TINJAUAN YURIDIS MELALUI PENIPUAN LOWONGAN KERJA *ONLINE* BERDASARKAN PERSPEKTIF HUKUM UU NOMOR 11 TAHUN 2008 DAN KUHP

DISUSUN DAN DIAJUKAN OLEH :

OLIVIA QORINA AUDAH

ID No. 017201405002

PROGRAM STUDI ILMU HUKUM

UNIVERSITAS PRESIDEN

BEKASI

2017

PENGESAHAN SKRIPSI

Skripsi yang berjudul "TINJAUAN YURIDIS MELALUI PENIPUAN LOWONGAN KERJA *ONLINE* BERDASARKAN PERSPEKTIF HUKUM NOMOR 11 TAHUN 2008 DAN KUH PIDANA" disiapkan dan diajukan oleh Olivia Qorina Audah dalam memenuhi persyaratan untuk gelar S1 program studi Ilmu Hukum. Skripsi ini telah direview oleh dosen pembimbing sebagai persyaratan untuk siding skripsi.

Cikarang 22 Februari 2018

Pembimbing I	Pembimbing II
Fennieka Kristianto, S.H., M.H., M.A., M.Kn.	Mahayoni, S.H.,M.H

DEKLARASI SKRIPSI

Menyatakan bahwa skripsi yang berjudul “TINJAUAN YURIDIS MELALUI PENIPUAN LOWONGAN KERJA *ONLINE* BERDASARKAN PERSPEKTIF HUKUM UU ITE DAN KUH PIDANA “ adalah judul dan isi yang terbaik dari pengetahuan dan kepercayaan saya sendiri. Skripsi ini belum pernah diajukan sebagaian atau seluruhnya ke Universitas lain sebagai syarat mendapat gelar sarjana Program Studi Ilmu Hukum.

Bekasi, 22 Februari 2018

Olivia Qorina Audah

LEMBAR PERSETUJUAN DAN PEMERIKSAAN

Skripsi berjudul “TINJAUAN YURIDIS MELALUI PENIPUAN LOWONGAN KERJA ONLINE BERDASARKAN PERSPEKTIF HUKUM UU ITE DAN KUH PIDANA’’ telah selesai disusun dan diajukan oleh Olivia Qorina Audah jurusan Hukum Fakultas Humaniora telah dinilai dan disetujui untuk lulus ujian secara lisan pada tanggal 22 Februari 2018.

Sujana Donandi, S.H.,M.H

Penguji Skripsi

Fennieka Kristianto, S.H., M.H., M.A., M.Kn.

Pembimbing I

Mahayoni, S.H.,M.H

Pembimbing II

ABSTRAK

Penelitian ini untuk menganalisa unsur-unsur penipuan pada lowongan kerja *online* menurut KUHPidana dan UU Nomor 11 Tahun 2011dan penerapan Undang-Undang Nomor 11 Tahun 2011 dalam upaya menegakan hukum dan menanggulangi kejahatan penipuan lowongan kerja *online*.

Jenis metode digunakan normatif menganalisa peraturan terkait penerapan Undang-Undang penipuan lowongan kerja *online* dan data-data lapangan yang diberikan oleh DPRD Kab.Bekasi. Jenis data digunakan data sekunder yaitu buku, jurnal dan mengadakan wawancara kepada pemilik penyewaan internet untuk membuktikan bahwa penggunaan internet sangat murah dan mudah diakses. Analisis menggunakan metode analisis deskriptif yang akan menggunakan aspek hukum disertai dengan analisa berdasarkan KUHPidana dan UU Nomor 11 Tahun 2008. Hasil penelitian penipuan pada lowongan kerja *online* menurut KUHPidana dan UU Nomor 11 Tahun 2011 unsur-unsur pada pasal 378 KUHP, apabila pihak yang menyediakan informasi mengenai lowongan kerja *online* tersebut memenuhi unsur-unsur dalam Pasal 378 KUHP, yakni secara melawan hukum memakai nama palsu pada *website*, dengan tipu muslihat, rangkaian kebohongan, dan menggerakkan pelamar untuk menyerahkan sesuatu kepadanya, maka pihak yang dirugikan dapat menuntut secara pidana pihak yang menyediakan informasi lowongan kerja palsu tersebut atas dasar tindak pidana penipuan. Unsur-unsur pada pasal 28 ayat 1 UU Nomor 11 Tahun 2011perbuatan dengan sengaja memang terkandung niat jahat dalam perbuatan itu. Unsur lain mensyaratkan berita bohong dan menyesatkan tersebut mengakibatkan suatu kerugian konsumen maka dapat dilakukan pemidanaan dalam kasus ini. Hasil penelitian penerapan Undang-Undang Nomor 11 Tahun 2011 dalam upaya menegakan hukum dan menanggulangi kejahatan penipuan lowongan kerja *online* adalah dalam kasus ini penerapan Undang-Undang untuk pelanggar kasus penipuan lowongan kerja secara *online* dikenakan Pasal 28 ayat (1) UU No 11 Tahun 2008 dan Pasal 378 KUHPidana tetapi kasus ini diterapkan *lex specialis derogat legi generali* artinya UU No 11 Tahun 2008 bersifat khusus yang harus ditinjau terlebih dahulu untuk menjerat tersangka.

***Kata kunci** : Online*, Penipuan, UU Nomor 11 Tahun 2008, KUHpidana

KATA PENGANTAR

Puji syukur penulis panjatkan kepada Tuhan Yang Maha Kuasa yang telah memberikan semangat, bimbingan, kemampuan, serta kekuatan bagi Penulis dalam menyelesaikan penulisan hukum yang berjudul "ANALISIS MENGENAI PENIPUAN KERJA *ONLINE* DITINJAU DARI SEGI HUKUM PIDANA DAN UU ITE". Penulisan skripsi ini merupakan salah satu syarat untuk memperoleh gelar Sarjana Hukum pada Fakultas Hukum Universitas Presiden. Suka duka telah menyertai Penulis didalam menyelesaikan penulisan ini. Tidak terasa dengan berbagai upaya, cara, dan usaha Penulis dapat menyelesaikannya. Tetapi karena Penulis hanya seseorag manusia biasa yang tidak lepas dari kesalahan dan dengan segala keterbatasan kemampuan, waktu, pengetahuan serta pengalaman, maka dengan ini Penulis mengucapkan banyak terimakasih atas bantuan yang telah diberikan oleh berbagai pihak. Oleh karena itu penulis ucapkan terima kasih yang sebesar-besarnya kepada:

1. Ibu Fennieka Kristianto, S.H., M.H., M.A., M.Kn. selaku kaprodi Fakultas Hukum Universitas President dan selaku Pembimbing I yang sudah membimbing dan memberi banyak arahan dan sudah menyetujui judul skripsi yang diajukan.
2. Bapak Mahayoni, S.H.,M.H. selaku pembimbing II yang telah meluangkan waktunya disela kesibukannya untuk memberikan dukungan moril, masukan dan petunjuk, serta bantuan yang sangat besar baik secara teknis maupun non teknis kepada penulis dalam menyelesaikan skripsi ini.

3. Kedua orangtua Bapak Obon Tabroni dan Ibu Amalia yang sudah memberi dukungan dan nasihat sehingga dapat menyelesaikan studi S1 Fakultas Hukum.
4. Suami yang telah mendukung dan mengizinkan saya untuk melanjutkan dan menyelesaikan pendidikan S1 dan jenjang pendidikan yang lebih tinggi.
5. Teman-teman seperjuanagan Fakultas Hukum angkatan 2014 yang saling memberikan dukungan dan saling bertukar pikiran dalam hal pembelajaran. Tak terasa 3 tahun bersama diakhiri dengan kelulusan yang membahagiakan.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Komputer unggulan berupa kecepatan dan ketelitiannya sebagai alat bantu dalam menyelesaikan pekerjaan. Hal ini 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 atau pihak-pihak yang berkepentingan. Kesalahan yang disengaja mengarah kepada penyalahgunaan komputer.[1]

Usaha mewujudkan cita-cita hukum untuk mensejahterakan masyarakat melalui kebijakan hukum pidana,bukan merupakan satu-satunya cara yang memiliki peran paling strategis. Dikatakan demikian karena hukum pidana hanya sebagai salah satu dari sarana yang dimanfaatkan sebagai fungsi kontrol masyarakat. Teknologi informasi dan komunikasi telah mengubah perilaku masyarakat dan peradaban manusia secara global. Disamping itu, perkembangan teknologi informasi telah menyebabkan dunia menjadi tanpa batas dan menyebabkan perubahan sosial yang secara signifikan berlangsung demikian cepat. Teknologi informasi saat ini sangat

[1] http://www.scribd.com/doc/11654767/tinjauan - yuridis - pembuktian – cyber – crime – dalam – perspektif – hukum – positif - indonesia, 21 November 2011, 15.00 wib

berarti dalam memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, sekaligus menjadi arena efektif dalam upaya perbuatan melawan hukum.

Saat ini telah lahir suatu rezim hukum baru yang dikenal dengan Hukum *Cyber*, yang diambil dari kata *Cyber Law* adalah istilah hukum yang terkait dengan pemanfaatan teknologi informasi. Istilah lain yang digunakan adalah Hukum Teknologi Informasi *(Law Of Information Technology)*, Hukum Dunia Maya (*Virtual World Law*).[2] Istilah-istilah tersebut lahir mengingat kegiatan internet dan pemanfaatan teknologi informasi berbaris virtual. Istilah hukum *cyber* digunakan dalam tulisan ini dengan dilandasi pemikiran bahwa *cyber* diidentikan dengan "Dunia Maya" untuk itu akan cukup banyak menghadapi persoalan jika harus membuktikan suatu persoalan yang diasumsikan sebagai "maya", sesuatu yang tidak terlihat dan semu. Terdapat tiga pendekatan untuk mempertahankan keamanan pada *cyberspace*, pertama adalah pendekatan teknologi, kedua pendekatan sosial budaya-etika, dan ketiga pendekatan hukum. Untuk mengatasi keamanan gangguan pendekatan teknologi sifatnya mutlak dilakukan, sebab tanpa suatu pengamanan jaringan akan sangat mudah disusupi, diintersepsi, atau diakses secara ilegal dan tanpa hak. 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*

[2] http://www.tunardy.com/pengertian-cybercrime/

crime yang terjadi dapat dilakukan upaya penanggulangannya dengan hukum pidana, termasuk dalam hal ini adalah mengenai sistem pembuktiannya.

Dikatakan teramat penting karena dalam penegakan hukum pidana dasar pembenaran 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 I ayat (1) KUHP *"Nullum delictum nulla poena sine praevia lege poenali"* atau dalam istilah lain dapat dikenal, "tiada pidana tanpa kesalahan". [3]

Bertolak dari dasar pembenaran sebagaimana diuraikan diatas, bila dikaitkan dengan *Cyber crime*, maka unsur membuktikan dengan kekuatan alat bukti yang sah dalam hukum acara pidana merupakan masalah yang tidak kalah pentingnya untuk diantisipasi disamping unsur kesalahan dan adanya perbuatan pidana. Akhirnya dengan melihat pentingnya persoalan pembuktikan dalam *Cyber crime*, skripsi ini hendak mendeskripsikan pembahasan dalam fokus masalah hukum pembuktian terhadap *Cyber crime* dalam Hukum Pidana Indonesia.

Oleh karena alasan-alasan tersebut diatas, bagaimana pembuktian-pembuktian dalam *Cyber crime* cukup sulit dilakukan. mengingat, bahwa

[3] Molejatno, 2002, *Asas-Asas Hukum Pidana*, PT. Rineka Cipta, Jakarta, hal. 24

hukum di Indonesia yang mengatur masalah ini masih banyak ditemukan cacat hukum yang dapat dimanfaatkan oleh para pelaku *Cyber crime* untuk lepas dari proses pemidanaan.

Pasal 1 ayat (3) Undang-Undang Dasar 1945 menyatakan bahwa Negara Indonesia adalah negara hukum (*recht staat*).[4] Karena Indonesia merupakan negara yang berdasarkan pada hukum, maka idealnya kedudukan hukum harus ditempatkan diatas segalanya dan setiap orang dan perbuatan harus sesuai dengan aturan hukum tanpa terkecuali. Kriminalitas adalah suatu masalah sosial dalam kehidupan bermasyarakat.

Tingkat kriminalitas sekarang ini semakin meningkat baik dalam hal kuantitas maupun kualitas. Hal ini disebabkan oleh kemajuan dibidang ekonomi, teknologi, sosial dan budaya. Upaya pembangunan dan pembaharuan hukum harus dilakukan secara terarah dan terpadu. Kodifikasi dan unifikasi bidang-bidang hukum dan penyusunan perundang-undangan baru sangat dibutuhkan. Instrumen hukum baru dalam bentuk perundang-undangan sangat dibutuhkan sekarang ini. Karena sangat banyak undang-undang yang telah ketinggalan dan tidak dapat mengikuti zaman.

Perundang-undangan baru ini dibutuhkan juga untuk membangun kesadaran dan pandangan masyarakat tentang tingkah lakunya. Kemajuan teknologi informasi dan ilmu pengetahuan juga menjadi faktor yang menyebabkan perubahan cara berpikir, cara bertindak dan cara bersikap. Perubahan sikap, pandangan dan orientasi masyarakat inilah yang

[4] Undang-Undang dasar 1945

mempengaruhi kesadaran hukum dan penilaian terhadap suatu tingkah laku. Pertanyaannya apakah perubahan sikap warga masyarakat ini dianggap lazim atau menjadi suatu tindakan yang tidak lazim bahkan dapat menjadi suatu tindakan yang mengancam ketertiban sosial. Perbuatan yang mengancam ketertiban sosial yang tergolong dalam kejahatan sering kali memanfaatkan sarana teknologi informatika.

Kejahatan yang menggunakan sarana teknologi informatika ini tergolong baru serta berbahaya bagi ketertiban dan kesejahteraan masyarakat. Salah satu bentuk kejahatan yang akhir-akhir ini sedang marak dan sangat menghawatirkan adalah kejahatan penipuan lowongan kerja online. Kasus seperti ini diatur dalam Pasal 378 Buku II Kitab Undang-Undang Hukum Pidana (KUHP) pasal 28 ayat (1) Jo. Pasal 45 ayat (2) UU RI No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik Subs. Pasal 378 KUHPidana.

Bekerja adalah harapan semua orang untuk memenuhi kebutuhan ekonomi, membahagiakan keluarga, serta melakukan hal yang baik atas pencapaiannya. Menurut pendapat penulis yang dibutuhkan oleh masyarakat menjadi incaran bagi sekolompok orang untuk memanfaatkan kelemahan orang lain. Masalah penipuan lowongan kerja online sedang marak di daerah Kabupaten Bekasi tempat dimana Penulis dilahirkan. Pasalnya Bekasi adalah kawasan industri tersebesar se-Asia Tenggara namun fakta yang ada sebagian warga pribumi sulit mendapat pekerjaan di tanah kelahirannya sendiri. Hal ini yang menjadi pemicu banyak sekelompok orang yang tergiur dengan lowongan pekerjaan yang tidak pasti karena

keinginan bekerja mereka yang sangat tinggi sehingga jalur instan ditempuh.

Pemicu kedua, banyak oknum yang sangat tidak bertanggung jawab memanfaatkan kondisi seperti ini, tentunya mereka memberikan informasi lowongan pekerjaan palsu kepada orang yang tidak dikenal agar indentitas pelaku tidak mudah untuk dilacak. Pelaku memanfaatkan media internet *facebook* dan *website* untuk berinteraksi dengan korban, berbagai cara mereka lakukan agar korban terkena tipu dayanya. Kabupaten Bekasi sebagai salah satu kota besar di Indonesia tentu tidak luput dari yang namanya tindak kejahatan. Dengan mudahnya akses menuju dunia teknologi informatika maka kejahatan *cyber crime* juga dengan mudahnya dapat dilakukan, contohnya saja penipuan lowongan kerja *online*. Kejahatan ini dilakukan oleh sekelompok orang secara sadar. Pada dasarnya banyak upaya yang ditempuh oleh pemerintah dan para penegak hukum untuk mencegah dan memproses hukum tindak pidana penipuan online ini. Upaya melakukan blokir kepada situs-situs yang menjadi arena judi ataupun meningkatkan sistem keamanan nasional sehingga situs-situs penipuan ini dapat dihentikan, bahkan dengan cara menghukum pelaku tindak pidana penipuan online ini. Menurut pendapat penulis kenyataannya masih banyak terjadi tindak pidana penipuan online ini dimasyarakat. Hal ini disebabkan oleh sulitnya penegakan hukum dalam kasus penipuan online ini.

Bentuk-bentuk *Cyber crime* pada umumnya yang dikenal dalam masyarakat dibedakan menjadi 3 (tiga) kualifikasi umum yaitu :[5]

1.1.1. Kejahatan Dunia Maya yang berkaitan dengan kerahasiaan, integritas dan keberadaan data dan sistem komputer.

a) *Ilegal access* (akses secara tidak sah terhadap sistem komputer).

b) *Data interference* (mengganggu data komputer).

c) *System interference* (mengganggu sistem komputer).

d) *Illegal interception in the computers, systems and computer networks operation* (intersepsi secara tidak sah terhadap komputer, sistem, dan jaringan operasional komputer).

e) *Data Theft* (mencuri data).

f) *Data leakageand espionage* (membocorkan data dan memata-matai).

g) *Miss use of devices* (menyalahgunakan peralatan komputer).

Kegiatan *cyber* meskipun bersifat virtual dapat dikategorikan sebagai tindakan dan perbuatan hukum yang nyata. Secara yuridis dalam hal ruang *cyber* sudah tidak pada tempatnya lagi untuk dikategorikan sesuatu dengan ukuran dalam kualifikasi hukum konvensional untuk dijadikan obyek dan perbuatan, sebab jika cara ini yang ditempuh akan terlalu banyak kesulitan dan hal-hal yang lolos

[5] http://www.scribd.com/doc/11654767/tinjauan - yuridis - pembuktian – cyber – crime – dalam – perspektif – hukum – positif - indonesia, 21 November 2011, 15.00 wib

dari jerat hukum.[6] Kegiatan *cyber* adalah kegiatan virtual yang berdampak sangat nyata, meskipun alat buktinya bersifat elektronik. Dengan demikian, subyek pelakunya harus dikualifikasikan pula sebagai orang yang telah melakukan perbuatan hukum secara nyata.[3]

Penggunaan hukum pidana dalam mengatur masyarakat pada hakekatnya merupakan bagian dari suatu langkah kebijakan. Selanjutnya untuk menentukan bagaimana suatu usaha yang rasional dalam melakukan kebijakan tidak dapat pula dipisahkan dari tujuan kebijakan pembangunan itu sendiri secara integral. Dengan demikian dalam usaha untuk menentukan suatu kebijakan apapun termasuk kebijakan hukum pidana selalu terkait dan tidak terlepas dari tujuan pembangunan nasional itu sendiri yakni bagaimana mewujudkan kesejahteraan bagi masyarakat.

Selain itu, perkembangan hukum di Indonesia terkesan lambat, karena hukum hanya akan berkembang setelah ada bentuk kejahatan baru. Jadi hukum di Indonesia tidak ada kecenderungan yang mengarah pada usaha preventif atau pencegahan melainkan usaha penyelesaiannya setelah terjadi suatu akibat hukum.[7] Pada saat proses perkembangan hukum tersebut masih harus mengikuti proses yang sangat panjang dan dapat dikatakan setelah negara menderita kerugian yang cukup besar hukum tersebut baru disahkan. Kebijakan hukum nasional kita yang kurang.

---

[6] *Prof. Dr. Otje Salman Soemadiningrat, SH*

[7] http://www.lawskripsi.com/index.php?option=com_content&view=article&id=103&Itemid=103

1.2. Rumusan Masalah

Masalah yang dirumuskan dalam penelitian ini adalah:

a) Apakah unsur-unsur penipuan pada lowongan kerja secara *online* menurut KUHPidana Undang-Undang Informasi dan Transaksi Elektronik ?

b) Bagaimana penerapan Undang-Undang Informasi dan Transaksi Elektronik dalam upaya menegakan hukum dan menanggulangi kejahatan penipuan lowongan kerja *online*?

1.3. Tujuan Dan Kegunaan Penelitian

1.3.1. Tujuan Penelitian

Adapun tujuan penelitian ini sebagai berikut:

a) Mengkaji Unsur-Unsur penipuan lowongan kerja *online.*

b) Mengkaji dan menjelaskan penerapan Undang-Undang dan upaya penanggulangan terhadap kasus penipuan lowongan kerja *online*.

1.3.2. Kegunaan Penelitian

Dari hasil penelitian ini nantinya diharapkan dapat memberikan manfaat sebagai berikut:

a) Kegunaan Teoritis dari hasil penelitian ini diharapkan dapat dijadikan bahan kepustakaan dan bahan referensi hukum bagi mereka yang berminat pada kajian-kajian ilmu hukum pada umumnya dan hukum pidana pada khususnya.

b) Penelitian ini nantinya diharapkan dapat memberikan penjelaskan kepada instansi-instansi terkait, khususnya Aparat

Penegak Hukum untuk bagaimana melakukan upaya pencegahan penipuan lowongan kerja online.

1.4. Metode Penelitian

Pada penelitian ini, Peneliti menggunakan metode-metode sebagai berikut :

1.4.1. Spesifikasi Penelitian

Penelitian ini bersifat deskriptif analitis, yaitu ditujukan untuk memecahkan masalah *cyber crime* yang merupakan masalah aktual. Penelitian ini akan menggambarkan bentuk-bentuk *cyber crime* dan modus operandinya, selanjutnya bentuk-bentuk *cyber crime* tersebut dianalisa untuk dikualifikasikan dan sedapat mungkin dicari pengaturannya di dalam sistem perundang-undangan Indonesia.[8] Dihubungkan dengan teori hukum dan praktis pelaksanaannya, berupa data sekunder bahan hukum primer antara lain Kitab Undang-Undang Hukum Pidana (selanjutnya disebut KUHP), dan UU No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik.

Data sekunder bahan hukum sekunder yaitu pendapat para ahli hukum yang berkaitan dengan tindak pidana penipuan melalui internet sebagai yang melanggar hukum dan melibatkan Kitab Undang Undang Hukum Pidana dan UU No 11 tahun 2008 tentang Informasi dan Transaksi Elektronik.

[8]Nazir, moh. *Metode penelitian*. Ghalia Indonesia. 2005,

1.4.2. Metode Pendekatan

Pendekatan masalah merupakan proses pemecahan atau penyelesaian masalah melalui tahap-tahap yang telah ditentukan, sehingga mencapai tujuan penelitian. Penelitian ini merupakan penelitian hukum normatif yang ditujukan terhadap sistematika hukum khususnya mengenai peristiwa hukum berupa perilaku atau sikap tindak dalam hukum yang digolongkan sebagai perbuatan pidana (*strafbaarfeit*)[18] yang dikenal dengan *cyber crime.* Skripsi ini mengguakan cara meneliti bahan pustaka atau data sekunder sebagai bahan dasar untuk diteliti dengan cara mengadakan penelusuran terhadap peraturan perundangan peraturan dan literatur-literatur yang berkaitan dengan permasalahan yang diteliti.

1.5. Teknik Pengumpulan Data

Pada penelitian ini dilakukan teknik pengumpulan data dengan beberapa cara yaitu :

1.5.1. Penelitian Kepustakaan (*library research*).

Dalam hal ini Peneliti melakukan penelitian terhadap data sekunder bahan hukum primer seperti :

a) Kitab Undang-Undang Hukum Pidana
b) UU No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik
c) Kemudian data sekunder bahan hukum sekunder yaitu pendapat para ahli yang berkaitan dengan tindak pidana

penipuan melalui internet dengan menggunakan kamus hukum.

d) UU No. 19 tahun 2016 tentang Informasi dan Transaksi Elekrtonik perubahan atas UU No 11 Tahun 2008

e) UU No. 36 Tahun 1999 tentang Telekomunikasi

1.5.2. Penelitian Lapangan (*field research*)

Untuk menunjang dan melengkapi studi kepustakaan, maka peneliti melakukan penelitian lapangan antara lain, melakukan wawancara dengan pemilik warnet Palazo, pengambilan data di Polres Bekasi serta serah terima buku dengan anggota DPRD Kab Bekasi.

1.6. Metode Analisis Data

Seluruh data yang diperoleh dianalisis secara yuridis normatif, maksudnya bahwa analisis dilakukan dengan memperhatikan hierarki peraturan perundang-undangan agar peraturan yang satu tidak bertentangan dengan peraturan lainnya, serta tercapainya kepastian hukum.[9] Skripsi ini juga menggunakan data lapangan sebagai data pendukung untuk melengkapi.

[9] Soerjono Soekanto dan Sri Mamudji, Penelitian Hukum Normatif Suatu Tinjauan Singkat, Cetakan ke – 11. (Jakarta : PT Raja Grafindo Persada, 2009), hal. 13–14

BAB II

TINJAUAN PUSTAKA

2.1. Kriminologi

2.1.1. Pengertian Kriminologi

Kriminologi merupakan ilmu pengetahuan yang mempelajari tentang kejahatan. Nama kriminologi yang dikemukakan oleh *P.Topinard* seorang ahli antropologi Perancis, Secara harafiah berasal dari kata *"crimen"* yang berarti kejahatan atau penjatan dan *"logos"* yang berarti ilmu pengetahuan, maka kriminologi dapat berarti ilmu tentang kejahatan atau penjahat.[10] Beberapa sarjana terkemuka memberikan definisi kriminologi sebagai berikut :

a) *Edwin H. Sutherland* : *criminology is the body of knowledge regarding delinquency and crime as social phenomena* (Kriminologi adalah kumpulan pengetahuan yang membahas kenakalan remaja dan kejahatan sebagai gejala sosial).

b) *W.A. Bonger* : Kriminologi adalah ilmu pengetahuan yang bertujuan menyelidiki gejala kejahatan seluas-luasnya.

[10] Topo Santosao dkk, *Kriminologi*, 2010, hlm. 9

c) *J. Constant* : Kriminologi adalah ilmu pengetahuan yang bertujuan menentukan faktor-faktor yang menjadi sebabmusabab terjadinya kejahatan dan penjahat.[11]

2.1.2. Ruang Lingkup Kriminologi

Kriminologi, Ruang lingkup pembahasan kriminologi mencakup tiga hal pokok, yakni

a) Proses pembuatan hukum pidana dan acara pidana (*making laws*).

b) Etiologi Kriminal, yang membahas teori-teori yang menyebabkan terjadinya kejahatan (*breaking of laws*).

c) Reaksi terhadap pelanggaran hukum (*reacting toward the breaking of laws*). Reaksi dalam hal ini bukan hanya ditujukan kepada pelanggar hukum berupa tindakan represif tetapi juga reaksi terhadap "calon" pelanggaran hukum berupa upayaupaya pencagahan kejahatan (*criminal prevention*).

(1) Proses pembuatan hukum pidana (*process of making laws*) adalah;

a) Definisi kejahatan

b) Unsur-unsur kejahatan

c) Relativitas pengertian kejahatan

[11] A.S. Alam, *Pengantar Kriminologi*, 2010, Hlm. 2

d) Penggolongan kejahatan dan

e) Statistic kejahatan.

(2) Etiologi *criminal* (*breaking laws*) adalah :

a) Aliran-aliran (mazhab-mazhab) kriminologi

b) Teori-teori kriminologi dan

c) Berbagai perspektif kriminologi.

(3) Bagian ketiga adalah perlakuan terhadap pelanggar-pelanggar hukum (*reacting toward the breaking laws*) antara lain :[12]

a) Teori-teori penghukuman

b) Upaya-upaya penanggulangan/pencegahan kejahatan, baik berupa tindakan *pre-emtif, preventif, reprensif.*

2.2. Kejahatan

2.2.1. Pengertian Kejahatan

Pengertian kejahatan sangat relatif (selalu berubah) baik ditinjau dari sudut pandang hukum, maupun dari sudut pandang masyarakat. Kejahatan dari sudut pandang hukum adalah setiap perbuatan yang melanggar hukum pidana. Setiap perbuatan yang tidak melanggar aturan hukum pidana tidak dapat disebut kejahatan, dan perbuatan itu mengancam ketertiban sosial. Kejahatan dari sudut pandang masyarakat adalah setiap perbuatan yang melanggar norma-norma yang masih hidup didalam masyarakat. Norma hukum adalah sejumlah aturan-aturan yang mengatur tingkah laku orang-orang yang dikeluarkan oleh pejabat publik, yang berlaku secara sama untuk

[12] *ibid*

semua kelas dan golongan dan disertai sanksi kepada pelanggar-pelanggarnya yang dilakukan oleh negara.

Dengan memperhatikan definisi di atas, maka terlihat ada empat unsur pokok yang merupakan ciri khas hukum pidana, yaitu :

a) Sifat politisnya, yakni peraturan-peraturan yang dikeluarkan oleh pemerintah. Peraturan-peraturan yang dikeluarkan oleh organisasi buruh, gereja, sindikat dan lain-lainnya tidak dapat disebut hukum pidana meskipun peraturan tersebut sangat mengikat anggotanya dan mempunyai sanksi yang tegas.

b) Sifat spesifiknya, yakni hukum pidana memberikan batasan tertentu untuk setiap perbuatan. Contohnya, dibedakan antara pencurian biasa dengan pencurian dengan pemberatan.

c) Sifat *uniform*, yakni berusaha memberikan keadilan kepada setiap orang tanpa membedakan status sosial seseorang.

d) Sifat adanya sanksi pidana, yaitu adanya ancaman pidana oleh Negara.

2.2.2. Unsur-Unsur Kejahatan

Untuk menyebut suatu perbuatan sebagai kejahatan ada tujuh unsur pokok yang saling berkaitan yang harus dipenuhi. Ketujuh unsur tersebut adalah:[13]

a) Ada perbuatan yang menimbulkan kerugian(*harm*).

[13] *ibid*

b) Kerugian yang ada diatur di dalam baik didalam Kitab UndangUndang Hukum Pidana (dalam kodifikasi) maupun diluar kodifikasi.

c) Harus adanya perbuatan (*criminal act*).

d) Harus ada maksud jahat (*criminan intent = mens rea*).

e) Ada peleburan antara maksud jahat dengan perbuatan jahat.

f) Harus ada perbauran antara kerugian yang telah diatur dalam peraturan dengan perbuatan.

g) Harus ada sanksi pidana yang mengancam perbuatan tersebut.

h) Harus ada sanksi pidana yang mengancam perbuatan tersebut.

2.3. Kejahatan Teknologi Informasi (Cyber Crime)

2.3.1. Definisi Cybercrime

Pada masa awalnya, *cyber crime* didefinisikan sebagai kejahatan komputer. Mengenai definisi kejahatan komputer sendiri, sampai sekarang para sarjana belum sependapat mengenai pengertian atau definisi dari kejahatan komputer. Komputer dalam bahasa inggris masih belum seragam. Namun pada waktu itu, pada umumnya para sarjana lebih menerima pemakaian istilah "*computer crime*" oleh karena dianggap lebih luas dan biasa dipergunakan dalam hubungan internasional. *The British Law Commission* mengartikan "*computer fraud*" sebagai manipulasi komputer dengan cara apapun uang dilakukan dengan itikad buruk untuk memperoleh uang, barang atau keuntungan lainya atau dimaksudkan untuk menimbulkan kerugian

pada pihak lain. *Madeel* membagi "*computer crime"* atas dua kegiatan yaitu:[14]

a) Penggunaan komputer untuk melaksanakan perbuatan penipuan, pencurian atau penyembunyian yang dimaksud untuk memperoleh keuntungan keuangan, keuntungan bisnis, kekayaan atau pelayanan.

b) Ancaman terhadap komputer itu sendiri seperti pencurian perangkat keras atau lunak, sabotase dan pemerasan. Sistem teknologi informasi berupa internet telah dapat menggeser paradigma para ahli hukum terhadap definisi kejahatan komputer sebagaimana ditegaskan sebelumnya, bahwa pada awalnya para ahli hukum terfokus pada alat/perangkat keras yaitu komputer.[15] Namun dengan adanya perkembangan teknologi informasi berupa jaringan internet, maka fokus dari identifikasi terhadap definisi *cyber crime* lebih diperluas lagi yaitu seluas aktivitas yang dapat dilakukan di dunia internet/maya melalui sistem informasi yang digunakan. Jadi tidak sekedar pada komponen *hardware*nya saja kejahatan tersebut dimaknai *cyber crime*, tetapi sudah dapat diperluas dalam lingkup dunia yang dijelajah oleh sistem teknologi informasi yang bersangkutan, sehingga akan lebih tepat jika pemaknaan dari *cyber crime* adalah kejahatan teknologi

[14] *ibid*
[15] *ibid*

informasi, juga sebagaimana dikatakan Nawawi Arief sebagai kejahatan mayantara. Oleh karena itu, pada dasarnya *cyber crime* meliputi semua tindak pidana yang berkenaan dengan sistem informasi, sistem informasi itu sendiri, serta sistem komunikasi yang merupakan sarana untuk penyampaian/pertukaran informasi kepada pihak lainnya.

2.3.2. Karateristik Cyber crime

Globalisasi yang melanda dunia dewasa ini menyebabkan perubahan dalam seluruh aspek kehidupan manusia, terutama pada negara-negara berkembang, termasuk Indonesia. Perubahan yang terjadi itu dengan sendirinya terjadi pula pada perubahan hukum karena kebutuhan masyarakat akan berubah secara kuantitatif dan kualitatif. Permasalahan yang timbul dalam perubahan hukum itu adalah sejauh mana hukum bisa seusai dengan peruahan tersebut dan bagaimana tatanan hukum itu agar tidak tertinggal dengan perubahan masyarakat. Di samping itu, sejauh mana masyarakat dapat mengikat diri dalam perkembangan hukum agar ada keserasian antara masyarakat dan hukum supaya melahirkan ketertiban dan ketentraman yang diharapkan.[16]

Era globalisasi juga menyebabkan makin canggihnya teknologi informasi sehingga telah membawa pengaruh terhadap munculnya

[16] Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (cyber crime)*, (Jakarta: PT RajaGrafindo Persada, 2012), hlm. 11

berbagai bentuk kejahatan yang sifatnya yang berdampak lebih besar daripada kejahatan konvensional. Berbeda dengan kejahatan konvensional, yang bercirikan sertidaknya terdiri dari beberapa hal, di antaranya penjahat bisa siapa saja dan alat digunakan sederhana serta kejahatannya tidak perlu menggunakan suatu keahlian. Kejahatan dibidang teknologi informasi dapat digolongkan sebagai *white colour crime* karena pelaku *cyber crime* adalah orang yang menguasai penggunaan internet beserta aplikasinya atau ahli dibidangnya.

Selain itu perbuatan tersebut sering kali dilakukan secara transnasional atau melintasi batas Negara sehingga dua kriteria kejahatan melekat sekaligus dalam kejahatan *cyber* ini, yaitu *white colour crime* dan transnational crime.[17] *Modern* disini diartikan sebagai kecanggihan dari kejahatan tersebut sehingga pengungkapannya pun melalui saran yang canggih pula. [18]Perkembangan teknologi informasi termasuk internet di dalamnya juga memberikan tantangan tersendiri bagi perkembangan hukum di Indonesia. Hukum di Indonesia dituntut untuk dapat menyesuaikan dengan perubahan sosial yang terjadi. Perubahan perubahan sosial dan perubahan hukum atau sebaliknya tidak selalu berlangsung bersama-sama. Artinya pada keadaan tertentu perkembangan hukum mungkin tertinggal oleh perkembangan unsur-unsur lainnya dari masyarakat serta kebudayaannya atau mungkin hal yang sebaliknya.

2.3.3. Faktor Pendorong Cyber Crime Di Indonesia

Kejahatan merupakan salah satu bentuk dari perilaku menyimpang yang selalu ada dan melekat pada tiap bentuk masyarakat, tidak ada masyarakat yang sepi dari kejahatan.[19] Kejahatan terjadi tidak hanya disebabkan oleh faktor individu seseorang tetapi juga disebabkan oleh faktor eksternal seperti yang berasal dari lingkungan seskitar dan kehidupan sosialnya.

Cyber crime semakin marak terjadi, karena modus yang beraneka ragam. Para pelaku sangat lihai dalam menjalankan aksinya, mereka adalah individu yang cerdas dan kreatif, namun menggunakan hal tersebut untuk melakukan suatu kejahatan yang dapat menimbulkan kerugian bagi orang lain baik itu kerugian materiil maupun immaterial. Berikut ini adalah faktor-faktor yang menjadi penyebab maraknya *cyber crime*, antara lain:

a) Kurangnya kesadaran hukum masyarakat

Kesadaran hukum merupakan kesadaran tentang apa yang seharusnya atau tidak seharusnya kita lakukan berkaitan dengan aturan atau hukum yang berlaku di masyarakat. Saat ini kesadaran hukum masyarakat masih dinilai kurang terkait aktivitas *cyber crime.* Hal tersebut dikarenakan kurangnya pemahaman terkait *cyber crime* baik itu tindakan maupun efek yang ditimbulkannya. Banyak masyarakat kurang atau belum

[19] *ibid*

sadar akan perbuatan yang dilakukan terkait aktivitas di dunia maya.

Mulai dari maraknya perbuatan pencemaran nama baik hingga tindakan membajak akun sosial orang lain. Perbuatan kecil tersebut dianggap biasa dan lumrah dimasyarakat, bahkan cenderung sebagai candaan. Melalui pemahaman mengenai *cyber crime*, masyarakat sangat berperan penting dalam upaya penanggulangan *cyber crime*. Tanpa pemahaman pelaku *cyber crime*akan merajalela karena masyarakat tidak tahu apa yang sesungguhnya mereka lakukan hingga pada akhirnya mereka tertipu, rekening mereka dibobol dan berbagai kerugian lainnya.

b) Keamanan

Pelaku *cyber crime* tentunya akan merasa aman saat menjalankan aksinya, hal ini tidak lain karena media yang digunakan dalam menjalankan kejahatan berupa akses internet yang lazim digunakan dimana saja baik itu tempat tertutup maupun terbuka. Kurangnya sistem keamanan dari internet membuat siapapun bebas berekspresi di dunia maya tanpa memerlukan batasan sehingga mendorong pertumbuhan *cyber crime.* Hal yang senada diungkapkan oleh Ketua Pengelola Nama Domain Internet Indonesia (Pandi) Andi Budimansyah,

menurutnya:[20]"Kesadaran masyarakat Indonesia soal keamanan cyber masih lemah. Saat ini banyak pemilik website diIndonesia yang tidak mengetahui bahwa *website*-nya digunakan untuk pishing atau tindakan memalsukan *website* orang lain. *Website* palsu itu dibuat mirip dengan yang asli untuk mengambil keuntungan dari transaksi yang dilakukan *website* asli."

Selain *phising*, di Indonesia juga marak penanaman *malware* atau program jahat yang ditaruh orang lain di *server*-server Indonesia atau bahkan ditaruh di ponsel. Pada saat tertentu *malware* bisa meminta program untuk menyerang ke website tertentu. Hal tersebut menguatkan bahwa kesadaran keamanan kita masih lemah. Kita sendiri tidak bisa menjaga website kita, sehingga memungkinkan terjadinya perbuatan phisingdan juga malware. Sama halnya dengan pelaku menggunakan kita untuk melakukan suatu kejahatan tanpa sepengetahuan kita.

c) Aparat Penegak Hukum

Secara umum aparat penegak hukum masih sangat minim pengetahuan dalam penguasaan operasional komputer dan pemahaman terhadap *hacking computer* serta kemampuan melakukan penyidikan terhadap kasus-kasus kejahatan dunia

[20] Putlitbang Hukum dan Peradilan Mahkamah Agung RI, Naskah Akademis Kejahatan Internet (cyber crime), 2004, hlm.4

maya. Hal tersebut memungkinkan pelaku *cyber crime* jauh lebih hebat dibandingkan aparat penegak hukum yang mengakibatkan semakin meningkatnya intensitas *cyber crime* di Indonesia.

d) Undang-Undang

Saat ini Indonesia belum memiliki undang-undang khusus *cyber law* yang mengatur mengenai mengenai cyber *crime* tetapi sudah ada hukum yang berlaku umum dan dapat dikenakan bagi para pelaku *cyber crime* seperti aturan dalam KUHP dan UU ITE.[21]

2.4. Definisi Penipuan secara umum

Pengertian dari Penipuan menurut Kamus Besar Bahasa Indonesia dari kata dasar penipuan yaitu tipu adalah perbuatan atau perkataan yang tidak jujur (bohong, palsu, dan sebagainya) dengan maksud untuk menyesatkan, mengakali, atau mencari untung. Sedangkan penipuan adalah proses, perbuatan, cara menipu.

Seseorang yang melakukan suatu tindakan dengan mengatakan yang tidak sebenarnya kepada orang lain tentang suatu berita, kejadian, pesan dan lain-lain yang dengan maksud-maksud tertentu yang ingin dicapainya adalah suatu tindakan penipuan atau seseorang yang melakukan tindakan-tindakan yang bersifat menipu untuk memberikan kesan bahwa sesuatu itu benar dan tidak palsu, untuk kemudian mendapat kepercayaan dari orang lain.

Tindak pidana penipuan sangat sering terjadi di lingkungan masyarakat, untuk memenuhi kebutuhan atau keuntungan seseorang dapat

[21] Merry Magdalena dan Maswigrantoro Rous Setyandu, *cyber law tidak perlu takut*, (Yogyakarta: Andi:2007)hlm. 28

melakukan suatu tindak pidana penipuan. Di Indonesia seringnya terjadi tindak pidana penipuan dikarenakan banyak Faktor-faktor yang mendukung terjadinya suatu tindakan penipuan, misalnya karena kemajuan teknologi sehingga dengan mudah melakukan tindakan penipuan, keadaan ekonomi yang kurang sehingga memaksa seseorang untuk melakukan penipuan, terlibat suatu utang dan lain sebagainya.

Kejahatan penipuan di dalam bentuknya yang pokok diatur dalam Pasal 378 KUHP yang berbunyi sebagai berikut:

“Barangsiapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakan orang lain untuk menyerahkan barang atau sesuatu kepadanya, atau memberikan hutang atau menghapus piutang, diancam dengan pidana penjara paling lama empat tahun “

Sifat dari tindak pidana penipuan adalah dengan maksud menguntungkan diri sandiri atau orang lain secara melawan hukum, menggerakan orang lain untuk menyerahkan atau berbuat sesuatu dengan mempergunakan upaya-upaya penipuan seperti yang disebutkan secara linitatif di dalam Pasal 378 Kitab Undang-Undang Hukum Pidana, dan untuk mengetahui sesuatu upaya yang dipergunakan oleh si pelaku itu dapat menimbulkan perbuatan penipuan atau tindak pidana penipuan, haruslah diselidiki apakah orang yang melakukan atau pelaku tersebut mengetahui bahwa upaya yang dilakukannya bertentangan dengan kebenaran atau tidak.

Seseorang yang melakukan suatu tindak pidana penipuan biasanya melakukan beberapa cara-cara antara lain dengan pelayanan, suatu contoh perolehan pelayanan melalui penipuan misalanya dalam konteks komputer adalah apabila seseorang menggunakan tanpa hak sebuah sistem yang biasanya harus membayar seperti Prestel, persoalan tentang siapa yang yang telah ditipu masih tetap ada, tetapi apabila seseorang telah menipu orang lain dengan cara mengatakan bahwa ia memiliki izin sah untuk menggunakan terminal yang biasanya dipakai untuk akses ke dalam sistem,

maka tindak pidana itu telah dilakukan sesuai dengan apa yang diatur dalam *saction 1 Theft Act 1978*.

Perbuatan penipuan dalam pengertian bahwa seseorang telah berkata bohong atau dengan tipu muslihat untuk mendapatkan suatu keuntungan dan telah merugikan orang lain secara melawan hukum maka ia telah melakukan suatu tindak pidana yang telah diatur dalam Kitab Undang-Undang Hukum Pidana Pasal 378 tentang Tindak Pidana Penipuan. Menurut Brigjen. Drs. H. A. K. Moch.Anwar, S.H. dalam bukunya Hukum Pidana Bagian Khusus bahwa tindak pidana penipuan atau penipuan adalah "membujuk orang lain dengan tipu muslihat, rangkaian kata-kata bohong, nama palsu, keadaan palsu agar memberikan sesuatu" serta unsus-unsur dari tindak pidana penipuan yang dibagi menjadi dua yaitu unsur objektif dan subjektif.[22]

2.5. Definisi Penipuan menurut KUHPidana

Berkaitan dengan perumusan delik yang mempunyai beberapa elemen, di antara para ahli mempunyai jalan pikiran yang berlainan. Sebagian besar berpendapat membagi elemen perumusan delik secara mendasar saja, dan ada pendapat lain yang membagi elemen delik secara terperinci. Di antaranya unsur subjektif dan unsur objektif.

Penipuan "*BEDROG*" merupakan jenis-jenis kejahatan yang termasuk kedalam golongan kejahatan yang ditujukan terhadap hak milik dan lain-lain hak yang timbul dari hak milik atau dalam bahasa belanda disebut "*MISDRIJVEN TEGEN DE EIGENDOM EN DE DAARUIT VOORTLOEIENDE ZAKELIJK RECHTEN*". Kejahatan penipuan diatur dalam buku ke II bab XXV dari Pasal 378 sampai dengan Pasal 394 Kitab Undang-Undang Hukum Pidana. Digunakannya kata penipuan dalam bab tersebut karena dalam bab XXV diatur sejumlah perbuatan-perbuatan yang

[22] Muladi dan Barda Nawawi Arief, 2010. *Teori-Teori dan Kebijakan Pidana. Bandung*: PT Alumni. Hlm 148

ditujukan terhadap harta benda, dimana oleh si pelaku telah dipergunakan perbuatan-perbuatan yang bersifat menipu atau dipergunakan perbuatan tipu muslihat.[23]

Sebagaimana yang dirumuskan Pasal 378 KUHP, secara yuridis, penipuan berarti perbuatan dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum dengan memakai nama palsu, martabat palsu, tipu muslihat atau kebohongan yang dapat menyebabkan orang lain dengan mudah menyerahkan barang, uang atau kekayaannya. Perkataan penipuan itu sendiri memiliki 2 (dua) pengertian, yaitu :

a) Penipuan dalam arti luas, yaitu semua kejahatan yang yang dirumuskan dalam bab XXV KUHP.

b) Penipuan dalam arti sempit, yaitu bentuk penipuan yang dirumuskan dalam Pasal 378 (bentuk pokok) dan Pasal 379 (bentuk khusus), atau biasa dengan sebutan *OPLICHTING.*

Adapun seluruh ketentuan tindak pidana dalam Bab XXV ini disebut dengan penipuan, oleh karena dalam semua tindak pidana di sini terdapatnya perbuatan-perbuatan yang bersifat menipu atau membohongi oranglain.

Ketentuan dalam pasal 378 ini pun merumuskan tentang pengertian penipuan (*OPLICHTING*) itu sendiri. Rumusan ini adalah bentuk pokoknya, dan ada penipuan dalam arti sempit dalam bentuk khusus yang meringankan. Karena adanya unsur khusus yang bersifat meringankan sehingga diancam pidana sebagai penipuan ringan yakni dalam Pasal 379. Sedangkan penipuan dalam arti sempit tidak ada dalam bentuk diperberat.

---

[23] Moch. Anwar, *Hukum Pidana Bagian Khusus* (KUHP II), (Bandung: Percetakan Offset Alumni, 1979), hlm. 16

Rumusan penipuan tersebut terdiri dari unsur-unsur objektif yang meliputi perbuatan (menggerakkan), yang digerakkan (orang), perbuatan itu ditujukan pada orang lain (menyerahkan benda, memberi hutang, dan menghapuskan piutang), dan cara melakukan perbuatan menggerakkan dengan memakai nama palsu, memakai tipu muslihat, memakai martabat palsu, dan memakai rangkaian kebohongan. Selanjutnya adalah unsur-unsur subjektif yang meliputi maksud untuk menguntungkan diri sendiri atau orang lain dan maksud melawan hukum.[24]

2.6. Undang-Undang ITE

2.6.1. Pengertian Informasi, Transaksi Elektronik dan Dokumen Elektronik menurut Undang – Undang No. 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Dalam ketentuan umum pasal 1 undang – undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik bahwa disebutkan pengertian Informasi Elektronik, Transaksi Elektronik Dan Dokumen Elektronik :

a) Informasi Elektronik

adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *Electronik Data Interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau

[24] *ibid*

perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

b) Transaksi Elektronik

adalah perbuatan hukum yang dilakukan dengan menggunakan Komputer, jaringan Komputer, dan/atau media elektronik lainnya.

c) Dokumen Elektronik

adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

2.7. Latar Belakang Kejahatan Penipuan Online

2.7.1. Internet sangat mudah diakses

Hampir semua kalangan bisa mengakses internet dan mengoperasikan handphone dan komputer yang tersambung jaringan internet. Hal ini bisa memberi hal positive bahkan *negative*. *Positive* dalam hal mengakses keluarga yang berjauhan bisa mengguakan *facebook*,bisa membantu menyelesaikan pekerjaan dan tugas sekolah.

Negative apabila disalah gunakan oknum tertentu untuk memanfaatkan oranglain, melihat konten dewasa yang semestinya tidak dilihat oleh anak dibawah umur.

Semua ini kembali ke diri sendiri mau dibawa kemana arahnya. Modus operandi adalah pola suatu kejahatan yang dilakukan dalam penyalahgunaan internet, dalam kata lain dapat diartikan bagaimana suatu kejahatan bisa terlaksana. Modus operandi ini bermacam-macam. Ada yang masih dilakukan dengan cara konvensional ataupun dengan cara tersistematis. Berikut beberapa cara yang dilakukan operandi dalam kasus ini antara lain :

1. Penipuan Lowongan *Online* melalui *website*
2. Penipuan Online menggunakan *Broadcastin*g BBM.

2.7.2. Murahnya jaringan internet

Selain mudah diakses internet sangat murah dan terjangkau, para operator berlomba-lomba menarik simapatik masyarakat dengan harga murah dan diskon.

Sehingga untuk memiliki kuota atau pulsa bukan suatu hal yang sulit didapat. Saya sendiri menggunakan salah satu kartu handphone dengan biaya internet 50 GB seharga Rp.90.000 dengan jangka waktu masa aktif selama 3 bulan itu artinya penggunaan Rp.90.000 dibagi (/) 90 hari sebesar Rp. 1000 perhari. Jika yang belum memiliki handphone hal ini bukan suatu hal yang menyulitkan para pelaku melancarkan aksinya. Sekarang banyak sekali warung internet

(warnet) adalah tempat penyewaan penggunakan komputer di sertai jaringan internet. Berikut tarif warnet yang saya ambil berdasarka data lapangan.

Gambar 1.1

Tabel Tarif Warnet Palazo

PALAZO WARNET	
Tarif	Jam
Rp.3500,-	1 jam
Rp.7000,-	2 jam
Rp.10.000,-	3 jam
Rp.12.000	4 jam

D

Dari keteranagan di atas menunjukan biaya penyewaan intenet sangat terjangkau oleh berbagai kalangan.[25]

2.7.3. Angka pengangguran yang masih tinggi

Beberapa waktu lalu kepala Disnaker Kab Bekasi mengelurkan *statment* " jumlah pemohon kartu kuning di Dinas Tenaga Kerja Kabupaten Bekasi mengalami peningkatan signifikan. Jika di hari biasanya ada sekitar 100 pemohon, kini Disnaker menerima pemohon kartu kuning hingga 500 orang perhari. Tinggi jumlah pemohon kartu kuning itu secara tidak langsung menunjukkan angka pengangguran bertambah. Biasanya, pemohon kartu kuning merupakan lulusan baru dari SMA dan SMK. Sejak awal 2017 lalu jumlah pemohon kartu kuning di Disnaker berjumlah 9839 orang angka ini diprediksi aka terus bertambah mengingat jumlah Sekolah Menengah Atas sederajat di Kab Bekasi berjumlah 96 sekolah menampung 34.647 ribu siswa siswi.

[25] Warnet palazo

Tidak hanya kepala Disnaker mengeluarkan statment tentang angka pengangguran yang tinggi, mantan wakil bupati Bekasi mengatakan " jumlah pengangguran di Kab Bekasi masih tinggi diangka lebih dari 10%.

2.8 Kelompok Undang-Undang Informasi Transaksi Elektronik

Menjawab tuntutan dan tantangan komunikasi global lewat Internet, Undang-Undang yang diharapkan (*ius konstituendum*) adalah perangkat hukum yang akomodatif terhadap perkembangan serta antisipatif terhadap permasalahan. Salah satu dampak negatif penyalahgunaan Internet dengan berbagai motivasi yang dapat menimbulkan korban-korban yang mengalami kerugian seperti kerugian materi dan non materi. Saat ini, Indonesia belum memiliki Undang-Undang khusus atau *cyberlaw* yang mengatur mengenai *cybercrime.* [26]

Rancangan Undang-Undang tersebut sudah ada sejak tahun 2000 dan revisi terakhir dari rancangan undang-undang tindak pidana dibidang teknologi informasi sejak tahun 2004. Rancangan sudah dikirimkan ke Sekretariat Negara RI oleh Departemen Komunikasi dan Informasi serta dikirimkan ke DPR namun dikembalikan kembali ke Departemen Komunikasi dan Informasi untuk diperbaiki. Tetapi, terdapat beberapa hukum positif lain yang berlaku umum dan dapat dikenakan bagi para pelaku *cyber crime* terutama untuk kasus-kasus yang menggunakan komputer sebagai sarana, antara lain:

1) **Kitab Undang Undang Hukum Pidana**

[26] Didik M Arief Mansur dan Elisataris Ghukthom, *Cyber Law Aspek Hukum Teknologi Informasi*, (Bandung:Refika Aditama), hlm. 9-10

Dalam upaya menangani kasus-kasus yang terjadi para penyidik melakukan analogi dan persamaaan terhadap pasal-pasal yang ada dalam KUHP. Pasal-pasal didalam KUHP biasanya digunakan lebih dari satu Pasal karena melibatkan beberapa perbuatan sekaligus pasal-pasal yang dapat dikenakan dalam KUHP pada *cyber crime* antara lain:

a) Pasal 362 KUHP yang dikenakan untuk kasus *carding* dimana pelaku mencuri nomor kartu kredit milik orang lain tetapi tidak secara fisik. Terdapat nomor kartunya yang diambil dengan menggunakan *software* card generator di Internet untuk melakukan transaksi di *e-commerce*. Setelah dilakukan transaksi dan barang dikirimkan, kemudian penjual yang ingin mencairkan uangnya di Bank ternyata ditolak karena pemilik kartu bukan orang yang melakukan transaksi.

b) Pasal 378 KUHP dapat dikenakan untuk penipuan dengan seolah olah menawarkan dan menjual suatu produk atau barang dengan memasang iklan disalah satu *website*. Sehingga orang tertarik untuk membeli lalu mengirimkan uang kepada pemasang iklan. Tetapi, pada kenyataannya, barang tersebut tidak ada. Hal tersebut diketahui setelah uang dikirimkan dan barang yang dipesankan tidak datang sehingga pembeli tersebut menjadi tertipu.

c) Pasal 335 KUHP dapat dikenakan untuk kasus pengancaman dan pemerasan yang dilakukan melalui *e-mail* yang dikirimkan

oleh pelaku untuk memaksa korban melakukan sesuatu sesuai dengan yang diinginkan oleh pelaku dan jika tidak dilaksanakan akan membawa dampak yang membahayakan. Hal ini biasanya dilakukan karena pelaku biasanya mengetahui rahasia korban.

d) Pasal 311 KUHP dapat dikenakan untuk kasus pencemaran nama baik dengan menggunakan media Internet. Modusnya adalah pelaku menyebarkan *email* kepada teman-teman korban tentang suatu cerita yang tidak benar atau mengirimkan email ke suatu *mailing list* sehingga banyak orang mengetahui cerita tersebut.

e) Pasal 303 KUHP dapat dikenakan untuk menjerat permainan judi yang dilakukan secara online di Internet dengan penyelenggara dari Indonesia.

f) Pasal 282 KUHP dapat dikenakan untuk penyebaran pornografi maupun website porno yang banyak beredar dan mudah diakses di Internet. Berbahasa Indonesia, sangat sulit sekali untuk menindak pelakunya karena mereka melakukan pendaftaran domain tersebut diluar negeri dimana pornografi yang menampilkan orang dewasa bukan merupakan hal yang ilegal.

g) Pasal 282 dan 311 KUHP dapat dikenakan untuk kasus penyebaran foto atau film pribadi seseorang yang vulgar di Internet.

h) Pasal 378 dan 262 KUHP dapat dikenakan pada kasus carding, karena pelaku melakukan penipuan ingin membeli suatu barang

dan membayar dengan kartu kreditnya yang nomor kartu kreditnya merupakan curian.

i) Pasal 406 KUHP dapat dikenakan pada kasus deface atau hacking yang membuat sistem milik orang lain, seperti website atau program menjadi tidak berfungsi atau dapat digunakan sebagaimana mestinya.

2.8.1. Undang-Undang No 36 Tahun 1999 tentang Telekomunikasi

Menurut Pasal 1 angka (1) UndangUndang No 36 Tahun 1999, Telekomunikasi adalah setiap pemancaran, pengiriman, dan/atau penerimaan dan setiap informasi dalam bentuk tanda-tanda, isyarat, tulisan, gambar, suara, dan bunyi melalui sistem kawat, optik, radio, atau sistem elektromagnetik lainnya.

Definisi tersebut, maka Internet dan segala fasilitas yang dimilikinya merupakan salah satu bentuk alat komunikasi karena dapat mengirimkan dan menerima setiap informasi dalam bentuk gambar, suara maupun film dengan sistem *elektromagnetik*. Penyalahgunaan Internet yang mengganggu ketertiban umum atau pribadi dapat dikenakan sanksi dengan menggunakan UndangUndang ini, terutama bagi para *hacker* yang masuk ke sistem jaringan milik orang lain sebagaimana diatur pada Pasal 22, yaitu Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi:

a) Akses jaringan telekomunikasi .

b) Akses jasa telekomunikasi.[27]

[27] https://balianzahab.wordpress.com/artikel/penegakan-hukum-positif-di-indonesia terhadap-cyber crime/yang diakses pada tanggal 08 Januari 2017 pukul 13:04 Wita

BAB III

UNSUR-UNSUR PENIPUAN PADA LOWONGAN KERJA SECARA *ONLINE* MENURUT KUHPIDANA DAN UNDANG-UNDANG INFORMASI DAN TRANSAKSI

3.1. Analisis menurut KUHPidana

Untuk melihat apakah perbuatan yang dilakukan oleh orang yang menyediakan lowongan kerja tersebut dikatakan sebagai tindak pidana penipuan atau tidak, maka kita mengacu pada Pasal 378 KUHP yang berbunyi:

"Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi hutang maupun menghapuskan piutang, diancam karena penipuan dengan pidana penjara paling lama empat tahun".[28]

Menurut R. Soesilo dalam bukunya yang berjudul *Kitab* Undang-Undang Hukum Pidana (KUHP) kejahatan ini dinamakan "penipuan" dan uraian pekerjaan penipu:

Membujuk orang supaya memberikan barang, membuat utang atau menghapuskan piutang.

a. Maksud pembujukan itu ialah hendak menguntungkan diri sendiri atau orang lain dengan melawan hak.
b. Membujuknya itu dengan memakai:
    1) Nama palsu atau keadaan palsu atau
    2) Akal cerdik (tipu muslihat) atau
    3) Karangan perkataan bohong

[28] Politea Bogor, Tahun 1996. Hal.261

Penjelasan pasal 378 KUHP tentang penipuan berdasarkan Penjelasan R.Soesilo disebutkan bahwa :

a) Membujuk yaitu melakukan pengaruh dengan kelicikan terhadap orang, sehingga orang itu menurutinya berbuat sesuatu yang diinginkan.
b) Mengetahui duduk perkara yang sebenarnya, ia tidak akan berbuat demikian.
c) Memberikan barang yaitu barang itu tidak perlu harus diberikan (diserahkan) kepada terdakwa sendiri, sedang yang menyerahkan itupun tidak perlu harus orang yang dibujuk sendiri, bisa dilakukan oleh orang lain.
d) Menguntungkan diri sendiri dengan melawan hak yaitu menguntungkan diri sendiri dengan tidak berhak.
e) Nama palsu yaitu nama yang bukan namanya sendiri. Nama “Saimin” dikatakan “Zaimin” itu bukan menyebut nama palsu, akan tetapi kalau ditulis, itu dianggap sebagai menyebut nama palsu.
f) Keadaan palsu yaitu misalnya mengaku dan bertindak sebagai agen polisi, notaris, pastor, pegawai kotapraja, pengantar surat pos, dsb-nya yang sebenarnya ia bukan penjabat itu.
g) Akal cerdik atau tipu muslihat yaitu suatu tipuan yang demikian liciknya, sehingga seorang yang berpikiran normal dapat tertipu. Suatu tipu muslihat sudah cukup, asal cukup liciknya.
h) Rangkaian kata-kata bohong yaitu satu kata bohong tidak cukup, disini harus dipakai banyak kata-kata bohong yang tersusun sedemikian rupa, sehingga kebohongan yang satu dapat ditutup dengan kebohongan yang lain, sehingga keseluruhannya merupakan suatu ceritera sesuatu yang seakan-akan benar.
i) Tentang “barang” tidak disebutkan pembatasan, bahwa barang itu harus kepunyaan orang lain. Jadi membujuk orang untuk menyerahkan barang sendiri, juga dapat masuk penipuan, asal elemen-elemen lain dipenuhinya.

Mengacu pada pasal ini, apabila pihak yang menyediakan informasi mengenai lowongan kerja *online* tersebut memenuhi unsur-unsur dalam Pasal 378 KUHP, yakni secara melawan hukum memakai nama palsu pada *website*, dengan tipu muslihat, rangkaian kebohongan, dan menggerakkan pelamar untuk menyerahkan sesuatu kepadanya (mentransfer sejumlah uang) maka pihak yang dirugikan dapat saja menuntut secara pidana pihak yang menyediakan informasi lowongan kerja palsu tersebut atas dasar tindak pidana penipuan.

Pada dasarnya, penulis tidak menemukan peraturan khusus yang mengatur tentang persyaratan yang harus dipatuhi oleh lembaga atau perusahaan tertentu dalam penyediaan informasi lowongan kerja *online*.

Guna menghindari penipuan, calon pelamar kerja sebaiknya berhati-hati sebelum mengajukan lamaran pekerjaan. Masih bersumber dari laman yang sama, sehubungan dengan hal tersebut, ada beberapa saran untuk pelamar kerja agar tidak melakukan hal-hal sebagai berikut:[29]

a. Merespon tawaran bisnis atau pekerjaan yang tidak diminta (tidak jelas) dari orang yang tidak dikenal.
b. Menyampaikan informasi pribadi dan keuangan kepada siapapun yang tidak dikenal.
c. Mengirimkan uang (perusahaan di Inggris tidak meminta uang pembayaran atau transfer dari pelamar untuk mendapatkan pekerjaan atau visa masuk Inggris); dan
d. Melanjutkan komunikasi apabila diyakini hal itu sebagai upaya penipu

3.2. Analis menurut Undang-Undang No 11 Tahun 2008

Undang-Undang No 11 Tahun 2008 tidak secara khusus mengatur mengenai tindak pidana penipuan. Selama ini, tindak pidana penipuan

[29] http://kemlu.go.id/Pages/Highlights.aspx?IDP=87&l=id, diakses pada 28 Oktober 2013 pukul 14.53 WIB

sendiri diatur dalam Pasal 378 KUHP, dengan rumusan pasal sebagai berikut:

"Barangsiapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum dengan menggunakan nama palsu atau martabat palsu; dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi utang maupun menghapuskan piutang, diancam, karena penipuan, dengan pidana penjara paling lama empat tahun."[30]

UU No 8 Tahun 2011 tidak secara khusus mengatur mengenai tindak pidana penipuan, namun terkait dengan timbulnya kerugian konsumen dalam transaksi elektronik terdapat ketentuan Pasal 28 ayat (1) UU ITE yang menyatakan:

"Setiap Orang dengan sengaja, dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik."

Terhadap pelanggaran Pasal 28 ayat (1) UU ITE diancam pidana penjara paling lama enam tahun dan/atau denda paling banyak Rp 1 miliar, sesuai pengaturan Pasal 45 ayat (2) UU ITE.

Demikian kedua tindak pidana tersebut memiliki suatu kesamaan, yaitu dapat mengakibatkan kerugian bagi orang lain. Tapi, rumusan Pasal 28 ayat (1) UU ITE tidak mensyaratkan adanya unsur "menguntungkan diri sendiri atau orang lain" sebagaimana diatur dalam Pasal 378 KUHP tentang penipuan.

Pada akhirnya, dibutuhkan kejelian pihak penyidik kepolisian untuk menentukan kapan harus menggunakan Pasal 378 KUHP dan kapan harus menggunakan ketentuan-ketentuan dalam Pasal 28 ayat (1) UU ITE. Namun, pada praktiknya pihak kepolisian dapat mengenakan pasal-pasal berlapis terhadap suatu tindak pidana yang memenuhi unsur-unsur tindak pidana penipuan sebagaimana diatur dalam Pasal 378 KUHP dan memenuhi

[30] UU Nomor 8 Tahun 2011

unsur-unsur tindak pidana Pasal 28 ayat (1) UU ITE. Artinya, bila memang unsur-unsur tindak pidananya terpenuhi, polisi dapat menggunakan kedua pasal tersebut.

Terkait dengan rumusan Pasal 28 ayat (1) UU ITE yang menggunakan frasa "menyebarkan berita bohong", sebenarnya terdapat ketentuan serupa dalam Pasal 390 Kitab Undang-Undang Hukum Pidana dengan rumusan yang sedikit berbeda yaitu digunakannya frasa "menyiarkan kabar bohong". Menurut buku Kitab Undang-Undang Hukum Pidana terdakwa hanya dapat dihukum dengan Pasal 390 KUHP, apabila ternyata bahwa kabar yang disiarkan itu adalah kabar bohong. Pandangan sebagai kabar bohong, tidak saja memberitahukan suatu kabar yang kosong, akan tetapi juga menceritakan secara tidak betul tentang suatu kejadian.

Menurut penulis, penjelasan ini berlaku juga bagi Pasal 28 ayat (1) UU ITE. Suatu berita yang menceritakan secara tidak betul tentang suatu kejadian adalah termasuk juga berita bohong.

Menurut penulis, kata "bohong" dan "menyesatkan" adalah dua hal yang berbeda. Dalam frasa "menyebarkan berita bohong" yang diatur adalah perbuatannya, sedangkan dalam kata "menyesatkan" yang diatur adalah akibatnya. Selain itu, untuk membuktikan telah terjadi pelanggaran terhadap Pasal 28 ayat (1) UU ITE maka semua unsur dari pasal tersebut harus terpenuhi. Unsur-unsur tersebut yaitu

a. Setiap orang.
b. Dengan sengaja dan tanpa hak.

   Terkait unsur ini menyatakan antara lain bahwa perlu dicermati (unsur, *ed*) 'perbuatan dengan sengaja' itu, apakah memang terkandung niat jahat dalam perbuatan itu. Periksa juga apakah perbuatan itu dilakukan tanpa hak.
c. Menyebarkan berita bohong dan menyesatkan.

   Karena rumusan unsur menggunakan kata "dan", artinya kedua unsurnya harus terpenuhi untuk pemidanaan. yaitu menyebarkan berita bohong (tidak sesuai dengan hal/keadaan yang sebenarnya) dan

menyesatkan (menyebabkan seseorang berpandangan pemikiran salah/keliru). Apabila berita bohong tersebut tidak menyebabkan seseorang beranggapan salah, maka menurut penulis tidak dapat dilakukan pemidanaan.

d. Dapat mengakibatkan kerugian konsumen dalam transaksi elektronik. Unsur yang terakhir ini mensyaratkan berita bohong dan menyesatkan tersebut harus mengakibatkan suatu kerugian konsumen. Artinya, tidak dapat dilakukan pemidanaan, apabila tidak terjadi kerugian konsumen di dalam transaksi elektronik.

Jadi, dari rumusan-rumusan Pasal 28 ayat (1) UU ITE dan Pasal 378 KUHP tersebut dapat kita ketahui bahwa keduanya mengatur hal yang berbeda. Pasal 378 KUHP mengatur sementara Pasal 28 ayat (1) UU ITE mengatur mengenai berita bohong yang menyebabkan kerugian konsumen dalam transaksi elektronik.

3.3. Perbedaan KUHPidana dan UU ITE

Setelah membaca kembali putusan Mahkamah Konstitusi No. 50/PUU-VI/2008 tentang judicial review Pasal 27 ayat 3 UU ITE jo Pasal 45 ayat 1 UU ITE, alasan sanksi pidana pada UU ITE lebih berat dari sanksi di dalam KUHP adalah adanya efek masih dari penggunaan internet sebagai media yang berbeda dari media konvensional. Berdasarkan hal tersebut Mahkamah Konstitusi menganggap wajar perbedaan sanksi tersebut, dengan kata lain sudah sepantansnya jika di dalam UU ITE sanksinya lebih berat.

Alasan Mahkamah Konstitusi bahwa salah satu perbedaan antara komunikasi di dunia nyata dengan dunia maya (*cyberspace*) adalah media yang digunakan, sehingga setiap komunikasi dan aktivitas melalui internet akan memiliki dampak bagi kehidupan manusia dalam dunia nyata, misalnya melalui transfer data, melalui distribusi dan/atau transmisi dan/atau dapat diaksesnya informasi dan dokumentasi elektronik juga dapat menimbulkan dampak negatif yang sangat ekstrim dan masif di dunia nyata.

Oleh karena itu, meskipun berat ringannya sanksi adalah wewenang pembentuk undang-undang, namun menurut Mahkamah, konsep pemidanaan dalam UU ITE merupakan delik yang dikualifikasi sebagai penghinaan atau pencemaran nama baik sehingga konsepnya akan mengacu kepada KUHP namun ancaman pidananya lebih berat. Perbedaan ancaman pidana antara KUHP dengan UU ITE adalah wajar karena distribusi dan penyebaran informasi melalui media elektronik relatif lebih cepat, berjangkauan luas, dan memiliki dampak yang masif.

Jadi, apakah karena menggunakan media internet maka wajib hukumnya ketentuan pidana UU ITE dibuat lebih berat daripada ketentuan pidana konvensional di dalam KUHP atau UU yang mengatur perbuatan yang sama.

Jika mengikuti logika hukum putusan tersebut maka bisa dikatakan demikian. Tetapi jika kita merujuk kepada perundang-undangan lain, maka alasan ini tidak sepenuhnya benar.

Penyebaran berita bohong menurut UU ITE diancam dengan pidana penjara 6 tahun dan/atau denda 1 Milyar rupiah. Hal tersebut diatur di dalam Pasal 28 ayat jo Pasal 45 ayat 2 UU ITE:

Pasal 28

(1) Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik

Pasal 45

(2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 28 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

Bandingkan dengan ketentuan pidana Pasal 14 ayat 1 Undang-Undang No. 1 Tahun 1946 Tentang Peraturan Hukum Pidana:

Pasal 14

(1) Barang siapa, dengan menyiarkan berita atau pemberitahuan bohong, dengan sengaja menerbitkan keonaran dikalangan rakyat, dihukum dengan hukuman penjara setinggi-tingginya sepuluh tahun.[31]

Dapat diduga para penyusun Pasal 14 UU No. 1 Tahun 1946 tidak akan mengetahui bahwa kelak pada tahun 2008, puluhan tahun selepas meninggalnya mereka, internet akan berkembang begitu pesat sehingga muncul UU ITE yang justru memuat ancaman pidana yang lebih ringan terhadap penyebaran berita bohong dengan media internet. Patut diduga juga mereka tidak akan mengetahui bahwa sanksi pidana yang mereka buat lebih "*nendang*" ketimbang sanksi pidana yang dibuat oleh tim perumus UU ITE.

Jadi dari rumusan-rumusan Pasal 28 ayat (1) UU ITE dan Pasal 378 KUHP tersebut dapat kita ketahui bahwa keduanya mengatur hal yang berbeda. Pasal 378 KUHP mengatur penipuan (penjelasan mengenai unsur-unsur dalam Pasal 378 KUHP sementara Pasal 28 ayat (1) UU ITE mengatur mengenai berita bohong yang menyebabkan kerugian konsumen dalam transaksi elektronik penjelasan mengenai unsur-unsur dalam Pasal 28 ayat (1) UU ITE.

[31] UU Nomor 8 Tahun 2011

BAB IV

PENERAPAN UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK DALAM UPAYA MENEGAKAN HUKUM DAN MENANGGULANGI KEJAHATAN PENIPUAN LOWONGAN KERJA SECARA *ONLINE*

4.1. Penegakan Hukum

Hukum pembuktian adalah merupakan sebagian dari hukum acara pidana yang mengatur macam – macam alat bukti yang sah menurut hukum, sistem yang dianut dalam pembuktian, syarat – syarat dan tata cara mengajukan bukti tersebut serta kewenangan hakim untuk menerima, menolak, dan menilai suatu pembuktian.

Sumber hukum pembuktian adalah undang – undang, doktrin, ajaran dan jurisprudensi. Karena hukum pembuktian adalah bagian dari huku m acara pidana, maka sumber hukum yang pertama adalah undang – undang nomor 8 tahun 1981 tentang hukum acara pidana atau KUHAP. Pernipuan merupakan salah satu tindak kejahatan yang diatur dalam KUHP. Berbeda dengan Negara lain dimana penipuan merupakan perbuatan legal. Adapun ketentuan tentang perjudian diatar pada Pasal Pasal 28 ayat (1) Jo. Pasal 27 ayat (4) UU RI No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik Subs. Pasal 378 Kitab Undang-Undang Hukum Pidana.

a) Bunyi pasal 378 KUHP tentang penipuan adalah :

Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain dengan melawan hukum, dengan memakai nama palsu atau

martabat palsu, dengan tipu muslihat ataupun dengan rangkaian kebohongan menggerakan orang lain untuk menyerahkan sesuatu benda kepadanya, atau supaya memberi hutang maupun menghapuskan piutang, diancam karena penipuan dengan pidana penjara paling lama 4 (empat) tahun.[32]

b) Pasal 27 ayat (4) UU No 11 tahun 2008

Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.[6]

c) Ketentuan Pidana Pasal 45 (1) UU No 11 tahun 2008

Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3), atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

d) Pasal 28 (1) UU nomor 11 tahun 2008:

Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dan transaksi elektronik.

e) Ketentuan Pidana 45 (2) nomor 11 tahun 2008:

Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 28 (1) atau ayat (2) dipidana dengan pidana penjara

[32] Kitab Undang-Undang Hukum Pidana

selama 6 (enam) tahun/atau denda paling banyak Rp.700.000. 000,00 (tujuh ratus juta rupiah).[33]

4.1.1. Undang-undang Republik Indonesia Nomor 19 tahun 2016 tentang perubahan atas undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

(1) Pasal 45 ayat (1) UU No 19 Tahun 2016

Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/ atau membuat dapat diaksesnya Informasi Elektronik dan/ atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman sebagaimana dimaksud dalam Pasal 27 ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

(2) Pasal 45A ayat (4) UU No 19 Tahun 2016

Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik sebagaimana dimaksud dalam Pasal 28 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 1.000. 000.000,00 (satu miliar rupiah).

[33] Undang-Undang Nomor 11 Tahun 2008

4.1.2. Upaya Penanggulangan Kasus penipuan *online*

Kejahatan merupakan gejala sosial yang senantiasa dihadapi oleh setiap masyaraka. Kejahatan dalam kebenarannya dirasakan sangat meresahkan disamping itu juga mengganggu ketertiban dan ketentraman dalam masyarakat. Oleh karena itu, mesyarakat berupaya semaksimal mungkin untuk menanggulangi timbulnya kejahatan. Upaya penanggulangan kejahatan telah dan terus dilakukan oleh semua pihak, baik pemerintah maupun masyarakat pada umumnya.

Berbagai program dan kegiatan telah dilaksanakan sambil terus mencari cara tepat dan efektif untuk mengatasi masalah tersebut. Dalam hubungan ini E.H. Sutherland dan Cressesy mengemukakan bahwa dalam *crime prevention* dalam pelaksanaannya ada dua buah metode yang dipakai untuk mengurangi frekuensi kejahatan. Metode untuk mengurangi penanggulangan dari kejahatan, merupakan suatu cara yang ditujukan kepada pengurangan jumlah dilakukan secara konseptual.

Metode untuk mencegah kejahatan pertama kali, suatu cara yang ditujukan kepada upaya untuk mencegah terjadinya kejahatan yang pertama kali, yang akan dilakukan oleh seseorang dalam metode ini dikenal sebagai metode preventif. Berdasarkan uraian diatas dapat dilihat bahwa upaya penanggulangan kejahatan mencakup aktivitas preventif sekaligus berupaya memperbaiki prilaku seseorang dinyatakan telah bersalah (terpidana) di Lembaga Pemasyarakatan atau dengan kata lain, upaya kejahatan dapat dilakukan secara pre-

emptif, preventif dan represif. Menurut A.S. Alam, penanggulangan kejahatan terdiri atas tiga bagian pokok, yaitu :

a) Pre-Emtif

Yang dimaksud Pre-Emtif adalah upaya-upaya awal yang dilakukan oleh pihak kepolisian dan pemerintah untuk mencegah terjadinya tindak pidana[8]. Usaha-usaha yang dilakukan dalam kejahata secara pre-emtif adalah menanamkan nilai-nilai/norma-norma yang baik sehingga norma-norma tersebut terinternalisasikan dalam diri seseorang. Meskipun ada kesempatan untuk melakukan pelanggaran/kejahatan tapi tidak adaniatnya untuk melakukan hal tersebut maka tidak akan terjadi kejahatan.

Jadi dalam usaha pre-emtif faktor niat menjadi hilang . cara pencegahan ini berasai dari teori NKK, yaitu Niat dan Kesempatan terjadi kejahatan. Unsur-unsur penanggulangan upaya Pre-Emtif yaitu :

1) Sosialisasi kepolisian

Dalam melakukan upaya preventif ini pihak kepolisian khususnya unit *cyber crime* polres Bekasi telah melakukan berbagai upaya. Misalnya 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.

Selain sosialisasi mengenai bahaya melakukan tindak pidana *cyber crime* juga sosialisasi kerohanian agar norma dan kejujuran tetap tertanam dalam diri mereka.

b) Preventif

Upaya preventif adalah upaya pencegahan seseorang untuk melaku kan suatu pelanggaran atau kejahatan. Upaya preventif ini m enekankan kepada menghilangkan kesempatan seseorang untuk melakukan pelanggaran atau kejahatan. Contohnya apabila sudah beredar website dengan alamat tidak jelas segera keluar dari website tersebut, apabila pelaku bermain dengan mengunakan *facebook* dan BBM segera blokir akun tersebut.

Memang sangat beralasan bila upaya preventif diutamakan karena upaya preventif dapat dilakukan oleh siapa saja tanpa suatu keahlian yang khusus dan ekonomis, misalnya menjaga

diri, jangan sampai menjadi korban kriminalitas. Disamping itu upaya preventif tidak perlu suatu organisasi atau birokrasi dan lagi pula tidak menimbulkan akses lain.

Dalam upaya preventif (pencegahan) itu bagaimana upaya kita melakukan suatu usaha jadi positif, bagaimana kita menciptakan suatu kondisi seperti keadaan ekonomi, lingkungan juga budaya masyarakat menjadi suatu dinamika dalam pembangunan dan bukan sebaliknya seperti menimbulkan ketegangan-ketegangan sosial atau mendorong timbulnya perbuatan atau penyimpangan. Disamping itu bagaimana meningkatkan kesadaran dan partisipasi masyarakat bahwa keamanan dan ketertiban adalah tanggung jawab bersama. Unsur unsur upaya preventif.[34]

(1) Masyarakat ikut serta dalam pengawasan

Jangan percaya modus seperti ini, yang meminta anda menyetor sejumlah uang agar bisa mendapatkan posisi kerja yang ditawarkan. Apalagi kepada orang yang baru anda kenal secara online. Karena seharusnya pencari kerja siapapun tidak perlu untuk mengeluarkan uang dari kantong mereka untuk mempermudah proses lamaran

[34] Bambang Purnomo, *Perhatian Aspek Korban Dalam Penegakan Hukum Pidana*, Makalah panel diskusi hukum pidana, Universitas Proklamasi, Yogyakarta, 23 Januari 1989.

kerja ataupun pelatihan apapun yang diberikan perusahaan. Pencari tenaga dan masyarakat harus pandai mengikuti zaman jangan percaya dengan tipu daya menggunakan kata-kata yang mengagungkan perusahaan yang ditawarkan. Jika mencari pekerjaan melalui website bis lebih diteliti lagi nama domainnya dan yang lebih aman mencari pekerjaan langsung kirim CV langsung ke perusahaan yang bersangkutan melalui pos.

Jika yang sudah mentransfer uang ke pelaku dan menjadi korban penipuan segera siapkan bukti transaksi, bukti salinan email atau sms atau BBM. Lalu siapkan data pihak yang sudah menipu Anda, seperti nomor rekening dan juga nomor *handphon*e dan *email* atau *website*. Lalu siapkan juga bukti transfer bank, sms *banking*, atau internet *banking*. Buat kronologi kejadian diatas materai sebagai pelengkap laporan memblokir rekening penipu. Buat laporan penipuan ke kantor polisi terdekat dan minta surat pelaporan tadi untuk pelengkap laporan ke pihak bank. Laporkan ke kantor cabang Bank yang bersangkutan. Datang ke Bank terdekat dan sampaikan bahwa anda telah ditipu oleh orang yang mempunyai nomor rekening yang telah anda kirimi uang. Sertakan bukti transfer beserta Surat Laporan Polisi dan bank akan menampung laporan pelapor. Setelah mendatangi Cabang

Besar Bank karena akan cepat untuk ditindak lanjuti. Ajukan permohonan pemblokiran secara resmi sesuai aturan bank tersebut. Lalu isi form yang disediakan oleh pihak bank selanjutnya Anda menunggu proses pemblokiran oleh pihak Bank, jangan lupatinggalkan alamat dannomor telepon Anda agar mudah dihubungi oleh pihak Bank. Dari laporan Anda untuk memblokir rekening tersebut, bank akan melakukan investigasi dan segera memblokir rekening tersebut. Rekening yang terblokir hanya bisa di buka oleh yang punya rekening, sehingga jika si penipu akan membuka blokir maka investigasi mendalam akan di lakukan oleh bank dan tidak menutup kemungkinan akan melibatkan kepolisian.

Hal ini dilakukan agar pelaku mempertimbangkan perbuatan sebab masyarakat tidak lagi mudah untuk dibohongi begitu saja.

(2) Mengurangi angka pengangguran dengan latihan Wirausaha

Kab.Bekasi memiliki lebih dari 4000 pabrik dalam segala bidang tetapi fakta yang ada masih ada lebih 300.000 penggaguran, pemerintah harus ikut serta dalam kasus ini. Maka pemerintah harus melakukan sosialisasi tentang pelatihan kerja dalam berwirausaha sangat penting

dikarenakan mengingat jumlah penduduk yang sangat padat dan semakin sempitnya lahan pekerjaan berwirausaha sangat efektif jika dijadikan salah satu solusi dalam menanggulangi masalah pengangguran ini. Berwirausaha dikatakan efektif dan efisien karena jika usaha yang dilakukan tersebut itu berhasil dan maju maka dapat menyediakan lapangan pekerjaan dan juga mengurangi jumlah pengangguran yang semakin lama kian bertambah.

Dalam kegiatan pelatihan kerja dan berwirausaha ini masyarakat akan dikenalkan dengan apa – apa saja yang akan dilakukan dan diperhatikan dalam memulai suatu usaha. Karena sangat penting supaya nantinya masyarakat awam itu tidak terkejut dengan persaingan yang sangat ketat.

Selatan Kab. Bekasi merupakan kawasan industri hendaknya pemerintah memberikan pelatihan usaha mandiri seperti menjahit, membuat jok motor , bisa juga dibidang makanan sehingga masyarakat dalam kategori remaja tidak mengandalkan hanya untuk bekerja di pabrik. Utara Bekasi merupakan kawasan laut, namun fakta yang ada Kabupaten Bekasi memiliki potensi untuk membuka pariwisata tetapi itu semua belum terealisasikan. Jika Kabupaten Bekasi membuka sektor pariwisata bahari di

daerah Utara Bekasi banyak warga yang dapat memanfaatkan kondisi itu seperti berjualan, menyewakan tempat menginap, menyewakan ban sehingga dapat menekan angka pengangguran. Sepanjang tahun uang ratusan juta melayang ke wisata bahari disekitar Kabupaten Bekasi seperti Jakarta dan Karawang. Jika Kabupaten Bekasi mempunyai wisata bahari maka masyarakat memilih untuk berkunjung ke tempat terdekat maka penghasilannya akan membantu meningkatkan APBD.

c) Represif

Upaya represif adalah suatu upaya penanggulangan kejahatan secara konsepsional yang ditempuh setelah terjadinya kejahatan. Penanggulangan dengan upaya represif dimaksudkan untuk menindak para pelaku kejahatan sesuai dengan perbuatannya serta memperbaiki kembali agar mereka sadar bahwa perbuatan yang dilakukannya merupakan perbuatan yang melanggar hukum dan merugikan masyarakat. Sehingga tidak akan mengulanginya dan orang lain juga tidak akan melakukannya mengingat sanksi yang akan ditanggungnya sangat berat.[35]

[35] *ibid*

Dalam membahas sistem represif, kita tidak terlepas dari permasalahan sistem peradilan pidana kita, dalam sistem peradilan pidana kita, paling sedikit terdapat sub sistem Kehakiman, Kejaksaan, Kepolisian, Rutan, Pemasyarakatan, dan Kepengacaraan yang merupakan suatu keseluruhan yang terangkat dan berhubungan secara fungsional.

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.

d) Pelaksanaan Undang-Undang Informasi dan Transaksi Elektronik

Terhadap Kejahatan *Cyber Crime* Undang-undang ITE (Informasi dan Transaksi Elektronik) merupakan salah satu

peranti hukum di bidang *cyberspace* atau dunia maya yang diharapkan dapat mengakomodir segala persoalan yang menyangkut kejahatan atau pelanggaran dunia maya (*cyber crime*). Undang-Undang ITE berperan sangat penting dalam pemberantasan tindak pidana *cyber crime* di Indonesia. Selain memuat perlindungan hukum terhadap pemakai jasa internet juga memuat ancaman sanksi terhadap pelaku kejahatan cyber crime.

Dalam mengahadapi *cyber crime*, hukum positif di Indonesia masih bersifat *lex locus delicti*. 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.

Dalam kasusini selain melanggar pasal 378 KUHP tentang penipuan juga melanggar beberapa pasal yang ada dalam UU No 11 tahun 2008 . Pasal yang dilanggar dalam UU ITE sebagai berikut:

1) Penyebaran Berita Bohong dan Penyesatan Melalui Media Elektronik (Pasal 28 ayat 1 UU ITE) Penyebaran berita bohong dan penyesatan merupakan kata yang semakna dengan penipuan. Penipuan dapat dilakukan dengan motivasi, yaitu untuk menguntungkan dirinya sendiri atau paling tidak untuk merugikan orang lain. Dengan motivasi tersebut, maka penyebaran berita bohong dan penyesatan dapat dikategorikan sebagai penipuan.

2) Pemerasan dan/atau Pengancaman Melalui Internet (Pasal 27 ayat 4 UU ITE) Dengan adanya media internet yang memiliki berbagai bentuk variasi program dalam berkomunikasi seperti *email, blog, web, dan facebook,* dapat digunakan sebagai sarana kejahatan berupa pemerasan dan/atau pengancaman. Hal tersebut dapat disebabkan karena identitas pengguna internet sangat sulit untuk diidentifikasi karena pengguna media sosial rentan untuk memanipulasi identitasnya demi kepentingannya masing-masing. Dengan fenomena tersebut maka intensitas dan variasi kejahatan berupa terror sangat mudah dilakukan dan memiliki 60 banyak sasaran yang potensial. Pemerasan dan/atau pengancaman yang dilakukan melalui media internet diatur dalam pasal 27 ayat (4) yang berbunyi: “Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan

dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman."

4.1.3. Perlindungan Hukum terhadap Korban Penipuan Informasi Lowongan Kerja Berdasarkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Aparat penegak hukum dalam rangka menumbuhkan partisipasi masyarakat untuk mengungkap tindak pidana, perlu menciptakan iklim yang kondusif dengan cara memberikan perlindungan hukum terhadap korban oleh aparat penegak hukum,[8]sesuai dengan Pasal 13 Undang Undang 69 Nomor 2 Tahun 2002 Tentang Kepolisian Republik Indonesia, menyebutkan bahwa : " Tugas pokok Kepolisian Negara Republik Indonesia adalah :

a) Memelihara keamanan dan ketertiban masyarakat.
b) Menegakkan hukum.
c) Memberikan perlindungan, pengayoman, dan pelayanan kepada masyarakat.[36]

Pentingnya perlindungan hukum bagi korban kejahatan, selain dalam kerangka mewujudkan negara hukum, hal ini penting pula karena dalam kehidupan bermasyarakat pada umumnya dipandang sebagai suatu sistem yang mewajibkan seluruh anggotanya ikut berpartisipasi aktif mewujudkan adanya tertib sosial.

---

[36] Marcus Priyo Gunarto, *Perlindungan Hukum Bagi Korban Kejahatan Tinjauan Dari Segi Penegakan Hukum Dan Kepentingan Korban*, Http//www.Goggle.com//perlindungan hukum//. Diakses Pada Tanggal 12 Juni 2010 pukul 11.30. WIB

Tujuan mewujudkan tertib sosial bagi kepentingan masyarakat, maka dengan sendirinya di antara anggota masyarakat terdapat saling kepercayaan untuk mewujudkan kondisi yang dikehendaki secara bersamasama. Apabila ada salah satu pihak yang menjadi korban kejahatan, maka hal itu dapat melemahkan kepercayaan yang ada pada diri korban untuk ikut berpartisipasi mewujudkan tertib sosial sebagaimana menjadi tujuan bagi seluruh warga. Bangunan kepercayaan yang rusak akibat adanya kejahatan perlu dipulihkan melalui sarana hukum agar dapat memulihkan kepercayaan korban kejahatan terhadap sistem untuk mewujudkan tertib sosial.

Alasan lain perlunya perlindungan korban menurut Muladi adalah :

a) Berdasarkan Kontrak Sosial (*Social Contract Argument*).

   Alasan berdasarkan kontrak sosial berpijak pada pengertian bahwa negara memonopoli seluruh reaksi sosial terhadap kejahatan dan melarang tindakan-tindakan yang bersifat pribadi, dengan terjadinya kejahatan dan menimbulkan adanya korban, negara berkewajiban memperhatikan kebutuhan korban. [37]

b) Alasan Solidaritas Sosial (*Social Solidarity Argument*).

   Alasan berdasarkan solidaritas sosial berpijak pada pengertian bahwa negara harus menjaga warganegaranya yang mengalami kesukaran, dalam hal ini dapat melalui kerjasama dengan masyarakat berdasar atau menggunakan sarana-sarana yang disediakan oleh negara. Di samping hal di atas, dengan

[37] *ibid*

memperhatikan kepentingan korban kejahatan, maka konflik yang mungkin akan terjadi secara berkepanjangan antara korban kejahatan dengan pelaku kejáhatan dapat diatasi, karena dengan adanya perhatian kepada korban, secara psikologis korban merasa masih ditempatkan sebagai anggota masyarakat yang berharga.[38]

Penegakan hukum dalam Undang Undang No 11 tahun 2008 tentang informasi dan transaksi elektronik, khususnya terkait dengan penanganan tindak pidana *cyberlaw* di Indonesia dipengaruhi oleh berbagai faktor , antara lain faktor hukum, faktor penegak hukum, faktor sarana/fasilitas penegakan hukum, faktor masyarakt dan faktor budaya yaitu seperti :

a) Perlunya pembentukan unit/satuan baru dengan spesialisasi khusus dalam penanganan tindak pidana *cyberlaw* di setiap kepolisian daerah (Polda) diseluruh Indonesia dengan diawaki sumber daya manusia yang berkualitas, memiliki kemampuan dan kemauan tinggi dalam mengungkap kasus-kasus *cyberlaw*.

b) Perlunya dibentuk lembaga koordinasi khusus bagi elemen *Criminal Justice System* (CJS) yang terdiri dari Polisi, Jaksa dan Hakim yang berkompeten dalam penanganan tindak pidana *cyber crime* karena teknis dan taktis penanganan tindak pidana tersebut tidak dapat disamakan begitu saja dengan penanganan tindak pidana konvensional, khususnya dalam hal pembuktian.

[38] *ibid*

c) Perlunya meningkatkan motivasi masyarakat agar berperan serta aktif turut mencegah dan menanggulangi tindak pidana *cyber crime* melalui kepedulian terhadap situasi dan kondisi di sekitarnya masing-masing manakala terdapat indikasi terjadinya tindak pidana tersebut segera memberikan informasi kepada satuan kerja Kepolisian Negara Republik Indonesia (POLRI) setempat (kepolisian sektor (Polsek), kepolisian resort (Polres), kepolisi wilayah (Polwil), kepolisian daerah (Polda)).

d) Aparat penegak hukum, khususnya Polri perlu meningkatkan kerjasama dengan pihak-pihak terkait, baik dari dalam negeri maupun luar negeri, khususnya aparat penegak hukum di bidang teknologi dan informasi dalam rangka optimalisasi penanganan tindak pidana *cyber crime.*

e) Pemerintah perlu membentuk kelompok kerja (Pokja) khusus guna mengevaluasi kelemahan-kelemahan dalam Undang Undang Nomor 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik, baik terkait dengan delik-delik pidana yang ada maupun hukum acara pidananya untuk selanjutnya dilakukan revisi.

f) Masih diperlukan sosialisasi lebih lanjut terhadap masyarakat tentang materi-materi dalam Undang Undang Nomor 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik sehingga masyarakat pun mengetahui dan memahami daya jangkau Undang Undang Nomor 11 tahun 2008 Tentang Informasi dan

Transaksi Elektronik tersebut terhadap tindak pidana di bidang teknologi dan informasi (*cyber crime*).

g) Sangat diperlukan para penegak hukum seperti polisi, hakim, jaksa penuntut umum yang berintegrasi khusus dibidang *cyber crime*, karena selama ini penyidik masih lemah dalam menangani kasus *cyber crime* karena kurangnya pengetahuan tentang komputer.

Keefektifan Kitab Undang Undang Hukum Pidana dan Undang Undang Nomor 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik dalam menanggulangi perkembangan kejahatan hingga saat ini belum efektif dikarenakan pemerintah khususnya instansi penegak hukum masih menemukan kendala yaitu terhadap alat bukti, pelacakan pelaku, sanksi dan realisasi pembentukan *cyber police.*

4.2. Perlindungan hukum terhadap korban kejahatan diatur dalam Undang-Undang Nomor 13 Tahun 2006 Tentang Perlindungan Saksi dan Korban.

Pasal 5 Undang-Undang Nomor 13 Tahun 2006 Tentang Perlindungan Saksi dan Korban, yang menyatakan bahwa :

a) Seorang Saksi dan Korban berhak :

1) Memperoleh perlindungan atas keamanan pribadi, keluarga, dan harta bendanya, serta bebas dari Ancaman yang berkenaan dengan kesaksian yang akan, sedang, atau telah diberikannya.
2) Ikut serta dalam proses memilih dan menentukan bentuk perlindungan dan dukungan keamanan.
3) Memberikan keterangan tanpa tekanan;
4) Mendapat penerjemah.
5) Bebas dari pertanyaan yang menjerat.
6) Mendapatkan informasi mengenai perkembangan kasus.
7) Mendapatkan informasi mengenai putusan pengadilan.
8) Mengetahui dalam hal terpidana dibebaskan.
9) i. Mendapat identitas baru.
10) Mendapatkan tempat kediaman baru.
11) Memperoleh penggantian biaya transportasi sesuai dengan kebutuhan.
12) Mendapat nasihat hukum, dan/atau
13) Memperoleh bantuan biaya hidup sementara sampai batas waktu perlindungan berakhir.

b) Hak sebagaimana dimaksud pada ayat (1) diberikan kepada Saksi dan/atau Korban tindak pidana dalam kasus-kasus tertentu sesuai dengan keputusan LPSK.

Definisi korban diatur dalam Pasal 1 angka 2 Undang-Undang Nomor 13 Tahun 2006 Tentang Perlindungan Saksi dan Korban, yang menyatakan, bahwa:

"Seseorang yang mengalami penderitaan fisik, mental, dan/atau kerugian ekonomi yang diakibatkan oleh suatu tindak pidana"

Korban dalam hal ini adalah masyarakat pencari kerja dan perusahaan, perlindungan hukum diberikan dalam rangka mengembalikan kepercayaan diri korban.

Perlindungan hukum terhadap korban kejahatan mengenai beberapa model tertentu, yaitu :

a) Model Hak-hak Prosedural (*Prosedural Right Model*).

Pada model hak-hak prosedural, korban kejahatan diberikan hak untuk mengadakan tuntutan pidana atau membantu jaksa, atau hak untuk dihadirkan pada setiap tingkatan peradilan di mana kepentingannya terkait di dalamnya. Pada model ini secara implisit nampaknya ingin memberikan kesempatan kepada korban untuk membalas kepada pelaku kejahatan. Secara positif hal ini dapat mengembalikan kepercayaan dan harga diri bagi korban setelah dirinya dirugikan oleh kelakuan terdakwa. hal ini juga dapat menjadi imbangan bagi jaksa dalam hal jaksa membuat tuntutan yang terlalu ringan, tetapi model hak-hak prosedural dapat menimbulkan persoalan baru dalam penegakan hukum pidana, yaitu kepentingan pribadi dari korban akan lebih menonjol dibandingkan dengan kepentingan umum. Ini adalah suatu hal yang tidak diharapkan dalam penegakan hukum pidana,

karena pada umumnya di dalam penegakan hukum pidana yang dilindungi tidak hanya kepentingan pribadi saja, melainkan juga kepentingan umum.

b) Model Pelayanan (*Service Model*)

Model pelayanan bertitik berat terletak pada perlunya diciptakan standar-standar baku bagi pembinaan korban kejahatan. Model ini melihat korban sebagai sosok yang harus dilayani oleh Polisi dan aparat penegak hukum yang lain, pelayanan terhadap korban oleh aparat penegak hukum, diharapkan pihak korban akan lebih mudah untuk kembali mempercayai institusi penegak hukum dengan adanya pelayanan terhadap korban, hal ini maka korban akan merasa dijamin kembali kepentingannya dalam suasana yang adil[11] . Pada proses persidangan, terutama yang berkenaan dengan saksi, banyak kasus yang tidak terungkap akibat tidak adanya saksi yang dapat mendukung tugas penegak hukum. Keberadaan saksi dan korban merupakan unsur yang sangat menentukan dalam proses peradilan pidana.

Korban dapat melaporkan tindak pidana penipuan dengan cara mendatangi instansi penegak hukum untuk diproses lebih lanjut dengan cara membuat berita acara yaitu :

a) Penyidikan

Menerima Laporan yang masuk dari korban yang merasa dirugikan atas tindak kejahatan yang dilakukan pelaku penipuan melalui internet.

b) Penyelidikan

Mencari kebenaran dari laporan yang telah dilaporkan oleh korban atas tindak pidana penipuan tersebut dengan mencari alat bukti yang dapat membantu korban dalam penuntutan yaitu dengan mendatangi pihak perusahaan terkait tentang kebenaran informasi tersebut dan dengan mencari tahu proxi atau IP adrres yang ada dalam situs tersebut.

c) Pemeriksaan tersangka

Melakukan introgasi lebih lanjut yang dilakukan oleh pihak berwajib.

d) Penangkapan

e) Menangkap

Pelaku kejahatan yang terbukti telah melakukan tindak kejahatan penipuan informasi lowongan kerja pada internet dengan bukti yang didapat aparat penegak hukum dari hasil penyelidikan.

f) Penahanan

Aparat penegak hukum wajib menahan pelaku untuk pemeriksaan lebih lanjut

g) Penggeledahan

h) Penggeledahan dilakukan atas dasar mencari alat bukti kejahatan yang dilakukan pihak berwenang kepada tersangka.

i) Pemasukan rumah

Dilakukan pihak berwenang dengan dasar mencari alat bukti kejahatan yang dilakukan pihak berwenang kepada tersangka berdasarkan surat penggeledahan yang sah.

j) Pemeriksaan surat

Surat disini yaitu merupakan alat bukti elektronik berupa situs dan isian informasi yang telah di cetak.

k) Pemeriksaan saksi

Saksi atau korban yang merasa dirugikan diperiksa untuk kepentingan hukum tentang waktu dan tempat kejadian.

l) Pemeriksaan ditempat kejadian

Yaitu dengan menelusuri tempat dimana korban mengalami tindak kejahatan penipuan yang dilakukan melalui media intenet dengan membuka situs yang disebutkan

m) Penuntutan

Jaksa penuntut umum melakukan pengumpulan berkas perkara yang sudah dimiliki oleh pihak aparat dalam melakukan penyidikan dan penyelidikan disertai alat bukti sebagai bukti yang dapat menguatkan pelaku bersalah.

n) Pemeriksaan dimuka pengadilan

Selanjutnya dilakukan proses penyerahan berkas perkara disertai penyerahan tersangka dan barang bukti kepada Jaksa Penuntut Umum untuk membuat dakwaan agar selanjutnya perkara tersebut dapat diproses di pengadilan.

Pelapor atau korban yang demikian itu harus diberi perlindungan hukum dan keamanan yang memadai atas laporannya. Sehingga korban tidak merasa terancam atau terintimidasi baik hak maupun jiwanya. Dengan

jaminan perlindungan hukum dan keamanan tersebut, diharapkan tercipta suatu keadaan yang memungkinkan masyarakat tidak lagi merasa takut untuk melaporkan suatu tindak pidana yang diketahuinya kepada penegak hukum, karena khawatir atau takut jiwanya terancam oleh pihak tertentu.

Peran Penegak hukum selain pemerintah dalam mengurangi jumlah korban secara berkelanjutan dalam kejahatan *cyber* dengan melakukan himbauan/penyuluhan kepada masyarakat Menurut Ahmad M Ramli terdapat 3 pendekatan untuk mempertahankan keamanan di *cyberspace* yaitu [12] :

a) Pendekatan Teknologi merupakan subsistem dalam sebuah sistem yang lebih besar, yaitu pendekatan budaya, karena teknologi merupakan hasil dari kebudayaan atau merupakan kebudayaan itu sendiri

b) Pendekatan Sosial, Budaya Etika dilakukan untuk membangun atau membangkitkan kepekaan warga masyarakat dan aparat penegak hukum terhadap masalah *cyber crime* khususnya scam dan menyebarluaskan atau mengajarkan etika penggunaan komputer melalui media pendidikan. Pentingnya pendekatan budaya ini, khususnya upaya mengembangkan kode etik dan perilaku c.

c) Pendekatan Hukum Hal yang dilakukan untuk mengantisipasi tindak kejahatan secara terus menerus dengan melakukan pendekatan hukum mengenai sosialisasi dari instansi pemerintah dan penegak hukum kepada masyarakat.

Ketidaksiapan hukum dan penegak hukum dalam menanggulangi tindak pidana penipuan dengan cara membuat informasi palsu melalui internet (scam) ini menyebabkan pencegahan dengan menggunakan teknologi dan budaya menjadi alat yang ampuh. tindak pidana penipuan (daftarpustaka Ahmad M Ramli, Op Cit., Hlm 3) dengan cara membuat informasi palsu melalui internet (scam) ini dapat dicegah oleh masyarakat dengan cara sebagai berikut[13] :

a) Tidak merespon terhadap permintaan informasi pribadi lewat email atau *pop-up window*.

b) Kunjungi situs pada link yang ada dengan menulis URL pada address bar browser, jangan percaya dengan cara mengklik langsung pada link tersebut. Apabila menganggap bahwa e-mail dari perusahaan atau situs web tersebut bukan asli, jangan mengikuti link yang menunjukkan ke situsnya dari e-mail tersebut. Link tersebut dapat berupa link palsu, dimana tertulis resmi, tetapi mengarah ke situs web yang palsu.

c) Cek security untuk memastikan situs web tersebut memakai enkripsi. Sebelum memasukan informasi, cek terlebih dahulu apakah situs tersebut memakai enkripsi atau tidak. Netter dapat memastikan situs tersebut memakai enkripsi bila situs tersebut alamatnya berawalan https:// dan bukan http://. Pada browser, akan terlihat tanda aman pada bagian bawah browser, di status bar, yaitu adanya sebuah tanda gembok yang terkunci. Tanda gembok tersebut menandakan bahwa

situs itu memakai enkripsi untuk melindungi keabsahan informasi dan sebagainya.

d) konfirmasikan kepada pihak Dinas KetenagaKerjaan dan Transmigrasi (Disnakertrans) terhadap situs atau informasi tersebut.

e) Laporkan tindakan kriminal dari tersangka ke instansi yang berwenang.

4.3. Permasalahan dalam Penyidikan terhadap Cybercrime

Berdasarkan hasil penelitian yang dilakukan, hambatan-hambatan yang ditemukan di dalam proses penyidikan antara lain adalah sebagai berikut:

1. Perangkat hukum yang belum memadai.
2. Kemampuan penyidik Secara umum penyidik Polri masih sangat minim dalam penguasaan operasional komputerdan pemahaman terhadap hacking komputer serta kemampuan melakukan penyidikan terhadap kasus-kasus itu. Beberapa faktor yang sangat berpengaruh (determinan) adalah:
   a) Kurangnya pengetahuan tentang komputer
   b) Pengetahuan teknis dan pengalaman para penyidik dalam menangani kasus-kasus *cyber crime* masih terbatas.
   c) Faktor sistem pembuktian yang menyulitkan para penyidik.

   Dari penelitian dilakukan, ternyata masih sangat kurang jumlah penyidik yang pernah terlibat dalam penanganan kasus *cyber*

crime(10%), bahkan dari 30 orang responden yang ada, tidak ada satu orang pun yang pernah mendapat pendidikan khusus untuk melakukan penyidikan terhadap kasus *cyber crime*. Dalam hal menangani kasus *cyber crime* diperlukan penyidik yang cukup berpengalaman (bukan penyidik pemula), pendidikannya diarahkan untuk menguasai teknis penyidikan dan menguasai administrasi penyidikan serta dasar-dasar pengetahuan di bidang komputer dan profil hacker.

4.3.1. Alat Bukti

Persoalan alat bukti yang dihadapi di dalam penyidikan terhadap *Cyber crime* antara lain berkaitan dengan karakteristik kejahatan *cyber crime*itu sendiri, yaitu:

a) Sasaran atau media *cybercrime* adalah data dan atau sistem komputer atau sistem internet yang sifatnya mudah diubah, dihapus, atau disembunyikan oleh pelakunya. Oleh karena itu, data atau sistem komputer atau internet yang berhubungan dengan 25 kejahatan tersebut harus direkam sebagai bukti dari kejahatan yang telah dilakukan. Permasalahan timbul berkaitan dengan kedudukan media alat rekaman (*recorder*) yang belum diakui KUHAP sebagai alat bukti yang sah.

b) Kedudukan saksi korban dalam *cybercrime* sangat penting disebabkan cyber crime seringkali dilakukan hampir-hampir tanpa saksi. Di sisi lain, saksi korban seringkali berada jauh di luar negeri sehingga menyulitkan penyidik melakukan

pemeriksaan saksi dan pemberkasan hasil penyidikan. Penuntut umum juga tidak mau menerima berkas perkara yang tidak dilengkapi Berita Acara Pemeriksaan Saksi khususnya saksi korban dan harus dilengkapi dengan Berita Acara Penyumpahan Saksi disebabkan kemungkinan besar saksi tidak dapat hadir di persidangan mengingat jauhnya tempat kediaman saksi. Hal ini mengakibatkan kurangnya alat bukti yang sah jika berkas perkara tersebut dilimpahkan ke pengadilan untuk disidangkan sehingga beresiko terdakwa akan dinyatakan bebas. 23 Mengingat karakteristik *cybercrime,* diperlukan aturan khusus terhadap beberapa ketentuan hukum acara untuk *cybercrime.* Pada saat ini, yang dianggap paling mendesak oleh Peneliti adalah pengaturan tentang kedudukan alat bukti yang sah bagi beberapa alat bukti yang sering ditemukan di dalam *Cyber crime*seperti data atau sistem program yang disimpan di dalam disket, hard disk, chip, atau media recorder lainnya.

4.3.2. Fasilitas komputer forensik

Untuk membuktikan jejak-jejak para *hacker, cracker dan phreacker* dalam melakukan aksinya terutama yang berhubungan dengan program-program dan data-data komputer, sarana Polri belum memadai karena belum ada komputer forensik. Fasilitas ini diperlukan untuk mengungkap data-data digital serta merekam dan menyimpan bukti-bukti berupa soft copy (*image, program*, dsb). Dalam hal ini

Polri masih belum mempunyai fasilitas forensik komputer yang memadai. Fasilitas forensik komputer yang akan didirikan Polri diharapkan akan dapat melayani tiga hal penting yaitu *evidence collection, forensic analysis, expert witness.*

4.3.3. Kepastian hukum terhadap pelaku dan korban

a) Pokok-pokok hak korban kejahatan diantaranya mencakup :

1) Untuk dapt diakui seseorang harus diakui sebagai korban terlepas apakah pelaku teridentifikasi, tertangkap, diadili,atau dihukum, dan terlepas apakah ada hubungan antara pelaku dan korban.

2) Hak atas informasi (*right to information*)

3) Korban berhak mendapatkan informasi, misalnya korban akan menerima informasi saat itu juga ketika melakukan kontak pertama dengan penegak hukum (polisi atau penenegak hukum lainnya). Informasi diberikan dengan cara yang paling efektif, dengan penggunaan teknologi mutakhir. Informasi tersebut setidaknya mencakup; i) bentuk pelayanan yang dapat diterima, bentuk dukungan yang bisa diakses misalnya kesehatan, pelayanan sosial dan pelayanan yang relevan lainnya, ii) tentang kapan dan bagaimana mereka dapat melaporkan kejahatan dan apakah mereka dapat memilih untuk melaporkan atau tidak, iii) prosedur tentang proses penegakan hukum, iv)

peranan mereka dalam peradilan, v) dalam situasi apa mereka akan mendapatkan perlindungan, vi) dalam situasi apa mereka akan mendapatkan bantuan hukum, vii) syarat-syarat yang dibutuhkan untuk mendapatkan kompensasi, dan sebagainya. Korban juga berhak atas informasi; i) hasil dan perkembangan laporan mereka, ii) perkembangan kasusnya, iii) putusan pengadilan.

4) Hak atas pendampingan (*right to assistance*)

5) Korban dapat menerima pendampingan material, medis, psikologis, dan sosial dari pemerintah, lembaga sosial, komunitas, dan sebagainya. Pendampingan itu dapat dilakukan melalui badan-badan khusus atau lainnya. Pendampingan dapat berupa; i) pendampingan seketika (misalnya pendampingan medis, dukungan material-shelter, rumah dan transportasi, dan lainnya), ii) pendampingan jangka menengah (keberlanjutan pelayanan dari pendampingan seketika, pelayanan psikologis dan intervensi spiritual, pendampingan untuk kebutuhan finansial, dan lainnya), iii) pendampingan jangka panjang (keberlanjutan pendampingan sebelumnya, memastikan kembalinya korban ke komunitas, pendampingan korban dalam proses peradilan, dan lain sebagainya).

6) Hak atas reparasi (*rights to reparations*)

7) Restitusi dari pelaku, kompensasi dari negara, rehabilitasi, kepuasan, dan sebagainya.

8) Hak untuk berpatisipasi (*right to participation*)

9) Para korban harus mampu berpatisipasi dan terwakili dan proses peradilan untuk mempertahakan kepentingannya. Kepentingan para korban adalah mempunyai suara terkait dengan keamanannya, reparasi kepada mereka dan keadilan. Hak atas partisipasi ini membuat mereka akan mempertahankan kepentingannya dengan cara yang sama dengan pelaku.[39]

b) Kepastian hukum terhadap pelaku *cyber crime*

Memberikan kepastian hukum kepada pelaku dapat menimbulkan rasa aman kepada korban sebab minimnya laporan kepada kepolisian tentang kasus *cyber crime* disebabkan karena banyak lolosnya pelaku dari jeratan hukum. Hal ini membuat para korban tidak melapor ketika mengalami kejahatan kasus penipuan online.

Kasus *cyber crime* terutama peipuan online lowongan kerja yang sedang marak terjadi tetapi polisi mempersulit laporan. Contoh kasus penipuan online yang terjado di Kabupten Bekasi maka korban harus melapor ke Polda Metro Jaya Jakarta. Jika laporan bisa

[39] N.N. Tips Aman Online, http://buletin.melsa.net//idjan1001scam6/html, Diekses Pada Tanggal 18 Mei 2008, Pukul 15.00 WIB

dilakukan di Bekasi maka hal ini bisa mempermudah korban dalam membuat laporan.

Sejauh ini sudah banyak upaya demi kepastian hukum salah satunya tidak hanya UU ITE dan KUHP untuk menjerat kasus *cyber crime.* Tetapi ada UU pendukung agar pelaku tidak lepas dari hukuman. Seperti dibawah ini :

a) UU hak Cipta No 19 Tahun 2002.

b) UU Telekomunikasi No 36 Tahun 1992.

c) UU Document Perusahaan No.8 Tahun 1997.

d) UU Terorisme No15 Tahun 2003.

e) UU Pencucian uang No 25 Tahun 2003.

f) UU ITE, 14/2008, perubahanya UU 9/2016.

g) UU Pornografi Nomor 44 Tahun 2008.

Selain itu kepolisian harus memperketat proses penyidikan. Karena penyidikan adalah proses yang menentukan apakah pelaku lolos atau tidak. Kepolisian harus membuat tim khusus penyidik yang berkompetensi dibidang *cybercrime* untuk pembuktian alat bukti.

BAB V

PENUTUP

5.1. Kesimpulan

Pihak yang menyediakan informasi mengenai lowongan kerja *online* tersebut memenuhi unsur-unsur dalam Pasal 378 KUHP, yakni secara melawan hukum memakai nama palsu pada *website*, dengan tipu muslihat, rangkaian kebohongan, dan menggerakkan pelamar untuk menyerahkan sesuatu kepadanya (mentransfer sejumlah uang) maka pihak yang dirugikan dapat saja menuntut secara pidana pihak yang menyediakan informasi lowongan kerja palsu tersebut atas dasar tindak pidana penipuan. Dalam UU ITE memenuhi unsur-unsur pasal 28 ayat (1) kerugian konsumen dalam transaksi elektronik. Pelamar kerja online termasuk ke dalam konsumen media sosial. Demikian kedua tindak pidana tersebut memiliki suatu kesamaan, yaitu dapat mengakibatkan kerugian bagi orang lain.

Dalam kasus ini penerapan Undang-Undang untuk pelanggar kasus penipuan lowongan kerja secara *online* dikenakan Pasal 28 ayat (1) UU No 11 Tahun 2008 dengan ketentuan Pidana 45 (2) nomor 11 tahun 2008 dan Pasal 378 KUHPidana tetapi kasus ini diterapkan *lex specialis derogat legi generali* artinya hukum yang bersifat khusus mengesampingkan hukum yang bersifat umum. Tetapi tetap dibutuhkan kejelian kepolisian dalam tahap penyidikan. Dalam kasus ini UU ITE termasuk Undang-Undang Khusus, pihak penyidik terlebih dahulu mengkaji Pasal 28 ayat (1) dan Pasal 378 KUHP sebagai Undang-Undang penopang jika pasal 28 ayat (1) tidak mampu menjerat pelaku agar tidak lepas dari hukuman.

5.2. Saran

5.2.1. Bagi Masyarakat

a) Jangan mudah terhasut

Perkembangan yang sangat pesat, terknologi mudah di akses oleh berbagai kalangan. Saat ini pola pikir masyarakat harus mengikuti bahkan harus lebih maju dari dunia maya. Masyarakat harus cerdas mengikuti zaman jangan mudah terhasut oleh hasutan orang lain yang menjanjikan keuntungan berupa pekerjaan. Lebih baik mencari pekerjaan sesuai prosedur jangan melalui oknum yang tidak jelas.

b) Banyaknya warga yang tidak mengetahui tentang UU ITE. Hal ini menyebabkan mereka tidak menyadari perbuatan yang mereka lakukan akan mendapatkan sanksi pidana. Sehingga untuk menanggulangi penipuan online yang dilakukan oleh sekelompok orang di Kab Bekasi seharusnya para pihak terkait selalu memberikan sosialisasi mengenai UU ITE.

5.2.2. Bagi Pemerintah

a) Mengurangi Angka Pengangguran

Kab.Bekasi mempunyai kurang lebih 5000 pabrik tetapi fakta yang ada mencari pekerjaan sangat sulit. Pemrerintah harus ikut berupaya dalam kasus ini untuk menekan angka pengangguran dengan mengadakan BKK, memberi Usaha Mandiri seperti

menjahit, membuka sektor baru seperti pariwisata. Karena sebelah Utara Kab.Bekasi memiliki hamparan laut yang indah dan luas sehingga dapat menjadi mata pencari bagi warga sekitar dan menekan angka pengangguran.

b) Membuka *Job Fair*

Job Fair adalah tempat dimana para HRD perusahaan memberi kesempatan kepada warga sekitar untuk mengikuti test recruitment langsung ditempat. Pemerintah harus mengadakan *Job Fair* setiap Kecamatan. Sehingga menekan angka masyarakat yang mencari pekerjaan melalui oknum atau *website* palsu.

5.2.3. Bagi Kepolisian

a) Perlunya pembentukan unit/satuan baru dengan spesialisasi khusus dalam penanganan tindak pidana *cyberlaw* di setiap kepolisian daerah (Polda) di seluruh Indonesia. Fakor penunjang sumber daya manusia yang berkualitas, memiliki kemampuan dan kemauan tinggi dalam mengungkap kasus-kasus *cyberlaw*.

b) Perlunya penyidik, hakim dan jaksa penuntut umum yang berkompetensi dibidng *cybercrime.*

c) Sosialisasi kepolisian

Dalam melakukan upaya preventif ini pihak kepolisian khususnya unit *cybercrime* Polres Bekasi telah melakukan berbagai upaya. Seperti memberikan himbauan ke masyarakat

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

d) Memberi fasilitas kepada masyarakat

Maksud fasilitas disini kepolisian harus menanggapi dengan sigap atas laporan masyarakat terhadap kasus penipuan lowongan kerja online. Karena dalam kasus ini jumlah pelapor lebih sedikit dibanding jumlah kasus yang banyak. Maka dari itu kepolisian harus sungguh-sungguh menangani semua laporan masyarakat demi menjamin kepastian pelapor dan korban dengan melakukan tindakan hukum yang pasti.

5.2.4. Dunia pendidikan dan peneliti berikutnya

Dalam melakukan reset kasus penipuan online diharapkan peneliti dapat meninjau ruang lingkup yang lebih jauh, karena penelitian hanya ruang lingkup Kab.Bekasi dan Jawa Barat. Bagi dunia pendidikan diharapkan tulisan ini dapat membantu di bidang edukasi untuk para pelajar lainnya.

DAFTAR PUSTAKA

- Molejatno, 2002, *Asas-Asas Hukum Pidana*, PT. Rineka Cipta, Jakarta, hal. 24.
- Undang-Undang dasar 1945
- Prof. Dr. Otje Salman Soemadiningrat, SH.
- Moh, Nazir. *Metode penelitian*. Ghalia Indonesia. 2005,)
- Soekanto, Soerjono dan Mamudji, Sri. *Penelitian Hukum Normatif Suatu Tinjauan Singkat*, Cetakan ke – 11. (Jakarta : PT Raja Grafindo Persada, 2009), hal. 13–14.
- Topo Santosao dkk, *Kriminologi*, 2010, hlm. 9
- A.S. Alam, *Pengantar Kriminologi*, 2010, Hlm. 2
- Putlitbang Hukum dan Peradilan Mahkamah Agung RI, Naskah Akademik *Kejahatan Internet (Cyber Crime)*, 2004, hlm.4
- Suhariyanto, Budi. *Tindak Pidana Teknologi Informasi (Cyber Crime)*, (Jakarta: PT RajaGrafindo Persada, 2012), hlm. 11
- Manan, Abdul. *Apek-aspek Pengubah Hukum*, (Jakarta : Kencana, 2006) hal. 63
- Magdalena, Merry dan Rous, Maswigrantoro, *Cyber Law tidak perlu takut*, (Yogyakarta: Andi:2007)hlm. 28.
- Wahid, Abdul. dan Labib, Moh, *Kejahaan Mayantara*, (Bandung: Refika Aditama, 2005), hlm. 76.
- Arief, Mansur dan Ghukthom, Elisataris, *Cyber Law Aspek Hukum Teknologi Informasi*, (Bandung:Refika Aditama), hlm. 9-10.

- Ade Arie Sam Indradi, *carding-modus operandi, Penyidikan dan Penindakan*, (Jakarta: Grafika Indah,2006), hlm. 1.
- Muladi dan Nawawi, Barda, 2010. *Teori-Teori dan Kebijakan Pidana*. Bandung: PT Alumni. Hlm 148
- Tim Penyusun Kamus Pusat Pembinaan dan Pengembangan Bahasa. *Kamus Besar Bahasa Indonesia*, (Jakarta: Balai Pustaka, 1990), hlm. 952.
- Anwar, Moch. *Hukum Pidana Bagian Khusus* (KUHP II), (Bandung: Percetakan Offset Alumni, 1979), hlm. 16.
- Kitab Undang Undang Hukum Pidana.
- UU No 11 Tahun 2008
- UU No 19 tahun 2016
- Purnomo, Bambang. *Perhatian Aspek Korban Dalam Penegakan Hukum Pidana*, Makalah panel diskusi hukum pidana, Universitas Proklamasi, Yogyakarta, 23 Januari 1989.

JURNAL

Urgensi *Cyber Law* Di Indonesia dalam rangka penanganan *Cyber Law* disektor.

Strategi kepolisian dalam menanggulangi penipuan yang dilakukan melalui *Online.*

Optimalisasi *Cyber Law* untuk penanganan *Cyber Crime* pada *E-Commerce.*

Tindak pidana *Cyber Crime* dalam perspektif Undang-Undang Nomor 11 Tahun 2008.

Analisasi Hukum terhadap tindak pidana penipuan Informasi lowongan kerja pada internet dihubungkan dengan UU Nomor 11 Tahun 2008.

Elektronik sebagai alat bukti.

Penipuan menggunakan media internet berupa jual beli *Online.*

Mekanisme penyidik tindak penipuan melalui internet menurut UU Nomor 11 Tahun 2008.

Cyber Crime di Indonesia.

INTERNET

- http://www.scribd.com/doc/11654767/tinjauan - yuridis - pembuktian – cyber – crime – dalam – perspektif – hukum – positif - indonesia, 21 November 2011, 15.00 wib.
- http://www.tunardy.com/pengertian-cybercrime
- http://www.lawskripsi.com/index.php?option=com_content&view=article&id=103&Itemid=103
- https://pandi.id/berita/kesadaran-keamanan-cyber-indonesia-masih-rendah-kata-pandi/ yang diakses pada tanggal 08 Januari 2017 Pukul 12:32 Wita
- https://balianzahab.wordpress.com/artikel/penegakan-hukum-positif-di-indonesiaterhadap-cyber crime/yang diakses pada tanggal 08 Januari 2017 pukul 13:04 Wita
- N.N. Tips Aman Online, http://buletin.melsa.net//idjan1001scam6/html, Diekses Pada Tanggal 18 Mei 2008, Pukul 15.00 WIB