



Bentuk Penanggulangan dan Pencegahan terhadap Tindak Pidana Penipuan Lowongan Kerja Online

Alifia Risma Marselyna, Indrawati, Nahdiya Sabrina

Fakultas Hukum UniversitasMerdeka; Jl. Terusan Raya Dieng Nomor 62-64; Malang; 65146; JawaTimur; Indonesia

Abstrak

Saat ini telah banyak ditemui kejahatan yang memanfaatkan kecanggihan perkembangan internet yaitu seperti kejahatan yang dilakukan melalui online atau biasa disebut Cyber Crime. Hal ini didasari pada argumentasi bahwa Cyber Crime merupakan kegiatan yang memanfaatkan komputer sebagai media yang didukung oleh sistem komunikasi baik itu Dial Up System, menggunakan jalur telepon, ataukah wireless system yang menggunakan antena khusus yang nirkabel. Salah satu bentuk kejahatan yang berkaitan dengan penyalahgunaan sarana teknologi informatika adalah kejahatan atau tindak pidana lowongan kerja online yang diatur dalam Pasal 378 Buku II Kitab Undang-Undang Hukum Pidana (KUHP) dan Pasal 28 ayat (1) Jo. Pasal 45 ayat (2) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Tranaksi Elektronik. Penelitian ini berusaha menjawab latar belakang penipuan dalam lowongan pekerjaan online serta bentuk penanggulangan terhadap tindak pidana penipuan lowongan kerja online. Penelitian ini menggunakan metode penelitian yuridis normatif.

Abstract

Currently, there are many crimes that take advantage of the sophistication of internet developments, such as crimes that are committed online or commonly called Cyber Crime. This is based on the argument that Cyber Crime is an activity that uses computers as a medium that is supported by a communication system, whether it's a Dial Up System, using a telephone line, or a wireless system that uses a special wireless antenna. One form of crime related to the misuse of information technology facilities is a crime or criminal act of online job vacancies as regulated in Article 378 Book II of the Criminal Code (KUHP) and Article 28 paragraph (1) Jo. Article 45 paragraph (2) of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transaction. This study seeks to answer the background of fraud in online job vacancies as well as a form of countermeasures against fraud in online job vacancies. This study uses a normative juridical research method.

Kata kunci:

Penanggulangan; tindak pidana penipuan; lowongan kerja online

Keywords:

Countermeasures; fraud; online job vacancies

Korespondensi Penulis:

Nahdiya Sabrina

Email: sabrina.nahdiya@unmer.ac.id

1. Pendahuluan

Di era globalisasi saat ini telah banyak kemajuan akan adanya perkembangan media elektronik yang semakin pesat misalnya komputer sebagai salah satu contoh alat bantu dalam menyelesaikan sebuah pekerjaan. Tidak hanya komputer saja tetapi masih banyak lagi media elektronik lainnya yang semakin hari semakin pesat perkembangannya. Perkembangan teknologi informasi di era modern telah menyebabkan dunia menjadi tanpa batas dan menyebabkan perubahan sosial yang secara signifikan akan berlangsung secara cepat. Negara Indonesia merupakan negara berkembang yang kaya akan sumber daya manusianya. Tidak heran jika setiap manusia yang hidup sebagai bagian dari masyarakat dan juga warga negara Indonesia pasti membutuhkan lapangan pekerjaan guna menghidupi kehidupan sehari-harinya. Akan tetapi seiring berjalannya waktu semuanya lebih terasa mudah. Misalnya terkait lapangan pekerjaan yang masyarakat dapat mengaksesnya melalui media dan sarana komunikasi online.

Teknologi informasi yang seperti ini akan cukup berpengaruh dan berarti dalam memberikan kontribusi bagi peningkatan kesejahteraan taraf hidup masyarakat demi kemajuan dan peradaban manusia yang sekaligus dapat berpotensi menjadi arena efektif dalam upaya perbuatan melawan hukum. Usaha mewujudkan cita-cita hukum untuk mensejahterakan masyarakat melalui kebijakan hukum pidana bukanlah merupakan satu-satunya cara yang memiliki peran paling efektif. Dikatakan demikian, karena pada dasarnya bukanlah hanya hukum pidana yang juga menjadi satu-satunya sarana yang dimanfaatkan sebagai fungsi kontrol sosial dalam masyarakat. Kecanggihan teknologi komputer disadari telah memberikan kemudahan, terutama dalam membantu pekerjaan manusia. Selain itu, perkembangan teknologi komputer menyebabkan munculnya kejahatan-kejahatan baru, yaitu dengan memanfaatkan komputer sebagai modus operandinya. Penyalahgunaan

komputer dalam perkembangannya menimbulkan persoalan yang sangat rumit, terutama kaitannya dengan proses pembuktian pidana (Maskun, 2013)

Saat ini telah banyak ditemui kejahatan yang memanfaatkan kecanggihan perkembangan internet yaitu seperti kejahatan yang dilakukan melalui online atau biasa disebut Cyber Crime. Hal ini didasari pada argumentasi bahwa Cyber Crime merupakan kegiatan yang memanfaatkan komputer sebagai media yang didukung oleh sistem komunikasi baik itu Dial Up System, menggunakan jalur telepon, ataukah wireless system yang menggunakan antena khusus yang nirkabel (Raodia; 2019)

Konvergensi antara komputer dan sistem telekomunikasi sebagaimana di ataslah yang disebut dengan telematika. Sehingga jika menyebutkan kejahatan telematika, maka yang dimaksud juga adalah Cyber Crime. Akan tetapi di sisi lain, beberapa pakar tetap berpendapat bahwa baik kejahatan komputer, kejahatan Cyber, maupun kejahatan telematika adalah kejahatan yang sama dengan penamaan yang berbeda.

Beberapa kasus kejahatan Cyber yang sering ditemui adalah penipuan lowongan kerja online. Seperti halnya beberapa korban lulusan baru mahasiswa Unmer yang salah satu diantaranya bernama Bunga Ruthika Sari alumni Jurusan Akuntansi Fakultas Ekonomi dan Bisnis merasa dirugikan atas penipuan lowongan kerja online yang dialaminya. Terlebih penipuan tersebut menggunakan nama instansi atau perusahaan besar di Indonesia yaitu Pertamina dan PT. Angkasa Pura. Oleh karena korban bukan merupakan seseorang yang memahami hukum di Indonesia sangat disayangkan karena korban membiarkan dan mengacuhkan penipuan lowongan kerja online tersebut.

Kembali lagi seperti kasus yang sebelumnya sangatlah disayangkan ketika seseorang tersebut mengacuhkan kejadian tersebut. Terlebih lagi dan sangat jelas apabila korban telah mengalami kerugian nyata. Melihat fakta hukum sebagaimana

yang ada pada saat ini, dampak perkembangan ilmu pengetahuan dan teknologi yang telah disalahgunakan sebagai sarana kejahatan ini menjadi teramat penting untuk diantisipasi bagaimana kebijakan hukumnya, sehingga *Cyber Crime* yang terjadi dapat dilakukan upaya penanggulangannya dengan hukum pidana termasuk dalam hal ini adalah sistem pembuktiannya yang dapat dibidang lebih rumit daripada sistem pembuktian hukum pidana lainnya karena persoalan yang diasumsikan sebagai “maya” yaitu sesuatu yang tidak dapat dilihat atau semu. Dikatakan teramat penting karena dalam penegakan hukum pidana dasar kebenaran seseorang dapat dikatakan bersalah atau tidak melakukan tindak pidana, disamping perbuatannya dapat dipersalahkan atas kekuatan Undang-Undang yang telah ada sebelumnya (asas legalitas), juga perbuatan mana didukung oleh kekuatan bukti yang sah dan kepadanya dapat dipertanggungjawabkan (unsur kesalahan). Pemikiran demikian telah sesuai dengan penerapan asas legalitas dalam hukum pidana (KUHP) yakni sebagaimana dirumuskan secara tegas dalam Pasal 1 ayat (1) KUHPidana “Nullum delictum nulla poena sine praevia lege poenali” atau dalam istilah lain dapat dikenal “tiada pidana tanpa kesalahan” (Moeljatno ; 2002)

Mengingat berbagai bentuk pembuktian terkait *Cyber Crime* yang cukup sulit untuk dilakukan maka sudah seharusnya pengakuan hukum di Indonesia lebih ditegakkan yang mengatur masalah ini karena akan berdampak pula pada cacat hukum yang dapat dimanfaatkan oleh pelaku *Cyber Crime* untuk lepas atau bebas dari pemidanaan. Pasal 1 ayat (3) Undang-Undang Dasar 1945 menyatakan bahwa Indonesia adalah negara hukum (*recht staat*). Mengingat karena idealnya Negara Indonesia sebagai negara hukum maka kedudukan hukum di Indonesia harus ditempatkan diatas segalanya tanpa ada perkecualian terkait perbuatan yang dilakukan oleh setiap orang yang harus sesuai dengan aturan hukum yang ada. Kejahatan yang menggunakan sarana

teknologi informatika ini tergolong baru serta dapat berdampak bagi ketertiban dan kesejahteraan dalam masyarakat.

2. Metode Penelitian

Jenis penelitian yang digunakan adalah penelitian hukum normatif (yuridis normatif). Penelitian hukum normatif yaitu penelitian yang difokuskan untuk mengkaji penerapan kaidah atau norma yang ada dalam hukum positif. Dimana penelitian hukum ini dilakukan dengan cara mengkaji berbagai aturan-aturan hukum yang bersifat formil seperti halnya peraturan perundang-undangan. Maka dari itu berkaitan dengan penelitian ini adalah bertujuan untuk mengkaji terkait tinjauan yuridis terhadap tindak pidana penipuan lowongan kerja online ditinjau dari hierarki peraturan perundangundangan yang ada khususnya Pasal 28 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik.

3. Pembahasan

3.1. Latar belakang kejahatan penipuan online

Modus kejahatan dalam dunia maya memang agak sulit dimengerti oleh orang-orang yang tidak menguasai pengetahuan teknologi informasi. Sebab salah satu karakter pokok *Cyber Crime* adalah penggunaan teknologi informasi dalam modus operandinya (Sutarman; 2007). Sifat inilah yang membuat *Cyber Crime* berbeda dengan tindak pidana lainnya.

Latar belakang dari kejahatan penipuan lowongan online lainnya antara lain Internet yang sangat mudah diakses, hampir semua orang dan kalangan dapat mengakses internet melalui media komunikasi baik handphone maupun komputer yang tersambung jaringan internet. Hal tersebut memiliki nilai positif dan juga nilai negatif. Akan dapat bernilai positif apabila seseorang tersebut

menggunakan atau memanfaatkan internet sebagaimana mestinya sesuai fungsinya yang mungkin dapat memberikan keuntungan atau manfaat bagi pengguna internet tersebut. Hal tersebut akan bernilai negatif apabila seseorang menggunakan atau mengakses internet dengan maksud menyalahgunakan sehingga dapat dikatakan melakukan perbuatan melawan hukum.

Semua hal diatas kembali kepada masing-masing individu dari pengguna internet tergantung dari tujuan penggunaan internet itu sendiri. Modus operandi adalah pola suatu kejahatan yang dilakukan dalam penggunaan internet khususnya penyalahgunaan internet itu sendiri, dalam arti kata lain dapat diartikan bagaimana suatu kejahatan bisa terlaksana. Modus operandi itu sendiri ada 2 (dua) macam yaitu dengan cara konvensional yang artinya diselingi dengan pendapatan keuntungan dari pelaku kejahatan tersebut dan dengan cara sistematis yang artinya telah tersusun rapi atas segala sesuatu yang berkaitan dengan modus operandi tersebut.

Latar belakang selanjutnya adalah murahnya jaringan internet. Selain mudah diakses, internet juga sangat murah dan mudah untuk dijangkau. Seperti halnya penggunaan kuota atau pulsa bukan suatu hal yang sulit didapat. Dengan harga 15 ribu rupiah kita sudah mendapatkan 1 GB kuota yang pastinya bermanfaat guna membantu aktivitas keseharian pengguna internet dalam menjalankan aktivitasnya.

Selain beberapa latar belakang diatas, selanjutnya adalah Angka pengangguran yang masih tinggi menjadi latar belakang penipuan online. Angka pengangguran yang tinggi di negara indonesia juga bisa menjadi salah satu latar belakang terjadinya kejahatan penipuan online. Hal ini dibuktikan dengan adanya laporan oleh Deputi Bidang Koordinasi Ekonomi Kreatif, Kewirausahaan, dan Daya Saing Koperasi dan Usaha Kecil dan Menengah Kemenko Perekonomian, Rudy Salahudin, bebrapa waktu lalu yang sempat meng-

atakan bahwa saat ini pengangguran di Indonesia masih cukup tinggi. Ia mengatakan jumlah pengangguran di Indonesia masih cukup banyak yakni sekitar 70 juta orang. Menyambung dari pernyataan diatas dengan adanya tingkat pengangguran yang tinggi maka terdapat beberapa kemungkinan seseorang yang menganggur tersebut melakukan aktivitas yang dirasa mampu memberikan keuntungan baginya. Meskipun tanpa disadari perbuatan tersebut dilakukan dengan cara menipu dan melawan hukum.

Beberapa contoh kasus sebagai berikut diantaranya adalah penipuan lowongan kerja online yang mengatasnamakan PT. PERTAMINA dimana korban tersebut merupakan teman dari penulis sendiri. Dimana kejadian tersebut berawal dari korban atas nama Bunga Ruthika Sari yang melamar pekerjaan pada PT. PERTAMINA tersebut melalui salah satu website di Internet. Setelah itu korban mengirimkan semua persyaratannya melalui email. Akan tetapi setelah 2 hari berikutnya korban mendapatkan balasan email yang menyatakan bahwa korban diterima dan harus melwati test wawancara dengan syarat harus membayar beberapa biaya terlebih dahulu. Lowongan kerja tersebut adalah salah satu bagian dari penipuan lowongan kerja online namun sangat disayangkan pula karena kejadian tersebut tidak dilaporkan kepada pihak penegak hukum karena awam akan pemahaman hukumnya.

Kejadian lainnya juga menimpa Khanisa seorang mahasiswa yang baru saja lulus dari sebuah univesitas dan sedang melamar pekerjaan di beberapa perusahaan besar sesuai dengan bidang yang ia geluti. Tak berselang lama setelah korban mengirimkan beberapa surat lamaran secara *online* kepada perusahaan yang korban incar, Khanisa mendapatkan SMS dari nomor seluler yang tidak dikenal. Korban mendapatkan informasi bahwa korban telah diterima bekerja di sebuah perusahaan besar sesuai dengan aplikasi yang telah ia kirimkan melalui alamat *email* yang tertera

di *website*. Kemudian, korban diminta untuk mengirimkan sejumlah uang untuk keperluannya berangkat ke luar pulau untuk keperluan masa percobaan. Korban tidak mencurigai sesuatu apapun dan langsung saja mengirimkan sejumlah uang kepada pihak yang memintainya uang. Alhasil, uang korban raib dan pihak tak bertanggung jawab itu tidak dapat dihubungi kembali oleh korban. Kembali lagi seperti kasus yang sebelumnya sangatlah disayangkan ketika seseorang tersebut mengacuhkan kejadian tersebut. Terlebih lagi dan sangat jelas apabila korban telah mengalami kerugian nyata.

Kasus serupa lainnya adalah beberapa mahasiswa lulusan Fakultas Ilmu Sosial dan Politik Universitas Merdeka Malang yang juga mengalami hal serupa. Mereka adalah Bunga, Anggun, Dayu, Diana, Vita, dan Rendra. Pada awalnya mereka mendapatkan info lowongan kerja melalui *website* PT. Angkasa Pura yang dibagikan oleh teman-temannya melalui grup Whatsapnya. Hingga pada akhirnya para korban tersebut berniat untuk mencoba melamar dan mengirimkan persyaratannya melalui email tersebut. Setelah sehari berikutnya, mereka mendapatkan telepon yang mengatasnamakan perusahaan tersebut. Akan tetapi pada perbincangan tersebut, pihaknya meminta beberapa besaaran uang sebesar Rp. 7.500.000,- (tujuh setengah juta rupiah) yang disebutkan untuk keperluan administrasi. Dan anehnya mereka dinjanka 80% diterima menjadi karyawan pada perusahaan tersebut. Mirisnya, salah satu korban diantaranya yaitu dayu telah mentransfer uang tersebut kepada pihaknya dan berakhir hilang kontak setelah itu tidak ada kelanjutan berikutnya. Dari situ beberapa korban lainnya mengaku bahwa telah mengalami penipuan lowongan kerja online yang dilamarnya melalui *website online* tersebut. Akan tetapi sama saja korban tidak ada upaya untuk melaporkan kerugiannya kepada pihak yang berwenang karena alasannya korban pernah melapor namun tidak ada kelanjutan dari laporannya tersebut. Maka dari itu, miris sekali akan penega-

kan hukum di Indonesia sendiri yang kurang tegas dalam menangani beberapa kejahatan diantaranya penipuan lowongan kerja seperti yang dibahas dalam artikel ini.

3.2. Bentuk penanggulangan dan pencegahan terhadap tindak pidana penipuan lowongan kerja online.

Secara luas, tindak pidana siber ialah semua tindak pidana yang menggunakan sarana atau dengan bantuan Sistem Elektronik. Itu artinya semua tindak pidana konvensional dalam Kitab Undang-Undang Hukum Pidana (KUHP) sepanjang dengan menggunakan bantuan atau sarana Sistem Elektronik seperti perdagangan orang, dapat termasuk dalam kategori tindak pidana siber dalam arti luas. Akan tetapi, dalam pengertian yang lebih sempit, pengaturan tindak pidana siber diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Sejak tahun 2008 kejahatan yang berkaitan dengan komputer sudah banyak diadili berdasarkan Undang-Undang No. 11 Tahun 2008.

Kejahatan komputer adalah perbuatan melawan hukum yang dilakukan dengan memakai komputer sebagai sarana/alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. Secara ringkas kejahatan komputer didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan penggunaan teknologi komputer yang canggih (Brisilia;2018).

Sanksi yang diberikan oleh tata hukum dengan maksud untuk menimbulkan perbuatan tertentu yang dianggap sudah semestinya dikehendaki oleh pembuat Undang-Undang. Pelanggaran terhadap norma hukum akan berakibat adanya sanksi hukum yang sifatnya memaksa, yaitu hukuman mati, hukuman penjara atau kurungan, dan hukuman denda. Saksi disini juga berfungsi sebagai salah satu upaya untuk melindungi pihak-pihak yang terancam kepentingannya. Sehingga dengan

sanksi tersebut dapat terlaksana upaya preventif dan represif dalam penegakan hukum sebagai upaya perlindungan hukum kepentingan masyarakat (Timbul Mangaratua;2018).

Perkembangan ilmu pengetahuan dan teknologi memberikan dampak pada munculnya kejahatan berdimensi baru, yang termasuk di dalamnya *Cyber Crime*. Kriminalisasi tindak pidana siber dalam peraturan perundang-undangan Indonesia tersebut memiliki implikasi terhadap upaya penanggulangan atau pemberantasan tindak pidana siber di Indonesia (Supanto;2016). Sejalan dengan hal itu diperlukan upaya penanggulangan untuk menjamin ketertiban di dalam masyarakat. Dalam perspektif hukum, upaya ini direalisasikan dengan hukum pidana.

Hukum pidana diharapkan mampu memenuhi cita ketertiban masyarakat. Akan tetapi dalam menghadapi dalam menghadapi perkembangan masyarakat, hukum pidana tidak selamanya mampu menjawab terhadap dampak negatif yang timbul, yang disebut kejahatan. Ini dikarenakan teknologi yang membawa perubahan dalam masyarakat berkembang begitu pesat, sementara hukum pidana merupakan produk sejarah yang sudah berjalan dalam logika sejarah yang menaunginya, walaupun dalam batas tertentu mempunyai prediktabilitas atas perkembangan masyarakat (Marita; 2019).

Sarana kebijakan penanggulangan tindak pidana *Cyber Crime* dapat dilakukan dengan menggunakan sarana *penal* (hukum pidana), maka kebijakan hukum pidana (*penal policy*) harus memperhatikan dan mengarah pada tercapainya tujuan dari kebijakan sosial berupa *social welfare* dan *social defence*. Penanggulangan kejahatan harus ada keseimbangan antara sarana *penal* dan *non penal*.

Penanggulangan *Cyber Crime* memerlukan panduan kebijakan penal dan non penal secara terencana, terarah, dan profesional. Langkah kebijakan penal adalah melakukan kriminalisasi terhadap perbuatan yang berkategori *Cyber Crime*, dan

penalisasi sebagaimana diatur dalam hukum pidana, pembaruan hukum acara pidana, dan pembaruan hukum penitensir. Sedangkan langkah-langkah kebijakan non penal di Indonesia, yaitu melakukan upaya berikut (Barda Nawawi Arief; 2007):

Pertama; Mempengaruhi pandangan masyarakat tentang kejahatan dan pidanaan melalui media massa, yaitu dengan cara mendeskripsikan, menayangkan, meneliti, dan membahas berdasarkan kajian ilmiah tentang *Cyber Crime* di media massa oleh pihak-pihak yang kompeten secara proporsional.

Kedua ;Pencegahan tanpa menggunakan pidana, meliputi kerjasama antarnegara, kerjasama antar pelaku atau antarpraktisi teknologi informasi, meningkatkan pengamanan sistem atau jaringan komputer, mengembangkan kode etik profesi teknologi informasi dan sertifikasi teknologi informasi, meningkatkan kebijakan sosial, mengembangkan kesehatan mental masyarakat, perbaikan kesehatan mental secara nasional, meningkatkan kesejahteraan sosial dan kesejahteraan anak-anak, dan optimalisasi penerapan hukum.prasarana sistem, peningkatan kualitas sumber daya manusia, dan peningkatan partisipasi masyarakat dalam sistem peradilan pidana.

Berdasarkan hal tersebut, penggunaan hukum pidana untuk mencegah dan memberantas tindak pidana siber pada hakekatnya sesuai dengan *cost and benefit principle*. Penggunaan hukum pidana dalam mencegah dan memberantas tindak pidana siber lebih menguntungkan dibanding dengan potensial kerugian yang terjadi oleh tindak pidana siber yang sangat besar dan luas. Permasalahan dalam penggunaan hukum pidana untuk mencegah dan memberantas tindak pidana siber adalah bagaimana mengefektifkan perundang-perundangan dan meningkatkan sumber daya manusia dan sarana prasarana dalam penegakan hukum.

Usaha Pencegahan tindak pidana penipuan yang dilakukan secara online melalui sarana penal diatur dalam Pasal 28 ayat 1 UU ITE yang mengatur bahwa penyebaran berita bohong dan penyesatan merupakan padanan kata yang semaksa dengan penipuan. Tujuan dari penipuan bisa untuk menguntungkan dirinya yang berakibat kerugian kepada orang lain. Kebijakan perundang-undangan terkait penipuan secara fungsional merupakan prioritas yang harus diterapkan oleh Pemerintah guna menanggulangi cyber crime.

Keberadaan hukum pidana bertujuan untuk menyelamatkan kerugian yang diderita oleh masyarakat karena kejahatan yang mengganggu aktivitas sosio-ekonomi mereka. Penegakan hukum harus diprioritaskan dalam masalah ini agar supaya peran hukum pidana menjadi fungsional dalam menanggulangi penipuan secara online.

4. Simpulan

Modus kejahatan dalam dunia maya memang agak sulit dimengerti oleh orang-orang yang tidak menguasai pengetahuan teknologi informasi. Karakter pokok cyber crime yang tidak sama dengan tindak pidana lainnya, membuat kejahatan seperti ini membutuhkan formula yang lebih optimal dalam penegakannya. Formula itu telah diterapkan oleh Pemerintah melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang dijadikan asas legalitas disetiap tindak pidana yang berkaitan dengan cyber crime.

Penanggulangan *Cyber Crime* tidak cukup dengan adanya Undang-undang yang mengaturnya, tetapi memerlukan panduan kebijakan penal dan non penal secara terencana, terarah, dan profesional. Pertama langkah kebijakan penal, yaitu melakukan kriminalisasi terhadap perbuatan yang berkategori *Cyber Crime*, dan penalisasi sebagaimana diatur dalam hukum pidana, pembaruan hukum acara pidana, dan pembaruan hukum peni-

tensir. Kedua kebijakan non penal, yaitu melalui memberikan wawasan kepada masyarakat terkait cyber crime dengan menayangkan melalui media massa dan Pencegahan tanpa menggunakan pidana, meliputi kerjasama antarnegara, kerjasama antar pelaku atau antarpraktisi teknologi informasi, meningkatkan pengamanan sistem atau jaringan komputer, mengembangkan kode etik profesi teknologi informasi dan sertifikasi teknologi informasi.

Harapan kedepannya adalah adanya dasar hukum melalui Undang-Undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta adanya konsep kebijakan penal dan non penal terkait cyber crime dapat dioptimalkan oleh aparat penegak hukum, serta adanya partisipasi oleh masyarakat. Penegakan hukum pidana yang terpadu diharapkan dapat menjadi fungsionalisasi hukum pidana dalam penanggulangan tindak pidana penipuan secara online.

Daftar pustaka

- Barda Nawawi Arief, (2007), *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, Jakarta: Kencana
- H. Sutarman, (2007), *Cyber Crime, Modus Operandi dan Penanggulangannya*. Yogyakarta : PRESSindo.
- Maskun, (2013), *Kejahatan Siber (Cyber Crime) Suatu Pengantar*, Jakarta: Kencana.
- JURNAL
- Brisilia Tumulun, *Upaya Penanggulangan Kejahatan Komputer dalam Sistem Elektronik Menurut Pasal 30 Undang-Undang Nomor 11 Tahun 2008*, Lex Et Societatis Vol. VI/No. 2/April/2018
- Marita, Lita Sari. *Cyber Crime dan Penerapan Cyber Law dalam Pemberantasan Cyber Law di Indonesia*. Cakrawala - Jurnal Humaniora, [S.l.], v. 15, n. 2, jan. 2019. ISSN 2579-3314.
- Raodia Raodia, *Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (Cyber Crime)*, Jurnal Jurisprudentie vol. 6 No. 2 2019,

Bhirawa Law Journal

Volume 1, Issue 1, May 2020

Universitas Islam Negeri Alauddin Makassar ISSN
Print: 2355-9640 ISSN Online: 2580-5738

Supanto, *Perkembangan Kejahatan Teknoogi Informasi (Cyber Crime) dan Antisipasinya dengan Penal Policy, Yustisia*. Vol.5 No.1 Januari - April 2016

Timbul Mangaratua Simbolon dkk, *Kebijakan Hukum Pidana Terhadap Tindak Pidana Penghinaan Atau Pencemaran Nama Baik Melalui Internet Di Indonesia Sebagai Cybercrime*, *Jurnal Daulat Hukum* Vol. 1. No. 1 Maret 2018 ISSN: 2614-560X