PENANGANAN KASUS *CYBER CRIME* DI KOTA MAKASSAR (STUDI PADA KANTOR KEPOLISIAN RESORT KOTA BESAR MAKASSAR)

Oleh :
RISKAWATI
Mahasiswa Jurusan PPKn FIS UNM
HERI TAHIR
Dosen PPKn FIS UNM

ABSTRAK: Tujuan dari penelitian ini yaitu: 1) untuk mengetahui proses penyidikan kasus *cyber crime*, 2) cara penyelesaian kasus *cyber crime* serta 3) kendala-kendala yang dihadapi dalam proses penyidikan kasus *cyber crime* yang dilakukan oleh pihak Polrestabes Makassar.Penelitian ini menggunakan metode deskriptif kualitatif dengan pendekatan studi kasus. Lokasi penelitian yaitu Polrestabes Makassar dan teknik pengumpulan data menggunakan teknik wawancara dan dokumentai. Sementara, dalam penelitian ini sumber data diperoleh dari data primer dan sekunder. Hasil penelitian menunjukkan bahwa penanganan kasus *cyber crime* dalam hal ini proses penyidikan pada umumnya sama dengan penanganan kasus konvensional yang lain. Seperti dalam hal pengumpulan barang bukti, penggeledahan dan proses penyelesaiannya. Sementara perbedaanya terdapat pada proses penangkapan pelaku kejahatan beserta koordinasi dengan pihak-pihak tertentu. terlihat bahwa penanganan tindak kejahatan *cyber crime* sedikit rumit dibandingkan kejahatan konvensional, sebab terlebih dahulu harus berkoordinasi dengan beberapa pihak tertentu seperti saksi ahli untuk mendapatkan kepastian bahwa hal tersebut benar-benar merupakan tindak kejahatan pidana atau bukan,. kendala dalam proses penyidikan ini adalah kurangnya saksi ahli baik saksi ahli gambar maupun saksi ahli bahasa, serta tidak adanya unit yang secara khusus menangani kasus *cyber crime*. oleh karena itu sangat dibutuhkan peran saksi ahli dalam penanganan kasus *cyber crime* dan pentingnya melakukan sosialisasi kepada masyarakat tentang bahaya *cyber crime.*

Kata Kunci : Penanganan, Kasus *Cyber Crime*

ABSTRACT: The purpose of this study are: 1) to know the process of investigation of cases of cyber crime, 2) way of solving cases of cyber crime as well as 3) the constraints faced in the case of cyber crime investigation process conducted by the method of this Makassar.Penelitian Polrestabes descriptive qualitative case study approach. The location is Polrestabes Makassar research and data collection techniques using interview techniques and dokumentai. Meanwhile, in this study the data sources obtained from primary and secondary data. The results showed that the handling of cyber crime cases in this respect the investigation process was generally similar to other conventional case management. As for the collection of evidence, searches and the process of completion. While the difference is found in the process of catching offenders and their coordination with certain parties. seen that the handling of cyber crime a little complicated compared to conventional crime, because it must first be coordinated with several parties such as expert witnesses to obtain assurance that it is actually a crime to criminal or not ,. obstacles in the investigation process is the lack of a good expert witness expert witness expert witness images and language, as well as the absence of a unit that deals specifically with cases of cyber crime. therefore it is very necessary role of expert witnesses in handling cases of cyber crime and the importance to disseminate to the public about the dangers of cyber crime.

Keywords: Management, Cyber Crime Cases

PENDAHULUAN

Pemanfaatan teknologi informasi, media dan komunikasi telah mengubah baik perilaku masyarakat maupun peradaban manusia secara global. Perkembangan teknologi informasi telah pula menyebabkan hubungan dunia menjadi tanpa batas dan menyebabkan perubahan sosial, ekonomi, dan budaya secara signifikan berlangsung demikian cepat.

Teknologi informasi saat ini menjadi pedang bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan , kemajuan dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum.

Salah satu perkembangan teknologi yang sering digunakan dan dibutuhkan semua kalangan masyarakat adalah komputer. Dengan komputer seseorang dapat dengan mudah menyelesaikan pekerjaan, tetapi dengan adanya komputer seseorang menggunakannya pada hal-hal yang baik atau hal-hal yang buruk. Keunggulan komputer berupa kecepatan dan ketelitiannya dalam menyelesaikan pekerjaan sehingga dapat menekan jumlah tenaga kerja, biaya serta memperkecil kemungkinan melakukan kesalahan, mengakibatkan masyarakat semakin mengalami ketergantungan kepada komputer. Dampak negatif dapat timbul apabila terjadi kesalahan yang ditimbulkan oleh peralatan komputer yang akan mengakibatkan kerugian besar bagi pemakai (*user*) atau pihak-pihak yang berkepentingan. Kesalahan yang disengaja mengarah kepada penyalahgunaan komputer.

Saat ini telah lahir suatu rezim hukum baru yang dikenal dengan hukum siber. IsTilah "hukum siber" diartikan dari kata *cyber law*. Saat ini secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan teknologi informasi. istilah lain yang digunakan adalah hukum dunia maya (*virtual word law)*, hukum teknologi informasi (*law of information technology)*. Istilah tersebut lahir mengingat kegiatan yang dilakukan melalui jaringan sistem komputer dan sistem komunikasi baik dalam lingkup lokal maupun global (internet) dengan memanfaatkan teknologi informasi berbasis sistem komputer yang merupakan sistem elektronik yang dapat dilihat secara virtual atau maya. Kemudian setelah itu, muncul istilah baru dari kejahatan komputer yaitu C*yber crime. Cyber Crime* merupakan perkembangan dari *computer crime*. *Cyber crime* dan *cyber law* dimana kejahatan ini sudah melanggar hukum pidana. Dengan adanya kasus yang terjadi di dunia maya tersebut, telah banyak menjatuhkan korban, bukan hanya pada kalangan remaja namun disemua usia. Hal tersebut mengharuskan satuan kepolisian untuk segera bertindak dalam menangani kasus *cyber crime* (kejahatan dunia maya) yang cakupan kejahatannya sangat luas bahkan tidak terbatas.

Cara pandang konvensional terhadap tindak pidana *cyber crime* akan menimbulkan kesulitan dan ketimpangan dalam proses penyelidikan, penyidikan dan pembuktian dimana proses tersebut tidaklah sama dengan proses penyelidikan, penyidikan dan pembuktian pada kasus-kasus tindak pidana konvensional, namun sikap positif tetap harus kita ambil terhadap Undang-Undang Nomor 11 Tahun 2008 tentang Internet dan Transaksi Elektronik sebagai payung hukum dalam dunia *Cyber Crime*, dengan harapan dapat menjadi acuan dan salah satu literatur undang-undang dalam hal penegakan *cyberlaw* di Indonesia. Dalam penanganan kasus *cybercrime* pula diharapkan kemaksimalan dari pihak kepolisian untuk menghindari agar kasus *cyber crime* yang telah terjadi dapat begitu saja terlepas dari pengawasan hukum,

Cyber crime memiliki sifat efisien dan cepat serta sangat menyulitkan bagi pihak penyidik dalam melakukan penangkapan terhadap pelakunya. Hal ini disebabkan antara lain oleh kurangnya pemahaman dan pengetahuan masyarakat terhadap jenis kejahatan *cyber crime*, pemahaman dan pengetahuan ini menyebabkan upaya penanggulangan *cyber crime* mengalami kendala, dalam hal ini kendala yang berkenaan dengan penataan hukum dan proses pengawasan

masyarakat terhadap setiap aktivitas yang diduga berkaitan dengan kejahatan *cyber crime* tersebut.

Berdasarkan obserfasi awal di polrestabes Makassar, bahwa terdapat beberapa kasus *cyber crime* yang pernah ditangani oleh pihak kepolisian Makassar, dan tentunya hal ini sangat mengancam masyarakat. Oleh karena itu penulis berusaha melihat bagaimana proses penanganan dari kasus *Cyber crime* itu sendiri dalam hal ini baik dari segi metode penyelesaian kasus hingga sampai pada kendala yang dihadapi oleh pihak kepolisian dalam penanganan kasus *cyber crime* (kejahatan dunia maya). Sehingga penulis mengambil judul "Penanganan Kasus ***Cyber Crime*** di Kota Makassar (studi pada kantor kepolisian Resort Kota Besar Makassar" dengan menggunakan landasan yuridis UU ITE Nomor 11 tahun 2008.

Tujuan pelaksanaan penelitian ini adalah untuk mengetahui dan menjelaskan : (1) proses penyidikan tindak pidana *cyber crime* yang dilakukan oleh pihak Polrestabes Makassar, (2) bentuk penyelesaian *cyber crime* menurut UU ITE nomor 11 tahun 2008, (3) kendala yang dihadapi oleh pihak Polrestabes Makassar dalam penyidikan tindak pidana *cyber crime*

TINJAUAN PUSTAKA

A. Kepolisian Resort

Kepolisian Resort (disingkat POLRES) adalah struktur komando Kepolisian Republik Indonesia di daerah Kabupaten atau kota. Kepolisian Resort di wilayah perkotaan biasa disebut kepolisian Resort Kota (Kapolres). Kepolisian Resor Kota Besar (Polrestabes) biasanya digunakan untuk ibukota provinsi. Kepolisian Resor dikepalai oleh seorang kepala kepolisian Resor, Kepolisian Rresor kota biasanya dikepalai oleh seorang Kepala Kepolisian Resor Kota dan kepolisian Resor Kota Besar dikepalai oleh seorang Kepala kepolisian Resor Kota Besar.

Jadi kepolisian Resor Kota Besar adalah Kepolisian Yang bertempat di Ibu kota Provinsi dan dikepalai oleh seorang kepala Kepolisian Resor Kota Besar (Kapolrestabes).

B. Tugas dan Wewenang Kepolisian Resort

Tugas pokok Kepolisian Negara Republik Indonesia adalah:

a. memelihara keamanan dan ketertiban masyarakat;
b. menegakkan hukum; dan
c. memberikan perlindungan, pengayoman, dan pelayanan kepada masyarakat.

a. Dalam rangka menyelenggarakan tugas sebagaimana dimaksud dalam Pasal 13 Kepolisian Negara Republik Indonesia secara umum berwenang: menerima laporan dan/atau pengaduan;
b. membantu menyelesaikan perselisihan warga masyarakat yang dapat mengganggu ketertiban umum;
c. mencegah dan menanggulangi tumbuhnya penyakit masyarakat;
d. mengawasi aliran yang dapat menimbulkan perpecahan atau mengancam persatuan dan kesatuan bangsa;
e. mengeluarkan peraturan kepolisian dalam lingkup kewenangan administratif kepolisian;
f. melaksanakan pemeriksaan khusus sebagai bagian dari tindakan kepolisian dalam rangka pencegahan;

C. *Cyber Crime*

Perkembangan teknologi komputer juga menghasilkan berbagai bentuk kejahatan komputer di lingkungan *cyberspace* yang kemudian melahirkan istilah baru yang dikenal dengan *Cybercrime*, *Internet Fraud*, dan lain-lain.

Sebagian besar dari perbuatan *Cybercrime* dilakukan oleh seseorang yang sering disebut dengan *cracker*. Berdasarkan catatan Robert H'obbes'Zakon, seorang internet Evangelist, *hacking* yang dilakukan oleh *cracker* pertama kali terjadi padatanggal 12 Juni 1995 terhadap The Spot dan tanggal 12 Agustus 1995 terhadap *Crackers Move Page*. Berdasarkan catatan itu pula, situs pemerintah Indonesiapertama kali mengalami serangan *cracker* pada tahun 1997 sebanyak 5 (lima) kali.

Kegiatan *hacking* atau *cracking* yang merupakan salah satu bentuk *cybercrime* tersebut telah membentuk opini umum para

pemakai jasa internet bahwa *Cyber crime* merupakan suatu perbuatan yang merugikan bahkan amoral. Para korban menganggap atau memberi stigma bahwa *cracker* adalah penjahat. Perbuatan *cracker* juga telah melanggar hak-hak pengguna jasa internet sebagaimana digariskan dalam The Declaration of the Rights of Netizens yang disusun oleh Ronda Hauben.

"*cyber crime*" adalah salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian luas di dunia internasional. Volodymyr Golubev menyebutkan sebagai "*the new form of anti social behavior"* . beberapa julukan/sebutan lainnya yang cukup keren diberikan kepada kejahatan baru ini dalam berbagai tulisan, antara lain sebagai "kejahatan dunia maya".

"*cyber crime*" selanjutnya merupakan salah satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negative sangat luar bagi seluruh bidang kehidupan modern saat ini. Sehubung dengan kekhawatiran akan ancaman/bahaya *cyber crime* ini, karena berkaitan erat dengan "*economi crime"* dan "*organized crime"* (terutama untuk tujuan "money laundering).

Jadi *cyber crime* dapat didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan internet yang berbasis pada kecanggihan teknologi computer dan telekomunikasi.

D. Modus Kejahatan *Cyber Crime*

a. *Unauthorized Access to Computer System and Service* (Akses tidak sah ke sistem computer dan layanan)

Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik system jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan (hacker) melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun begitu, ada juga yang melakukan hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Kejahatan ini semakin marak dengan berkembangnya teknologi internet/intranet.

b. *Illegal Contents* (isi tidak sah)

Merupakan kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Sebagai contohnya adalah pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau harga diri pihak lain, hal-hal yang berhubungan dengan pornografi atau pemuatan suatu informasi yang merupakan rahasia negara, agitasi dan propaganda untuk melawan pemerintahan yang sah, dan sebagainya.

c. *Data Forgery* (pemalsuan data)

Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai scriptless document melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen e-commerce dengan membuat seolah-olah terjadi "salah ketik" yang pada akhirnya akan menguntungkan pelaku.

d. *Cyber Espionage* (spionase cyber)

Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer(computer network system) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu system yang computerized.

e. *Cyber Sabotage and Extortion* (sabotese dan pemerasan)

Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu logic bomb, virus komputer ataupun suatu program tertentu,

sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku. Dalam beberapa kasus setelah hal tersebut terjadi, maka pelaku kejahatan tersebut menawarkan diri kepada korban untuk memperbaiki data, program komputer atau sistem jaringan komputer yang telah disabotase tersebut, tentunya dengan bayaran tertentu. Kejahatan ini sering disebut sebagai cyberterrorism.

f. *Offense against Intellectual Property* (kejahatan terhadap proporti intelektual)

Kejahatan ini ditujukan terhadap Hak atas Kekayaan Intelektual yang dimiliki pihak lain di internet. Sebagai contoh adalah peniruan tampilan pada web page suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.

g. *Infringements of Privacy* (pelanggaran privasi)

Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara computerized,yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materilmaupun immateril, seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.

h. *Cracking*

Kejahatan dengan menggunakan teknologi computer yang dilakukan untuk merusak system keamaanan suatu system computer dan biasanya melakukan pencurian, tindakan anarkis begitu merekan mendapatkan akses. Biasanya kita sering salah menafsirkan antara seorang hacker dan cracker dimana hacker sendiri identetik dengan perbuatan negative, padahal hacker adalah orang yang senang memprogram dan percaya bahwa informasi adalah sesuatu hal yang sangat berharga dan ada yang bersifat dapat dipublikasikan dan rahasia.

i. *Carding*

Adalah kejahatan dengan menggunakan teknologi computer untuk melakukan transaksi dengan menggunakan card credit orang lain sehingga dapat merugikan orang tersebut baik materil maupun non materil.

METODE PENELITIAN

Dalam penelitian ini, jenis penelitian yang digunakan adalah deskriptif kualitatif. Metode penilitian ini digunakan untuk meneliti pada kondisi obyek alamiah, yaitu peniliti merupakan instrument kunci. Metode ini berusaha memahami fakta dibalik kenyataan yang dapat diamati atau diindra secara langsung.

Lokasi peneltian ini adalah kantor Polrestabes Makassar, jalan Jend. Ahmad Yani No.9 Makassar. Alasan penulis mengambil lokasi tersebut karena penelitian ini adalah penelitian studi kasus yang mana setelah dialakukan observasi ternyata diketahui ada beberapa kasus yang berkaitan dengan judul penelitian ini yaitu mengenai kasus *cyber crime*.

Peran polisi dalam hal ini adalah menangani kasus *Cyber crime* yang dilakukan oleh pihak kepolisian dengan menggunakan UU No.11 tahun 2008 tentang ITE, namun tidak terlepas dari ketentuan dalam KUHAP. Hal ini dilakukan guna memelihara keamanan dan ketertiban masyarakat, menegakkan hukum, serta memberikan perlindungan, pengayoman, dan pelayanan kepada masyarakat dalam rangka terpeliharanya keamanan dalam masyarakat.

Cyber Crime adalah kejahatan yang berkaitan langsung dengan Media elektronik yang dihasilkan oleh jaringan komputer yang digunakan sebagai tempat melakukan komunikasi sambungan langsung (*on-line*). kejahatan ini terjadi tanpa adanya tatap muka antara pelaku dan korban, seperti dalam hal penipuan secara *on line* , berupa penipuan dalam penjualan barang, dan pencemaran nama baik.

jenis dan sumber data dalam penelitin ini yaitu (1) Data primer adalah data yang

diperoleh secara langsung dari setiap informan yang akan diwawancarai dilokasi penelitian, dalam hal ini kepolisian yang berkantor di Polrestabes Makassar, dan sebanyak 3 orang polisi pada unit sidik yang menjadi informan peneliti. Sementara populasi dan sampel pada penelitian ini adalah kasus *cyber crime* yang terjadi selama 3 tahun terakhir (2013,2014,2015) yaitu sebanyak 34 kasus dan 90% adalah kasus pencemaran nama baik yang banyak terjadi ditahun 2014, selain itu juga terdapat kasus pelanggaran asusila yang terjadi ditahun 2015.

(2) Data sekunder adalah sebagai data pendukung data primer dari literatur dan dokumen serta data yang diambil dari kantor Polrestabes Makassar. Dalam penelitian ini data-data diambil dari sumber-sumber data barupa bahan bacaan, bahan pustaka dan laporan-laporan penelitian serta laporan kasus yang masuk di Polrestabes Makassar.

Teknik pengumpulan data dalam penelitian ini adalah (1) Wawancara adalah bentuk komunikasi antara dua orang yang melibatkan seseorang yang ingin memperoleh informasi dari orang lain dengan mengajukan pertanyaan, berdasarkan tujuan tertentu. Penelitian ini menggunakan teknik wawancara dalam proses pengumpulan data mengenai kasus cyber crime. Dan yang menjadi informan peneliti adalah pihak kepolisian, dalam hal ini sebanyak 3 orang polisi. (2) Dokumentasi merupakan tehnik pengumpulan data yang dilakukan pada saat penelitian berlangsung. Yang didokumentasikan berupa foto data kasus yang pernah ditangani oleh polisi, rekaman suara. Dokumentasi inilah yang akan memperjelas data-data yang didapatkan dari hasil observasi dan wawancara.

Teknik keabsahan data dalam penelitian ini yaitu Data yang diperoleh dalam penelitian ini agar terjamin tingkat validitasinya, maka perlu dilakukan pengecekan atau pemeriksaan keabsahan data. Adapun penelitian ini dalam melakukan pemerikasaan keabsahan data melakukan Tringulasi.(1)Tringulasi Sumber, Untuk menguji kredibilitas data tentang *cyber crime* maka pengumpulan data dan pengujian data yang telah diperoleh dilakukan kepada pihak kepolisian dari beberapa unit sidik. Data dari sumber tersebut dideskripsikan, dikategorisasikan, mana pandangan yang sama dan yang berbeda, dan mana spesifik dari ketiga data tersebut. Data yang telah dianalisis oleh peneliti sehingga menghasilkan suatu kesimpulan dari tiga sumber data tersebut.(2)Tringulasi Teknik, Dalam tringulasi teknik ini dilakukan pengecekan data kepada sumber yang sama dengan teknik yang berbeda. Namun peneliti tidak menggunakan tringulasi teknik.(3) Tringulasi Waktu, Dalam rangka pengujian kredibilitas pada tringulasi waktu ini peneliti melakukannya dengan cara pengecekan dengan wawancara, observasi dan dokumentasi dalam waktu atau situasi berbeda. Namun jika hasil uji menghasilkan data yang berbeda, maka peneliti melakukannya berulang-ulang sehingga ditemukan kepastian datanya.

Analisis data disebut juga pengolahan dan penafsiran data. Analisis data merupakan upaya mencari dan menata secara sistematis catatan hasil observasi, wawancara dan lainnya untuk meningkatkan pemahaman peneliti tentang kasus yang diteliti dan menyajikan sebagai temuan bagi orang lain. Sedangkan untuk meningkatkan pemahaman tersebut perlu dilanjutkan dengan berupaya mencari makna.

Sifat analisis dalam penelitian kualitatif adalah penguraian apa adanya fenomena yang terjadi (deskriptif) disertai penafsiran terhadap arti yang terkandung dibalik yang tampak (interpretif). Dalam penelitian ini peneliti melakukan analisis interpretatif dengan mengandalkan daya imajinasi, intuisi, dan daya kreasi peneliti dalam proses yang disebut reflektif dalam menangkap makna dari objek penelitian. Tujuan analisis tersebut adalah untuk menemukan makna peristiwa yang ada pada objek penelitian dan menginterpretasikan makna dari hal yang diteliti. Data-data yang nantinya diperoleh dari penelitian tentang *Cyber Crime* (kejahatan dunia maya), akan dianalisis dan ditafsirkan kedalam kata-kata atau penjelasan yang bisa dipahami dengan jelas oleh orang

lain, untuk kemudian disajikan secara tertulis dalam bentuk laporan penelitian

PEMBAHASAN

A. Proses Penyidikan Tindak Pidana *Cyber Crime* Yang Dilakukan Oleh Pihak Polrestabes Makassar

jumlah laporan kasus *Cyber Crime* pada kurun waktu 3 tahun terakhir yaitu tahun 2013, 2014 dan 2015. Kasus yang masih dalam proses penyidikan oleh Polrestaber Makassar sebanyak 12 kasus, dan 22 kasus yang lainnya berhasil diselesaikan oleh Polrestabes Makassar. Dari 34 kasus *Cyber Crime* yang masuk sebagian besar mengenai kasus pencemaran nama baik, atau sekitar 90% dari total kasus yang masuk. Tingginya jumlah kasus *cyber crime* terjadi ditahun 2014 dan sebagian besar adalah kasus pencemaran nama baik, kemudian diakhir tahun 2015 terjadi pula kasus kejahatan asusila melalui dunia maya.

secara umum proses penyidikan kejahatan *Cyber Crime* sama dengan proses penyidikan kejahatan konvensional lainnya. Bedanya hanya dari segi proses penangkapan pelaku kejahatan beserta koordinasi dengan pihak-pihak tertentu. terlihat bahwa penanganan tindak kejahatan *cyber crime* sedikit rumit dibandingkan kejahatan konvensional, sebab terlebih dahulu harus berkoordinasi dengan beberapa pihak tertentu untuk mendapatkan kepastian bahwa hal tersebut benar-benar merupakan tindak kejahatan pidana atau bukan. Sementara dalam menetapkan tersangka kejahatan *cyber crime*, memiliki tingkat kesulitan yang lebih rendah dibanding kejahatan konvensional, dengan melihat barang bukti berupa nomor handphone atau alamat sosial media yang dimiliki pelaku dan tentunya dengan barang bukti tersebut maka akan tertuju secara langsung kepada pihak yang melakukan tindakan kejahatan.

Sebagaimana kasus pencemaran nama baik yang banyak ditangani oleh pihak kepolisian. Perbuatan tersebut dilakukan pelaku melalui media internet dengan menyebarkan berita bohong/tidak benar dan berita yang bersifat rahasia sehingga berakibat mencemarkan nama baik orang lain atau instansi tertentu. Perbutan pelaku tersebut merupakan pelanggaran terhadap ketentuan Undang-undang Nomor 11 tahun 2008 tentang informasi dan transaksi elektronik pasal 27 ayat 3 dan lebih jelas diatur dalam KUHP pasal 310 tentang penghinaan. Dalam proses penyidikannya harus melibatkan saksi ahli bahasa untuk mengetahui apakah konteks bahasa yang digunakan oleh pelaku adalah tindak pidana atau bukan. Namun berdasarkan hasil wawancara, pihak kepolisian Polrestabes Makassar tidak dapat memberikan informasi terkait proses penangkapan pelaku pada kasus *Cyber Crime* dalam hal ini pencemaran nama baik yang berhasil diselesaikan oleh pihak kepolisian karena bersifat rahasia. Dalm proses penyidikan kasus ini, dilakukan berdaasarkan ketentuan dalam UU ITE pasal 42 yang menegaskan "penyidikan terhadap tindak pidana sebagaimana yang dimaksud dalam Undang-undang ini dilakukan berdasarkan ketentuan dalam hukum acara pidana dan ketentuan dalam undang-undang ini". Dalam KUHAP diatur pada BAB penyidikan pasal 107, dan ini sebagaimana diatur pula pada pasal 43 UU ITE, bahwa selain penyidik pejabat polisi Negara Republik Indonesia, juga bekerja sama dengan pejabat pegawai Negeri sipil.

Sementara dalam hal penggeledahan, pihak kepolisian harus mendapatkan izin dari ketua pengadilan. Sebagaimana yang terdapat pada pasal 43 ayat 3 UU N0.11 tahun 2008 tentang ITE yang menerangkan bahwa "penggeledahan dan/atau penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan atas izin ketuan pengadilan setempat" Hal ini juga sebagaimana yang terdapat pada pasal 33 ayat 1 KUHAP. Proses ini dilakukan untuk kepentingan penyidikan dengan tetap memperhatikan perlindungan terhadap privasi, kerahasiaan dan kelancararan layanan publik sebagaimana diatur dalam pasal 43 (2) UU ITE. Dengan demikian, proses penyidikan yang dilakukan oleh pihak kepolisian polrestabes Makassar menggunakan payung hukum dari UU No.11

tahun 2008 tentang informasi dan transaksi elektronik, namun dalam pelaksanaannya tidak dapat terlepas dari ketentuan KUHP dan KUHAP, dan beberapa pasal dalam UU ITE tetap mempertimbangkan ketentuan dalam KUHAP karena ada hal-hal yang tidak diatur dala UU ITE namun diatur dalam KUHP dan KUHAP.

B. Bentuk Penyelesaian Kasus *Cyber Crime* menurut UU No.11 Tahun 2008 Tentang ITE

1. Setiap orang dapat mengajukan gugatan terhadap pihak yang menyelenggarakan sistem elektronik dan/atau menggunakan teknologi informasi yang menimbulkan kerugian
2. Masyarakat dapat mengajukan gugatan secara perwakilan terhadap pihak yang menyelenggarakan sistem elektronik dan/atau menggunakan informasi yang berakibat merugikan masyarakat, sesuai dengan ketentuan peraturan perundang-undangan
3. Gugatan perdata dilakukan sesuai dengan ketentuan peraturan perundang-undangan
4. Selain penyelesaian gugatan perdata sebagaimana dimaksud pada ayat (1), para pihak dapat menyelesaikan sengketa melalui arbitrase, atau lembaga penyelesaian sengketa alternatif lainnya, sesuai dengan peraturan perundang-undangan.

Dari seluruh laporan kasus *cyber crime* yang masuk, 90% adalah kasus pencemaran nama baik yang mana merupakan delik aduan sehingga kasus tersebut bisa saja ditarik. Namun, sejauh ini semua kasus *cyber crime* yang masuk di Polrestabes Makassar dibawa ketahap pengadilan,begitupun juga dengan kasus asusila sebagaimana yang kita bahas sebelumnya.

Informasi yang kami dapatkan diatas, dalam hal bentuk penyelesaiannya sebagaimana yang diatur dalam UU No.11 tahun 2008 tentang ITE pada pasal 38-39. Bahwa setiap orang yang menjadi korban dari tindak pidana *cyber crime* dapat melakukan gugatan. Namun selain dari gugatan perdata tersebut, peyelesaian kasus dapat pula dilakukan arbitrase yaitu usaha perantara dalam meleraikan sebuah sengketa atau dengan kata lain kedua pihak telah berdamai. Hal ini dapat terjadi karena kasus *cyber crime* dalam hal pencemaran nama baik dan tindakan asusila adalah delik aduan yang berarti delik yang hanya bisa diproses apabila ada pengaduan atau laporan dari orang yang menjadi korban tindak pidana. Dalam delik aduan, penuntut terhadap delik tersebut digantungkan pada persetujuan dari yang dirugikan. Pada delik aduan ini korban tindak pidana dapat mencabut laporannya kepada pihak yang berwenang apabila diantara mereka telah terjadi suatu perdamaian. Delik aduan ini banyak diatur dalam KUHAP seperti pasal 310 tentang pencemaran nama baik, pasal 355 tentang perbuatan yang tidak menyenangkan, dan pasal 284,287,289 tentang kejahatan asusila. Dan ketentuan seperti ini tidak diatur dalam UU ITE.

Sehingga dari pembahasan ini, meskipun dalam proses penyelesaian kasus menggunakan sistem UU ITE, namun pelaksanaannya tidak dapat terlepas dari KUHAP sebagai salah-satu payung hukum yang menjadi acuan dalam penyelesaian perkara pidana, termasuk didalamnya kasus *cyber crime*. Dan laporan yang sampai kepada polrestabes Makassar, semuanya sampai pada tahap mengadili. Sekalipun hal ini merupakan delik aduan.

C. Kendala Yang Dihadapi Oleh Pihak Polrestabes Makassar Dalam Penyidikan Tindak Pidana *Cyber Crime*

1. Kendala Internal

kendala yang dihadapi adalah pada pelakunya , saksi dari kasus serta tidak adanya unit khusus menangani masalah kejahatan dunia maya yang kita kenal dengan unit *cyber crime*, sementara pihak penyidik terkadang sulit mengetahui keberadaan pelaku sekalipun menggunakan teknologi. Selanjutnya berdasarkan wawancara tersebut, penelti merangkum beberapa kendala yaitu:

a. Kurangnya saksi ahli, dalam hal ini saksi ahli gambar dan saksi ahli bahasa.

b. Tidak adanya unit *cyber crime* di Polrestabes Makassar.
c. Sulit memperoleh saksi kejahatan.
d. Keberadaan pelaku yang sulit dideteksi sekalipun menggunnakan teknologi.

2. Kendala Eksternal

a. Izin ketua pengadilan untuk penggeledahan dan penyitaan serta izin melaui penuntut umum dari ketua pengadilan untuk penangkapan dan penahanan.
b. Masyarakat yang kurang memahami masalah tindak pidana *Cyber Crime* sebagai tindak pidana kejahatan.
c. Faktor teknologi, mengenai kemajuan teknologi informasi yang ada saat ini. Kemajuan teknologi mempengaruhi dalam menemukan alat bukti khususnya menganai data elektronik dari suatu pembuktian tindak pidana *Cyber Crime.*

PENUTUP

Berdasarkan hasil penelitian berkenaan dengan penanganan kasus *cyber crime* di kota Makassar, maka dapat ditarik keimpulan sebagai berikut: (1) Proses penyidikan kasus *cyber crime* pada umumnya sama dengan proses penyidikan pada kejahatan konvensional lainnya. Bedanya hanya dari segi proses penangkapan pelaku kejahatan beserta koordinasi dengan pihak-pihak tertentu. (2) Bentuk penyelesaian kasus *cyber crime* adalah diselesaikan melalui proses pengadilan, jika korban dari kejahatan tersebut memaafkan pelaku kejahatan maka dapat diselesaikan secara kekeluargaan atau dengan kata lain tidak sampai pada proses pengadilan, sebab kasus *cyber crime* adalah tingkat kejahatan delik aduan sehingga memungkinkan untuk ditarik.(2) Kendala-kendala yang dihadapi dalam proses penyidikan yaitu secara internal meliputi proses penangkapan pelaku kejahatan dalam hal mendeteksi keberadaan pelaku, kurangnya saksi ahli gambar, kesulitan dalam hal pengadaan saksi serta tidak adanya init khusus yang menangani kasus *cyber crime*. Selain dari itu juga terdapat kendala-kendala eksternal berupa surat izin penggeledahan dan penyitaan dari ketua pengadilan melalui penuntut umum, kurangnya pengetahuan mesyarakat terkait kejahatan *cyber crime*, serta semakin canggihnya teknologi yang berakibat sulitnya ditemukan barang bukti.

Berdasarkan kesimpulan diatas, maka diajukan beberapa saran sebagai berikut : (1) Pelretabes Makassar harus memiliki unit *Cyber Crime* agar dalam proses penanganan kasus *cyber crime* dapat dilakukan secara terstruktur dan efisien.(2) Agar penanganan kasus tidak memakan waktu yang lama maka dibutuhkan saksi ahli yang bertempat tinggal di Makassar.(3) Pihak kepolisian Perlu melakukan sosialisasi kepada masyarakat tentang bahaya kejahatan *cyber crime* karena masih banyaknya masyarakat yang tidak tau bahwa adanya undang-undang yang mengatur hal tersebut.

DAFTAR PUSTAKA

BUKU

Agus Raharjo, 2002, "Cybercrime", cetakan pertama, PT. Citra Aditya Bakti, Bandung.

Andi Mappiare AT,2009, *Dasar-dasar Metodologi Riset Kualitatif Untuk Ilmu Sosial dan Profesi,* (Malang: Jenggala Pustaka Utama.

Dedi Mulyana. 2006, *Metodologi penelitian kualitatif.* Rosda. Bandung.

Didik M. Mansur Arief, Dkk. 2005. *Cyber Law* Aspek Hukum Technologi Informasi, Refika Aditama. Bandung.

Nawawi Arif,2000,*masalah penegak hukum dan kebijakan penanggulangan kejahatan*, Bandung, PT Citra aditya Bhakti

Noeng Muhajir, 1996, *Metodologi penelitian Kualitatif*, Yogyakarta: Rake Sarasin.

Partodiharjo, Soemarno. 2009. Tentang *informasi dan Transaksi Elektronik*. Gramedia Pusaka Utama. Jakarta.

Ramli, ahmad. 2006. *Cyber Law* dan HAKI Dalam Sistem Hukum Indonesia. Refika Aditama. Bandung.

Rene L. Pattiradjawane, 2000 "*Media Konverjensi dan Tantangan Masa Depan*", Kompas

Tohirin. 2012, *Metode Penelitian Kualitatif Dalam Pendidikan dan Bimbingan Konseling.* Jakarta: Penerbit Rajawali Pers.

Institut Komputer Indonesia (IKI), 1981, *Pengenalan Komputer (Introduction to Computer).*

Andi Hamzah. 1990. *Aspek-aspek pidana di bidang computer.* Jakarta. Sinar grafika.

Kamus Besar Bahasa Indonesia

UNDANG-UNDANG

Undang-undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 2 tahun 2002 tentang Kepolisian Negara Republik Indonesia

Buku Luks KUHP (Kitab Undang-undang Hukum Pidana) dan KUHAP (Kitab Undang-undang Hukum Acara Pidana.

JURNAL

Jurnal,Dista amalia Arifah,2011, "*Indonesia's cyber crime case"*

Jurnal,jatnika sari dan Rezah Zulfikar, "*ancaman dan modus kejahaan dibidang teknologi informasi"*

Jurnal. Irhamni Ali. 2011. *Kejahatan terhadap informasi (cyber crime) dalam konteks perpustakaan digital*

HASIL WAWANCARA

Wawancara dengan Bapak Bripka Adhi Darmawan selaku ketua unit JATANRAS (kejahatan dan kekerasan)

Wawancara dengan Bapak Iptu Awaluddin selaku ketua Kourbin

Wawancara dengan Bapak Brigpol Riswandi selaku anggota dari Unit Kourbin