suatu satuan kerja tidak ada Inspektur Dua Polisi yang berpendidikan paling rendah sarjana strata satu atau yang setara, Kepala Kepolisian Negara Republik Indonesia atau pejabat Kepolisian Negara Republik Indonesia yang ditunjuk dapat menunjuk Inspektur Dua Polisi lain sebagai penyidik [Pasal 2B PP 58/2010].

Dalam PP 58/2010 juga dikenal Penyidik pembantu yang diatur dalam Pasal 3 ayat (1) PP 58/2010 berbunyi:

(1) Penyidik pembantu adalah pejabat Kepolisian Negara Republik Indonesia yang memenuhi persyaratan sebagai berikut:

- a. berpangkat paling rendah Brigadir Dua Polisi;

- b. mengikuti dan lulus pendidikan pengembangan spesialisasi fungsi reserse kriminal;
- c. bertugas dibidang fungsi penyidikan paling singkat 2 (dua) tahun;
- d. sehat jasmani dan rohani yang dibuktikan dengan surat keterangan dokter; dan
- e. memiliki kemampuan dan integritas moral yang tinggi.

2. Kendala Teknis Internal Di Polres Aceh Tenggara

1. Kurangnya pemahaman dan Penguasaan penyidik di bidang teknologi informasi.

Sebagian besar personil penyidik Kepolisian Resor Aceh Tenggara masih belum menguasai teknologi informasi dan kurang adanya sosialisasi internet di Kepolisian Resor Aceh Tenggara. Mengingat sangat pentingnya penunjang sumber daya manusia untuk menunjang kelancaran suatu proses penyelidikan, penyidikan, serta proses penangkapan. Menurut keterangan penyidik hanya beberapa personil dan tidak banyak penyidik di Kepolisian Resor Aceh Tenggara yang memahami bidang teknologi informasi, hal ini kurang seimbang dengan adanya kasus yang ada, seiring begitu maraknya tindak pidana perjudian bola melalui internet yang masih bisa terjadi kapan saja di dalam masyarakat dan masih banyaknya kasus perjudian bola melalui internet yang masih belum terungkap atau hentinya tenaga lidik dikarenakan kurangnya tenaga ahli di Kepolisian Resor Aceh Tenggara, sehingga perlu dipikirkan oleh pemerintah untuk memberikan pelatihan TI kepada aparat kepolisian baik di setiap Polres maupun Polsek khusus Cyber Crime.

Terlalu Banyaknya Beban Pekerjaan Penyidik Yang Ada Di Unit Tipidter Kepolisian Resor Aceh Tenggara. Penyidik tidak terfokus untuk menangani *cybercrime* khususnya Pencemaran nama baik melalui Facebook konsentrasi mereka terpecah kepada perkara-perkara yang sudah ada terkadang menyimpang jauh contohnya penggelapan, penipuan, tanah dan bangunan. Di Satreskrim Kepolisian Resor Aceh Tenggara sudah dibagi-bagi spesifikasinya namun karena laporan polisi dari masyarakat di Kepolisian Resor Aceh Tenggara beraneka ragam dan banyak di luar *cybercrime* sehingga ideal di dalam penanganan kepolisian terlampaui dan ini berimplikasi terhadap kecepatan

penanganan perkara baik yang dilaporkan oleh masyarakat maupun yang ditemukan oleh penyidik itu sendiri.

2. Kurangnya Fasilitas Yang Modern Dalam Pencarian Barang Bukti.

Pemahaman Penyidik yang masih belum memahami tindak pidana umum dengan *cyber crime* bagaimana secara teknis memperlakukan baik saksi maupun barang bukti, karena *cyber crime* diolah dan diperlakukan secara khusus tidak seperti barang bukti tindak pidana yang lain. Contohnya software ketika penyidik mematikan dan mencabut laptop atau komputer yang digunakan menjadikan hilang barang buktinya dan bagaimana memecahkan kode-kode yang sudah di setting sedemikian rupa oleh pelaku sehingga ketika penyidik mencoba membuka kode-kode tersebut sudah berubah data yang ditampilkan.

3. Proses pelacakan dan penyelidikan ini dilakukan secara manual dengan cara menelusuri data-data yang ada, tidak terdapat alat-alat yang canggih yang digunakan oleh penyidik di Kantor Kepolisian Resor Aceh Tenggara, alat-alat yang canggih hanya terdapat di Markas Besar Kepolisian Republik Indonesia (MABES POLRI) dan Kepolisian Daerah Aceh (POLDA Aceh). Namun demikian penyidik tetap diperbolehkan menggunakan alat canggih tersebut pada saat keadaan yang mendesak dan proses perijinannya pun sangat diperhitungkan dikarenakan mengingat alat canggih tersebut mencapai milyaran rupiah, alat tersebut bisa melacak arah sinyal, tetapi menurut Iptu Kabri, S.H., MM sampai sejauh ini semua kasus pencemaran nama baik melalui *Facebook* cara penanganannya dilakukan secara manual dengan melakukan kerjasama dengan instansi lain yang terkait serta menelusuri situs-situs web yang terkait dengan perjudian bola melalui internet dan belum pernah meminjam alat canggih tersebut. Jadi kepolisian dituntut untuk harus benar-benar mencermati dan teliti dalam melakukan pelacakan tersangka sehingga tidak salah sasaran pada waktu penangkapan dan pengumpulan barang bukti.

Kesulitan lainnya yang sering dialami Penyidik Polres Aceh Tenggara Adalah:

1. Sulitnya memperoleh alat bukti yang terdapat di dalam kasus pencemaran nama baik melalui *Facebook* mengakibatkan proses penyelidikan dan penyidikan sering terhenti, karena ini termasuk kasus Cyber Crime maka alat bukti untuk melakukan proses penyelidikan hanya berupa informasi elektronik dan dokumen elektronik. Hasil wawancara dengan Ipd Djuliar Yousnadi, S.H, Selaku Kanit Idik II

Tindak Pidana Tertentu Kepolisian Resor Aceh Tenggara, tanggal 04 Desember 2018.

2. Tempat Kejadian Perkara (TKP) terjadi di dalam internet maka penyidik menelusuri dan mengamati dengan menggunakan internet serta jika diperlukan penyidik mengadakan kerjasama dengan instansi lain yang terkait dalam perjudian bola melalui internet, jika di dalam kasus ini ditemukan tidak cukup bukti maka proses penyelidikan dihentikan. Menurut Ipd Djuliar Yousnadi, S.H, Selaku Kanit Idik II Tindak Pidana Tertentu Kepolisian Resor Aceh Tenggara kendala eksternal yang sering dialami di lapangan selama proses penyelidikan yaitu:

a) Sulit Mendapatkan Alamat Tersangka
Kendala yang paling sering terjadi dalam proses penyelidikan adalah alamat yang terdaftar pada identitas tersangka fiktif, karena pelaku dengan mudahnya membuat Akun *Facebook* dengan nama dan alamat palsu, untuk melakukan aksinya pelaku tidak berdiam di satu tempat, dengan menggunakan peralatan atau gadget canggih pelaku melakukan aksinya dimana saja, dan juga pelaku menghilangkan jejak dengan mengganti akun *Facebook* pelaku sehingga tidak bisa dilacak posisinya, untuk selanjutnya alamat yang masih bisa ditelusuri dan masih bisa dicari keberadaannya maka kepolisian akan terus mencari.

b) Tingginya Penguasaan Pelaku Dalam Mengoperasikan Teknologi Informasi. Akses internet yang melayani seluruh akun media sosial semakin marak di masyarakat karena kemudahan akses, dibarengi dengan kemampuan pelaku tindak pidana pencemaran nama baik melalui *Facebook* melalui internet yang semakin canggih dalam mengoperasikan akun-akun *Facebook* tersebut. Dan untuk mengungkap kejahatan pencemaran nama baik melalui *Facebook* di Kantor Kepolisian Resor Aceh Tenggara harus meminta bantuan kepada Kepolisian Daerah Aceh untuk melakukan tracking keberadaan pelaku, karena kurang lengkapnya peralatan yang menunjang di Kantor Kepolisian Aceh Tenggara. Sehingga penyidik harus menunggu informasi yang diberikan kepada Polda, dan apabila Polda tidak memberikan informasi apapun maka tindak pidana pencemaran nama baik melalui *Facebook* tidak bisa diungkap oleh Polres Aceh Tenggara sampai ketika Polda memberikan informasi keberadaan pelaku, sehingga ini berpengaruh kepada

kecepatan penanganan perkara, seumpama Polres Aceh Tenggara memiliki sarana dan prasarana yang memadai serta peralatan yang menunjang tentu bisa mengungkap pelaku, sehingga selama ini dilakukan secara manual dan untung-untungan dalam menangkap pelaku.

4. KESIMPULAN

Kejahatan *cyber crime* di Indonesia telah ada regulasinya dalam beberapa undang-undang. Kebijakan kriminal terhadap tindak pidana mayantara telah tegas dan jelas dalam undang-undang tersebut. Beberapa kasus kejahatan mayantara di Aceh telah diselesaikan dengan baik oleh pihak kepolisian. Meskipun terjadi beberapa kendala dan hambatan yang dihadapi oleh pihak kepolisian, tetapi semua kasus kejahatan dunia mayantara, dapat diselesaikan dengan baik.

DAFTAR PUSTAKA

- Abdul Wahid, Muhammad Labib, 2005, *Kejahatan Mayantara (Cyber Crime)*, Bandung: PT Refika Aditama.
- Abdul Wahid. 2005. *Kejahatan Mayantara (Cyber Crime)*. Malang: Fakultas Hukum Unisma.
- Agus Raharjo, 2002, *Cyber Crime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Bandung: Citra Aditya Bakti.
- Ahmad M. Ramli, 2004, *Cyber Law Dan Haki Dalam Sistem Hukum Di Indonesia*, Bandung: PT Refika Aditama.
- Barda Nawawi Arief, "Antisipasi Hukum Pidana Dan Perlindungan Korban Cyber Crime Di Bidang Kesusilaan", makalah pada Seminar "Kejahatan Seks melalui *Cyber Crime* dalam Perspektif Agama, Hukum, dan Perlindungan Korban", Makalah Pada Seminar F.H UNSWAGATI, Hotel Zamrud Cirebon, tanggal 22 Agustus 2005.
- _____, 2003, *Kapita Selekta Hukum Pidana*, Bandung: Citra Aditya Bhakti.
- _____, 2006, *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime di Indonesia*. Jakarta: Raja Grafindo Persada.
- Hasil wawancara dengan Ipda. Djuliar Yousnadi Selaku Kanit Idik II Tipidter Kepolisian Resor Aceh Tenggara, tanggal 04 Desember 2018.
- Muhammad Haidar Ali, "Cyber Crime Menurut Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang ITE (Perspektif Hukum Pidana

- Islam)". *Tesis*. Program Pascasarjana Universitas Alauddin Makassar, 2012.
- Sri Sumarwani, "Tinjauan Yuridis Pemidanaan Cybercrime Dalam Perspektif Hukum Pidana Positif", dalam *Jurnal Pembaharuan Hukum*, Vol. I, September-Desember 2014.
- Tb. Ronny Rahman Nitibaskara, 2001, *Ketika Kejahatan Berdaulat*, Jakarta: Peradaban.