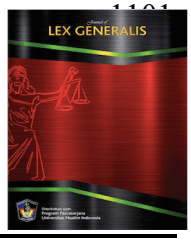
Journal of Lex Generalis (JLS)
Volume 2, Nomor 3, Maret 2021
P-ISSN: 2722-288X, E-ISSN: 2722-7871
Website: http: pasca-umi.ac.id/indez.php/jlg
This work is licensed under a Creative Commons Attribution 4.0 International License.



Upaya Kepolisian Dalam Penanggulangan Tindak Pidana Kejahatan Dunia Maya (*Cyber Crime*) Pada Kepolisian Daerah Sulawesi Selatan

Adam Mulqadrin[1,2], Kamri Ahmad[1] & Hamza Baharuddin[1]

[1]*Magister Ilmu Hukum, Universitas Muslim Indonesia.*
[2]*Koresponden Penulis, E-mail: adam.mulqadrin@gmail.com*

ABSTRAK

Tujuan penelitian menganalisis Upaya Hukum Kepolisian Dalam Penanggulangan Tindak Pidana Kejahatan Dunia Maya (Cyber Crime) pada Kepolisian Daerah Sulawesi Selatan dan faktor–faktor yang menjadi penghambat Upaya Kepolisian dalam penanggulangan kasus kejahatan Cyber Crime di sulawesi selatan. Penelitian ini menggunakan data primer melalui survey di Kepolisian Daerah Sulawesi Selatan Direktorat Reserse Kriminal Khusus pada unit IV Cyber Crime, Hasil Penelitian menunjukkan bahwa: (1) Upaya yang dilakukan oleh Kepolisian Daerah Sulawesi Selatan Direktorat Reserse Kriminal Khusus pada unit IV Cyber Crime terhadap Tindak Pidana ini adalah Upaya Preventif dan Upaya Represif (2) Faktor yang menjadi penghambat upaya kepolisian dalam penanggulangan kejahatan Cyber Crime di Sulawesi Selatan yaitu faktor internal dan eksternal Hal ini berarti bahwa tindakan kepolisian yang dilakukan berdasarkan paraturan yang berlaku dan masih adanya kendala dari sarana dan prasarana dalam penanganan tindak pidana Cyber Crime yang masih belum memadai.

Kata Kunci: *Polisi, Penanggulangan; Cyber Crime*

ABSTRACT

The research objective is to analyze the Police's Legal Efforts in Handling Cyber Crime at the South Sulawesi Regional Police and the factors that hamper the Police's efforts to handle cyber crime cases in South Sulawesi. This study uses primary data through a survey at the South Sulawesi Regional Police, the Directorate of Special Crime Investigation at unit IV Cyber Crime. The results show that: (1) Efforts made by the South Sulawesi Regional Police, Directorate of Special Criminal Investigation at unit IV Cyber Crime against Crime These are Preventive Efforts and Repressive Efforts (2) The factors that hamper police efforts in overcoming cyber crime crimes in South Sulawesi are internal and external factors. inadequate handling of cyber crime crimes.

Keywords*: Police, Countermeasures; Cyber Crime*

PENDAHULUAN

Teknologi informasi (*information technology*) membawa dampak bagi masyarakat secara luas, pertumbuhan teknologi berkembang kian pesat setiap harinya dan memuat kehidupan menjadi lebih mudah (Fonna, 2019). Terlebih lagi dimasa pademi kita harus tetap berada dirumah dan tetap melakukan pekerjaan tetap berjalan sesuai protokol yang berlaku (Pariputna, 2008). Bukti kecil dari perkembangan teknologi pada saat ini di buktikan dengan kemudahan akses untuk menjalankan pekerjaan hanya beberapa "klik" dari komputer/smartphone dan lain lain sudah dapat berbelanja seperti layaknya di toko pada umumnya. Seperti itulah perkembangan teknologi yang semakin mempermudah masyarakat dalam beraktifitas pada zaman 4.0 saat ini (Kasemin, 2016).

Perkembangan positif dari teknologi ini dapat di gambarkan secara umum seperti, menghubungkan orang di seluruh dunia, penyebaran informasi yang sangat cepat, memajukan di bidang pendidikan dan lain lain (Riwayadi, 2013). Dampak positif ini mengundang berbagai pihak dalam pengembangan teknologi informasi ini, dimana dampak positif pasti akan mengundang sisi negatif dalam pengembangan teknologi ini tanpa kita sadari ada juga orang orang yang memiliki keilmuan dalam bidang ini yang menyalahgunakan bidang keilmuannya dalam perkembangan teknologi ini. Dampak negatifnya adalah memberikan peluang untuk melakukan berbagai kejahatan, seperti penipuan, pencurian, pencemaran nama baik, kesusilaan, perjudian, pengancaman, perusakan dan teror yang seluruhnya dikenal dengan *Cyber Crime.*

Perilaku yang sesuai dengan norma (hukum) yang berlaku, tidak menjadi masalah tetapi perilaku yang tidak sesuai norma biasanya dapat meimbulkan permasalahan di bidang hukum dan merugikan masyarakat (Manan, 2018). Perilaku yang tidak sesuai atau dapat disebut sebagai penyelewengan terhadap norma yang disepakati, ternyata menyebabkan terganggunya ketertiban dan ketentraman kehidupan manusia. Penyelewengan yang demikian, biasanya oleh masyarakat dicap sebagai suatu pelanggaran dan bahkan suatu kejahatan. Kejahatan dalam kehidupan manusia merupakan gejala sosial yang akan selalu dihadapi oleh setiap manusia, masyarakat, bahkan Negara.

Hukum merupakan sarana yang ditujukan untuk mengubah perilaku masyarakat. Sesuai dengan tujuan yang telah ditetapkan sebelumnya, hukum merupakan sarana yang dipilih untuk mencapai tujuan-tujuan tersebut, maka prosesnya tidak hanya berhenti pada pemilihan hukum sebagai sarana saja. Kecuali pengetahuan yang mantap tentang sifat hakikat hukum (Lathif, 2017).

Sesungguhnya tata negara ialah penataan atau menata negara melalui peraturan perundang-undangan sesuai kebutuhan dari pada kehidupan Berbangsa Dan bernegara pada sektor atau bagian tersebut, sehingga mempermudah penanganan penegakan hukum. Karena sudah ditata dengan baik menurut kesepakatan masyarakat yang diwujudkan dalam bentuk undang undang atau peraturan perundang undangan. Misalnya kebutuhan mengatur masalah olahraga, maka ditetapkan peraturan atau undang undang masalah ke olahragaan, Kebutuhan menangani korupsi, maka ditetapkan peraturan berkaitan dengan antikorupsi serius menata lembaga dan struktur yang menangani masalah korupsi bahkan, adanya

kebutuhan mengatur masalah media pers, maka ditetapkan peraturan dan perundang undangan tentang pers dan seterusnya.

Menurut Agus Raharjo bahwa sebagai sebuah gejala sosial, kejahatan telah ada sejak awal kehidupan manusia di dunia, namun kemajuan teknologi komunikasi membuat kejahatan dalam bentuk primitif berubah menjadi sebuah kejahatan yang lebih maju (modern) (Raharjo, 2002). Kejahatan konvensional di dunia nyata muncul dalam dunia maya (virtual) dengan wajah kejahatan yang telah diperhalus sedemikian rupa. Kehalusan kejahatan virtual atau *Cyber Crime* membuat masyarakat luas, khususnya di negara berkembang yang memiliki kesenjangan digital seperti Indonesia, tidak merasakannya sebagai sebuah bentuk kejahatan.

Kenyataan telah membuktikan bahwa kejahatan hanya dapat dicegah atau dikurangi tetapi sulit untuk diberantas secara tuntas. Kejahatan perlu mendapat perhatian secara serius mengingat kerugian yang dapat ditimbulkannya yang dampaknya akan berakibat merugikan Negara, masyarakat maupun individu. Oleh karena itu Negara memberikan reaksi berupa larangan terhadap perbuatan melawan hukum serta sanksi bagi pelanggarnya. Penerapan hukum dengan cara menjunjung tinggi nilai-nilai Pancasila, merupakan suatu upaya untuk meningkatkan kualitas penegakan hukum, dengan cara memanfaatkan ilmu pengetahuan dan teknologi serta memperhatikan perkembangan globalisasi yang modern.

Fenomena ini terjadi dalam satu dunia kemudahan dan kecanggihan berdatangan titik mengakibatkan munculnya paradoks semakin mudah dan semakin rentan mengucapkan dunia yang dianggap sempurna titik dunia yang diidamkan kaum Utopia titik sehingga terjadi perang antar autopi anisme dan vandalisme orang ini sejatinya tidak memiliki aturan namun ketika jumlah korban lebih banyak membutuhkan regulasi salah satunya hukum pidana. Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi ini dikelompokkan dalam beberapa bentuk sesuai modus operandi yang ada.

Sebagai sebuah gejala sosial, kejahatan telah sejak awal kehidupan manusia di dunia, namun kemajuan teknologi membuat kejahatan dalam bentuk primitif berubah menjadi sebuah kejahatan yang lebih maju dan modern. Kejahatan konvensional di dunia nyata muncul di dunia maya dengan wajah kejahatan yang diperhalus sedemikian rupa. Kehalusan kejahatan virtual atau *Cyber Crime* membuat masyarakat luas, khususnya di negara berkembang yang memiliki kesenjangan digital seperti Indonesia (Fuadi, 2005), tidak merasakannya sebagai sebuah bentuk kejahatan. Padahal, sudah begitu banyak korban dan kerugian moril dan materil akibat *Cyber Crime*. Korbannya dapat berupa netizen (penduduk dunia virtual/penghuni cyberspace) dan masyarakat luas yang awam (Azis, 2016).

Begitu halnya di kasus *Cyber Crime* di Propinsi Sulawesi Selatan yang ditangani oleh Kepolisian Daerah Sulawesi Selatan melalui Sub Direktorat V Tindak Pidana *Cyber Crime* Polda Sulawesi Selatan, yang mana sejak tahun 2019 sampai dengan tahun 2020 telah ditangani kasus *cyber crime,* diantaranta: Pengungkapan Kasus Peretasan Sistus DPRD Pare-Pare, Pengungkapan Kasus Pinjaman Online Modus penipuan Online; Pengangkapan Kasus Arisan Online Kerugian Milyaran Rupiah dan Pengungkapan Kasus Skimmer Makassar Warga Rumania.

METODE PENELITIAN

Metode Pendekatan Masalah yang digunakan dalam penelitian Tesis ini adalah pendekatan empiris. yang dilakukan untuk mengetahui penegakan hukum terhadap pelaku kejahatan *Cyber Crime* yang dipaparkan oleh narasumber dan/atau aparat penegak hukum sebagai data penunjang. Pemilihan Polda Sulawesi selatan untuk pelaksanaan studi ini didasarkan atas beberapa pertimbangan tertentu. Pertimbangannya unsur keterjangkauan lokasi penelitian oleh peneliti, baik dilihat dari segi tenaga, dan segi efisiensi waktu. Termasuk pada pengumpulan data yang merupakan tempat terkumpulnya data pada tingkat berjenjang di daerah Sulawesi Selatan, merupakan alasan mendasar pada pemilihan lokasi.

PEMBAHASAN

A. Upaya Kepolisian Dalam Menanggulangi Kejahatan *Cyber Crime* Di Sulawesi Selatan

Aturan hukum Indonesia adalah hasil yang logis yang membutuhkan lembaga yang bisa mengawasi penegakan hukum salah satunya adalah kepolisian. Semua orang berharap kepolisian bisa menjalankan tugas kepolisian Menangani kasus pidana agar dapat diselesaikan secara optimal. hal Ini untuk menentukan sejauh mana optimalisasi peran penyidik dalam proses Menyelidiki tindakan kriminal penyalahgunaan informasi dan transaksi elektronik, dan kemudian pertama, harus bisa mengukur kinerja penyidik kepolisian (Usman, 2015).

Disini penulis akan memaparkan sejauh mana optimalisasi kebijakan penyidik kepolisian dalam penyidikan tindak pidana cybercrime dalam menanggulangi tindak pidana cybercrime. Kebijakan penanggulangan cyber crime dengan hukum pidana termasuk bidang *Penal Policy* yang merupakan bagian dari *Criminal Policy* (kebijakan penanggulangan kejahatan). Dilihat dari sudut *Criminal Policy*, upaya penanggulangan kejahatan (termasuk penanggulangan *Cyber Crime*) tidak dapat dilakukan semata-mata secara parsial dengan hukum pidana (sarana penal), tetapi harus pula ditempuh dengan pendekatan integral/sistemik.

Dalam menanggulangi terjadinya kasus *Cyber Crime* ini pihak kepolisian telah melakukan berbagai upaya penanggulangan *Cyber Crime*. Dengan melakuka Penerapan hukum pidana (criminal law application) maupun pencegahantanpa pidana (prevention without punishment), hingga memberikan pandangan kemasyarakat mengenai kejahatan dan pemidanaan lewat mass media (influencing views of society on crime and punishment/mass media)

Berdasarkan wawancara dengan Bripka Yudhiyanto selaku Ba nit *Cyber Crime* Reskrimsus Polda Sulsel pada kamis 8 oktober 2020 yang menyatakan bahwa pihak kepolisian telah melakukan upaya-upaya penanggulangan yang bersifat preventif dan represif.

1. Upaya Preventif

Dalam melakukan upaya preventif ini pihak kepolisian khususnya unit *Cyber Crime* polda sulsel telah melakukan berbagai upaya seperti memberikan himbauan ke

masyarakat melalui media elektronik maupun media sosial dengan menyebarkan broadcast berupa himbauan-himbauan terkait *Cyber Crime* untuk di forward ke masyarakat luas. Selain itu dilakukan juga penerangan ke masyarakat melalui media surat kabar dan radio, serta pada saat mengisi acara talkshow pihak kepolisian tidak henti-hentinya memberikan himbauan kemasyarakat.

Pihak kepolisian juga menjalankan fungsi teknis yang khusus menangani kasus *Cyber Crime*, yaitu dengan melakukan penegakan aturan, melakukan penjagaan di lokasi-lokasi yang diduga sering terjadi kasus *Cyber Crime* dan melakukan patroli cyber rutin di dunia maya seperti media-media sosial.

2. Upaya Represif

Dalam melakukan upaya represif ini, pihak kepolisian telah mengambil tindakan dengan memproses setiap kasus *Cyber Crime* yang ditangani sesuai dengan aturan yang berlaku. Pihak kepolisian bekerja sama dengan stakeholder yang ada yaitu bagaimana menangkap pelaku yang tertangkap tangan melakukan kejahatan ataupun melalui laporan masyarakat kemudian mendatangi tempat kejadian perkara (TKP) guna melakukan penangkapan dan penahanan terhadap tersangka kasus *Cyber Crime*, setelah dilakukan penangkapan kemudian diproses dikepolisian dan sebelum dilimpahkan berkas perkaranya ke kejaksaan terlebih dahulu diadakan konferensi pers dengan media dimana pihak media hadir untuk mewawancarai tersangka dan petugas yang menangani kasus tersebut. Lalu hasil wawancara tersebut disiarkan atau disebarkan kemasyarakat luas, sehingga masyarakat mengetahui kasus-kasus yang ditangani oleh aparat kepolisian khususnya kepolisian Polda Sulsel.

Dalam mengahadapi *Cyber Crime*, hukum positif di Indonesia masih bersifat lex locus delicti. Namun beda halnya dengan situasi dan kondisi pelanggaran hukum yang terjadi atas *Cyber Crime* dimana pelaku kejahatan cyber dan korban berada ditempat yang berbeda. Wilayah kejahatan dunia maya yang begitu luas namun mudah diakses menyebabkan maraknya terjadi kejahatan. Kepolisian Republik Indonesia (POLRI) sebagai salah satu alat kelengkapan negara dalam menegakkan hukum tidak dapat lagi tinggal diam setelah lahirnya UU no. 11 tahun 2008 tentang informasi dan transaksi elektronik. Aparat penegak hukum dalam hal ini penyidik kepolisian harus bergerak secara aktif untuk menindak kejahatan di dunia maya. Aparat kepolisian harus dapat menangani kasus-kasus kejahatan yang terjadi di dunia maya. Berikut ini akan dipaparkan beberapa kasus *Cyber Crime* yang telah ditangani oleh Kepolisan Daerah Sulawesi Selatan tahun 2016 - 2020:

Tabel 1. Jumlah kasus *Cyber Crime* yang ditangani Polda Sulsel

No.	Kasus	Ketentuan Pidana	Jumlah Kasus
1	Pornografi dan/atau Pelanggaran Kesusilaan	Pasal 27 Ayat 1	21
2	Penghinaan / Pencemaran	Pasal 27 Ayat 3	64
3	Pemerasan dan/atau Pengancaman	Pasal 27 Ayat 4 dan Pasal 29	16
4	Penyebaran Berita Bohong dan Penyesatan	Pasal 28 Ayat 1	237
5	Provokasi	Pasal 28 Ayat 2	26

6	Hacking	Pasal 30	22
7	Plagiat (Pembajakan)	Pasal 35	15
	Total		***401 kasus***

Sumber: Data Penanganan Kasus Unit Cyber Crime Polda Sulsel

Berdasarkan hasil penelitian tersebut di atas dapat dilihat bahwa jumlah penyalahgunaan Informasi dan Transaksi Elektronik (ITE) pada *Cyber Crime* Reskrimsus Polda Sulsel yang terjadi tiap tahunnya yakni, pada tahun Jumlah keseluruhan kejahatan penyalahgunaan Informasi dan Transaksi Elektronik (ITE) pada *Cyber Crime* Reskrimsus Polda Sulsel dalam kurun waktu 5 tahun terakhir sejak 2016 sampai tahun 2020 yakni terdapat *401 kasus* penyalahgunaan Informasi dan Transaksi Elektronik (ITE). Yang dimana menurut Bripka yudhiyanto selaku Ba nit *Cyber Crime* Reskrimsus Polda Sulsel Tindak pidana cyber secara umum thn 2020 .Lapor sebanyak 54 kasus dan penyelesaian sebanyak 42 kasus dari 192 target yg harus diselesaikan utk tahun 2020. Dari data tersebut dapat disimpulkan bahwa kasus kejahatan kasus penyalahgunaan Informasi dan Transaksi Elektronik (ITE) tiap tahunnya terjadi kenaikan kasus penyalahgunaan Informasi dan Transaksi Elektronik (ITE) yang terjadi di sekeliling.

Berdasarkan hasil wawancara dengan Reskrimsus Polda Sulsel, urutan dari penegakan hukum terhadap *Cyber Crime* laporan polisinya kebanyakan menggunakan model B, sebagaimana dimaksud pada pasal 5 ayat (1) huruf b Peraturan Kapolri Nomor 14 Tahun 2012 tentang Manajemen Pendidikan Tindak Pidana yaitu adalah Laporan Polisi yang dibuat oleh anggota Polri atas laporan/pengaduan yang diterima dari masyarakat. Secara lengkap urut-urutannya adalah sebagai berikut:

a) Pada proses pertama, karena petugas melakukan laporan/pengaduan kejahatan *Cyber Crime*, maka petugas menerbitkan laporan polisi terkait tindak pidana

Laporan Polisi adalah laporan tertulis yang dibuat oleh petugas Polri tentang adanya suatu peristiwa yang diduga terdapat pidananya baik yang ditemukan sendiri maupun melalui pemberitahuan yang disampaikan oleh seseorang karena hak atau kewajiban berdasarkan peraturan perudang-undangan. (Pasal 1 butir 16 Peraturan Kapolri Nomor 14 Tahun 2012 tentang Manajemen Pendidikan Tindak Pidana)

b) Kemudian penyidik melakukan pemeriksaan saksi-saksi yang terkait dalam kejahatan *Cyber Crime* tersebut dan memeriksa barang bukti, guna membuat terang kejahatan *Cyber Crime* yang terjadi.

Pada prinsipnya semua orang bisa menjadi saksi dan menjadi sebuah kewajiban memberikan sebuah keterangan apabila dipanggil oleh penyidik. Pasal 1 butir 26 KUHAP menyebutkan pengertian saksi, yaitu sebagai berikut, Saksi adalah orang yang dapat memberikan keterangan guna kepentingan penyidikan, penuntutan dan peradilan tentang suatu perkara pidana yang ia dengar sendiri, ia lihat sendiri dan ia alami sendiri. Menurut Pasal 63 ayat (2) Perkap No 14 Tahun 2012 tujuan dari pemeriksaan saksi ialah guna membuat terang suatu perkara pidana sehingga peran seseorang maupun barang bukti dalam peristiwa pidana yang terjadi menjadi jelas.

c). Selanjutnya penyidik melakukan gelar perkara.

Gelar perkara dilakukan guna menentukan tersangka, menentukan perbuatan tersebut merupakan sebuah tindak pidana atau bukan dan menentukan unsur-unsur pasal yang dipersangkakan; Gelar Perkara menurut Pasal 1 angka 17 Peraturan Kepala Badan Reserse Kriminal Kepolisian Republik Indonesia (Perkaba) No 4 Tahun 2014 tentang Standar Operasional Prosedur Pengawasan Penyidikan Tindak Pidana menyebutkan:

Gelar Perkara adalah kegiatan penyampaian pejelasan tentang proses atau hasil penyelidikan oleh penyidik kepada peserta gelar perkara dalam bentuk diskusi kelompok untuk mendapatkan tanggapan/masukan/koreksi dalam rangka menghasilkan rekomendasi untuk menentukan tindaklanjut proses penyidikan.

Gelar Perkara biasa dilaksanakan dengan tahap:

1) Awal proses penyidikan;
2) Pertengahan proses penyidikan; dan
3) Akhir proses penyidikan.

Pada Kasus yang ditangani oleh Unit 4 *Cyber Crime*Subdit II Ditreskrimsus PoldaJateng tersebut pihak penyidik melakukan gelar perkara pada tahap awal penyidikan, dimana tujuan dari gelar perkara yang dilakukan oleh penyidik adalah sebagai berikut:

1) Menentukan status perkara pidana atau bukan;
2) Merumuskan rencana penyidikan;
3) Menentukan unsur-unsur pasal yang dipersangkakan;
4) Menentukan saksi, tersangka, dan barang bukti;
5) Menentukan target waktu; dan
6) Penerapan teknik dan taktik penyidikan.

d). Setelah dilakukan gelar perkara, penyidik melakukan Penetapan tersangka.

Pasal 1 butir 14 KUHAP memberikan pengertian mengenai Tersangka yang berbunyi, Tersangka adalah seorang yang karena perbuatannya atau keadaannya, berdasarkan bukti permulaan patut diduga sebagai pelaku tindak pidana. Untuk penetapkan seseorang berstatus tersangka harus memenuhi syarat-syarat yang telah ditentukan, sebagaimana diatur dalam Pasal 66 Peraturan Kapolri Nomor 12 Tahun 2009 tentang Pengawasan dan Pengendalian Penanganan Perkara Pidana di Lingkungan Kepolisian Negara Republik Indonesia, yaitu sebagai berikut:

a. Status tersangka hanya dapat ditetapkan oleh penyidik kepada seseorang setelah hasil penyelidikan yang memperoleh bukti permulaan yang cukup yaitu paling sedikit 2 (dua) jenis alat bukti, yaitu sebagai berikut:
   Bukti permulaan yang cukup sekurangkurangnya adanya Laporan Polisi ditambah dengan 2 (dua) jenis alat bukti seperti:
   a) Keterangan saksi yang diperoleh penyidik;
   b) Keterangan ahli yang diperoleh penyidik;
   c) Surat;
   d) Petunjuk.

b. Untuk menentukan bukti permulaan tersebut harus ditentukan melalui gelar perkara.

d). Kemudian penyidik melakukan digital forensik terhadap barang bukti digital di Labfor Polda, untuk memeriksa barang bukti yang telah disita oleh penyidik.

Forensik merupakan suatu kegiatan untuk melakukan investigasi dan menetapkan fakta yang berhubungan dengan suatu tindak kriminal dan permasalahan hukum lainnya. Sedangkan digital forensik merupakan bagian dari ilmu forensik yang melingkupi penemuan dan investigasi materi (data) yang temukan pada perangkat digital seperti; komputer, handphone, tablet, PDA, networking devices, dan sejenisnya *Raharjo, 2013).

Ada 3 (tiga) kelompok sebagai pelaku digital forensik, yaitu:

a. Collection Specialist,yang bertugas sebagai pengumpul barang bukti, yang berupa digital evidence;
b. Examiner, yang memiliki kemampuan sebagai penguji terhadap media dan untuk mengekstrak data;
c. Investigator, yang memiliki keahlian yaitu ahli atau sebagai penyidik.

e). Pemeriksaan terhadap ahli-ahli, dalam kasus *Cyber Crime* yang terkait adalah Ahli Informasi dan Transaksi Elektronik (ITE), dan Ahli Digital Forensik.

Berdasarkan Pasal 120 KUHAP, apabila dianggap perlu oleh penyidik, ia dapat meminta bantuan pendapat seorang ahli atau orang yang memiliki keahlian khusus untuk membantu proses penyidikan.

Ahli Digital Forensik bertugas untuk menganalisis bukti digital, bukti yang telah didapatkan oleh penyidik perlu di explore kembali guna untuk melakukan pengusutan suatu perkara seperti:

1) Siapa yang telah melakukan;
2) Apa yang telah dilakukan;
3) Apa saja software yang digunakan;
4) Hasil proses apa yangdigunakan;
5) Waktu melakukan

f). Mengirim berkas perkara tindak pidana perjudian online kepada Jaksa Penuntut Umum (JPU).

Dalam mengirim berkas perkara tindak pidana perjudian secara online ini harus berdasarkan ketentuan yang tercantum dalam KUHAP. Pasal 8 ayat (3) KUHAP, menyebutkan penyerahan berkas perkara ke JPU, yaitu sebagai berikut:

Penyerahan berkas perkara sebagaimana dimaksud dalam ayat (2) dilakukan:

1. pada tahap pertama penyidik hanya menyerahkan berkas perkara.
2. dalam hal penyidikan sudah dianggap selesai, penyidik menyerahkan tanggung jawab atas tersangka dan barang bukti kepada penuntut umum.

g). Ketika penyidikan dianggap sudah selesai, maka penyidik menyerahkan tersangka dan barang bukti ke JPU

Menanggapi hal tersebut di atas, menurut Bripka yudhiyanto Ba nit *Cyber Crime* Reskrimsus Polda Sulsel, menyatakan bahwa secara umum proses penyidikan kejahatan *Cyber Crime* tidak jauh beda 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, dikarenakan mudah hilangnya alat bukti dann juga 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. (Wawancara 8 oktober 2020).

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 dilakukan dengan cara penyelidikan pelacakan (tracking) dan harus melibatkan saksi ahli bahasa untuk mengetahui apakah konteks bahasa yang digunakan oleh pelaku adalah tindak pidana atau bukan. Dalam hal penyelidikan yang dilakukan secara pelacakan (tracking) diatur dalam Pasal 24 huruf e Perkap No 14 Tahun 2012, sebagai berikut:

1. mencari dan mengikuti keberadaan pelaku tindak pidana dengan menggunakan teknologi informasi;
2. melakukan pelacakan melalui kerja sama dengan Interpol, kementrian/lembaga/badan/komisi/instansi terkait;dan
3. melakukan pelacakan aliran dana yang diduga dari hasil kejahatan.

Namun berdasarkan hasil wawancara, pihak Polda Sulsel 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. Dalam proses penyidikan kasus ini, dilakukan berdasarkan 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 polda sulsel 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.

Setelah penyidikan lengkap dan dituangkan dalam bentuk berkas perkara maka permasalahan yang ada adalah masalah barang bukti karena belum samanya persepsi diantara aparat penegak hukum, barang bukti digital adalah barang bukti dalam kasus *Cyber Crime* yang belum memiliki rumusan yang jelas dalam penentuannya sebab digital evidence tidak selalu dalam bentuk fisik yang nyata. Misalnya untuk kasus pembunuhan sebuah pisau merupakan barang bukti utama dalam melakukan pembunuhan sedangkan dalam kasus *Cyber Crime* barang bukti utamanya adalah komputer tetapi komputer tersebut hanya merupakan fisiknya saja sedangkan yang utama adalah data di dalam hard disk komputer tersebut yang berbentuk file, yang apabila dibuat nyata dengan print membutuhkan banyak kertas untuk menuangkannya, apakah dapat nantinya barang bukti tersebut dalam bentuk compact disc saja, hingga saat ini belum ada Undang-Undang yang mengatur mengenai bentuk dari pada barang bukti digital (digital evidence) apabila dihadirkan sebagai barang bukti di persidangan (Wawancara 8 oktober 2020).

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 perundangundangan.
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, 80% 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 Reskrimsus Polda Sulsel dibawa ketahap pengadilan.

Informasi yang kami dapatkan di atas, dalam hal bentuk penyelesaiannya sebagaimana yang diatur dalam UU No.11 tahun 2008 tentang ITE pada pasal 38 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 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.

Menurut Soerjono Soekanto bahwa untuk mengukur apakah hukum itu, berhasil atau gagal dalam mencapai tujuannya, maka hal itu biasanya diukur, apakah pengaruhnya berhasil mengatur sikap tindak atau perilaku tertentu, sehingga tercapai dengan tujuannya atau tidak (Soekanto, 1985).

Pernyataan tersebut di atas, pada dasarnya memperlihatkan bahwa hal berlakunya hukum, ialah mewujudkan hukum itu sebagai perilaku. Hukum yang dimaksud disini, adalah dalam kaidah yang terkait denganhukum substansi (hukum materil) dan hukum tata cara (hukum formal).

Agar hukum dapat efektif dalam masyarakat menurut Lawrence M. Friendman dalam Achmad Ali, maka hal ini terkait dengan legal system sebagai unsur-unsurnya. Adapaun unsur-unsur tersebut, adalah:

1. *Substantive rules of law;*
2. *Legal institution; dan*
3. *The legal culture* (Ali, 1998).

Agar hukum berfungsi melindungi kepentingan manusia dalam pergaulan hidupnya, maka hukum harus dilaksanakan. Pelaksanaan hukum dapat berlangsung secara normal, dan juga dapat berlangsung karena adanya pelanggaran hukum melalui penegakan hukum. Artinya hukum yang telah dilanggar harus dipulihkan melalui penegakan hukum, agar kembali normal. Namun demikian, oleh Sudikno dan A. Pitlo dinyatakan bahwa, dalam menegakkan hukum ada tiga unsur yang selalu harus diperhatikan, yaitu: kepastian hukum (rechtzekerheid), kemanfaatan (zwechtigheid)

dan keadilan (gerechtigheid). Ketiga unsur tersebut, harus diterapkan secara proporsional dan berimbang.

Demikian pula Soerjono Soekanto memandang bahwa penegakan hukum dipengaruhi oleh lima faktor, yaitu: (Soekanto, 1993)

a. materi hukum atau undang-undang;
b. penegakan hukum;
c. sarana dan fasilitas;
d. masyarakat, yakni lingkungan dimana hukum tersebut berlaku;

Budaya masyarakat. Kelima faktor tersebut, saling berkaitan erat karena merupakan esensi dari penegakan hokum demi mencapai sebuah keefektifan dalam penerapan hukum .

B. Faktor Penghambat Upaya Kepolisian dalam penanggulangan kejahatan *Cyber Crime* di Sulawesi Selatan

Efektivitas berlakunya aspek pidana dalam UU ITE dapat dilihat dari aspek subtansi dan struktur hukumnya yang meliputi penegak hukum, sumber aparatur penegak hukumnya peran serta masyarakat dalam konteks penegakan hukum dan juga harus didukung sarana dan prasarana supaya penegakan hukum dengan teknologi informasi pemerintah terwujud. Berikut adalah Faktor Pendukung & Penghambat upaya kepolisian dalam penanggulangan kejahatan Cyber Crime di Sulawesi Selatan.

Dalam upaya penanggulangan *Cyber Crime* oleh aparat kepolisian terdapat beberapa kendala yang menghambat upaya penanggulangan *Cyber Crime*, penulis kemudian memaparkannya berdasarkan hasil wawancara dan penelusuran referensi, bahwa penindakan kasus *Cyber Crime* sering mengalami hambatan yaitu:

1. Dalam Hal Penangkapan Tersangka Dan Penyitaan Barang Bukti.

Dalam penangkapan tersangka sering kali kita tidak dapat menentukan secara pasti siapa pelakunya karena mereka melakukannya cukup melalui komputer yang dapat dilakukan dimana saja tanpa ada yang mengetahuinya sehingga tidak ada saksi yang mengetahui secara langsung. Hasil pelacakan paling jauh hanya dapat menemukan IP Address dari pelaku dan komputer yang digunakan. Hal itu akan semakin sulit apabila menggunakan warnet sebab saat ini masih jarang sekali warnet yang melakukan registrasi terhadap pengguna jasa mereka sehingga kita tidak dapat mengetahui siapa yang menggunakan komputer tersebut pada saat terjadi tindak pidana.

Penyitaan barang bukti banyak menemui permasalahan karena biasanya pelapor sangat lambat dalam melakukan pelaporan, hal tersebut membuat data serangan di log server sudah dihapus biasanya terjadi pada kasus deface, sehingga penyidik menemui kesulitan dalam mencari log statistik yang terdapat di dalam server sebab biasanya secara otomatis server menghapus log yang ada untuk mengurangi beban server. Hal ini membuat penyidik tidak menemukan data yang dibutuhkan untuk dijadikan barang bukti sedangkan data log statistik merupakan salah satu bukti vital dalam kasus hacking untuk menentukan arah datangnya serangan (Wawancara 8 oktober 2020)

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

Keterbatsan tenaga ahli pada pihak kepolisian memang merupakan factor yang sangat besar, dengan jumlah anggota ahli yang terbatas ini pengungkapan dan penyidikan kasus kejahatan dunia maya tidak bisa diselesaikan dengan waktu yang cepat, sehingga akan membuat para pelaku lebih leluasa dalam beraksi Keterbatasan jumlah personil tenaga ahli sebenarnya bisa diatasi dengan adanya pelatihan-pelatihan baik oleh kepolisian atau pihak universitas dan perguruan tinggi negri atau swasta yang terdapat fakultas teknologi informasi.

Langkah ini perlu dilakukan untuk merekrut tenaga-tenaga ahli teknologi informasi terutama sekali para pelajar dan mahasiswa yang memiliki keahlian dibidang IT (Information technology) pihak dosen dan mahasiswa memiliki peran yang sangat startegis sebab merekalah yang paling bisa mengikuti perkembangan IT. Para praktisi juga bisa memebrikan peran penting dalam memberikan masukanmasukan kepada pihak pemerintah dalam keamanan jaringan computer dan internet. Mendesaknya kebutuhan tenaga ahli juga harus diimbangi dengan adanya sarana dan prasarana serta fasilitas peralatan yang canggih dan maju dalam mendukung keamanan jaringan dan juga untuk memudahkan pelacakan pelaku kejahatan agar kasus kejahatan dunia maya dapat di atasi dengan cepat

3. Sulit memperoleh saksi kejahatan.

Saat ini sistem pembuktian hukum di Indonesia (khusunya dalam Pasal 184 KUHAP) belum mengenal istilah bukti elektronik/digital (digital evidence) sebagai bukti yang sah menurut undang-undang. Masih banyak perdebatan khususnya antara akademisi dan praktisi mengenai alat bukti elektronik tersebut.

Sementara itu dalam proses penyidikan kasus *Cyber Crime*, alat bukti elektronik memiliki peran penting dalam penanganan kasus. Alat bukti dalam kasus *Cyber Crime* berbeda dengan alat bukti kejahatan lainnya dimana sasaran atau media *Cyber Crime* merupakan data-data atau sistem komputer / internet yang sifatnya mudah diubah, dihapus, atau disembunyikan oleh pelaku kejahatan. Selain itu saksi korban.

Dalam Kasus *Cyber Crime* berperan sangat penting dimana jarang sekali terdapat saksi dalam kasus *Cyber Crime* dikarenakan saksi korban yang berada di luar daerah atau bahkan berada di luar negeri yang mengakibatkan penyidik sulit untuk melakukan pemeriksaan saksi dan pemberkasan hasil penyelidikan. Penuntut umumu 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. Hal serupa dialami oleh penyidik Reskrimsus *Cyber Crime* Polda Sulsel dimana sangat kesulitan menangani kasus *Cyber Crime* terkait aspek alat bukti karena terkadang alat bukti yang berupa data-data tersebut telah diubah atau dihapus, namun beda halnya ketika pelaku *Cyber Crime* tertangkap tangan dalam melakukan aksi kejahatannya dimana alat bukti dapat langsung diamankan oleh petugas kepolisian.

1. Keberadaan pelaku yang sulit dideteksi di karenakan fasilitas yang kurang memadai.

Dalam mengungkap kasus-kasus *Cyber Crime* dibutuhkan fasilitas yang mampu menunjang kinerja aparat kepolisian. Fasilitas tersebut berupa laboratorium forensik komputer yang digunakan untuk mengungkap data-data yang bersifat digital serta merekam dan menyimpan bukti-bukti yang berupa soft copy (gambar, program, html, suara, dan lain sebagainya).

Komputer forensik merupakan salah satu cabang ilmu forensik yang berhubungan dengan bukti hukum yang ditemukan dalam komputer maupun media penyimpanan secara digital. Computer forensic dikenal sebagai digital forensic. 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. Contohnya, melalui Forensik Internet, kita dapat megetahui siapa saja orang yang mengirim email kepada kita, kapan dan dimana keberadaan pengirim. Dalam contoh lain kita bisa melihat siapa pengunjung website secara lengkap dengan informasi IP Address, komputer yang dipakainya dan keberadaannya serta kegiatan apa yang dilakukan pada website kita tersebut .

Kemampuan forensik digital menggunakan fasilitas yang hanya dimiliki oleh laboratorium forensik komputer. Terkait dengan hal tersebut unit *Cyber Crime* Polda Sulsel belum memiliki fasilitas berupa laboratorium forensik komputer, yang mengakibatkan terkendalanya upaya penanggulangan *Cyber Crime* diwilayah hukum Polda Sulsel.

1. Akun anonimus (akun yg tdk mencantumkan identitas asli).

Dalam penangkapan tersangka sering kali kita tidak dapat menentukan secara pasti siapa pelakunya karena mereka melakukannya dengan mengunakan Akun anonimus (akun yg tdk mencantumkan identitas asli) dan cukup melalui komputer yang dapat dilakukan dimana saja tanpa ada yang mengetahuinya sehingga tidak ada saksi yang mengetahui secara langsung (Djanggih % Qamar, 2018). Hasil pelacakan paling jauh hanya dapat menemukan IP Address dari pelaku dan komputer yang digunakan. Hal itu akan semakin sulit apabila menggunakan warnet sebab saat ini masih jarang sekali warnet yang melakukan registrasi terhadap pengguna jasa mereka sehingga kita tidak dapat mengetahui siapa yang menggunakan komputer tersebut pada saat terjadi tindak pidana.

Berdasarkan faktor-faktor diatas jika dilihat dari teori efektivitas implementasi UU ITE memang belum efektif dalam menanggulangi cyber Dalam kasus kasus yang terjadi seperti cyber crime sering mengalami hambatan terutama dalam hal penangkapan tersangka dan penyitaan barang bukti, seringkali kepolisian tidak dapat menentu kan secara pasti siapa pelakunya, karena para pelaku kejahatan dalam melakukan aksinya sehingga sangat menyulitkan dalam melakukan pelaporan dan pemeriksaan untuk dimintai keterangan dalam berita acara pemeriksaan saksi korban. Dan juga Undang-Undang ITE tidak akan dapat dijalankan dan diterapakan dengan baik apabila tidak adanya kerjasama antara aparat penegak hukum dengan masyarakat luas. Dengan demikian faktor yang dapat mem pengaruhi efektivitas suatu perundang-undangan adalah profesional dan optimal pelaksanaan peran, wewenang dan fungsi dari para penegak hukum, baik didalam menjalankan tugas

yang dibebankan terhadap diri mereka ataupun dalam menegakkan peundang-undangan tersebut

KESIMPULAN

1. Upaya Kepolisian terhadap penyidikan Tindak Pidana penyalahgunaan Informasi dan Transaksi Elektronik (ITE) yaitu dengan melakukan upaya *Preventif* yaitu dengan mencegah sebelum terjadinya pelanggaran tindak pidana dan upaya *Represif* yaitu upaya penegakan hukum kepada pelanggar tindak pidana sesuai dengan ketentuan yang berlaku dengan menjalankan prosedur KUHAP dan Peraturan Kabareskrim nomor 14 tahun 2012.
2. Faktor-faktor penghambat pencegahan dan penanggulangan *cybercrime* sebagai upaya pembaharuan hukum adalah: Pertama, Dalam Hal Penangkapan Tersangka Dan Penyitaan Barang Bukti.. Kedua, Kurangnya saksi ahli, dalam hal ini saksi ahli gambar dan saksi ahli bahasa.. Ketiga, Sulit memperoleh saksi kejahatan. Keempat, Keberadaan pelaku yang sulit dideteksi di karenakan fasilitas yang kurang memadai.Kelima, Akun anonimus (akun yg tdk mencantumkan identitas asli.

SARAN

1. Perbaikan substansi hukum tentang *cybercrime* dalam UU ITE, serta bagi aparat penegak hukum harus lebih menguasi tentang teknologi komputer serta memperbaiki sarana prasarana yang ada guna mendukung dalam penanganan perkara tindak pidana siber.
2. Pemerintah harus ikut membantu upaya penanggulangan dengan cara menyediakan lapangan kerja yang layak untuk sumber daya manusia yang belum terpakai agar kemampuan mereka tidak lagi disalahgunakan untuk melakukan kejahatan, juga harus memperhatikan aturan-aturan terkait informasi dan transaksi elektronik guna mengurangi celah hukum yang dapat timbul, dan pemerintah harus menyediakan fasilitas yang mampu mendukung upaya penindakan penyalahgunaan informasi dan transaksi elektronik (ITE).
3. Perlunya untuk meningkatkan kemampuan penyidik khususnya pada aparat kepolisian dengan memberikan pendidikan khusus terkait masalah *Cyber Crime*. Untuk masyarakat sebaiknya membekali atau meningkatkan system keamanan media elektronik yang terhubung dengan internet guna menghindari adanya aksesakses illegal dari pihak luar serta masyarakat juga harus turut membantu penegakan hukum terkait *Cyber Crime*, dengan melaporkannya keaparat kepolisian jika melihat atau pun menjadi korban penyalahgunaan informasi dan transaksi elektronik (ITE

DAFTAR PUSTAKA

Ali, A. (1998). *Menjelajahi kajian empiris terhadap hukum*. Yarsif Watampone.

Azis, A. (2016). Tindak Pidana Penyebaran Informasi Yang Menimbulkan Rasa Kebencian Atau Permusuhan Melalui Internet Di Indonesia (Kajian Terhadap Pasal 28 Ayat (2) Uu No. 11 Th 2008 Juncto Pasal 45 Ayat (2) Uu No. 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik). *Pakuan Law Review*, *2*(2), 325-358.

Djanggih, H., & Qamar, N. (2018). Penerapan Teori-Teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime). *Pandecta Research Law Journal*, *13*(1), 10-23.

Fonna, N. (2019). *Pengembangan Revolusi Industri 4.0 dalam Berbagai Bidang*. Guepedia.

Fuady, M. E. (2005). "Cybercrime": Fenomena Kejahatan melalui Internet di Indonesia. *Mediator: Jurnal Komunikasi*, *6*(2), 255-264.

Kasemin, H. K. (2016). *Agresi Perkembangan Teknologi Informasi*. Prenada Media.

Manan, H. A., & SH, S. (2018). *Aspek-aspek pengubah hukum*. Prenada Media.

Lathif, N. (2017). Teori Hukum Sebagai Sarana Alat Untuk Memperbaharui Atau Merekayasa Masyarakat. *Pakuan Law Review*, *3*(1), 73-94.

Paripurna, G. T. (2008). Sekilas tentang kejahatan transnasional.

Raharjo, A. (2002). *Cybercrime: Pemahaman dan upaya pencegahan kejahatan berteknologi*. Citra Aditya Bakti.

Riwayadi, P. (2013). Pemanfaatan Perkembangan Teknologi Informasi Dan Komunikasi Untuk Kemajuan Pendidikan Di Indonesia. *available at PLS-UM Database*.

Soekanto, S. (1993). *Beberapa teori sosiologi tentang struktur masyarakat*. PT RajaGrafindo Persada.

Soekanto, S. (1985). *Perspektif Teoritis Studi Hukum dalam Masyarakat*. Rajawali, Jakarta.

Usman, A. H. (2015). Kesadaran Hukum Masyarakat Dan Pemerintah Sebagai Faktor Tegaknya Negara Hukum Di Indonesia. *Jurnal Wawasan Yuridika*, *30*(1), 26-53.